

## **Urgensi Sertifikat Keandalan Privasi Dalam Menghadapi Kebocoran Data Pribadi**

### ***The Urgency of Reliability Certificates in the Face of Personal Data Leaks***

**Zandra Azelia Savitri, Muhamad Amirulloh, Mei Susanto**  
Fakultas Hukum, Universitas Padjajaran, Bandung, Indonesia  
zandra20001@mail.unpad.ac.id

#### **Abstract**

*This study examines the urgency of privacy reliability certificates in addressing the increasing prevalence of personal data breaches due to the rapid advancement of information and communication technology. In Indonesia, data breaches have significantly increased, with nearly 160 million personal data records exposed since 2004. These breaches have severe consequences, including identity theft and declining public trust in electronic systems. Although Law No. 27 of 2022 on Personal Data Protection has been enacted, its implementation and data security mechanisms remain suboptimal. This research adopts a normative juridical approach to analyze the legal standing of privacy reliability certificates under Law No. 20 of 2014 on Standardization and Conformity Assessment, as well as the legal obligations of electronic system operators in ensuring data security. The findings reveal that privacy reliability certificates are not yet mandatory for non-strategic electronic system operators in Indonesia, unlike in developed countries where similar certifications are required to enhance cybersecurity. The government should accelerate the adoption of privacy reliability certificates as a national standard (SNI) to strengthen personal data protection, increase transparency, and provide legal certainty for electronic system operators and users.*

**Keywords:** *Cybersecurity; Data Breach; Privacy Reliability Certificate*

#### **Abstrak**

Penelitian ini mengkaji urgensi sertifikat keandalan privasi dalam mengatasi kebocoran data pribadi yang semakin meningkat seiring dengan perkembangan teknologi informasi dan komunikasi. Di Indonesia, kasus kebocoran data telah meningkat secara signifikan, dengan hampir 160 juta data pribadi terekspos sejak 2004. Hal ini berdampak serius terhadap individu dan bisnis, termasuk risiko pencurian identitas dan penurunan kepercayaan publik terhadap sistem elektronik. Meskipun Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi telah diberlakukan, implementasi regulasi dan mekanisme perlindungan masih belum optimal. Penelitian ini menggunakan pendekatan yuridis normatif untuk menganalisis kedudukan hukum sertifikat keandalan privasi berdasarkan Undang-Undang No. 20 Tahun 2014 tentang Standardisasi dan Penilaian Kesesuaian serta kewajiban hukum penyelenggara sistem elektronik dalam menerapkan standar keamanan data. Hasil penelitian menunjukkan bahwa sertifikat keandalan privasi belum menjadi persyaratan wajib bagi operator sistem elektronik non-strategis di Indonesia, berbeda dengan praktik di negara-negara maju yang telah mewajibkan sertifikasi serupa untuk meningkatkan keamanan siber. Diperlukan percepatan adopsi sertifikat keandalan privasi sebagai standar nasional (SNI) untuk memastikan perlindungan data pribadi yang lebih kuat, meningkatkan transparansi, serta memberikan kepastian hukum bagi penyelenggara sistem elektronik dan pengguna.

**Kata kunci:** Keamanan Siber; Kebocoran Data; Sertifikat Keandalan Privasi

## 1. PENDAHULUAN

Di era digital, keberadaan TIK berperan penting dalam kehidupan masyarakat, karena pemenuhan berbagai kebutuhan di era ini diakses melalui komputer atau media elektronik lainnya, dalam suatu transaksi elektronik,<sup>1</sup> seperti di bidang kesehatan,<sup>2</sup> kependudukan,<sup>3</sup> budaya, hingga kegiatan bisnis.<sup>4</sup> Ketergantungan yang sangat besar pada aplikasi TIK *online* untuk memenuhi berbagai tujuan, termasuk pendidikan dan ritel *online*.<sup>5</sup>

Di Indonesia, pemerintah telah merespons tantangan ini dengan mengesahkan Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (“UU PDP”), Hal ini diantisipasi untuk menawarkan kerangka hukum yang berbeda untuk melindungi informasi pribadi dalam menghadapi kemajuan teknologi yang cepat. Hak-hak pemilik data, kewajiban pengontrol data, dan hukuman atas pelanggaran data hanyalah beberapa bidang perlindungan data pribadi yang diatur oleh UU PDP ini. Pertanggungjawaban hukum pengontrol data - mereka yang mengumpulkan, menangani, dan memproses data pribadi - adalah salah satu topik yang diatur oleh undang-undang ini. Pengontrol data harus menerapkan perlindungan yang diperlukan untuk mencegah data diakses, dihancurkan, atau dibocorkan oleh pihak yang tidak berwenang. Mereka juga bertanggung jawab atas keamanan data yang mereka awasi.

Sertifikat keandalan privasi memiliki potensi untuk diakui sebagai bagian dari Standar Nasional Indonesia (“SNI”). Standarisasi ini penting mengingat kebutuhan akan sistem keamanan yang seragam dan dapat diandalkan dalam pengelolaan data pribadi, baik di sektor publik maupun swasta. SNI telah diterapkan di berbagai sektor, termasuk teknologi informasi, dan memungkinkan adanya jaminan kualitas yang lebih tinggi dalam proses pengelolaan data. Pengakuan sertifikat keandalan privasi sebagai bagian dari SNI, Indonesia dapat memastikan bahwa pengendali data yang memiliki sertifikat tersebut telah memenuhi standar keamanan yang diakui secara nasional.<sup>6</sup> Hal ini juga dapat memberikan kepercayaan

---

<sup>1</sup> Muhamad Amirulloh and Vidya Noor Rachmadani, “Legal Certainty in the Use of Certification of Trustworthiness by Indonesian E-Commerce Business,” *Central European Journal of International and Security Studies* 12, no. 4 (2018): 565–75.

<sup>2</sup> Charles Amirul Hanif, Muhamad Amirulloh, and Helitha Novianty Muchtar, “Reliability and Security in the Implementation of Digital Health Service Application with the Application of ‘Reliability Certification or Electronic Certification’ Based on Indonesian Law,” *Padjadjaran Jurnal Ilmu Hukum* 8, no. 3 (2021): 417–38, <https://doi.org/10.22304/pjih.v8n3.a6>.

<sup>3</sup> Sondika Ragani, Adrian Rompis, and Muhamad Amirulloh, “Implementation of Legal Certainty Principle and Economic Analysis of Law Regarding Online Services of Demographic Administration in Bandar Lampung in Implementing an Electronic Based Government System,” *Cepalo* 7, no. 2 (2023): 117–28, <https://doi.org/10.25041/cepalo.v7no2.2975>.

<sup>4</sup> Nizda Azzima Fauzianti and Muhamad Amirulloh, “Fungsi Sertifikat Keandalan Registrasi Bagi Donation Based Crowdfunding Berdasarkan Hukum Cyber Di Indonesia,” *Comserva: Jurnal Penelitian Dan Pengabdian Masyarakat* 3, no. 5 (2023): 1736–47, <https://doi.org/10.59141/comserva.v3i5.969>.

<sup>5</sup> Kemala Megahayati, Muhamad Amirulloh, and Helitha Novianty Muchtar, “Perlindungan Hukum Sinematografi Terhadap Pengaksesan Tanpa Hak Oleh Pengguna Aplikasi Telegram Berdasarkan Undang-Undang Hak Cipta Dan Undang-Undang Informasi Dan Transaksi Elektronik Di Indonesia,” *Ajudikasi : Jurnal Ilmu Hukum* 5, no. 1 (2021): 1–16, <https://doi.org/10.30656/ajudikasi.v5i1.3218>.

<sup>6</sup> Fasa Muhamad Hapid, Ija Suntana, and Muhammad Yayan Royani, “Penerapan Asas Geen Straf Zonder Schuld Dalam Penindakan Terhadap Kejahatan Penyalahgunaan Teknologi Deepfake Application of the Geen Straf Zonder Schuld Principle in Taking Action Against Crimes of Misuse of Deepfake Technology” 7, no. 3 (2024): 4–7.

lebih besar kepada masyarakat dan pelaku industri terhadap integritas sistem pengelolaan data di Indonesia.<sup>7</sup>

Wahyudi Djafar, Direktur Eksekutif Lembaga Studi dan Advokasi Masyarakat (ELSAM), perlindungan terhadap data pribadi di Indonesia menjadi salah satu isu krusial. Dalam konteks ini, penerapan sertifikat keandalan privasi (*privacy assurance certificate*) muncul sebagai solusi yang mendesak dan relevan untuk memperkuat upaya perlindungan data pribadi dalam menghadapi ancaman kebocoran yang semakin marak. Pernyataan Wahyudi yang menyoroti lemahnya sistem autentifikasi dan verifikasi oleh penyedia layanan digital, yang menyebabkan kebocoran data pribadi dan penyalahgunaan data seperti kasus pinjaman *online* yang menggunakan data KTP orang lain tanpa sepengetahuan pemiliknya, menunjukkan betapa pentingnya langkah-langkah konkret dalam mencegah kebocoran data pribadi. Sertifikat keandalan privasi dapat berperan sebagai bukti bahwa penyedia layanan digital telah memenuhi standar tinggi dalam hal perlindungan data pribadi dan keamanan informasi.

Sertifikat ini penting untuk memastikan bahwa penyedia layanan tidak hanya memenuhi persyaratan hukum yang ada dalam UU PDP, tetapi juga berkomitmen untuk menerapkan praktik terbaik dalam menjaga kerahasiaan, integritas, dan aksesibilitas data pribadi pengguna. Selain itu, sertifikat keandalan privasi juga akan memberikan kepercayaan kepada pengguna bahwa data mereka diperlakukan dengan hati-hati dan tidak akan disalahgunakan oleh pihak ketiga, sebagaimana yang telah terjadi dalam berbagai kasus kebocoran data sebelumnya.

Sertifikat ini juga akan mendorong penyedia layanan untuk melibatkan diri dalam audit dan evaluasi sistem secara berkala, guna memastikan bahwa langkah-langkah yang diambil untuk melindungi data pribadi pengguna selalu terkini dan efektif. Hal ini sejalan dengan kebutuhan untuk memperkuat sistem autentifikasi dan verifikasi data yang diungkapkan oleh Wahyudi Djafar, guna mencegah kebocoran data yang tidak hanya merugikan individu tetapi juga menciptakan kerugian sosial dan ekonomi yang lebih luas, sertifikat keandalan privasi sangat penting dalam mendukung implementasi UU PDP dan mengatasi ancaman kebocoran data yang kian marak di Indonesia. Keberadaan sertifikat ini dapat membantu menciptakan ekosistem digital yang lebih aman, dimana setiap penyedia layanan digital akan lebih bertanggung jawab atas perlindungan data pribadi, serta meningkatkan transparansi dan akuntabilitas dalam pengelolaan data pribadi pengguna.

Penelitian yang dilakukan oleh Lutfi (2024) berfokus pada perlindungan hukum terhadap data privasi nasabah bank di era digital. Penelitian ini menggunakan metode yuridis normatif dengan menelaah berbagai peraturan perundang-undangan yang relevan, seperti Undang-Undang Perbankan, Undang-Undang Telekomunikasi, Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), serta Peraturan Pemerintah Nomor 71 Tahun

---

<sup>7</sup> Rinastiti Dwi Anggraeni, Fadilla Putri Alsabilla, and Jeferson Kameo, "Pelindungan Data Pribadi Anak Yang Berhadapan Dengan Hukum Di Dunia Siber Personal Data Protection of Children in Conflict with the Law in Cyberspace" 7, no. 3 (2024): 2–12.

2019 tentang Penyelenggaraan Sistem Elektronik. Studi ini menyoroiti bahwa meskipun terdapat regulasi yang mengatur perlindungan data nasabah bank, kasus kebocoran data di sektor perbankan masih menjadi isu serius yang perlu mendapatkan perhatian lebih lanjut.<sup>8</sup>

Sementara itu, penelitian yang dilakukan oleh Rima (2023) lebih berfokus pada perlindungan data pribadi secara umum di Indonesia sebagai bagian dari hak privasi warga negara. Penelitian ini mengidentifikasi bahwa meskipun hak atas privasi telah diakui dalam konstitusi, Indonesia masih menghadapi tantangan besar dalam implementasi perlindungan data pribadi akibat belum adanya regulasi yang benar-benar komprehensif.<sup>9</sup> Melalui pendekatan konseptual dan metode yuridis normatif, studi ini menyoroiti pentingnya RUU PDP sebagai upaya untuk memperkuat perlindungan hukum di Indonesia. Penelitian ini juga membandingkan regulasi perlindungan data pribadi di Indonesia dengan negara lain seperti Malaysia, Singapura, dan Korea Selatan, yang telah memiliki regulasi perlindungan data yang lebih ketat dan implementatif. Namun, studi ini belum secara mendalam membahas dampak kebocoran data dalam sektor perbankan secara spesifik, yang menjadi fokus utama dalam penelitian.

Dari kedua penelitian ini, terdapat gap penelitian yang dapat menjadi peluang untuk penelitian lebih lanjut. Penelitian Lutfi lebih terfokus pada sektor perbankan dan regulasi yang mengatur perlindungan data nasabah, tetapi belum membahas efektivitas implementasi kebijakan serta perbandingan dengan sistem perlindungan data di negara lain. Sebaliknya, penelitian Rima membahas perlindungan data pribadi secara umum dengan pendekatan perbandingan internasional, tetapi tidak secara khusus menyoroiti dampak kebocoran data dalam sektor perbankan.

Artikel ini akan mengkaji secara mendalam bagaimana status hukum sertifikat keandalan privasi berdasarkan ketentuan peraturan perundang-undangan di Indonesia. Serta mengkaji tanggung jawab hukum penyelenggara sistem elektronik terkait dengan implementasi sertifikat keandalan privasi berdasarkan hukum siber di Indonesia. Kajian ini penting untuk memahami sejauh mana sertifikat keandalan privasi dapat berperan dalam membatasi tanggung jawab hukum bagi pengendali data, serta bagaimana upaya standarisasi ini dapat memberikan perlindungan lebih besar bagi pemilik data pribadi di Indonesia. Maka dibutuhkan penelitian lebih mendalam untuk mengkaji pentingnya sertifikat keandalan dalam mengatasi kebocoran data pribadi karena untuk menjaga keseimbangan antara kepentingan industri dan hak-hak individu terkait privasi dan keamanan data pribadi.

## **2. METODE**

Penelitian ini menggunakan pendekatan studi hukum yuridis normatif sehubungan dengan masalah yang diteliti. Metode penelitian hukum kepustakaan, yang juga dikenal

---

<sup>8</sup> Melinda Putri Lutfi, "Urgensi Perlindungan Hukum Terhadap Data Privasi Nasabah Bank di Era Perkembangan Digital" 1, no. 5 (2024): 210–18.

<sup>9</sup> Kadek Rima Anggen Suari and I Made Sarjana, "Menjaga Privasi Di Era Digital: Perlindungan Data Pribadi Di Indonesia," *Jurnal Analisis Hukum* 6, no. 1 (2023): 132–42, <https://doi.org/10.38043/jah.v6i1.4484>.

sebagai metode penelitian hukum yuridis normatif, adalah metodologi penelitian hukum yang melibatkan pemeriksaan literatur yang telah diterbitkan sebelumnya. Penelitian ini menggunakan metode hukum untuk menyelidiki status hukum sertifikat keandalan dan kewajiban operator sistem elektronik. Sumber hukum yang digunakan adalah Undang-Undang No. 27 tahun 2022 tentang Perlindungan Data Pribadi, Undang-Undang No. 19 tahun 2016 tentang perubahan atas Undang-Undang No. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik, Peraturan Pemerintah No. 71 tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, Peraturan Badan Siber dan Sandi Negara Republik Indonesia No. 7 tahun 2024 tentang Penyelenggaraan Penilaian Kesesuaian Kriteria Umum Evaluasi Keamanan Teknologi Informasi Indonesia, Undang-Undang No. 20 tahun 2014 tentang Standarisasi dan Penilaian Kesesuaian, bahan hukum sekunder berupa buku-buku dan jurnal-jurnal penelitian terdahulu, dan bahan hukum tersier berupa artikel ilmiah yang menjadi sumber informasi hukum utama. Penelitian ini akan menganalisis permasalahan mengenai sertifikat keandalan privasi berdasarkan undang-undang yang berlaku.

### **3. HASIL DAN PEMBAHASAN**

#### **3.1 Status Hukum Sertifikat Keandalan Privasi Berdasarkan Ketentuan Hukum Siber di Indonesia**

Di era digital yang semakin maju, urgensi perlindungan data pribadi menjadi krusial karena data pribadi kini memiliki nilai ekonomis dan strategis yang tinggi, sering kali dimanfaatkan oleh berbagai pihak untuk keperluan komersial, survei, hingga tujuan-tujuan lain yang berpotensi merugikan individu. Semakin banyaknya transaksi dan aktivitas berbasis daring, data pribadi seseorang-mulai dari informasi identitas, kontak, hingga data kesehatan dan finansial-menjadi semakin rentan terhadap penyalahgunaan, pencurian, atau eksploitasi oleh pihak-pihak yang tidak bertanggung jawab.<sup>10</sup> Ancaman siber seperti hacking, pencurian identitas, dan eksploitasi data menjadi momok yang menghantui masyarakat global.<sup>11</sup>

Melihat tingginya risiko ini, keamanan sistem elektronik menjadi prioritas utama untuk mencegah akses tidak sah dan pelanggaran privasi. Tanpa perlindungan yang memadai, data pribadi yang seharusnya aman justru bisa dimanfaatkan oleh oknum tak bertanggung jawab yang mengaksesnya tanpa izin. Pembentukan hukum hendaknya mengarahkan kepada hakikat hukum (*law truth*). Artinya, pembentukan undang-undang merupakan suatu cara untuk memajukan dan melindungi kepentingan tertentu atau mengutamakan suatu kepentingan di atas yang lain.<sup>12</sup> Hal ini semakin ditekankan di

---

<sup>10</sup> Tito Wira Eka Suryawijaya, "Memperkuat Keamanan Data Melalui Teknologi Blockchain: Mengeksplorasi Implementasi Sukses Dalam Transformasi Digital Di Indonesia," *Jurnal Studi Kebijakan Publik* 2, no. 1 (2023): 55–68, <https://doi.org/10.21787/jskp.2.2023.55-68>.

<sup>11</sup> Elsa Pebiyanti et al., "Pengaruh Kualitas Informasi, Persepsi Keamanan, Dan Persepsi Privasi Terhadap Kepercayaan Pengguna Belanja Online (Literature Review)," *Jurnal Ekonomi Manajemen Sistem Informasi* 4, no. 5 (2023): 850–58, <https://doi.org/10.31933/jemsi.v4i5.1548>.

<sup>12</sup> Arif Hidayat and Zaenal Arifin, "Politik Hukum Legislasi Sebagai Socio-Equilibrium Di Indonesia," *Jurnal Ius Constituendum* 4, no. 2 (2019): 147–59, <https://doi.org/10.26623/jic.v4i2.1654>.

Indonesia dengan diterbitkannya UU PDP sebagai landasan hukum yang mengatur hak-hak subjek data dan kewajiban pengendali data. UU PDP menjadi payung utama dalam melindungi hak masyarakat atas privasi dan memberikan kerangka hukum yang mengatur pengumpulan, pemrosesan, dan penyimpanan data pribadi oleh institusi, perusahaan, atau organisasi yang mengelolanya.<sup>13</sup>

Dalam upaya meningkatkan keamanan elektronik, sertifikat keandalan juga hadir sebagai standar yang perlu dipenuhi oleh para pengendali data. Sertifikat ini bertujuan untuk menjamin bahwa sistem elektronik yang digunakan telah sesuai dengan standar keamanan yang ditetapkan pemerintah, memberikan bukti bahwa institusi tersebut telah mengambil langkah-langkah pencegahan dan pengamanan yang diakui secara hukum.<sup>14</sup> Hal ini sejalan dengan Pasal 76 Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (“PP PSTE”) yang menjelaskan bahwa Sertifikat Keandalan yang diterbitkan oleh Lembaga Sertifikasi Keandalan meliputi kategori; a. registrasi identitas; b. keamanan Sistem Elektronik; dan c. kebijakan privasi. Pada bagian Penjelasan Pasal 76 huruf c yang memuat isi jika menggunakan sertifikat keandalan maka mendapat jaminan keandalan dan dapat dipastikan bahwa data pribadi siapapun termasuk konsumen sangat terjaga dan dilindungi kerahasiaannya. Ketentuan ini sejalan dengan Pasal 1 PP PSTE bahwa yang dimaksud Sertifikat Keandalan adalah dokumen yang menyatakan pelaku usaha yang menyelenggarakan transaksi elektronik telah lulus audit atau uji kesesuaian dari lembaga sertifikasi keandalan.<sup>15</sup>

Regulasi yang mendasari penggunaan sertifikat keandalan privasi ditemukan dalam Pasal 39 ayat (1) dan (2) UU PDP. Namun dalam praktiknya, kasus kebocoran data masih marak terjadi di berbagai institusi dan perusahaan, seperti yang dialami oleh Bank Syariah Indonesia (BSI),<sup>16</sup> BPJS,<sup>17</sup> Direktorat Jenderal Pajak,<sup>18</sup> dan aplikasi Peduli Lindungi,<sup>19</sup> mengindikasikan adanya kelemahan yang signifikan dalam sistem keamanan data yang diterapkan oleh institusi tersebut, di mana data pribadi yang seharusnya dilindungi justru menjadi rentan terhadap ancaman penyalahgunaan. Kebocoran data bukan hanya menjadi masalah teknis, tetapi juga berdampak serius pada reputasi institusi dan kepercayaan publik, yang pada gilirannya dapat merugikan individu yang datanya terekspos. Situasi ini

---

<sup>13</sup> Muhammad Bahram, “Transformasi Masyarakat Di Era Digital: Menjaga Kaidah Hukum Sebagai Landasan Utama,” *Sentri: Jurnal Riset Ilmiah* 2, no. 5 (2023): 1733–46, <https://doi.org/10.55681/sentri.v2i5.884>.

<sup>14</sup> Domi Dwi Kurniasandi et al., “Regulasi Terkait Perlindungan Data Pribadi Dalam Penggunaan Jasa E-Commerce” 21, no. 1 (2022): 103–14.

<sup>15</sup> Muhammad Ali Anhar and Teguh Agum Pratama, “Analisis Implementasi Keamanan Data Melalui Teknologi Blockchain,” *Program Studi Ilmu Komunikasi* 4, no. 2 (2035): 20353.

<sup>16</sup> Anggi Muhammad et al., “Perlindungan Terhadap Konsumen Dalam Kasus Kebocoran Data Bank Syariah Indonesia,” *Jurnal Ilmu Hukum, Sosial, Dan Humaniora* 2, no. 1 (2024): 156–65.

<sup>17</sup> Shella Oktaviani, Yeremia Juan Dewata, and Aryo Fadlian, “Pertanggung Jawaban Pidana Kebocoran Data Bpjs Dalam Perspektif Uu Ite,” *De Juncto Delicti: Journal of Law* 1, no. 2 (2021): 146–57, <https://doi.org/10.35706/djd.v1i2.5732>.

<sup>18</sup> Imam Sukadi, Musleh Harry, and Teguh Setyobudi, “Legal Politics Electronic Land Certificate in Indonesia” 7, no. 53 (2024): 23–34.

<sup>19</sup> Rista Maharani and Andria Luhur Prakoso, “Perlindungan Data Pribadi Konsumen Oleh Penyelenggara Sistem Elektronik Dalam Transaksi Digital,” *Jurnal USM Law Review* 7, no. 1 (2024): 333, <https://doi.org/10.26623/julr.v7i1.8705>.

memunculkan kebutuhan mendesak akan regulasi yang kuat dan efektif untuk mengatur penggunaan data pribadi serta memastikan adanya mekanisme perlindungan hukum yang memadai bagi pemilik data.<sup>20</sup> Kebutuhan akan sertifikat keandalan privasi menjadi semakin mendesak sebagai upaya untuk mencegah risiko kebocoran data, di mana sertifikat ini berfungsi sebagai alat untuk memastikan bahwa pengendali data telah mengoptimalkan perlindungan data dan mematuhi standar keamanan yang tinggi sesuai dengan kriteria perlindungan data yang ditetapkan oleh regulasi.<sup>21</sup>

Namun dalam praktiknya, kasus kebocoran data masih marak terjadi di berbagai institusi dan perusahaan, seperti yang dialami oleh Bank Syariah Indonesia (BSI) yakni serangan ransomware yang dilakukan untuk mengenkripsi data pribadi nasabah dan karyawan pada sistem komputer atau jaringan, dan kemudian mengancam dengan meminta pembayaran tebusan agar data tersebut bisa dikembalikan. Hal ini merupakan pelanggaran terhadap perlindungan data pribadi yang merupakan dokumen elektronik yang bersifat rahasia.<sup>22</sup> Hal serupa juga terjadi pada aplikasi Peduli Lindungi, di mana 3,2 miliar data pengguna aplikasi Peduli Lindungi telah diretas dan dibocorkan Bjorka dalam situs BreachForums. Data Peduli Lindungi yang dibocorkan itu berjumlah 3.250.144.777, mencakup 48 Gigabyte data terkompresi dan riwayat pelacakan kontak (1,5 miliar) data Peduli Lindungi yang ada di tangan Bjorka meliputi data pengguna atau (94 juta), akun yang diurutkan (94 juta), data vaksinasi 209 juta, riwayat check-in (1,3 miliar), dan riwayat pelacakan kontak (1,5 miliar).<sup>23</sup> Dari contoh kasus kebocoran data pribadi tersebut mengindikasikan adanya kelemahan yang signifikan dalam sistem keamanan data yang diterapkan oleh PSE, di mana data pribadi yang seharusnya dilindungi justru menjadi rentan terhadap ancaman penyalahgunaan. Kebocoran data bukan hanya menjadi masalah teknis, tetapi juga berdampak serius pada reputasi institusi dan kepercayaan publik, yang pada gilirannya dapat merugikan individu yang datanya terekspos. Situasi ini memunculkan kebutuhan mendesak akan regulasi yang kuat dan efektif untuk mengatur penggunaan data pribadi serta memastikan adanya mekanisme perlindungan hukum yang memadai bagi pemilik data.<sup>24</sup> Dalam konteks ini, kebutuhan akan sertifikat keandalan privasi menjadi semakin mendesak sebagai upaya untuk mencegah risiko kebocoran data, di mana sertifikat ini berfungsi sebagai alat untuk memastikan bahwa pengendali data telah mengoptimalkan perlindungan data dan mematuhi standar keamanan yang tinggi sesuai dengan kriteria

---

<sup>20</sup> Florianus Yudhi Priyo Amboro and Viona Puspita, "Perlindungan Hukum Atas Data Pribadi (Studi Perbandingan Hukum Indonesia Dan Norwegia)," *Combines- Conference on Management, Business, Innovation, Education and Social Sciences* 1, no. 1 (2021): 415–27.

<sup>21</sup> Adinda Putri Denisa, Muhamad Amirulloh, and Helitha Novianty Muchtar, "Sertifikat Keandalan Privasi Sebagai Salah Satu Bentuk Pelindungan Konsumen Di Bidang Informasi Dan Transaksi Elektronik," *Jurnal Rechtsvinding Media Pembinaan Hukum Nasional* 12, no. 2 (2023): 167–84.

<sup>22</sup> Hutagalung, A.M.C., Marendra, N.R., Hosnah, A.U. (2024). Perlindungan Terhadap Konsumen Dalam Kasus Kebocoran Data Bank Syariah Indonesia. *Jurnal Ilmu Hukum dan Humaniora*

<sup>23</sup> <https://nasional.kompas.com/read/2022/11/18/05230361/data-pedulilindungi-bocor-pemerintah-diminta-tak-saling-lempar-tanggung?page=all> diakses pada tanggal 20 November 2024

<sup>24</sup> Amboro, F. Y. P., & Puspita, V. (2021, March). Perlindungan Hukum Atas Data Pribadi (Studi Perbandingan Hukum Indonesia dan Norwegia). In *CoMBInES-Conference on Management, Business, Innovation, Education and Social Sciences* (Vol. 1, No. 1, pp. 415-427).

perlindungan data yang ditetapkan oleh regulasi.<sup>25</sup>

Sertifikat keandalan privasi bertindak sebagai tameng hukum yang memberikan perlindungan kepada pengendali data dari risiko hukum yang tidak proporsional. Salah satu konsep kunci yang terkait dengan perlindungan hukum ini adalah penerapan teori *safe harbor* yang secara normatif telah diatur dalam Pasal 26 UU ITE. Doktrin *safe harbor* merupakan pembatasan tanggung jawab kepada penyelenggara sistem elektronik apabila penyelenggara elektronik telah melaksanakan langkah preventif yakni langkah yang mewajibkan penyelenggara sistem elektronik untuk membentuk sarana kontrol dalam rangka mengantisipasi kebocoran data yang akan terjadi.<sup>26</sup> Sebagai contoh, jika sebuah perusahaan telah memiliki sertifikat keandalan privasi dapat menunjukkan bahwa mereka telah menerapkan semua langkah yang diwajibkan untuk menjaga keamanan data, tetapi data tersebut tetap bocor akibat serangan siber yang canggih dari pihak ketiga, perusahaan tersebut dapat berargumen bahwa mereka tidak dapat dimintai pertanggungjawaban penuh atas insiden tersebut.

Berdasarkan *safe harbour*, sertifikat keandalan privasi dapat melindungi pengendali data dari tanggung jawab hukum penuh jika terjadi kebocoran data yang disebabkan oleh pihak ketiga, asalkan pengendali data tersebut telah mematuhi standar keandalan yang diwajibkan eksternal.<sup>27</sup> Jika pengendali data dapat membuktikan bahwa mereka telah menerapkan semua langkah keamanan yang diperlukan sesuai dengan regulasi dan standar yang ada, maka mereka tidak akan sepenuhnya bertanggung jawab atas kebocoran yang terjadi akibat tindakan pihak ketiga yang tidak terduga.

Tantangan dalam penerapan sertifikat keandalan privasi di Indonesia tidak bisa diabaikan. Masih ada sejumlah kendala, baik dari segi regulasi maupun implementasi teknis. Di satu sisi, Indonesia masih menghadapi masalah kurangnya infrastruktur teknologi yang mendukung penerapan sertifikat ini secara luas. Di sisi lain, masih perlu ada kejelasan regulasi mengenai mekanisme sertifikasi, termasuk siapa yang berwenang mengeluarkan sertifikat tersebut dan bagaimana pengawasannya. Di negara-negara maju, mekanisme sertifikasi sering kali melibatkan badan independen yang memiliki otoritas untuk melakukan audit terhadap pengendali data. Indonesia perlu membangun sistem yang serupa untuk memastikan bahwa sertifikat keandalan privasi tidak hanya menjadi formalitas, tetapi benar-benar mencerminkan standar perlindungan yang tinggi.

Untuk mewujudkan perlindungan data pribadi yang optimal, sertifikat keandalan privasi juga memiliki potensi untuk diakui sebagai bagian dari SNI. Standarisasi ini penting mengingat kebutuhan akan sistem keamanan yang seragam dan dapat diandalkan dalam pengelolaan data pribadi, baik di sektor publik maupun swasta. SNI telah diterapkan di

---

<sup>25</sup> Denisa, A. P., Amirulloh, M., & Muchtar, H. N. (2023). Sertifikat Keandalan Privasi Sebagai Salah Satu Bentuk Pelindungan Konsumen Di Bidang Informasi Dan Transaksi Elektronik. *Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional*, 12(2).

<sup>26</sup> Syarafina Ramadhanty et al., "Doktrin Safe Harbor: Upaya Perlindungan Hak Cipta Konten Dalam Platform User Generated Content," *Legalitas: Jurnal Hukum* 12, no. 2 (2020): 267, <https://doi.org/10.33087/legalitas.v12i2.226>.

<sup>27</sup> Kadek Dio Ramadi Natha., I Nyoman Putu Budiarta., and Ni Gusti Ketut Sri Astiti, "Perlindungan Hukum Atas Kebocoran Data Pribadi Konsumen Pada E-Commerce," *Heylaw.Edu* 3, no. 1 (2022): 143–48.

berbagai sektor, termasuk teknologi informasi, dan memungkinkan adanya jaminan kualitas yang lebih tinggi dalam proses pengelolaan data. Pengakuan sertifikat keandalan privasi sebagai bagian dari SNI, Indonesia dapat memastikan bahwa pengendali data yang memiliki sertifikat tersebut telah memenuhi standar keamanan yang diakui secara nasional. Hal ini juga dapat memberikan kepercayaan lebih besar kepada masyarakat dan pelaku industri terhadap integritas sistem pengelolaan data di Indonesia.

Pengaturan terkait penggunaan sertifikat yang sebelumnya bersifat volunteer menjadi wajib dapat diterapkan melalui Peraturan Menteri atau Peraturan Kepala Lembaga, sebagaimana bunyi Pasal 24 ayat (1) UU No 20 Tahun 2014 yang berbunyi: “Dalam hal berkaitan dengan kepentingan keselamatan, keamanan, kesehatan, atau pelestarian fungsi lingkungan hidup, kementerian/lembaga pemerintah nonkementerian berwenang menetapkan pemberlakuan SNI secara wajib dengan Peraturan Menteri atau Peraturan Kepala Lembaga Pemerintah Nonkementerian.”

Kementerian Komunikasi dan Informatika telah mengeluarkan peraturan terkait kewajiban sertifikasi oleh penyelenggara sistem elektronik dalam Pasal 28 huruf Permenkominfo No 20 Tahun 2016 yang berbunyi: ”Setiap Penyelenggara Sistem Elektronik wajib: melakukan sertifikasi Sistem Elektronik yang dikelolanya sesuai dengan ketentuan peraturan perundang-undangan;” Permenkominfo No 20 Tahun 2016 dalam hal ini telah mengatur tata cara perlindungan data pribadi dan mewajibkan penyelenggara sistem elektronik untuk memenuhi standar keamanan tertentu. Peraturan ini sudah dapat dianggap sebagai peraturan yang mewajibkan adanya Sertifikasi Keandalan Privasi melalui ketentuan yang mengharuskan penerapan standar teknis tertentu dalam menjaga data pribadi yang dikelola oleh penyelenggara sistem elektronik.

Selain itu, Peraturan Badan Siber Dan Sandi Negara Republik Indonesia Nomor 7 Tahun 2024 Tentang Penyelenggaraan Penilaian Kesesuaian Kriteria Umum Untuk Evaluasi Keamanan Teknologi Informasi Indonesia (“PBSSN 7/2024”) juga menambahkan dimensi penting dalam konteks regulasi keamanan informasi, keamanan siber dan proteksi privasi. PBSSN 7/2024 mengatur penilaian kesesuaian kriteria umum untuk evaluasi keamanan teknologi informasi Indonesia. Peraturan ini menetapkan bahwa setiap organisasi yang mengelola data sensitif atau yang memiliki dampak signifikan terhadap keamanan nasional harus mematuhi standar dan prosedur keamanan yang ketat, termasuk dalam hal sertifikasi keandalan privasi. Adanya PBSSN 7/2024 menegaskan bahwa sertifikasi keandalan privasi menjadi sebuah keharusan yang tidak hanya untuk memenuhi standar nasional tetapi juga untuk melindungi kepentingan publik yang lebih luas. Dengan kata lain, sertifikat keandalan privasi SNI ISO/IEC 15408-2, 15048-3 dan 15408-5 adalah standar teknis yang diacu sebagai standar dari sertifikat keandalan privasi yang telah menjadi SNI wajib bagi setiap organisasi yang mengelola data sensitif atau yang memiliki dampak signifikan terhadap keamanan nasional. Berdasarkan Pasal 99 PP PSTE, pengelola data sensitif atau yang memiliki dampak signifikan terhadap keamanan nasional ialah sektor administrasi pemerintahan, sektor energi dan sumber daya mineral, sektortransportasi,

sektor keuangan, sektor kesehatan, sektor teknologi informasi dan komunikasi, sektor pangan, sektor pertahanan, dan sektor lain yang ditetapkan oleh presiden.

Pengaturan mewajibkan sertifikat keandalan privasi sebagai SNI tidak hanya berfungsi sebagai alat untuk mengukur kepatuhan pengendali data terhadap regulasi, tetapi juga sebagai jaminan bahwa standar perlindungan data yang diterapkan adalah terukur, dapat diandalkan, dan sesuai dengan praktik terbaik yang telah diakui secara nasional. Manfaat kepastian hukum dan standar perlindungan yang seragam sangat signifikan, karena dengan status SNI, sertifikat keandalan akan menjadi standar yang wajib diikuti oleh semua pengendali data, baik itu lembaga publik maupun swasta, sehingga mengurangi keraguan dan ketidakpastian di antara pemangku kepentingan terkait perlindungan data pribadi. Hal ini juga akan menciptakan keseragaman dalam penerapan perlindungan data, yang pada gilirannya akan mempermudah proses audit dan evaluasi terhadap kepatuhan pengendali data terhadap standar yang telah ditetapkan.<sup>28</sup>

Adanya kewajiban ini, semua pengendali data akan terdorong untuk berinvestasi dalam sistem keamanan yang lebih baik dan mengikuti perkembangan teknologi yang dapat membantu melindungi data pribadi. Dalam konteks regulasi yang semakin ketat terkait perlindungan data, pengakuan sertifikat keandalan privasi sebagai SNI juga akan memberikan insentif bagi pengendali data untuk lebih proaktif dalam memenuhi kewajiban hukum mereka. Ini akan mengarah pada pengembangan kebijakan internal yang lebih baik dalam mengelola data pribadi dan melindungi informasi sensitif.<sup>29</sup> Kewajiban ini juga menciptakan rasa tanggung jawab yang lebih besar di antara pengendali data untuk menjaga keamanan data yang mereka kelola, karena mereka akan diharuskan untuk memenuhi standar yang telah ditetapkan. Dalam jangka panjang, semua ini akan berkontribusi pada terciptanya budaya perlindungan data yang lebih baik di Indonesia, di mana lembaga dan pengendali data memiliki kesadaran yang tinggi akan pentingnya menjaga keamanan informasi yang mereka kelola. Dengan mengedepankan standarisasi sertifikat keandalan privasi sebagai SNI, Indonesia akan menunjukkan komitmennya terhadap perlindungan data pribadi dan keamanan informasi, serta berkontribusi pada pengembangan ekosistem digital yang lebih aman dan berkelanjutan bagi seluruh masyarakat.

Struktur organisasi kementerian komunikasi dan digital (dahulu dikenal dengan nama Kominfo) baru saja mengalami restrukturisasi berdasarkan Perpres No 174 tahun 2024 tentang Komunikasi dan Digital.<sup>30</sup> Data pribadi termasuk kedalam ruang lingkup Direktorat Jendral Pengawasan Ruang Digital sebagaimana diatur dalam Pasal 21 Perpres 174/2024. Dengan demikian Kementerian Komdigi memiliki kewenangan pula untuk melakukan perlindungan data pribadi, termasuk mengeluarkan regulasi terkait penetapan sistem

---

<sup>28</sup> Suryati, S., Sardana, L., Disurya, R., & Putra, Y. S. (2024). Penguatan Literasi Digital Dalam Pencegahan Pelanggaran Hukum Siber (Cyber Law). *Wajah Hukum*, 8(1), 84-94.

<sup>29</sup> Septiriani, V., Sofyan, T., & Rosari, W. N. (2024). Tanggung Jawab Pelaku Usaha Terhadap Kebocoran Informasi Data Pribadi Konsumen Dalam Pelaksanaan Perdagangan Elektronik (E-Commerce). *Jurnal Ilmiah Kutei*, 23(1), 127-136.

<sup>30</sup> <https://www.tempo.co/politik/meutya-hafid-tunjuk-brigjen-pol-alexander-sabar-jadi-plt-dirjen-pengawasan-ruang-digital-apa-tugasnya--1178323> diakses pada tanggal 10 Desember 2024

pengamanan terhadap sistem elektronik yang mengelola data pribadi. Kewenangan ini sejalan dengan Pasal 58 UU PDP yang menyebutkan bahwa penyelenggaraan perlindungan data pribadi dilaksanakan oleh lembaga yang ditetapkan melalui peraturan presiden. Oleh karena itu, kedepannya Komdigi dapat membuat peraturan menteri yang mewajibkan sertifikat keandalan privasi dan menetapkan standar teknis yang diacu bagi penyelenggara sistem elektronik non-strategis.

### **3.2 Tanggung Jawab Hukum Penyelenggara Sistem Elektronik Terkait Dengan Implementasi Sertifikat Keandalan Privasi Berdasarkan Hukum Cyber Di Indonesia**

Dari perspektif etimologis, kewajiban sering kali dipertukarkan dengan tanggung jawab hukum atau tanggung gugat. Menurut Black Law Dictionary, istilah “tanggung jawab” memiliki definisi yang luas. Tanggung jawab hukum adalah tanggung jawab yang diakui dan ditegakkan oleh pengadilan sebagai sesuatu yang ada di antara para pihak.<sup>31</sup> Segala sesuatu yang dapat dipertanggungjawabkan, seperti tugas, pilihan, bakat, dan keterampilan, serta pertanggungjawaban atas penerapan hukum, disebut sebagai tanggung jawab. Pertanggungjawaban, seperti yang digunakan dalam pengetahuan dan praktik, mengacu pada pertanggungjawaban hukum, sedangkan tanggung jawab secara lebih khusus mengacu pada tanggung jawab politik.<sup>32</sup>

Tanggung jawab hukum terlihat jelas dalam banyak bidang hukum. Misalnya, dalam hukum perdata, tanggung jawab hukum mengacu pada kewajiban individu untuk menahan diri dari perilaku ilegal.<sup>33</sup> Tidak seperti kegiatan kriminal, tindakan melanggar hukum memiliki jangkauan yang lebih luas. pelanggaran hukum lain dan ketentuan hukum tidak tertulis juga termasuk dalam pelanggaran hukum pidana. Tujuan dari ketentuan-ketentuan yang berkaitan dengan kegiatan yang melanggar hukum adalah untuk melindungi orang yang telah dirugikan dan memberikan kompensasi atas kerugian mereka.<sup>34</sup>

Penyelenggara sistem elektronik memiliki kewajiban hukum yang jelas untuk mengelola data pribadi. Karena negara telah memberlakukan kewajiban hukum ini melalui ketentuan Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi dan Peraturan Pemerintah No. 7 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Sebagai contoh, ketentuan-ketentuan dalam UU PDP diterbitkan dengan tujuan untuk memastikan hak-hak masyarakat atas perlindungan pribadi, meningkatkan kesadaran

---

<sup>31</sup> Anisa Isti Briliany and Anajeng Esri Edhi Mahanani, “Tinjauan Yuridis Perbuatan Melanggar Hukum ( PMH ),” *Jurnal Yustika: Media Hukum Dan Keadilan* 24, no. 02 (2021): 63–75.

<sup>32</sup> Totok Wahyu Abadi et al., *Buku Ajar Governance Digital Berbasis Riset Anggota IKAPI Nomor : 218 / Anggota Luar Biasa / JTI / 2019 Diterbitkan Oleh Jl . Mojopahit 666 B Sidoarjo ISBN : 978-623-464-102-8 Copyright © 2024 Authors All Rights Reserved*, 2024.

<sup>33</sup> Jurnal Penelitian and Jenda Ingan Mahuli, “All Fields of Science J-LAS Perlindungan Hukum Terhadap Data Pribadi Dalam Era Digital Legal Protection of Personal Data in the Digital Era,” *AFoSJ-LAS* 3, no. 4 (2023): 188–94.

<sup>34</sup> Dinda Aprilita Herera and Muhamad Hasan Sebyar, “Perlindungan Hukum Terhadap Serangan Siber: Tinjauan Atas Kebijakan Dan Regulasi Terbaru,” *Jurnal Hukum Dan Kewarganegaraan* 1, no. 5 (2023): 1–16.

masyarakat, dan memastikan bahwa pentingnya melindungi data pribadi diakui dan dihormati.<sup>35</sup>

“Penyelenggara Sistem Elektronik adalah Setiap Orang, Penyelenggara Negara, Badan Usaha, dan Masyarakat yang menyediakan, mengelola, dan/atau mengoperasikan Sistem Elektronik secara sendiri-sendiri atau bersama-sama kepada Pengguna Sistem Elektronik untuk keperluan dirinya sendiri dan/atau keperluan pihak lain,” demikian bunyi pasal 1 angka 4 definisi tersebut. Seperti yang dinyatakan dalam Pasal 3 UU PDP, penyelenggara sistem elektronik diwajibkan untuk menangani data pribadi sesuai dengan nilai-nilai dasar kehati-hatian, tanggung jawab, keseimbangan, dan kerahasiaan. Oleh karena itu, sangat penting bagi operator sistem elektronik untuk melindungi kerahasiaan data.<sup>36</sup>

Tanggung jawab hukum penyelenggara data pribadi yang dalam hal ini mencakup penyelenggara sistem elektronik, baik yang bersifat swasta maupun instansi pemerintahan menjadi satu hal yang wajib. Kewajiban hukum ini merupakan kewajiban untuk menyelenggarakan pengelolaan dan pemrosesan data pribadi secara aman dan terpercaya.<sup>37</sup> Sebab kerentanan akan bocornya data pribadi merupakan hal yang harus diantisipasi secara serius. Ketentuan mengenai kewajiban menjaga keandalan privasi data pribadi milik masyarakat yang diproses oleh pengendali data pribadi dalam hal ini adalah penyelenggara sistem elektronik dapat dilihat dalam ketentuan hukum pada Pasal 39 ayat (1) dan (2) UU PDP yang mengemukakan tentang data pribadi wajib dilindungi menggunakan sistem elektronik secara aman dan tanggungjawab oleh pengendali data pribadi guna mencegah kebocoran data yang diakses secara tidak sah. Sistem keamanan tersebut adalah Sertifikat Keandalan Privasi yang harus dibuat oleh penyelenggara sistem elektronik.<sup>38</sup>

Kebocoran data pribadi di Indonesia telah menjadi isu yang semakin mencuat, dengan jumlah kasus yang meningkat signifikan dalam beberapa tahun terakhir. Pada kuartal II 2022, tercatat bahwa lebih dari 1 juta akun mengalami kebocoran data, sebuah lonjakan yang meningkat sebesar 143% dibandingkan dengan kuartal sebelumnya. Indonesia kini menjadi salah satu negara dengan kebocoran data terbesar di dunia, dengan hampir 160 juta data pribadi yang bocor sejak 2004. Angka ini menunjukkan betapa seriusnya masalah kebocoran data yang terjadi, terutama karena dampaknya yang luas terhadap privasi dan keamanan individu.<sup>39</sup>

Sebagai perbandingan, beberapa negara lain telah memiliki langkah-langkah yang lebih ketat dalam penanganan kebocoran data. Di Eropa, misalnya, penerapan regulasi

---

<sup>35</sup> R. E. Purba et al., “Peranan Hukum Positif Dalam Mengatur Cyberspace Untuk Menghadapi Tantangan Dan Peluang Di Era Digital,” *Mandub: Jurnal Politik, Sosial, Hukum Dan Humaniora* 2, no. 2 (2024): 167–76.

<sup>36</sup> Ni Putu Riyani Kartika Sari, “Aktual Justice,” *Jurnal Aktual Justice* 6, no. 2 (2021): 211–29.

<sup>37</sup> Maharani and Prakoso, “Perlindungan Data Pribadi Konsumen Oleh Penyelenggara Sistem Elektronik Dalam Transaksi Digital.”

<sup>38</sup> Denisa, Amirulloh, and Muchtar, “Sertifikat Keandalan Privasi Sebagai Salah Satu Bentuk Pelindungan Konsumen Di Bidang Informasi Dan Transaksi Elektronik.”

<sup>39</sup> Muhammad Fikri and Shelvi Rusdiana, “Ruang Lingkup Perlindungan Data Pribadi: Kajian Hukum Positif Indonesia,” *Ganesha Law Review* 5, no. 1 (2023): 45–46.

seperti *General Data Protection Regulation* (GDPR) memberikan sanksi yang berat bagi pelanggar perlindungan data pribadi, termasuk denda yang dapat mencapai 4% dari pendapatan tahunan global perusahaan yang melakukan pelanggaran. Negara-negara seperti Amerika Serikat dan Australia juga menerapkan regulasi serupa untuk mengatasi kebocoran data yang sering terjadi. Hal ini menunjukkan bahwa Indonesia masih memiliki banyak pekerjaan rumah dalam memperkuat pengawasan dan penegakan hukum terkait kebocoran data pribadi.<sup>40</sup>

Di Indonesia, meskipun UU PDP sudah disahkan, implementasi dan pengawasan yang efektif masih menjadi tantangan. UU PDP mewajibkan pengendali data untuk menjaga kerahasiaan dan keamanan data pribadi yang mereka kelola, namun pelaksanaan regulasi ini masih mengalami kendala, penegakan hukum terkait kebocoran data pribadi juga belum sepenuhnya efektif. Penegakan hukum yang lemah ini berdampak pada rendahnya tingkat kepatuhan terhadap peraturan yang ada, sehingga membuat perlindungan data pribadi di Indonesia masih kurang optimal.

Berdasarkan aturan hukum yang ada, kewajiban menggunakan sertifikat keandalan privasi sebenarnya telah ada, namun belum dapat ditegakkan secara tegas kepada pengelola data pribadi selaku penyelenggara sistem elektronik karena belum ada aturan teknis dalam hal peraturan kepala lembaga dan kementerian. Sebab tanpa aturan teknis dalam menjalankan kewajiban kerahasiaan data tersebut, apabila terjadi pelanggaran maka tanggung jawabnya hanya terbatas pada tanggung jawab secara keperdataan, sebagaimana telah diatur dalam:

- Pasal 38 ayat (1) UU ITE yang memuat tentang setiap orang dapat menuntut kepada pihak yang merugikan kita terhadap penggunaan sistem elektronik.
- Pasal 12 ayat (1) UU PDP yang memuat tentang setiap orang berhak menerima ganti rugi apabila data dirinya diakses secara tidak sah dan dilanggar dalam pemrosesan datanya.

Selain tanggung jawab secara keperdataan, terdapat tanggung jawab secara administratif yang diatur dalam Pasal 57 UU PDP. Untuk saat ini tanggung jawab secara pidana tidak dapat diberlakukan, karena belum ada satu standar khusus yang menjadi batasan pemberlakuan sertifikat keandalan privasi. Tanggung jawab secara pidana dapat diberlakukan apabila sertifikat keandalan privasi telah ditetapkan sebagai SNI di Indonesia. Tanggung jawab pidana terkait SNI telah diatur dalam Pasal 65 UU SPK yang mengemukakan bahwa setiap orang yang tidak memiliki sertifikat atau sertifikat tersebut telah melewati masa berlaku serta sertifikat sengaja dicabut ataupun dibekukan sementara yakni jika menjalankan proses atau sistem tetapi tidak sesuai dengan SNI dapat dipidana penjara paling lama lima tahun atau dapat membayar denda paling banyak Rp. 35.000.000.000,00 (tiga puluh lima miliar rupiah).

Melihat dalam ketentuan hukum yang ada, batasan tanggung jawab penyelenggara sistem elektronik sebagai salah satu pihak pengelola data pribadi dan pemroses data pribadi

---

<sup>40</sup> Simorangkir, Arnold Hiras and Arthur Josias Simon Runtutambi, "Budaya & Masyarakat Digital Dalam Ketahanan Siber Di Indonesia: Sebuah Adaptasi Dari Pendekatan Capacity Maturity Model (CMM)," *Jurnal Manajemen Pendidikan Dan Ilmu Sosial* 5, no. 4 (2024): 922–38.

masih hanya sampai kepada batasan tanggung jawab keperdataan. Harus ada tindakan perbuatan melawan hukum baru dapat dikatakan bahwa penyelenggara sistem elektronik dapat dijatuhi sanksi hukuman baik itu ganti kerugian maupun sanksi lainnya dengan mekanisme pembuktian yang jelas dan terbuka.

Hukum *cyber* Indonesia melalui instrumen hukum produk undang-undang dan turunan aturan pelaksanaannya dibentuk atas dasar melindungi kepentingan masyarakat secara luas.<sup>41</sup> Dalam hukum *cyber* Indonesia, bahwa salah satu instrumen penting adalah menjaga keamanan data, sehingga keseriusan negara dalam hal tersebut juga tampak tertera jelas dalam pembentukan UU PDP. Secara tegas bahwa tanggung jawab akan kerahasiaan data pribadi yang wajib dikelola dan diproses secara andal merupakan kewajiban penyelenggara sistem elektronik. Adanya penerapan kewajiban sertifikat andal harus dimaknai sebagai bentuk kepedulian negara dalam melindungi kepentingan hukum masyarakat, sebab perlindungan hukum merupakan kewenangan negara melalui lembaga legislasi dengan membentuk dan merumuskan bagaimana idealitas instrumen hukumnya (peraturan perundang-undangan).<sup>42</sup> Pengaturan sertifikat keandalan privasi sebagai SNI tidak hanya berfungsi sebagai turunan teknis dari undang-undang, tetapi juga sebagai sarana untuk menyesuaikan ketentuan normatif dengan kebutuhan faktual yang terjadi dalam masyarakat.<sup>43</sup> Keberadaan sertifikat keandalan tidak hanya menjadi syarat administratif, tetapi juga menjadi bagian integral dari strategi keamanan yang komprehensif dalam pengelolaan data pribadi di era digital ini.<sup>44</sup>

Implementasi sertifikat keandalan privasi sebagai SNI menghadapi berbagai tantangan teknis dan regulasi yang perlu diatasi untuk memastikan perlindungan data pribadi yang optimal. Salah satu tantangan teknis utama adalah memastikan bahwa infrastruktur digital yang digunakan oleh penyedia layanan sudah memenuhi standar keamanan yang ketat. Hal ini mencakup perlindungan terhadap ancaman siber, seperti peretasan dan kebocoran data, serta penerapan sistem autentikasi yang kuat dan verifikasi untuk menghindari akses oleh pihak yang tidak berwenang. Selain itu, penyedia layanan yang mengelola data dalam jumlah besar juga harus memiliki sistem yang memadai untuk menjaga integritas dan kerahasiaan data pribadi, dengan memanfaatkan teknologi seperti enkripsi dan cloud computing.

Di sisi regulasi, tantangan utama adalah kesesuaian implementasi sertifikat ini dengan peraturan yang ada, seperti UU PDP. Untuk itu, pemerintah harus segera merumuskan

---

<sup>41</sup> Maichle Delpiero et al., "Analisis Yuridis Kebijakan Privasi Dan Pertanggungjawaban Online Marketplace Dalam Perlindungan Data Pribadi Pengguna Pada Kasus Kebocoran Data," *Padjadjaran Law Review* 9, no. 1 (2021): 1–22.

<sup>42</sup> Reza Andriansyah Putra and Atik Winanti, "Urgensi Dan Kendala Dalam Penerbitan Dokumen Sertifikat Tanah Elektronik Pasca Peraturan Menteri ATR/BPN Nomor 3 Tahun 2023," *Jurnal USM Law Review* 7, no. 2 (2024): 835, <https://doi.org/10.26623/julr.v7i2.9178>.

<sup>43</sup> Jefferson Hakim and Azeem Marhendra Amedi, "Prosecutorial Application of Restorative Justice: Overview, Mechanism, and Commentary on Prosecution Cessation," *Jurnal Hukum Dan Peradilan* 12, no. 2 (2023): 319, <https://doi.org/10.25216/jhp.12.2.2023.319-346>.

<sup>44</sup> Muhammad Raihan, "Perlindungan Data Diri Konsumen Dan Tanggungjawab Marketplace Terhadap Data Diri Konsumen (Studi Kasus: Kebocoran Data 91 Juta Akun Tokopedia)," *Jurnal Inovasi Penelitian* 3, no. 10 (2023): 7849–50.

peraturan turunan yang jelas agar SNI ini dapat diimplementasikan dengan efektif. Selain itu, masih terdapat kekosongan dalam penegakan hukum terkait pelanggaran terhadap perlindungan data pribadi, khususnya yang melibatkan instansi pemerintah, yang dapat menyebabkan ketidakseimbangan dalam penegakan hukum. Koordinasi yang baik antar lembaga pemerintah, seperti Kementerian Komunikasi dan Informatika (Kominfo) dan Badan Standardisasi Nasional (BSN), juga diperlukan agar standar privasi ini dapat dijalankan dengan baik.<sup>45</sup>

Mekanisme audit dan pengawasan sertifikasi keandalan privasi pun harus diperjelas. Audit ini dapat dilakukan oleh lembaga independen yang ditunjuk oleh pemerintah, seperti BSN atau lembaga eksternal yang memiliki kompetensi di bidang perlindungan data. Proses audit yang berkelanjutan juga penting agar penyedia layanan tetap mematuhi standar yang telah ditetapkan dalam jangka panjang. Selain itu, akuntabilitas penyedia layanan yang gagal memenuhi standar harus ditegakkan melalui sanksi yang sesuai, baik dalam bentuk denda atau pencabutan sertifikat. Mekanisme sertifikasi yang efektif juga harus mencakup sistem penghargaan bagi penyedia layanan yang berhasil memperoleh sertifikat keandalan privasi, sekaligus memberikan efek jera bagi yang melanggar. Semua tantangan ini memerlukan perhatian serius untuk mewujudkan perlindungan data pribadi yang maksimal melalui sertifikat keandalan privasi sebagai SNI.

#### **4. PENUTUP**

Meskipun kebocoran data terus meningkat dan menimbulkan dampak signifikan terhadap individu maupun bisnis, sertifikat keandalan privasi belum menjadi persyaratan wajib bagi penyelenggara sistem elektronik non-strategis. Hal ini berbeda dengan praktik di beberapa negara maju yang telah mewajibkan sertifikasi serupa guna memperkuat keamanan siber. Percepatan adopsi sertifikat keandalan privasi sebagai SNI menjadi langkah strategis dalam meningkatkan perlindungan data pribadi dan kepastian hukum bagi penyelenggara sistem elektronik. Kebaruan penelitian ini terletak pada analisis mendalam mengenai kedudukan hukum sertifikat keandalan privasi dalam sistem hukum Indonesia serta kewajiban penyelenggara sistem elektronik dalam menerapkannya. Tidak banyak penelitian sebelumnya yang secara spesifik membahas hubungan antara regulasi perlindungan data pribadi dengan sertifikat keandalan sebagai instrumen hukum yang dapat mengurangi risiko kebocoran data. Studi ini juga menawarkan perspektif baru dengan mengusulkan agar sertifikat keandalan privasi diakui sebagai SNI dan menjadi persyaratan wajib bagi seluruh penyelenggara sistem elektronik, baik strategis maupun non-strategis. Pemerintah perlu segera mengeluarkan regulasi teknis yang mengatur kewajiban sertifikasi bagi seluruh penyelenggara sistem elektronik untuk meningkatkan keamanan data pribadi di Indonesia. Selain itu, investasi dalam infrastruktur keamanan, peningkatan kesadaran akan pentingnya sertifikasi, serta penguatan mekanisme audit dan pengawasan menjadi faktor penting dalam memastikan implementasi sertifikat keandalan privasi yang efektif.

---

<sup>45</sup> Muhammad Firman and Al Ghani, "Urgensi Pengaturan Perlindungan Data Pribadi" 3 (2022): 38–58.

## DAFTAR PUSTAKA

- Abadi, Totok Wahyu, Mochammad Arifin, Ahmad Riyadh, Umar Balar, and Ilmi Usrotin Choiriyah. *Buku Ajar Governance Digital Berbasis Riset Anggota IKAPI Nomor : 218 / Anggota Luar Biasa / JTI / 2019 Diterbitkan Oleh Jl . Mojopahit 666 B Sidoarjo ISBN : 978-623-464-102-8 Copyright © 2024 Authors All Rights Reserved, 2024.*
- Achmad Rizal Maulana, dkk. “Perlindungan Konsumen Terhadap Kebocoran Data Pada Marketplace Ditinjau Dari Perundang-Undangan Di Indonesia.” *Kultura Jurnal Ilmu Sosial Dan Humaniora* 2 (2024): 297–308.
- Amirulloh, Muhamad, and Vidya Noor Rachmadini. “Legal Certainty in the Use of Certification of Trustworthiness by Indonesian E-Commerce Business.” *Central European Journal of International and Security Studies* 12, no. 4 (2018): 565–75.
- Anggara, Apryan, and Muhammad Ruhly Kesuma Dinata. “Hacker Bjorka: Pihak Yang Berperan Dalam Mencegah Kebocoran Data.” *Jurnal Hukum Magnum Opus* 6, no. 1 (2023): 14–26. <https://doi.org/10.30996/jhmo.v6i1.8293>.
- Anggen Suari, Kadek Rima, and I Made Sarjana. “Menjaga Privasi Di Era Digital: Perlindungan Data Pribadi Di Indonesia.” *Jurnal Analisis Hukum* 6, no. 1 (2023): 132–42. <https://doi.org/10.38043/jah.v6i1.4484>.
- Anggraeni, Rinastiti Dwi, Fadilla Putri Alsabilla, and Jeferson Kameo. “Pelindungan Data Pribadi Anak Yang Berhadapan Dengan Hukum Di Dunia Siber Personal Data Protection of Children in Conflict with the Law in Cyberspace” 7, no. 3 (2024): 2–12.
- Anhar, Muhammad Ali, and Teguh Agung Pratama. “Analisis Implementasi Keamanan Data Melalui Teknologi Blockchain.” *Program Studi Ilmu Komunikasi* 4, no. 2 (2023): 20353.
- Bahram, Muhammad. “Transformasi Masyarakat Di Era Digital: Menjaga Kaidah Hukum Sebagai Landasan Utama.” *Sentri: Jurnal Riset Ilmiah* 2, no. 5 (2023): 1733–46. <https://doi.org/10.55681/sentri.v2i5.884>.
- Briliany, Anisa Isti, and Anajeng Esri Edhi Mahanani. “Tinjauan Yuridis Perbuatan Melanggar Hukum ( PMH ).” *Jurnal Yustika: Media Hukum Dan Keadilan* 24, no. 02 (2021): 63–75.
- Delpiero, Maichle, Farah Azzahra Reynaldi, Istiwati Utami Ningdiah, and Nafisah Muthmainnah. “Analisis Yuridis Kebijakan Privasi Dan Pertanggungjawaban Online Marketplace Dalam Perlindungan Data Pribadi Pengguna Pada Kasus Kebocoran Data.” *Padjadjaran Law Review* 9, no. 1 (2021): 1–22.
- Denisa, Adinda Putri, Muhamad Amirulloh, and Helitha Novianty Muchtar. “Sertifikat Keandalan Privasi Sebagai Salah Satu Bentuk Perlindungan Konsumen Di Bidang Informasi Dan Transaksi Elektronik.” *Jurnal Rechtsvinding Media Pembinaan Hukum Nasional* 12, no. 2 (2023): 167–84.
- Fauzianti, Nizda Azzima, and Muhamad Amirulloh. “Fungsi Sertifikat Keandalan Registrasi Bagi Donation Based Crowdfunding Berdasarkan Hukum Cyber Di Indonesia.” *Comserva: Jurnal Penelitian Dan Pengabdian Masyarakat* 3, no. 5 (2023): 1736–47. <https://doi.org/10.59141/comserva.v3i5.969>.
- Fikri, Muhammad, and Shelvi Rusdiana. “Ruang Lingkup Perlindungan Data Pribadi: Kajian Hukum Positif Indonesia.” *Ganesha Law Review* 5, no. 1 (2023): 45–46.
- Firman, Muhammad, and Al Ghani. “Urgensi Pengaturan Perlindungan Data Pribadi” 3

- (2022): 38–58.
- Hakim, Jefferson, and Azeem Marhendra Amedi. “Prosecutorial Application of Restorative Justice: Overview, Mechanism, and Commentary on Prosecution Cessation.” *Jurnal Hukum Dan Peradilan* 12, no. 2 (2023): 319. <https://doi.org/10.25216/jhp.12.2.2023.319-346>.
- Hanif, Charles Amirul, Muhamad Amirulloh, and Helitha Novianty Muchtar. “Reliability and Security in the Implementation of Digital Health Service Application with the Application of ‘Reliability Certification or Electronic Certification’ Based on Indonesian Law.” *Padjadjaran Jurnal Ilmu Hukum* 8, no. 3 (2021): 417–38. <https://doi.org/10.22304/pjih.v8n3.a6>.
- Hapid, Fasa Muhamad, Ija Suntana, and Muhammad Yayan Royani. “Penerapan Asas Geen Straf Zonder Schuld Dalam Penindakan Terhadap Kejahatan Penyalahgunaan Teknologi Deepfake Application of the Geen Straf Zonder Schuld Principle in Taking Action Against Crimes of Misuse of Deepfake Technology” 7, no. 3 (2024): 4–7.
- Herera, Dinda Aprilita, and Muhamad Hasan Sebyar. “Perlindungan Hukum Terhadap Serangan Siber: Tinjauan Atas Kebijakan Dan Regulasi Terbaru.” *Jurnal Hukum Dan Kewarganegaraan* 1, no. 5 (2023): 1–16.
- Hidayat, Arif, and Zaenal Arifin. “Politik Hukum Legislasi Sebagai Socio-Equilibrium Di Indonesia.” *Jurnal Ius Constituendum* 4, no. 2 (2019): 147–59. <https://doi.org/10.26623/jic.v4i2.1654>.
- Inayah, Justin Nurul, and Taufiq Nugroho. “Criminal Implementation of Cyberbullying Based on Electronic Information and Transaction Law and Islamic Law.” *Jurnal Usm Law Review* 7, no. 1 (2024): 252. <https://doi.org/10.26623/julr.v7i1.8665>.
- Kurniasandi, Domi Dwi, Sherly Nanda Aprilia, Nobella Indradjaja, Fakultas Hukum, Universitas Wijaya, Putra Surabaya, Kampus Prigen, et al. “Regulasi Terkait Perlindungan Data Pribadi Dalam Penggunaan Jasa E-Commerce” 21, no. 1 (2022): 103–14.
- Lutfi, Melinda Putri. “Urgensi Perlindungan Hukum Terhadap Data Privasi Nasabah Bank Di Era Perkembangan Digital” 1, no. 5 (2024): 210–18.
- Maharani, Rista, and Andria Luhur Prakoso. “Perlindungan Data Pribadi Konsumen Oleh Penyelenggara Sistem Elektronik Dalam Transaksi Digital.” *Jurnal USM Law Review* 7, no. 1 (2024): 333. <https://doi.org/10.26623/julr.v7i1.8705>.
- Megahayati, Kemala, Muhamad Amirulloh, and Helitha Novianty Muchtar. “Perlindungan Hukum Sinematografi Terhadap Pengaksesan Tanpa Hak Oleh Pengguna Aplikasi Telegram Berdasarkan Undang-Undang Hak Cipta Dan Undang-Undang Informasi Dan Transaksi Elektronik Di Indonesia.” *Ajudikasi : Jurnal Ilmu Hukum* 5, no. 1 (2021): 1–16. <https://doi.org/10.30656/ajudikasi.v5i1.3218>.
- Muhammad, Anggi, Chandraca Hutagalung, Nadia Rhaesa Marendra, and Asmak Ul. “Perlindungan Terhadap Konsumen Dalam Kasus Kebocoran Data Bank Syariah Indonesia.” *Jurnal Ilmu Hukum, Sosial, Dan Humaniora* 2, no. 1 (2024): 156–65.
- Natha., Kadek Dio Ramadi, I Nyoman Putu Budiarta., and Ni Gusti Ketut Sri Astiti. “Perlindungan Hukum Atas Kebocoran Data Pribadi Konsumen Pada E-Commerce.” *Heylaw.Edu* 3, no. 1 (2022): 143–48.
- Oktaviani, Shella, Yeremia Juan Dewata, and Aryo Fadlian. “Pertanggung Jawaban Pidana Kebocoran Data Bpjs Dalam Perspektif Uu Ite.” *De Juncto Delicti: Journal of Law* 1, no. 2 (2021): 146–57. <https://doi.org/10.35706/djd.v1i2.5732>.

- Pebiyanti, Elsa, Achmad Fauzi, Tsamara Husniyyah, Sarah Intan Tasia, Zhakila Sutendi, and Anisa Elsa Vitri. "Pengaruh Kualitas Informasi, Persepsi Keamanan, Dan Persepsi Privasi Terhadap Kepercayaan Pengguna Belanja Online (Literature Review)." *Jurnal Ekonomi Manajemen Sistem Informasi* 4, no. 5 (2023): 850–58. <https://doi.org/10.31933/jemsi.v4i5.1548>.
- Penelitian, Jurnal, and Jenda Ingan Mahuli. "All Fields of Science J-LAS Perlindungan Hukum Terhadap Data Pribadi Dalam Era Digital Legal Protection of Personal Data in the Digital Era." *AFoSJ-LAS* 3, no. 4 (2023): 188–94.
- Purba, R. E., D. Maharani, M. A. A. BMY, and R. Z. Al Zahra. "Peranan Hukum Positif Dalam Mengatur Cyberspace Untuk Menghadapi Tantangan Dan Peluang Di Era Digital." *Mandub: Jurnal Politik, Sosial, Hukum Dan Humaniora* 2, no. 2 (2024): 167–76.
- Putra, Reza Andriansyah, and Atik Winanti. "Urgensi Dan Kendala Dalam Penerbitan Dokumen Sertifikat Tanah Elektronik Pasca Peraturan Menteri ATR/BPN Nomor 3 Tahun 2023." *Jurnal USM Law Review* 7, no. 2 (2024): 835. <https://doi.org/10.26623/julr.v7i2.9178>.
- Ragani, Sondika, Adrian Rompis, and Muhamad Amirullah. "Implementation of Legal Certainty Principle and Economic Analysis of Law Regarding Online Services of Demographic Administration in Bandar Lampung in Implementing an Electronic Based Government System." *Cepalo* 7, no. 2 (2023): 117–28. <https://doi.org/10.25041/cepalo.v7no2.2975>.
- Raihan, Muhammad. "Perlindungan Data Diri Konsumen Dan Tanggungjawab Marketplace Terhadap Data Diri Konsumen (Studi Kasus: Kebocoran Data 91 Juta Akun Tokopedia)." *Jurnal Inovasi Penelitian* 3, no. 10 (2023): 7849–50.
- Ramadhanty, Syarafina, Naila Amatullah, Niki Anane Setyadani, and Tasya Safiranita Ramli. "Doktrin Safe Harbor: Upaya Perlindungan Hak Cipta Konten Dalam Platform User Generated Content." *Legalitas: Jurnal Hukum* 12, no. 2 (2020): 267. <https://doi.org/10.33087/legalitas.v12i2.226>.
- Sari, Ni Putu Riyani Kartika. "Aktual Justice." *Jurnal Aktual Justice* 6, no. 2 (2021): 211–29.
- Septiriani, Vita, Tito Sofyan, Widiya N Rosari, Tanggung Jawab, Pelaku Usaha, Terhadap Kebocoran, Informasi Data, Pribadi Konsumen, Dalam Pelaksanaan, and Perdagangan Elektronik. "Tanggung Jawab Pelaku Usaha Terhadap Kebocoran Informasi Data Pribadi Konsumen Dalam Pelaksanaan Perdagangan Elektronik (E-Commerce)." *Jurnal Ilmiah Kutei* 23, no. 1 (2024): 127–36.
- Simorangkir, Arnold Hiras, and Arthur Josias Simon Runtutambi. "Budaya & Masyarakat Digital Dalam Ketahanan Siber Di Indonesia: Sebuah Adaptasi Dari Pendekatan Capacity Maturity Model (CMM)." *Jurnal Manajemen Pendidikan Dan Ilmu Sosial* 5, no. 4 (2024): 922–38.
- Sukadi, Imam, Musleh Harry, and Teguh Setyobudi. "Legal Politics Electronic Land Certificate in Indonesia" 7, no. 53 (2024): 23–34.
- Suryati, Suryati, Layang Sardana, Ramanata Disurya, and Yanuar Syam Putra. "Penguatan Literasi Digital Dalam Pencegahan Pelanggaran Hukum Siber (Cyber Law)." *Wajah Hukum* 8, no. 1 (2024): 84. <https://doi.org/10.33087/wjh.v8i1.1447>.
- Suryawijaya, Tito Wira Eka. "Memperkuat Keamanan Data Melalui Teknologi Blockchain: Mengeksplorasi Implementasi Sukses Dalam Transformasi Digital Di Indonesia."

- Jurnal Studi Kebijakan Publik* 2, no. 1 (2023): 55–68.  
<https://doi.org/10.21787/jskp.2.2023.55-68>.
- Unggul, Satria, and Wicaksana Prakasa. “Doktrina Legal Protection of Personal Data and Responsibility of Authorities For” 7, no. 27 (2024): 178–201.
- Vanessa, Victoria, and Aji Lukman Ibrahim. “Clickbait as a Potential Threat in the Development of Cybercrime in Indonesia.” *Jurnal USM Law Review* 7, no. 1 (2023): 1. <https://doi.org/10.26623/julr.v7i1.8024>.
- Yudhi Priyo Amboro, Florianus, and Viona Puspita. “Perlindungan Hukum Atas Data Pribadi (Studi Perbandingan Hukum Indonesia Dan Norwegia).” *Combines-Conference on Management, Business, Innovation, Education and Social Sciences* 1, no. 1 (2021): 415–27.