Vol 1 No. 2, November 2025
E-ISSN: 3110-3898; P-ISSN: 3110-4657; Page 132-141

Tanggung Jawab Hukum Penyelenggara Sistem Elektronik Terhadap Kebocoran Data Pribadi Pengguna

Shelomita Putri Amelia[1*]

[1*]Universitas Pembangunan Nasional Veteran, Jakarta, Indonesia
2210611205@mahasiswa.upnvj.ac.id

ABSTRAK

Penelitian ini bertujuan menganalisis tanggung jawab hukum penyelenggara sistem elektronik terhadap kebocoran data pribadi pengguna berdasarkan kerangka hukum nasional serta pola insiden yang terjadi dalam beberapa tahun terakhir. Perkembangan layanan digital yang semakin masif meningkatkan risiko kebocoran data akibat serangan siber maupun kelalaian internal, sehingga penguatan kewajiban hukum PSE menjadi kebutuhan mendesak. Hasil kajian menunjukkan bahwa UU Perlindungan Data Pribadi, PP 71/2019, dan peraturan pendukung lainnya telah memberikan landasan normatif yang jelas mengenai kewajiban pengendali data dalam memastikan keamanan teknis, pemberitahuan insiden, dan pemulihan kerugian pengguna. Analisis kasus pada sektor e-commerce, layanan publik, dan cloud computing memperlihatkan bahwa sebagian besar kebocoran terjadi karena lemahnya enkripsi, manajemen akses, dan pemantauan keamanan real-time. Penelitian ini menyimpulkan bahwa pertanggungjawaban hukum PSE mencakup sanksi perdata, pidana, dan administratif yang dapat diterapkan apabila terbukti lalai dalam menjaga data pribadi. Penguatan audit keamanan, peningkatan transparansi, serta edukasi perlindungan data bagi pengguna menjadi langkah penting untuk menjaga kepercayaan publik di era digital yang penuh risiko.

***Kata Kunci**: Tanggung jawab hukum; Kebocoran data pribadi; Penyelenggara sistem elektronik; Perlindungan data; Regulasi digital.*

PENDAHULUAN

Isu kebocoran data pribadi serta praktik penawaran dan transaksi atas data pribadi yang telah bocor kembali menjadi perhatian serius dalam ruang publik. Fenomena tersebut tidak hanya menimpa data pribadi yang dikelola oleh sektor korporasi swasta, tetapi juga mencakup data yang berada di bawah pengelolaan lembaga pemerintahan. Kondisi ini mengindikasikan bahwa sistem perlindungan data di Indonesia masih

Submitted: 19-09-2025
Revised: 18-10-2025
Acepted: 19-11-2025

menghadapi berbagai kelemahan, baik dari aspek teknis, kelembagaan, maupun regulatif. Dampaknya, tingkat kepercayaan masyarakat terhadap keamanan informasi pribadinya semakin menurun, terutama terhadap penyelenggara sistem elektronik yang memiliki kewajiban hukum untuk melindungi data tersebut. Lebih lanjut, meningkatnya frekuensi kasus kebocoran data menimbulkan pertanyaan kritis mengenai efektivitas kebijakan yang telah diterapkan serta lemahnya penegakan hukum dalam menjamin pelindungan data pribadi. Tercatat bahwa pada tahun 2024, berdasarkan data dari Surfshark, Indonesia berada di urutan ketiga dengan total 21.769.496 kasus pembajakan email. (Alfathi, 2025)

Berdasarkan Pasal 1 Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, yang dimaksud dengan Penyelenggara Sistem Elektronik adalah setiap pihak, baik perorangan, lembaga negara, badan usaha, hingga komunitas masyarakat, yang bertanggung jawab dalam penyediaan, pengelolaan, atau pengoperasian sistem elektronik, baik secara mandiri maupun kolektif, untuk memenuhi kebutuhan sendiri maupun untuk mendukung kegiatan pihak lain. Dari pengertian tersebut maka kebocoran data pribadi yang dikelola oleh Penyelenggara Sistem Elektronik (PSE) sudah seharusnya menjadi tanggung jawab Penyelenggara Sistem Elektronik (PSE), baik kebocoran data yang disebabkan oleh tindakan peretasan yang dilakukan oleh pihak eksternal *(hacker)*, maupun yang terjadi akibat adanya unsur kesengajaan dari pihak Penyelenggara Sistem Elektronik (PSE) itu sendiri. Terjadinya kebocoran data pribadi dapat dikategorikan sebagai bentuk pelanggaran terhadap prinsip-prinsip perlindungan data pribadi, khususnya dalam aspek menjaga kerahasiaan dan keamanan informasi milik subjek data. Insiden tersebut mencerminkan adanya kegagalan dalam pengawasan, penyimpanan, serta pengelolaan data secara aman dan bertanggung jawab, yang pada akhirnya menunjukkan adanya unsur kelalaian dari pihak Penyelenggara Sistem Elektronik (PSE). (Uz Zaman, 2021)

Sebagai bentuk respons terhadap meningkatnya kasus pelanggaran data pribadi, Indonesia melalui kebijakan strategisnya telah mengesahkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Keberadaan undang-undang ini dimaksudkan untuk menjadi payung hukum yang komprehensif guna memperkuat kerangka regulasi perlindungan data di tengar pesatnya kemajuan era transformasi digital. Regulasi ini memberikan pijakan yuridis yang komprehensif terhadap proses pengumpulan, penyimpanan, pengolahan, serta pendistribusian data pribadi, sekaligus menegaskan tanggung jawab hukum bagi Penyelenggara Sistem Elektronik (PSE) dan pihak lain yang terlibat dalam pengelolaannya. Meskipun demikian, pelaksanaan dan penegakan UU PDP masih menemui berbagai hambatan, seperti keterbatasan kapasitas keamanan siber, belum optimalnya kesiapan lembaga dan sektor usaha dalam menyesuaikan diri terhadap ketentuan baru, serta lemahnya mekanisme pengawasan dan penegakan hukum atas pelanggaran yang terjadi. (Fitria dkk., 2025)

Salah satunya pada tahun 2024, terjadi gangguan pada PDNS 2 di Surabaya berupa serangan siber dalam bentuk ransomware bernama *Brain Cipher Ransomware*. Insiden ersebut menimbulkan gangguan serius terhadap berbagai layanan publik dan menyebabkan tidak dapat diaksesnya sejumlah sistem pemerintahan. Selain itu, insiden ini juga berujung pada penguncian serta penyanderaan data milik sekitar 282 kementerian, lembaga, dan pemerintah daerah yang tersimpan di Pusat Data Nasional (PDN), sehingga menghambat operasional administrasi pemerintahan dan pelayanan masyarakat secara luas. (Dirgantara & Ramadhan, 2024)

Berdasarkan penjelasan di atas, permasalahan kebocoran data pribadi di Indonesia

tidak dapat dipandang semata-mata sebagai gangguan teknis pada sistem keamanan digital. Lebih dari itu, persoalan ini menyentuh ranah hukum yang menekankan pada kewajiban dan akuntabilitas penyedia layanan sistem elektronik untuk menjamin keamanan informasi pribadi para penggunanya. Kasus kebocoran data yang terjadi, termasuk pada lembaga keuangan nasional, menunjukkan bahwa masih terdapat celah dalam implementasi prinsip-prinsip perlindungan data sebagaimana diatur dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Oleh karena itu, penelitian ini bertujuan untuk menganalisis bagaimana pengaturan tanggung jawab hukum Penyelenggara Sistem Elektronik (PSE) terhadap kebocoran data pribadi menurut peraturan perundang-undangan serta ketentuan sanksi hukum yang dapat dikenakan kepada Penyelenggara Sistem Elektronik (PSE) yang terbukti lalai dalam melindungi data pribadi pengguna. Hasil penelitian ini diharapkan dapat memberikan kontribusi bagi pengembangan kajian hukum siber, khususnya dalam memperkuat pemahaman mengenai tanggung jawab hukum Penyelenggara Sistem Elektronik (PSE) terhadap kebocoran data pribadi.

METODE

Penelitian menggunakan penelitian hukum normatif yang mengkaji tanggung jawab hukum Penyelenggara Sistem Elektronik (PSE) atas kebocoran data pribadi. Fokus penelitian adalah menganalisis ketentuan perundang-undangan yang mengatur pertanggungjawaban serta sanksi hukum yang dapat dijatuhkan kepada PSE yang terbukti lalai dalam melindungi data pribadi pengguna. Pendekatan penelitian meliputi pendekatan perundang-undangan dengan menganalisis Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik serta peraturan terkait lainnya. Selain itu, digunakan pula pendekatan konseptual untuk menelaah teori-teori mendasar mengenai tanggung jawab hukum, perlindungan data pribadi, dan sanksi dalam hukum siber. Sumber data penelitian terdiri dari bahan hukum primer berupa peraturan perundang-undangan, bahan hukum sekunder seperti buku dan jurnal, serta bahan hukum tersier. Teknik pengumpulan data dilakukan melalui studi kepustakaan, sedangkan analisis data menggunakan metode kualitatif dengan menafsirkan dan menghubungkan berbagai norma hukum untuk merumuskan kesimpulan yang sistematis tentang bentuk dan implementasi tanggung jawab hukum PSE di Indonesia.

HASIL DAN PEMBAHASAN

Tanggung Jawab Hukum PSE Berdasarkan Regulasi Nasional

Pengaturan tanggung jawab hukum penyelenggara sistem elektronik telah dibangun melalui kerangka regulasi yang menuntut setiap PSE menjaga keamanan data pribadi tanpa pengecualian. Kewajiban ini dipertegas dalam UU PDP yang menetapkan bahwa pengendali data harus memastikan seluruh proses pengumpulan, penyimpanan, dan pemrosesan dilakukan melalui standar keamanan tertinggi demi mencegah risiko kebocoran. Ketika terjadi pelanggaran, undang-undang menempatkan tanggung jawab utama pada PSE karena kedudukannya sebagai pihak yang menikmati manfaat ekonomi dari pengoperasian sistem digital. Posisi ini memperjelas bahwa setiap kegagalan memberikan perlindungan menjadi bentuk kelalaian yang dapat dimintai pertanggungjawaban hukum (Undang-Undang Nomor 27 Tahun 2022).

PP 71/2019 secara khusus mengharuskan PSE menyediakan sistem yang andal, aman, dan bertanggung jawab, sehingga aspek kelayakan teknologi menjadi bagian integral dari analisis pertanggungjawaban. Setiap pengelola platform elektronik berkewajiban memastikan bahwa infrastruktur yang digunakan tidak memiliki celah yang dapat memicu akses ilegal pada data pengguna. Regulasi ini juga memberikan penekanan pada kewajiban pemeliharaan berkelanjutan agar risiko serangan siber dapat diantisipasi sedini mungkin. Ketidakpatuhan terhadap standar keamanan tersebut dapat dijadikan dasar gugatan ganti rugi dari pengguna yang menjadi korban (Peraturan Pemerintah Nomor 71 Tahun 2019).

Permenkominfo 20/2016 menempatkan kewajiban pemberitahuan insiden kebocoran data sebagai tindakan yang harus dilakukan secara cepat dan transparan. Kewajiban melapor kepada pemilik data menjadi sangat penting agar pengguna mengetahui potensi risiko penyalahgunaan data yang sedang mereka hadapi. PSE yang gagal memberikan pemberitahuan dapat dianggap menghalangi hak pengguna untuk melakukan mitigasi mandiri atas dampak yang muncul. Tanggung jawab ini mempertegas posisi PSE sebagai pihak yang wajib bersikap profesional dalam menangani insiden keamanan (Peraturan Menteri Kominfo No. 20 Tahun 2016).

Peringkat Indonesia sebagai salah satu negara dengan insiden kebocoran data tertinggi memperlihatkan bahwa tantangan keamanan digital masih sangat besar. Data statistik menunjukkan bahwa Indonesia berada pada posisi ketiga di ASEAN untuk jumlah kebocoran data selama tahun 2023, sehingga urusan perlindungan data tidak lagi dapat dianggap sebagai isu teknis semata. Trend ini menunjukkan bahwa sistem elektronik lokal masih memiliki banyak kelemahan yang belum tertangani secara efektif. Kondisi tersebut juga menegaskan bahwa pengaturan hukum belum sepenuhnya diikuti dengan kepatuhan operasional di lapangan (Alfathi, 2025).

Tabel 1. Peringkat Kebocoran Data di ASEAN (2023)

Negara	Jumlah Kasus Kebocoran	Peringkat
Singapura	91 kasus	1
Vietnam	74 kasus	2
Indonesia	71 kasus	3
Thailand	53 kasus	4
Malaysia	39 kasus	5

Sumber: GoodStats (Alfathi, 2025)

Statistik tersebut memberi gambaran bahwa peningkatan kuantitas platform digital tidak selalu diikuti dengan peningkatan kualitas perlindungan data yang memadai. Pertumbuhan cepat e-commerce, layanan cloud, dan aplikasi publik telah menciptakan ekosistem digital yang luas, tetapi tidak semuanya dibangun dengan fondasi keamanan yang kokoh. Kondisi ini berdampak langsung pada meningkatnya peluang kebocoran data akibat kelalaian, serangan eksternal, atau lemahnya sistem pengawasan internal. Pada titik inilah peran regulasi harus diperkuat agar PSE tidak hanya sekadar tunduk secara administratif, tetapi benar-benar menerapkan kontrol keamanan berstandar tinggi (Anugrah et al., 2023).

Kronologi serangan siber PDN pada 2024 menunjukkan bahwa koordinasi keamanan antara PSE dan pemerintah masih menghadapi tantangan struktural. Serangan yang berlangsung hingga melumpuhkan sejumlah layanan publik memperlihatkan lemahnya respons operasional serta ketidakpaduan sistem pertahanan digital. Peristiwa tersebut

menegaskan pentingnya sistem audit keamanan yang dilaksanakan secara berkala, terutama pada PSE yang mengelola data berskala nasional. Ketika audit tidak dilakukan secara ketat, potensi kebocoran meningkat dan beban tanggung jawab hukum terhadap PSE menjadi jauh lebih besar (Dirgantara & Ramadhan, 2024).

Analisis keseluruhan menunjukkan bahwa kerangka hukum nasional telah memberikan landasan kuat, tetapi efektivitas perlindungan data sangat bergantung pada keseriusan PSE dalam mengimplementasikan standar keamanan. Regulasi bukan hanya perangkat normatif, tetapi juga instrumen yang menuntut disiplin operasional melalui komitmen terhadap teknologi yang mutakhir. Keengganan berinvestasi pada sistem keamanan akan memperbesar potensi kerugian hukum dan ekonomi bagi penyelenggara sistem elektronik. Posisi ini menegaskan kembali bahwa tanggung jawab hukum PSE melekat sejak tahap pengumpulan data hingga pemusnahannya (Prijatna, 2024).

Bentuk Pelanggaran dan Pola Kebocoran Data pada Sistem Elektronik

Berbagai bentuk pelanggaran data menunjukkan bahwa kebocoran tidak hanya disebabkan oleh serangan siber, tetapi juga kelalaian internal yang sering kali diabaikan dalam penyelenggaraan sistem elektronik. Banyak kasus menunjukkan bahwa lemahnya manajemen akses menyebabkan data penting dapat diunduh atau dikonsumsi tanpa memperhatikan prinsip minimalisasi penggunaan. Ketika prosedur pengamanan tidak dijalankan dengan benar, peluang terjadinya eksploitasi data meningkat secara signifikan. Situasi ini memperlihatkan bahwa PSE harus menerapkan praktik keamanan tingkat tinggi dalam setiap tahap pengelolaan data (Uz Zaman, 2021).

Model kebocoran data juga dapat diamati dari beberapa kasus marketplace nasional yang telah terbukti lalai dalam menjaga kredensial pengguna. Studi mengenai kasus Tokopedia menunjukkan bahwa lemahnya enkripsi dan sistem keamanan menyebabkan lebih dari 91 juta akun terdampak, menggambarkan skala kerentanan yang cukup besar. Kebocoran data tersebut menimbulkan dampak psikologis, finansial, dan reputasional bagi pengguna maupun bagi penyelenggara platform itu sendiri. Kegagalan ini memperjelas bahwa sistem yang tidak diperbarui secara berkelanjutan akan mudah ditembus oleh pelaku kejahatan siber (Naufal, 2020).

Kasus BPJS Kesehatan juga memperlihatkan bahwa kebocoran data tidak hanya terjadi pada sektor komersial, tetapi juga pada layanan publik yang memiliki basis data terbesar di Indonesia. Kebocoran yang terjadi menyebabkan puluhan juta informasi sensitif beredar bebas, termasuk nomor induk kependudukan, alamat, dan data kesehatan. Kejadian ini menunjukkan bahwa lembaga publik pun tidak bisa mengabaikan standar keamanan tinggi dalam pengelolaan data masyarakat. Kelalaian tersebut menempatkan badan publik dalam posisi bertanggung jawab secara hukum maupun administratif (Maulida & Utomo, 2023).

Tabel 2. Kasus Kebocoran Data Berdasarkan Jenis Sektor (2019–2024)

Jenis Sektor	Jumlah Kasus	Contoh Kasus
E-commerce	3	Tokopedia, Bhinneka
Lembaga Publik	2	BPJS, PDN
Pendidikan	1	Sistem akademik kampus
Keuangan	2	Fintech, dompet digital

Sumber: Kompilasi data Tirto, Kompas, dan BPJS (2020–2024)

Data pada tabel tersebut menunjukkan bahwa sektor e-commerce menjadi penyumbang kasus terbesar, menunjukkan korelasi antara tingginya aktivitas digital dan

potensi eksploitasi data. Peningkatan jumlah pengguna baru yang belum memahami keamanan digital turut memperbesar risiko, karena celah bisa muncul dari pengguna maupun dari sistem penyedia layanan. PSE yang tidak melakukan edukasi keamanan secara aktif kepada konsumennya memiliki peluang lebih besar menghadapi serangan. Hal ini menunjukkan pentingnya pendekatan keamanan yang bersifat kolaboratif antara penyelenggara dan pengguna (Kantong & Saly, 2023).

Pelanggaran data pribadi berdampak luas karena memengaruhi dimensi sosial dan ekonomi masyarakat, termasuk potensi penyalahgunaan identitas dan penipuan digital yang semakin marak. Pengguna yang kehilangan kontrol atas datanya sering mengalami kerugian finansial akibat transaksi ilegal yang dilakukan pihak ketiga. Di sisi lain, reputasi PSE tercoreng dan kepercayaan publik menurun ketika terjadi insiden kebocoran. Keadaan tersebut menunjukkan bahwa kerugian tidak hanya menimpa pengguna, tetapi juga merugikan keberlangsungan bisnis penyelenggara platform (Jo, 2024).

Serangan siber PDN menunjukkan bahwa pola serangan modern bergeser dari sekadar pencurian data menjadi upaya untuk melumpuhkan infrastruktur digital secara keseluruhan. Penyerang memanfaatkan celah pada sistem autentikasi dan prosedur backup yang lemah, sehingga serangan dapat berlangsung dalam waktu cukup lama sebelum terdeteksi. Situasi ini menunjukkan bahwa PSE harus berinvestasi dalam sistem monitoring keamanan yang mampu mendeteksi pola serangan secara real time. Ketika deteksi dini gagal dilakukan, dampak kerusakan dapat meluas ke berbagai layanan masyarakat (Dirgantara & Ramadhan, 2024).

Gambaran keseluruhan dari kasus-kasus tersebut menunjukkan bahwa kebocoran data bukan lagi kejadian insidental, melainkan bagian dari pola kejahatan digital yang semakin terstruktur. Upaya mitigasi harus dilakukan tidak hanya setelah insiden terjadi, tetapi melalui rancangan arsitektur keamanan yang komprehensif. PSE yang mengelola data berskala besar dituntut untuk memastikan bahwa seluruh bagian sistem bekerja selaras demi mencegah akses ilegal. Ketika PSE lalai, ruang tanggung jawab hukum terbuka sangat luas karena kelalaian berpotensi merugikan masyarakat secara masif (Raihan, 2023).

Model Pertanggungjawaban Hukum dan Ganti Rugi terhadap Kebocoran Data

Model pertanggungjawaban hukum PSE menempatkan pengendali data sebagai pihak utama yang bertanggung jawab atas seluruh kerugian yang muncul akibat kebocoran data. Ketentuan ini didasarkan pada prinsip bahwa pihak yang mengumpulkan, menyimpan, dan memproses data wajib memberikan perlindungan maksimal melalui standar keamanan yang layak. Ketika tanggung jawab tersebut gagal dijalankan, PSE harus menanggung risiko hukum berupa sanksi administratif, sanksi perdata, bahkan pidana. Posisi ini memperkuat perlindungan terhadap pengguna agar tidak mengalami kerugian yang tidak dapat mereka antisipasi sendiri (Fitria et al., 2025).

Undang-Undang PDP memperkenalkan skema ganti rugi yang memungkinkan pemilik data mengajukan tuntutan apabila mereka merasa dirugikan akibat kelalaian penyelenggara sistem elektronik. Ganti rugi ini dapat berbentuk kompensasi finansial maupun pemulihan hak pengguna yang datanya telah beredar secara ilegal. Dalam beberapa kondisi, pemilik data juga dapat meminta penghapusan data yang bocor apabila masih berada di bawah kendali PSE. Mekanisme ini memberikan perlindungan tambahan agar pengguna merasa memiliki kendali atas informasi pribadinya (Yusuf, 2024).

Pertanggungjawaban pidana dapat diterapkan jika terbukti bahwa PSE sengaja membiarkan sistemnya tanpa perlindungan memadai atau mengabaikan peringatan risiko

yang telah teridentifikasi. Unsur kesengajaan dan kelalaian berat menjadi dasar pemberian sanksi pidana yang dapat mencakup denda besar maupun hukuman penjara bagi pengelola yang bertanggung jawab. Ketentuan ini diperlukan untuk memberikan efek jera karena kerugian akibat kebocoran data dapat merugikan jutaan orang sekaligus. Keberadaan sanksi pidana menjadi bagian dari upaya negara menjaga keamanan digital secara serius (Muhammad & Nugroho, 2021).

Kasus kebocoran data pada penyedia layanan cloud computing menunjukkan bahwa penempatan data pada pihak ketiga tidak menghapus tanggung jawab hukum PSE sebagai pengendali utama. Ketika sebuah sistem outsourcing gagal memberikan perlindungan memadai, PSE tetap harus menanggung keseluruhan implikasi hukum karena pengguna tidak memiliki hubungan kontraktual dengan penyedia cloud. Situasi ini mempertegas bahwa pengendali data harus melakukan due diligence dan audit keamanan sebelum memilih pihak ketiga. Apabila proses tersebut diabaikan, risiko kebocoran menjadi tanggung jawab penuh PSE (Arsjad et al., 2020).

Sanksi administratif yang tercantum dalam UU PDP meliputi peringatan tertulis, penghentian sementara layanan, denda administratif, hingga pemutusan akses sistem. Sanksi ini dapat dikenakan ketika PSE terbukti tidak mematuhi standar perlindungan data atau tidak memberikan laporan insiden sesuai prosedur. Keberadaan sanksi berlapis ini menunjukkan bahwa regulasi tidak sekadar memberikan pedoman, tetapi juga mekanisme penegakan hukum yang dapat diterapkan secara langsung. Dengan demikian, PSE dituntut menjaga integritas sistemnya agar tidak berhadapan dengan beban hukum yang lebih besar (Budiandru & Hidayat, 2025).

Penelusuran terhadap berbagai kasus menunjukkan bahwa pemulihan kerugian pengguna sering kali memerlukan proses panjang, karena pembuktiannya melibatkan aspek teknis dan hukum yang saling berkaitan. Pengguna harus menunjukkan bahwa kerugian yang mereka alami berhubungan langsung dengan insiden kebocoran data yang terjadi pada sistem tertentu. Pada tahap ini, transparansi PSE sangat penting untuk memastikan bahwa pengguna memperoleh bukti yang mereka perlukan untuk proses pemulihan. Kegagalan PSE menyediakan informasi dapat dianggap sebagai bentuk penghalangan proses hukum (Delpiero et al., 2021).

Pada akhirnya, penerapan pertanggungjawaban hukum terhadap PSE merupakan upaya untuk menyeimbangkan perkembangan teknologi dengan perlindungan hak warga negara. Sistem pertanggungjawaban harus berfungsi memastikan bahwa digitalisasi tidak mengorbankan keamanan data pribadi masyarakat. Semakin besar skala digitalisasi suatu layanan, semakin besar pula kewajiban moral dan hukum penyelenggara untuk menjaga kepercayaan publik. Prinsip ini menjadi fondasi bagi penguatan tata kelola keamanan data nasional di era digital (Fathur, 2020).

KESIMPULAN

Hasil kajian menunjukkan bahwa tanggung jawab hukum penyelenggara sistem elektronik dalam kebocoran data pribadi bergantung pada kewajiban yang telah ditetapkan dalam UU PDP, PP 71/2019, dan regulasi turunannya yang menempatkan PSE sebagai pihak utama yang wajib menjaga keamanan data pengguna. Setiap bentuk kelalaian, baik teknis maupun administratif, membuka ruang tanggung jawab perdata, pidana, dan administratif yang dapat menimbulkan konsekuensi hukum berlapis bagi penyelenggara. Analisis terhadap berbagai kasus, seperti kebocoran data e-commerce, layanan publik, dan platform digital lainnya memperlihatkan bahwa sebagian besar

insiden terjadi akibat lemahnya sistem autentikasi dan kurangnya pembaruan keamanan secara berkala. Keseluruhan temuan menegaskan perlunya penguatan tata kelola keamanan digital melalui audit berkelanjutan, peningkatan literasi keamanan, dan penerapan standar teknis yang sejalan dengan perkembangan ancaman siber agar hak atas data pribadi masyarakat tetap terlindungi secara optimal.

DAFTAR PUSTAKA

Alfathi, B. R. (2025, Februari 5). Indonesia Peringkat Ke-3 Negara ASEAN dengan Kebocoran Data Terbanyak. GoodStats. https://data.goodstats.id/statistic/indonesia-peringkat-ke-3-negara-asean-dengan-kebocoran-data-terbanyak-AtcAs

Anugrah, M., Syahid, M. N., Sahri, Azka, F. M., & Anwar, M. S. (2023). Tantangan Hukum dan Peran Pemerintah dalam Pembangunan E-Commerce di Indonesia. Jurnal Hukum dan HAM Wara Sains, 2(05), 421–438. https://doi.org/10.58812/jhhws.v2i05.354

Arsjad, J., Rosadi, S. D., & Permata, R. R. (2020). Pengaturan dan Tanggung Jawab Penyedia Jasa Layanan Komputasi Awan (Cloud Computing) atas Penyimpanan Data Pribadi Pengguna dari Kebocoran Data Elektronik. Jurnal Ilmu Hukum Kyadiren, 2(1), 97-106.

Budiandru, B., & Hidayat, R. S. (2025). Tanggung Jawab Hukum Marketplace terhadap Kebocoran Data Pribadi Pengguna dalam Perspektif UU ITE dan UU Perlindungan Data Pribadi. RIGGS: Journal of Artificial Intelligence and Digital Business, 4(3), 7738-7743.

Delpiero, M., Reynaldi, F. A., Ningdiah, I. U., & Muthmainnah, N. (2021). Analisis yuridis kebijakan privasi dan pertanggungjawaban online marketplace dalam perlindungan data pribadi pengguna pada kasus kebocoran data. Padjadjaran Law Review, 9(1).

Dirgantara, A., & Ramadhan, A. (2024, Juni 27). Budi Arie Beberkan Kronologi Serangan Siber ke PDN yang Bikin Layanan Lumpuh . Kompas.com. https://nasional.kompas.com/read/2024/06/27/17585061/budi-arie-beberkan-kronologi-serangan-siber-ke-pdn-yang-bikin-layanan-lumpuh

Fathur, M. (2020, November). Tanggung Jawab Tokopedia Terhadap Kebocoran Data Pribadi Konsumen. In National Conference on Law Studies (NCOLS) (Vol. 2, No. 1, pp. 43-60).

Fitria, M., Iryani, D., & Aji Hari Setiawan, P. (2025). PERLINDUNGAN DAN TANGGUNG JAWAB HUKUM KEBOCORAN INFORMASI DATA PRIBADI PADA PENYELENGGARA SISTEM ELEKTRONIK BERDASARKAN PERSPEKTIF RAHASIA DAGANG. Jurnal Ilmiah Indonesia, Januari, 2025(1), 1–8. https://doi.org/https://doi.org/10.59141/cerdika.v5i1.2408

Jo, B. (2024, Juli 5). 6 Dampak Bahaya Kebocoran Data Pribadi serta Cara Mengatasinya. tirto.id. https://tirto.id/dampak-bahaya-kebocoraan-data-pribadi-dan-cara-mengatasinya-gSTG#google_vignette

Kantong, B. C., & Saly, J. N. (2023). Tanggung jawab hukum E-Commerce Bhineka terhadap kebocoran data pribadi pengguna. Jurnal Kewarganegaraan, 7(2), 2396-2402.

Maulida, O., & Utomo, H. (2023). Pertanggungjawaban Badan Penyelenggara Jaminan Sosial (BPJS) Kesehatan atas kebocoran data pribadi pengguna dalam perspektif hukum pidana. Indonesian Journal of Law and Justice, 1(2), 10-10.

Muhammad, M. O., & Nugroho, L. D. (2021). Perlindungan Hukum Terhadap Pengguna Aplikasi E-Commerce Yang Terdampak Kebocoran Data Pribadi. Jurnal Pamator: Jurnal Ilmiah Universitas Trunojoyo, 14(2), 165-174.

Naufal, R. A. (2020). Tanggung Jawab PT Tokopedia dalam Kasus Kebocoran Data Pribadi

Pengguna.
Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik
Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik
Prijatna, W. H. R. (2024, Juni 12). Bagaimana Pertanggungjawaban Penyelenggara Sistem Elektronik (PSE) Selaku Pengendali Data Pribadi Saat Terjadi Kebocoran Data Pribadi? kdhplaw. https://kdhplaw.com/2024/06/12/bagaimana-pertanggungjawaban-penyelenggara-sistem-elektronik-pse-selaku-pengendali-data-pribadi-saat-terjadi-kebocoran-data-pribadi/
Raihan, M. (2023). Perlindungan Data Diri Konsumen Dan Tanggungjawab Marketplace Terhadap Data Diri Konsumen (Studi Kasus: Kebocoran Data 91 Juta Akun Tokopedia). Jurnal Inovasi Penelitian, 3(10), 7847-7856.
Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi
Uz Zaman, M. N. (2021, September 20). Pertanggungjawaban Penyelenggara Sistem Elektronik atas Pelanggaran Data Pribadi. Heylaw. https://heylaw.id/blog/pelanggaran-data-pribadi
Yusuf, P. A. (2024). Tanggung Jawab Keamanan Data Digital Oleh Penyelenggara Sistem Elektronik. Lex Privatum, 13(5).