

Privasi dan Keamanan Data: Tantangan Perlindungan Hak Asasi Manusia di Tengah Digitalisasi Nasional

Azanty Safitri¹, Siti Nur Azizah², Nafilah Khoirunnisa³

PGMI FITK UIN Syarif Hidayatullah Jakarta

Jl. Ir. H. Djuanda No. 95, Ciputat, Kota Tangerang Selatan, Banten 15412

Alamat e-mail : (¹ azanty.safitri25@mhs.uinjkt.ac.id), (² siti.nur25@mhs.uinjkt.ac.id), (³ nafilah.khoirunnisa25@mhs.uinjkt.ac.id) (zaenul_slam@uinjkt.ac.id)

ABSTRACT

The digital era in Indonesia has brought significant changes to various aspects of life, but it has also raised serious concerns regarding public privacy and data security. This study aims to examine the relationship between data security and the protection of human rights amid the rapid development of information technology. The methodology used is qualitative, with a focus on a literature review. The findings indicate that the concept of privacy has shifted to encompass the right to control one's information, where leaks of personal data directly result in violations of respect for human dignity. Although the government has sought to establish regulations through the Personal Data Protection Act (PDPA) (Kurniawan 2021), issues related to infrastructure and cyber threats remain major challenges in achieving comprehensive digital security. This article was written to examine the challenges in protecting human rights in the era of rapidly advancing digitalization in Indonesia.

Keywords: Data Privacy, Digital Security, Human Rights, National Digitalization, Data Protection.

ABSTRAK

Era digital di Indonesia membawa perubahan besar dalam banyak aspek kehidupan, tetapi juga menimbulkan masalah serius mengenai privasi dan keamanan data masyarakat. Studi ini bertujuan untuk mempelajari hubungan antara keamanan data dan perlindungan Hak Asasi Manusia di tengah perkembangan teknologi informasi yang cepat. Metode yang dipakai adalah kualitatif dengan fokus pada kajian literatur. Temuan dari penelitian menunjukkan bahwa makna privasi telah berubah menjadi hak untuk mengendalikan informasi, di mana kebocoran informasi pribadi langsung berpengaruh pada pelanggaran penghormatan terhadap manusia. Walaupun pemerintah telah berusaha membuat

peraturan melalui UU PDP (Kurniawan 2021), masalah infrastruktur dan ancaman dunia maya tetap menjadi tantangan besar untuk mencapai keamanan digital yang menyeluruh. Artikel ini ditulis untuk meneliti tantangan dalam melindungi HAM di era digitalisasi yang berkembang pesat di Indonesia.

Kata Kunci: Privasi Data, Keamanan Digital, Hak Asasi Manusia, Digitalisasi Nasional, Perlindungan Data.

A. Pendahuluan

Kondisi yang ideal dalam sebuah negara hukum yang mengalami transformasi digital adalah adanya jaminan perlindungan data pribadi sebagai bagian penting dari hak konstitusional warga negara. Dalam konteks Hak Asasi Manusia (HAM), privasi merupakan hak dasar (Mawati et al 2023) yang memungkinkan individu menjaga martabat, otonomi, dan kebebasan pribadinya tanpa campur tangan yang tidak sah. Secara teoritis, John Locke menekankan bahwa negara berkewajiban untuk melindungi hak milik warga negara, yang dalam konteks saat ini mencakup data pribadi sebagai aset intelektual dan identitas seseorang. Mengacu pada Pasal 28G ayat (1) UUD 1945, setiap individu berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, serta harta benda yang dimilikinya. Oleh karena itu, negara harus menyediakan infrastruktur hukum dan teknis yang kuat untuk memastikan bahwa

digitalisasi nasional dilakukan bersamaan dengan keamanan data masyarakat.

Namun, kenyataan saat ini menunjukkan adanya jurang yang cukup besar antara regulasi dan pelaksanaannya di lapangan. Digitalisasi nasional di Indonesia berkembang sangat cepat, tetapi seringkali tidak didukung dengan sistem keamanan siber yang memadai. Dalam praktiknya, terdapat banyak kasus kebocoran data yang memprihatinkan (Kurniawan 2021), seperti dugaan kebocoran data jutaan pengguna platform e-commerce, kebocoran data sertifikat vaksin dalam aplikasi PeduliLindungi, serta peretasan data di berbagai lembaga pemerintah oleh pihak yang tidak bertanggung jawab. Laporan tahunan keamanan siber seringkali menunjukkan bahwa Indonesia merupakan salah satu negara dengan jumlah serangan siber tertinggi di Asia Tenggara. Fenomena ini menciptakan risiko sistemik terhadap pelanggaran

HAM digital, di mana identitas masyarakat dapat dieksploitasi untuk penipuan finansial, profil ilegal, hingga pengawasan massal yang tidak etis.

Fokus utama dari penelitian ini adalah lemahnya sinergi antara percepatan teknologi dan kesiapan perlindungan hukum yang berpihak pada hak asasi pengguna (Prakoso 2022). Kebocoran data tidak hanya merupakan masalah teknis, tetapi juga merupakan ancaman nyata terhadap privasi yang dapat merusak kepercayaan publik terhadap ekosistem digital nasional. Jika tidak segera ditangani, dampak sosial dan hukum dari masalah ini akan semakin meluas, mulai dari kerugian materiil hingga pelanggaran hak atas rasa aman.

Berdasarkan latar belakang tersebut, tujuan dari penulisan artikel ini adalah untuk membahas tantangan perlindungan HAM dalam arus digitalisasi, menganalisis efektivitas regulasi yang ada, serta memberikan rekomendasi untuk penguatan kebijakan keamanan data guna menjamin martabat manusia di era digital nasional.

B. Metode Penelitian

Penelitian ini menerapkan metode kualitatif dengan pendekatan penelitian pustaka. Pendekatan ini dipilih karena tujuan utama penelitian adalah untuk mengkaji konsep, aturan, dan situasi terkait perlindungan data pribadi dengan melihat berbagai literatur ilmiah serta dokumen hukum. Khususnya, penelitian ini menggunakan pendekatan normatif-yuridis untuk menyelidiki tantangan perlindungan Hak Asasi Manusia (HAM) dalam konteks peraturan digitalisasi nasional di Indonesia.

Data untuk penelitian ini diambil dari sumber primer dan sekunder. Sumber primer mencakup peraturan perundang-undangan nasional, terutama Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) dan UUD 1945. Sumber sekunder diambil dari artikel jurnal ilmiah terkemuka, laporan resmi dari Badan Siber dan Sandi Negara (BSSN), buku tentang keamanan siber, serta dokumen internasional mengenai HAM digital. Teknik pengumpulan data dilakukan melalui dokumentasi dengan cara mengidentifikasi, mengelompokkan, dan menganalisis tulisan yang relevan

dengan topik privasi dan keamanan data.

Analisis data dilakukan secara deskriptif-analitis, di mana data yang terkumpul diolah untuk memberikan gambaran menyeluruh tentang kondisi ideal perlindungan data dibandingkan dengan kenyataan kebocoran data yang terjadi. Tujuan dari proses analisis ini adalah untuk menjawab pertanyaan penelitian mengenai seberapa efektif perlindungan HAM digital di tengah perkembangan pesat digitalisasi nasional seperti yang telah dijelaskan di bagian pendahuluan.

C. Hasil Penelitian dan Pembahasan

1. Konsep Privasi dan Keamanan Data

Konsep privasi dalam literatur hukum klasik seringkali didefinisikan sebagai the right to be let alone atau hak untuk dibiarkan sendiri tanpa gangguan dari pihak luar. Namun, di tengah arus digitalisasi nasional, makna privasi telah bergeser menjadi hak kendali informasi pribadi, di mana individu memiliki otoritas penuh untuk menentukan data mana yang boleh dikumpulkan, diproses, dan disebarkan oleh entitas lain. Hal ini sejalan dengan teori privasi modern yang menekankan bahwa data pribadi adalah bagian dari martabat manusia yang tidak boleh dieksploitasi tanpa izin (kurniawan, 2021).

Di sisi lain, keamanan data merupakan infrastruktur teknis dan prosedural yang menjamin kerahasiaan, keutuhan, dan ketersediaan informasi yang dimaksud. Tanpa sistem keamanan yang tangguh, privasi warga negara menjadi sangat rentan terhadap serangan siber yang dapat menyebabkan data jatuh ke tangan pihak yang tidak bertanggung jawab (Kurniawan, 2021). Hasil analisis terhadap Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) menegaskan bahwa keamanan data tidak hanya merupakan persoalan teknis dalam bidang teknologi informasi, melainkan kewajiban hukum yang harus dipenuhi oleh setiap pengendali data untuk menjamin hak-hak subjek data (kurniawan, 2021).

2. Hak Asasi Manusia dalam Era Digital

Evolusi teknologi telah melahirkan dimensi baru dalam instrumen Hak Asasi Manusia yang kini sering disebut sebagai HAM Digital (Mawati et al., 2023). Landasan hukum utama perlindungan HAM digital di Indonesia berpijak pada Pasal 28G ayat (1) UUD 1945, yang menyatakan bahwa setiap orang berhak atas perlindungan diri pribadi, kehormatan, dan martabatnya. Di era digital, hak privasi merupakan pintu masuk bagi pemenuhan hak-hak asasi lainnya; tanpa adanya jaminan privasi, kebebasan berekspresi dan hak atas rasa aman warga negara akan terancam oleh praktik pengawasan massal atau profiling ilegal (mawati et al., 2023).

Pelanggaran terhadap keamanan data kini dipandang sebagai pelanggaran HAM karena dampak yang ditimbulkan seringkali merusak martabat dan kesejahteraan individu secara luas. Sebagai contoh, kebocoran data pribadi dapat berujung pada tindakan diskriminasi, persekusi digital, hingga hilangnya hak finansial masyarakat akibat penipuan berbasis data (Prakoso, 2022). Oleh karena itu, negara memiliki kewajiban positif tidak hanya untuk menghormati hak privasi, tetapi juga aktif membangun sistem perlindungan data yang mampu mencegah pihak ketiga melakukan pelanggaran HAM di ruang digital (prakoso, 2022).

3. Perkembangan Digitalisasi di Indonesia

Perkembangan digitalisasi di Indonesia menunjukkan kemajuan yang sangat cepat dalam beberapa tahun terakhir. Perkembangan teknologi informasi dan komunikasi telah membawa perubahan di berbagai sektor kehidupan, seperti pendidikan, ekonomi, pemerintahan, dan pelayanan publik. Penggunaan internet, media sosial, ecommerce, serta berbagai layanan digital lainnya terus mengalami peningkatan serta menjadi unsur penting dalam masyarakat sehari-hari. Kehadiran digitalisasi juga memberikan kemudahan bagi masyarakat dalam memperoleh informasi, melakukan transaksi secara digital, dan memanfaatkan layanan berbasis internet dengan lebih praktis dan efisien (Aji et al., 2024).

Perkembangan digitalisasi di Indonesia turut mendapat dukungan melalui berbagai kebijakan dan regulasi yang dibuat oleh pemerintah. Salah satu landasan dalam perkembangan ekonomi sebagai dasar hukum dalam penyelenggaraan aktivitas digital di Indonesia, undang-undang Nomor 11 Tahun 2008 tentang informasi dan transaksi Elektronik (UU ITE) berperan dalam mengatur berbagai aspek penggunaan teknologi informasi dan transaksi elektronik. Seiring dengan perkembangan teknologi dan kebutuhan masyarakat, undang-undang Nomor 19 Tahun 2016 untuk memperkuat kepastian hukum serta meningkatkan keamanan dalam pelaksanaan transaksi elektronik. Selain itu, pemerintah juga menerbitkan berbagai aturan pendukung lainnya, sebagaimana diatur dalam peraturan Nomor 71 Tahun 2019 tentang penyelenggaraan sistem dan transaksi elektronik. (Adiningsih et al., 2019).

Berdasarkan penelitian Digital Landscape and Behavior in Indonesia 2024, transformasi digital di Indonesia menunjukkan adanya peningkatan penggunaan internet yang cukup tinggi di berbagai daerah (Aji et al., 2024). Meskipun demikian, penelitian tersebut juga mengungkapkan bahwa masih terdapat ketimpangan dalam akses digital serta meningkatnya risiko ancaman keamanan siber di tengah masyarakat. Di sisi lain, penelitian mengenai digitalisasi ekonomi di pedesaan Indonesia menjelaskan bahwa perkembangan digitalisasi di Indonesia masih belum

merata akibat keterbatasan infrastruktur teknologi dan rendahnya pemberdayaan digital di wilayah pedesaan (Rahmawati et al., 2024).

Selain itu, perkembangan digitalisasi juga tampak pada sektor bisnis dan ekonomi digital. Munculnya e-commerce, layanan keuangan digital, serta perubahan bisnis berbasis teknologi kondisi tersebut mengindikasikan bahwa teknologi digital telah menjadi bagian yang tidak terpisahkan dari kehidupan sehari-hari masyarakat Indonesia. Dalam penelitian perkembangan e-business dijelaskan bahwa digitalisasi menjadi kebutuhan penting bagi masyarakat maupun pelaku usaha agar mampu menyesuaikan diri dengan perkembangan revolusi industri (Pratama et al., 2024).

Menurut Erwin dkk. (2023), transformasi digital adalah proses perubahan yang memanfaatkan teknologi digital guna meningkatkan efektivitas dan efisiensi dalam berbagai aspek kehidupan masyarakat. Perkembangan digitalisasi di Indonesia tidak hanya memberikan dampak positif berupa peningkatan pertumbuhan ekonomi dan kemudahan dalam mengakses informasi, tetapi juga menghadirkan berbagai tantangan, seperti ketimpangan akses teknologi, rendahnya tingkat literasi digital, ancaman kejahatan siber, serta risiko kebocoran data pribadi masyarakat.

4. Tantangan Perlindungan Data Pribadi di Tengah digitalisasi

Pesatnya perkembangan teknologi digital telah memberikan banyak kemudahan bagi masyarakat dalam menjalankan berbagai aktivitas, seperti komunikasi, transaksi keuangan, hingga akses layanan publik secara daring. Akan tetapi, kemajuan tersebut juga menghadirkan tantangan baru berupa meningkatnya risiko terhadap perlindungan data pribadi. Kebocoran data, penyalahgunaan informasi, dan serangan siber menjadi persoalan yang semakin sering muncul seiring dengan tingginya penggunaan teknologi digital di Indonesia. Berbagai jenis data pribadi yang mencakup nomor identitas, alamat tempat tinggal, nomor telepon, serta informasi keuangan, kini tersimpan dalam sistem digital yang rentan disalahgunakan apabila tidak dikelola dengan baik (Kurniawan, 2021).

Di tengah era digital, data pribadi memiliki nilai yang sangat penting karena hampir seluruh aktivitas masyarakat meninggalkan jejak digital. Penggunaan media sosial, layanan belanja online, transportasi daring, maupun berbagai aplikasi digital lainnya membuat data pengguna terus dikumpulkan dan diproses oleh penyedia layanan. Kondisi tersebut meningkatkan risiko terjadinya pelanggaran privasi, seperti pencurian identitas, penipuan berbasis digital, hingga pemanfaatan data tanpa izin dari pemiliknya (Mawati et al., 2023).

Permasalahan perlindungan data pribadi di Indonesia dipengaruhi oleh berbagai faktor, salah satunya adalah rendahnya kesadaran masyarakat mengenai keamanan digital, lemahnya sistem perlindungan data, serta kurang transparannya pengelolaan informasi oleh sebagian pihak penyedia layanan. Banyak masyarakat yang masih kurang berhati-hati dalam membagikan informasi pribadi di ruang digital tanpa memahami dampak yang dapat ditimbulkan. Situasi ini menyebabkan data pribadi menjadi lebih mudah diakses serta digunakan oleh pihak yang tidak memiliki tanggung jawab (Kurniawan, 2021).

Perlindungan terhadap data pribadi pada hakikatnya merupakan bagian dari perlindungan hak asasi manusia, khususnya hak atas privasi. Oleh sebab itu, negara memiliki peran penting dalam memberikan jaminan hukum terhadap keamanan data masyarakat. Sebagai upaya menghadapi tantangan tersebut, pemerintah Indonesia telah menetapkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Regulasi ini mengatur hak pemilik data, kewajiban pihak pengelola data, serta sanksi bagi pelanggaran yang berkaitan dengan penyalahgunaan data pribadi.

Namun demikian, keberadaan regulasi belum sepenuhnya cukup untuk menjamin keamanan data pribadi. Diperlukan pengawasan yang lebih optimal melalui pembentukan lembaga pengawas independen, penegakan hukum yang tegas, serta

peningkatan literasi digital agar masyarakat lebih memahami pentingnya menjaga kerahasiaan data pribadi. Selain itu, perusahaan penyedia layanan digital juga diharuskan untuk memperkuat sistem keamanan dan menerapkan prinsip transparansi dalam pengelolaan data pengguna (Kurniawan, 2021).

Dengan demikian, tantangan perlindungan data pribadi di tengah perkembangan digitalisasi tidak hanya berkaitan dengan aspek teknologi, tetapi juga menyangkut kesiapan hukum, tanggung jawab penyedia layanan, dan kesadaran masyarakat dalam menjaga privasi. Kerja sama antara pemerintah, pelaku usaha, dan masyarakat diperlukan agar pemanfaatan teknologi digital dapat berlangsung secara aman serta tetap menghormati hak privasi setiap individu (Mawati et al., 2023).

5. Upaya Pemerintah dalam Melindungi Data dan HAM Digital

Pemerintah telah melakukan berbagai upaya untuk melindungi data pribadi masyarakat di era digital. Salah satunya adalah meningkatkan keamanan sistem digital melalui penggunaan enkripsi data, firewall, dan perlindungan terhadap serangan siber. Langkah ini dilakukan agar data masyarakat tidak mudah dicuri atau diakses oleh pihak yang tidak bertanggung jawab (Kurniawan, 2021).

Selain itu, pemerintah juga melakukan pemantauan terhadap aktivitas mencurigakan pada jaringan digital untuk mendeteksi kemungkinan peretasan. Pemerintah dapat bekerja sama dengan ahli keamanan siber dan melakukan audit keamanan secara rutin untuk

memastikan sistem berjalan dengan aman. Organisasi atau perusahaan yang mengelola data pribadi juga didorong untuk memiliki standar keamanan tertentu dan segera melaporkan apabila terjadi kebocoran data (Kurniawan, 2021).

Adapun upaya teknis yang dilakukan pemerintah hingga saat ini dalam perlindungan data pribadi warganegaraanya diantara adalah:

- a. Peningkatan Keamanan Sistem Pemerintah dapat menerapkan standar keamanan tinggi pada sistem dan infrastruktur yang mengelola data pribadi. Ini termasuk penggunaan enkripsi data, perlindungan terhadap serangan siber, dan penerapan firewall yang kuat.
- b. Pemantauan Aktivitas Anomali Pemerintah dapat menggunakan alat pemantauan untuk mendeteksi aktivitas anomali yang mencurigakan pada sistem atau jaringan. Ini bisa membantu mendeteksi upaya peretasan atau akses yang tidak sah.
- c. Sertifikasi Keamanan Pemerintah dapat mengeluarkan sertifikasi keamanan bagi organisasi atau layanan yang mengelola data pribadi, setelah mereka terbukti memenuhi standar keamanan tertentu.
- d. Auditor Keamanan Pemerintah dapat mempekerjakan atau melibatkan auditor keamanan independen untuk melakukan audit rutin terhadap sistem dan praktik yang berkaitan dengan perlindungan data pribadi.
- e. Pengaturan Kewajiban Melaporkan Pelanggaran Pemerintah dapat mengharuskan organisasi untuk melaporkan pelanggaran data pribadi secara segera kepada otoritas yang berwenang, sehingga tindakan cepat dapat diambil untuk meminimalkan dampaknya.
- f. Pelatihan Karyawan Pemerintah dapat mendorong organisasi untuk memberikan pelatihan kepada karyawan mengenai praktik keamanan data, seperti cara mengenali phishing atau mengamankan kata sandi.
- g. Pemisahan Data Sensitif Data pribadi yang sensitif dapat diisolasi atau dipisahkan dari data lainnya untuk mengurangi risiko akses yang tidak sah.
- h. Pengamanan Akses Pemerintah dapat mendorong implementasi mekanisme otentikasi ganda atau akses terbatas untuk menghindari akses yang tidak sah ke data pribadi.
- i. Perlindungan Data Selama Transit Pemerintah dapat mendorong penggunaan enkripsi selama data dalam perjalanan antara pengirim dan penerima, misalnya melalui protokol HTTPS.
- j. Penanganan Aman Data Tidak Terpakai Pemerintah dapat memberikan pedoman bagi organisasi tentang bagaimana data yang tidak lagi diperlukan harus dihapus atau dihancurkan secara aman.
- k. Pengujian Keamanan (Security Testing) Pemerintah dapat mendorong organisasi untuk secara teratur melakukan pengujian keamanan, seperti

uji penetrasi, untuk mengidentifikasi kerentanannya.

- I. Kerja Sama dengan Industri Keamanan Pemerintah dapat bekerja sama dengan perusahaan dan peneliti keamanan siber untuk memahami tren ancaman terbaru dan menerapkan langkah-langkah pencegahan yang sesuai.

Upaya lain yang dilakukan adalah memberikan edukasi dan pelatihan kepada masyarakat maupun karyawan perusahaan mengenai keamanan digital. Misalnya, cara mengenali penipuan online, menjaga kata sandi, serta menggunakan autentikasi ganda agar akun lebih aman. Pemerintah juga mendorong penghapusan data yang sudah tidak digunakan agar tidak disalahgunakan di kemudian hari.

6. Dampak Kebocoran Data terhadap Masyarakat

Di era digital yang berkembang pesat saat ini, informasi dan data telah menjadi aset yang sangat berharga bagi individu, organisasi, dan negara. Penggunaan teknologi informasi dan komunikasi yang luas telah mempermudah akses dan pertukaran data, namun juga membuka peluang bagi berbagai risiko, termasuk kebocoran data. Kebocoran data merupakan masalah signifikan yang dapat menimbulkan dampak negatif yang luas, baik bagi pihak yang mengalami kebocoran maupun bagi masyarakat secara keseluruhan. Kebocoran data mengacu pada situasi di mana data sensitif atau pribadi yang seharusnya dilindungi

bocor ke pihak yang tidak berwenang. Hal ini bisa terjadi akibat berbagai faktor, seperti serangan siber, kesalahan manusia, atau kerentanan sistem keamanan.

Dampaknya tidak hanya meliputi kerugian finansial, tetapi juga dapat merusak reputasi organisasi, melanggar privasi individu, dan menyebabkan kerugian hukum.

Studi menunjukkan bahwa kebocoran data telah meningkat secara signifikan dalam beberapa tahun terakhir. Menurut laporan yang diterbitkan oleh [nama lembaga atau perusahaan riset], ribuan insiden kebocoran data terjadi setiap tahun, mengungkapkan informasi pribadi jutaan individu dan organisasi.

Kasus-kasus terkenal seperti kebocoran data pada perusahaan [sebutkan nama perusahaan] atau [sebutkan nama perusahaan lain] menunjukkan betapa seriusnya ancaman ini. Dalam konteks ini, penting untuk memahami faktor-faktor yang menyebabkan kebocoran data, dampak yang ditimbulkan, serta langkah-langkah yang dapat diambil untuk mencegah dan menangani kebocoran tersebut. Artikel ini bertujuan untuk mengeksplorasi isu-isu tersebut secara mendalam, dengan menyoroti berbagai aspek seperti penyebab kebocoran, dampak terhadap pihak yang terdampak, dan strategi mitigasi yang efektif.

Faktor Penyebab Dan Dampak Dari Kebocoran Data

Kelemahan Sistem Keamanan: Kerentanan perangkat lunak, kelemahan dalam konfigurasi sistem, dan keamanan jaringan yang tidak memadai sering menjadi penyebab utama kebocoran data. **Kesalahan Manusia:** Human error, seperti

pengiriman email ke penerima yang salah atau pengelolaan password yang buruk, juga merupakan penyebab signifikan kebocoran data. Serangan Siber: Teknik serangan seperti phishing, malware, ransomware, dan hacking dapat menyebabkan kebocoran data dengan mengeksploitasi celah keamanan.

Dampak Kebocoran Data: Kerugian Finansial: Kebocoran data dapat menyebabkan kerugian finansial langsung melalui denda, biaya pemulihan, dan kehilangan pendapatan akibat reputasi yang rusak. Kerusakan Reputasi: Reputasi perusahaan atau individu dapat terganggu secara signifikan setelah kebocoran data, yang dapat mengakibatkan kehilangan kepercayaan dari pelanggan dan mitra. Implikasi Hukum: Pelanggaran terhadap peraturan perlindungan data, seperti GDPR atau UU Perlindungan Data Pribadi, dapat menyebabkan tindakan hukum dan denda yang berat. Standar Industri: Beberapa industri memiliki standar khusus, seperti PCI-DSS untuk data kartu kredit, yang menetapkan praktik terbaik dalam perlindungan data. Kajian teoritis ini akan memberikan pemahaman yang mendalam mengenai berbagai aspek kebocoran data dan membekali pembaca dengan kerangka kerja yang diperlukan untuk analisis dan solusi yang lebih baik terhadap masalah ini.

Dampak Kebocoran Data terhadap Masyarakat :

1. Pelanggaran Privasi Individu

Kebocoran data dapat menyebabkan informasi pribadi masyarakat tersebar tanpa izin, seperti nama, alamat,

nomor telepon, data kesehatan, hingga nomor identitas.

Penyalahgunaan data ini dapat mengganggu hak privasi seseorang dan membuat individu kehilangan kontrol atas informasi pribadinya.

Contohnya, data yang bocor dapat digunakan untuk:

- pencurian identitas,
- penipuan online,
- penyalahgunaan akun digital,
- pemalsuan dokumen.

Menurut Kementerian Komunikasi dan Digital Republik Indonesia, perlindungan data pribadi menjadi bagian penting dalam menjaga hak warga negara di era digital

2. Kerugian Finansial Masyarakat

Kebocoran data dapat menimbulkan kerugian ekonomi bagi masyarakat. Data rekening bank, kartu kredit, atau akun dompet digital yang bocor dapat dimanfaatkan oleh pelaku kejahatan siber untuk melakukan transaksi ilegal.

Masyarakat juga dapat menjadi korban:

- phishing,
- penipuan digital,
- pembobolan rekening,
- penyalahgunaan pinjaman online.

Kerugian ini tidak hanya berdampak pada individu, tetapi juga menurunkan kepercayaan masyarakat terhadap layanan digital dan sistem transaksi online.

3. Dampak Psikologis dan Sosial

Korban kebocoran data sering mengalami:

- rasa takut,
- kecemasan,
- stres,
- kehilangan rasa aman dalam menggunakan teknologi digital.

Selain itu, penyebaran data pribadi dapat menimbulkan cyberbullying, pemerasan digital, dan pencemaran nama baik. Dalam beberapa kasus, masyarakat menjadi enggan menggunakan layanan digital karena takut datanya disalahgunakan.

4. Menurunnya Kepercayaan Publik terhadap Teknologi

Seringnya kasus kebocoran data menyebabkan masyarakat kehilangan kepercayaan terhadap:

- perusahaan digital,
- layanan e-commerce,
- media sosial,
- lembaga pemerintah.

Jika kepercayaan publik menurun, perkembangan transformasi digital juga dapat terhambat karena masyarakat merasa tidak aman dalam menggunakan teknologi.

5. Ancaman terhadap Keamanan Nasional dan Sosial

Apabila data masyarakat bocor dalam jumlah besar, dampaknya dapat meluas hingga mengganggu stabilitas sosial dan keamanan negara. Data kependudukan yang bocor dapat dimanfaatkan untuk:

- penyebaran hoaks,
- manipulasi informasi,
- kejahatan siber berskala besar,

- serangan terhadap sistem pemerintahan.

Karena itu, perlindungan data pribadi menjadi tanggung jawab bersama antara pemerintah, perusahaan, dan masyarakat.

E. Kesimpulan

berdasarkan hasil analisis dan pembahasan, dapat disimpulkan bahwa perlindungan data pribadi dalam arus digitalisasi nasional di Indonesia merupakan prasyarat mutlak dalam pemenuhan Hak Asasi Manusia (HAM) digital yang dijamin oleh konstitusi. Kehadiran Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) memberikan landasan yuridis yang kuat, namun efektivitas implementasinya masih menghadapi tantangan besar berupa lemahnya infrastruktur keamanan siber, rendahnya literasi digital masyarakat, dan tingginya intensitas serangan siber yang berdampak sistemik pada kerugian finansial, psikologis, hingga stabilitas sosial nasional.

Sebagai rekomendasi, pemerintah perlu segera mempercepat pembentukan Lembaga

Pengawas Perlindungan Data Pribadi yang independen untuk mengoptimalkan penegakan sanksi hukum. Selain itu, para penyelenggara sistem elektronik (baik publik maupun swasta) wajib meningkatkan standar keamanan teknis melalui enkripsi end-to-end, audit siber berkala, dan transparansi tata kelola data. Masyarakat juga didorong untuk meningkatkan kewaspadaan digital dalam membagikan informasi pribadi demi memperkecil celah eksploitasi siber.

DAFTAR PUSTAKA

Buku :

- Miles, M. B., Huberman, A. M., & Saldaña, J. (2014). *Qualitative Data Analysis: A Methods Sourcebook*. SAGE Publications.
- M. A. Subandi. (2021). *Pemikiran Guru Besar Universitas Gadjah Mada Menuju Indonesia Maju 2045: Bidang Sosial Humaniora*. Yogyakarta: UGM Press.
- Soekanto, S., & Mamudji, S. (2015). *Penelitian Hukum Normatif: Suatu Tinjauan Singkat*. Rajawali Pers.
- Zed, M. (2014). *Metode Penelitian Kepustakaan*. Yayasan Obor Indonesia.

Jurnal :

- Aji, R., dkk. (2024). *Digital Landscape and Behavior in Indonesia 2024*. Jurnal Teknologi Informasi dan Ilmu

Komputer. Diakses dari [JUTIF Unsoed](#)

Kurniawan, A. (2021). Keamanan Siber dan Tantangan Perlindungan Data di Indonesia. *Jurnal Hukum Digital*, 5(2), 112-125.

Kepolisian Daerah Kepulauan Riau. (2024). *Perlindungan data pribadi di era digital: Tantangan dan solusi hukum Indonesia*.

Mawati, A. T., Nuraini, S., & Hidayat, R. (2023). Transformasi Digital dan Implikasinya terhadap Hak Privasi. *Jurnal Sosial dan Kebijakan*, 8(1), 45-60.

Prakoso, B. (2022). Dampak Sosial Kebocoran Data Pribadi pada Masyarakat Urban. *Jurnal Komunikasi Global*, 11(3), 301-315.

pratama, A., dkk. (2024). *Perkembangan E-Business di Negara Indonesia dalam Era Digital*. Jurnal Kajian Penelitian Ilmu Manajemen. Diakses dari [Jurnal Aksara Global](#)

Pusat Kajian dan Bantuan Hukum UIN Siber Syekh Nurjati Cirebon. (2024). *Perlindungan data pribadi dalam era digital: Antara hak privasi dan kepentingan publik*.

Rahmawati, S., dkk. (2024). *Digitalisasi Ekonomi di Pedesaan Indonesia*. Journal of Applied Islamic and Social Sciences. Diakses dari [Jurnal UAI](#)