KAJIAN HUKUM DALAM PERLINDUNGAN DATA PEMILIK TANAH PADA SERTIFIKAT ELEKTRONIK [1]

Oleh :
Amirah Jusuf [2]
Donna Okhtalia Setiabudh [3]
Revy Samuel Maynard Korah [4]

ABSTRAK

Penelitian ini bertujuan untuk mengetahui sejauh mana jaminan perlindungan data yang diberikan kepada pemilik sertifikat elektronik dan untuk mengidentifikasi hambatan hukum yang dihadapi dalam perlindungan data pribadi pemilik tanah pada sertifikat elektronik. Dengan menggunakan metode penelitian normatif, dapat ditarik kesimpulan yaitu : 1. Jaminan perlindungan data dalam sertifikat elektronik memberikan keutuhan data yang mana pemegang hak atas tanah akan selalu utuh, tidak berubah, dan untuk kerahasiannya telah dilindungi dengan menggunakan teknologi persandian dari Badan Siber dan Sandi Nasional (BSSN). Informasi dilindungi dengan kode-kode rumit dan hanya dapat dilihat oleh pihak-pihak tertentu saja, penerapan tanda tangan digital menjamin otentikasi data agar tidak terjadi pemalsuan tanda tangan. 2. Pada praktiknya masih terdapat hambatan yang dihadapi, serangan siber adalah ancaman yang memiliki risiko yang besar. Semakin canggih teknologi maka akan diikuti dengan riisiko yang besar juga, serangan berupa *malware* merupakan risiko yang sering dihadapi. Selain itu, belum terdapat lembaga perlindungan data yang diamanatkan oleh UndangUndang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi Pasal 58. Kuramgnya kesadaran masyarakat juga menjadi faktor penghambat karena kurangnya kewaspadaan dan kurangnya pemahaman mengenai isu-isu penyerangan data pribadi melalui pesan-pesan yang berisi *link phising.*

Kata Kunci : *perlindungan data pribadi, sertifikat elektronik*

PENDAHULUAN

A. Latar Belakang

Tanah adalah salah satu sumber daya alam yang menunjang kehidupan manusia di muka bumi, tanah menjadi kekayaan alam yang tak hanya menjadi tempat tinggal saja akan tetapi dimanfaatkan sebagai penunjang sektor ekonomi, perdagangan, pariwisata dan masih banyak hal-hal yang dapat dipergunakan untuk keberlangsungan hidup manusia. Tanah tak serta merta dipergunakan begitu saja akan tetapi terdapat pengelolaan yang dilakukan agar memastikan pemanfaatan tanah berlaku adil, pengelolaan tanah diatur agar tidak terjadinya sengketa yang dapat merugikan berbagai pihak yang ingin memanfaatkan tanah. Undang-Undang Nomor 5 Tahun 1960 tentang Peraturan Dasar PokokPokok Agraria menjadi landasan hukum mengenai pertanahan, UUPA mengatur mengenai hak-hak atas tanah baik yang bersifat tetap dan sementara. Hak-hak tersebut tertuang dalam Pasal 16 dan Pasal 53 UUPA memuat jenis-jenis hak atas tanah yang di dalamnya membagi tanah yang bersifat primer dan tanah yang bersifat sekunder. Tanah juga harus melakukan pendaftaran yang mana tujuan pendaftaran tanah terdapat dalam Pasal 19 UUPA yaitu untuk memberikan kepastian hukum dan perlindungan hukum kepada pemilik tanah agar terhindar dari sengketa yang timbul akibat tidak melakukan pendaftaran tanah.

Pendaftaran tanah adalah rangkaian kegiatan yang dilakukan oleh Pemerintah terus menerus berkesinambungan dan teratur meliputi pengumpulan, pengolahan pembukuan dan penyajian serta pemeliharaan data fisik dan data yuridis, dalam bentuk peta dan daftar, mengenai bidang-bidang tanah dan satuan rumah susun, termasuk pemberian sertipikat sebagai surat tanda bukti haknya bagi bidang-bidang tanah yang sudah ada haknya dan Hak Milik atas Satuan Rumah susun serta hak-hak tertentu yang membebaninya.[5] Pendaftaran Tanah dapat dilakukan dengan 2 (dua) cara, yaitu pendaftaran tanah secara sistematik dan pendaftaran tanah secara sporadik. Pendaftaran tanah secara sistematik adalah kegiatan pendaftaran tanah untuk pertama kali yang dilakukan secara serentak yang meliputi obyek pendaftaran tanah yang belum didaftar dalam wilayah atau bagian wilayah suatu desa/kelurahan, sedangkan Pendaftaran tanah secara sporadik adalah kegiatan pendaftaran tanah untuk pertama kali mengenai satu atau beberapa obyek pendaftaran tanah dalam wilayah atau bagian wilayah suatu desa/kelurahan secara individual atau massal. Pendaftaran tanah secara sporadik dilaksanakan atas permintaan pihak yang berkaitan.

Teknologi informasi memberikan dampak yang signifikan terhadap berbagai sektor kehidupan manusia, dampak digitalisasi

---

[1] Artikel Skripsi
[2] Mahasiswa Fakultas Hukum Unsrat, NIM 210711010005
[3] Fakultas Hukum Unsrat, Doktor Ilmu Hukum
[4] Fakultas Hukum Unsrat, Magister Ilmu Hukum

[5] FX. Sumarja, Hukum Pendaftaran Tanah (Bandar Lampung; Universitas Lampung, 2010), hlm 40

memberikan peluang baru dan tercipta inovasi-inovasi terbaru agar dapat meningkatkan efisiensi, transparansi, serta kemudahan akses dalam berbagai bidang ternasuk bidang hukum. Hukum bersifat dinamis maka dari itu hukum harus beradaptasi dengan perubahan sosial, ekonomi, dan teknologi agar tetap relevan mengenai isu-isu baru yang terus bermunculan akibat dampak dari digitalisasi. Salah satu dampak digitalisasi di bidang hukum adalah Sertifikat Elektronik atau disebut sertifikat-*el* yang merupakan salah satu dampak kemajuan teknologi yang membawa perubahan dalam sektor hukum, sistem ini menawarkan kemudahan administrasi dalam bidang pertanahan.

Peraturan Pemerintah (PP) Nomor 18 Tahun 2021 tentang Hak Pengelolaan, Hak Atas Tanah, Satuan Rumah Susun dan Pendaftaran Tanah dalam Pasal 84 ayat (1) memuat mengenai penyelenggaraan dan pelaksanaan pendaftaran tanah dapat dilakukan secara elektronik. Sertifikat elektronik memberikan efisiensi administrasi berupa mengurangi waktu dan biaya untuk proses dan penerbitan sertifikat tanah. Data pendaftaran tanah yang dilakukan secara elektronik dimuat dalam Peraturan Pemerintah (PP) No. 18 Tahun 2021 Pasal 85 ayat (1) : Seluruh data dan/atau dokumen dalam rangka kegiatan Pendaftaran Tanah secara bertahap disimpan dan disajikan dalam bentuk dokumen elektronik dengan memanfaatkan teknologi informasi dan komunikasi.

Berdasarkan simulasi yang telah dilakukan oleh Kementerian ATR/BPN pada dasarnya tidak ditemukan potensi hambatan untuk pemberlakuan aturan ini, sehingga yang menjadi fokus utama Kementerian adalah percepatan proses validasi dan upload pada aplikasi KKP (Komputerisasi Kantor Pertanahan). Terkait dengan masyarakat yang telah memiliki sertifikat tanah analog (sertifikat tanah yang digunakan saat ini) yang akan merubah sertifikatnya menjadi sertipikat-el sama sekali tidak dibebankan biaya karena perubahan tersebut ditanggung oleh Negara, dimana proses penggantian tersebut dilakukan secara bertahap berdasarkan permohonan pemeliharaan data oleh pemohon.[6]

Implementasi sertifikat elektronik ini diatur dalam Peraturan Menteri ATR/BPN Nomor 3 Tahun 2023 Tentang Penerbitan Dokumen Elektronik Dalam Kegiatan Pendaftaran Tanah, digitalisasi layanan pertanahan memberikan kemudahan terhadap masyarakat dalam mengakses hak atas tanah mereka, kemudahan yang diberikan kepada masyarakat dalam pengurusan sertifikat tanah elektronik lebih cepat dibandingkan dalam pengelolaan sertifikat tanah fisik konvensional. Dalam Peraturan Menteri ATR/BPN Nomor 3 Tahun 2023 Pasal 7 memuat bahwa kegiatan pendaftaran tanah pertama kali dapat diajukan melalui sistem elektronik atau loket pertanahan, sedangkan untuk yang telah memiliki sertifikat tanah analog dan ingin beralih ke sertifikat elektronik dapat dilakukan pemohonan untuk alih media.

Sertifikat elektronik merupakan sertifikat yang telah diterbitkan melalui sistem elektronik berupa dokumen digital yang menyimpan data fisik dan yuridis dalam Buku Tanah Elektronik (BT-el), buku tanah elektronik adalah buku yang telah disahkan dengan menggunakan tanda tangan elektronik menjadi blok data, blok data sendiri adalah kumpulan data alfanumerik yang disusun dalam format standar untuk menggambarkan satu kesatuan antara data yuridis dan data fisik tanah.[7]

Buku Tanah Elektronik berupa format digital yang menyimpan informasi pemilik, batas-batas tanah, jenis hak dan hak atas tanah. Keberadaan Peraturan Menteri tersebut menjadi polemik, masyarakat dibuat gelisah resah, karena belum lama masyarakat telah menerima jutaan sertipikat tanah (analog) melalui program Pendaftaran Tanah Sistematis Lengkap (PTSL), tibatiba masyarakat diminta untuk menukar dengan yang sertipikat-el. Seolaholah kebijakan yang dibuat pemerintah kontradiktif, tidak direncanakan dengan baik dan sistematis.[8]

Selain masyarakat yang gelisah dengan Peraturan Menteri tedapat sebuah tantangan hukum yang harus dihadapi dalam sertifikat elektronik yaitu berhubungan dengan data pribadi pemegang sertifikat elektronik, munculnya kekhawatiran dari masyarakat mengenai perlindungan data atas sertifikat elektronik. Aspek pengamanan pada sistem sertifikat elektronik diperlukan dengan mengambil langkah-langkah preventif serta regulasi yang jelas, dalam Peraturan Menteri ATR/BPN No. 3 Tahun 2023 juga mencakup mengenai keamanan data dan

[6] Nur Hidayani Alimuddin, "Implementasi Sertifikat Elektronik Sebagai Jaminan Kepastian Hukum Kepemilikan Hak Atas Tanah di Indonesia," *SASI* 27, no. 3 (7 Oktober 2021): 335, hlm 5. https://doi.org/10.47268/sasi.v27i3.509.

[7] Sapardiyono Sapardiyono dan Sukmo Pinuji, "Konsistensi Perlindungan Hukum Kepemilikan dan Hak Atas Tanah melalui Sertipikat Tanah Elektronik," *Widya Bhumi* 2, no. 1 (4 Juni 2022): 54–64, hlm 3. https://doi.org/10.31292/wb.v2i1.19.

[8] Dian Aries Mujiburohman dan Sekolah Tinggi Pertanahan Nasional Jalan Tata Bumi No, "BHUMI: Jurnal Agraria dan Pertanahan TRANSFORMASI DARI KERTAS KE ELEKTRONIK: TELAAH YURIDIS DAN TEKNIS SERTIPIKAT TANAH ELEKTRONIK" 7, no. 1 (t.t.): 57–67, hlm 4.

memastikan keamanan data pemilik tanah, meskipun begitu masih ada resiko penyalahgunaan dan kebocoran data masih dapat terjadi walaupun kerahasiaan data tersebut telah dijamin oleh undang-undang.

Perlindungan data pribadi merupakan bagian dari Hak Asasi Manusia yang tertuang dalam Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 dalam Pasal 28G ayat (1) : Bahwa setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang berada dibawah kekuasaannya.[9] Pasal tersebut memberikan hak merasa aman kepada warga negara, adanya jaminan dan berkekuatan hukum untuk mengontrol informasi yang berkaitan dengan data pribadi.

Kasus kebocoran data pribadi di Indonesia masih sering terjadi dan menjadi isu yang serius yang menarik perhatian publik belakangan sehingga memberikan kecemasan publik akan pengamanan data, kasus kebocoran data ini menyorot kerentanan dari sistem keamanan yang menjadi risiko penyalahgunaan oleh pihak yang tidak bertanggung jawab. Salah satu kasus kebocoran data yang menyorot perhatian publik adalah kebocoran data yang terjadi di Pusat Data Nasional Sementara (PNDS) yang terjadi pada Juni 2024 lalu, serangan siber berbentuk *ransomware* dengan nama *brain cipher ransomware.* Awal serangan ini diketahui setelah tim dari pemerintah dan pengelola melakukan investigasi karen terdapat gangguan pada layanan imigrasi di bandara pada 20 Juni 2024. Diketahui bahwa insiden ini mengunci 282 kementerian/lembaga serta meminta sebuah tebusan senilai Rp131 Miliar rupiah, ditemukan aktivitas membahayakan melakukan instalansi file yang berbahaya, menghapus file sistem penting serta menonaktifkan layanan yang sedang berjalan. *Ransomware* yang digunakan adalah tipe *Lockbit* 3.0. *Ransomware* adalah jenis *malware* yanng dikirim peretas untuk mengunci dan mengenkripsi perangkat komputer milik korban. Dampak dari serangan tersebut mulai dari saat pelayanan imigrasi di sejumlah bandara Indonesia mengalami gangguan yang menyebabkan layanan imigrasi dilakukan secara manual dan mengakibatkan antrean panjang, Kasus kebocoran data PNDS ini diselesaikan setelah enam hari pasca-serangan yang mana baru bisa memulihkan 5 dari 44 dari data layanan yang terkena dampak.[10] Pihak kominfo (pada saat itu masih bernama kominfo) mengonfirmasi lima layanan pulih terdiri dari layanan keimigrasian Kemenkumham, layanan perizinan Kementerian Koordinator Bidang Kemaritiman dan Investasi Republik Indonesia (Kemenkomarves), layanan SIKap dari Lembaga Kebijakan Pengadaann Barang/Jasa Pemerintah (LKPP), layanan Si Halal milik Kementerian Agama (Kemenag), dan ASN Digital Pemerintah Daerah Kediri.

Resiko kebocoran data dan penyalahgunaan data informasi perlu diperhatikan mengingat kasus kebocoran data merupakan ancaman yang serius yang dapat merugikan banyak pihak, Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik menyatakan bahwa perlindungan data pribadi adalah kewajiban yang harus dipenuhi oleh penyelenggara sertifikat elektronik. Beberapa waktu lalu Menteri Komunikasi dan Digital Meutya Hafid menyebut peringkat keamanan siber Indonesia terus meningkat dari tahun ke tahun. Saat ini Indonesia disebut berada di jajaran atas bersama negara-negara seperti Amerika Serikat (AS) dan Jepang.[11] Pernyataan tersebut membawa peluang baru dalam aspek pengamanan akan tetapi pemerinah tidak boleh lengah dan terus meningkatkan pengamanan terutama dalam pemberlakuan sertifikat elektronik.

Penerapan sertifikat elektronik merupakan langkah maju dalam perkembangan digitalisasi akan tetapi tantangan yang harus dihadapi semakin besar, pentingnya memberikan kepastian hukum dalam perlindungan data pada pemilik tanah pada sertifikat elektronik menjadi hal yang mendesak maka dibutuhkan regulasi yang kuat, implementasi yang efektif, pengawasan yang tepat dan audit sistem untuk mengevaluasi kesesuaian dengan undang-undang diikuti dengan kepatuhan terhadap perlindungan data pemilik tanah dalam sertifikat elektronik. Mekanisme pengawasan yang tepat dapat meningkatkan kepercayaan masayarakat terhadap sistem digitalisasi pertanahan.

Penelitian ini dilakukan untuk mengetahui sejauh mana regulasi yang ada mampu menjamin kepastian hukum dan perlindungan data pemilik tanah pada sertifikat elektronik serta untuk mengidentifikasi kendala dalam perlindungan data pemilik tanah pada sertifikat elektronik.

---

[9] Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, pasal 28G ayat (1)

[10] Zakia Machfir, https://goodstats.id/article/300-juta-data-pribadi-tersebar-pusat-data-nasional-sementara-pdns-dibobol-kapan-indonesia-merdeka-dari-serangan-siber-5Adzr

[11] https://www.cnnindonesia.com/teknologi/20250206153253-192-1195388/menkomdigi-peringkat-keamanan-siber-ri-naik-sejajar-as-hingga-jepang (Diakses 20 Februari 2025)

B. Rumusan Masalah

1. Bagaimana jaminan perlindungan data pemilik tanah pada sertifikat elektronik?
2. Bagaimana tantangan yang menghambat dalam upaya perlindungan data pemilik tanah pada sertifikat elektronik?

C. Metode Penelitian

Metode Penelitian yang digunakan adalah metode Yuridis Nomatif.

PEMBAHASAN

A. Jaminan Perlindungan Data Pemilik Tanah Pada Sertifikat Elektronik

Kemajuan tekonologi membuat pemerintah berupaya untuk menerapkan kerangka hukum mengenai perlindungan data, kasus-kasus kebocoran data yang terus bermunnculan memberikan dampak yang sangat besar berupa dampak psikologis berupa kecemasan di kalangan individu mengenai data pribadi mereka. Data Pribadi merupakan merupakan bagian dari hak privasi yang telah diakui secara internasional, perlindungan terhadap data pribadi dilakukan agar terhindar dari penyalahgunaan informasi yang dapat merugikan individu atau kelompok seperti risiko pencurian identitas berupa informasi informasi keuangan dan data-data penting yang menyebabkan kerugian finansial. Data pribadi yang tidak terlindungi dapat menjadi target yang bertujuan untuk melakukan penipuan, pemalsuan, atau serangan lainnya. Selain itu perlindungan data dapat meningkatkan kepercayaan masyarakat terhadap pemerintah maupun layanan diigital dan merupakan respon dari kepatuhan hukum dan tanggung jawab sosial.

Pemberlakuan Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi memberikan jaminan hukum mengenai perlindungan data pribadi terutama setelah penerbitan Peraturan Menteri ATR/BPN Nomor 1 Tahun 2021 Tentang Sertifikat Elektronik yang telah di perbarui dengan Peraturan Menteri ATR.BPN Nomor 3 Tahun 2023 Tentang

Penerbitan Dokumen Elektronik dan Pendaftaran Tanah yang merupakan bentuk modernisasi pertanahan dan memberikan banyak keuntungan. Sistem digital ini dirancang untuk mencatat perubahan status kepemilikan tanah dan hak-hak lainnya secara instan dan *real-time*, sehingga mempercepat proses administrasi yang biasanya memakan waktu. Manfaat lain dari sertifikat elektronik adalah meningkatkan efisiensi pelayanan publik. Pemilik properti, notaris, dan pihak lain yang terlibat dalam transaksi real estat dapat dengan cepat mengakses sertifikat elektronik tanpa harus mengunjungi Kantor Pendaftaran Tanah secara fisik. Anda dapat menyelesaikan prosedur seperti jual beli tanah, pemberian hipotek, dan konfirmasi kepemilikan secara online.[12]

Implementasi UU PDP terutama dalam bidang digitalisasi pertanahan sertifikat elektronik merupakan hal yang penting mengingat sertifikat elektronik menyimpan data-data sensitif yang menyangkut data pribadi, UU PDP berperan penting untuk melindungi data tersebut diikuti dengan Kementerian ATR/BPN untuk memastikan pengelolaaan data aman dan terjamin keamanannya sesuai dengan apa yang telah ditentukan dengan UU PDP. Kehadiran UU PDP mengatur larangan penggunaan data pribadi secara *illegal* dengan ditetapkan sanksi tegas bagi pelanggaran serta hak-hak yang kuat yang diberikan kepada individu pemilik data pribadi. Hak subjek data pribadi terdapat dalam pasal 5 Undang-Undang Perlindungan Data Pribadi yang dapat dihubungkan dengan sertifikat elektronik, yaiitu:

1) Hak untuk Mendapatkan Informasi : Pemilik tanah berhak
   mendapatkan informasi tentang kejelasan identitas, dasar kepentingan hukum, tujuan permintaan dan penggunaan data pribadi, serta akuntabilitas pihak yang meminta data.
2) Hak untuk Mengakses dan Memperbaiki Data : Pemilik tanah sertifikat elektronik berhak mengakses dan meminta perbaikan atau pembaruan data pribadi ereka jika terdapat ketidakakuratan.
3) Hak untuk Menarik Kembali Persetujuan : Pemilik tanah sertifikat elektronik memiliki hak untuk menarik kembali persetujuan pemrosesan data pribadi mereka.
4) Hak untuk Menuntut Ganti Rugi : Jika terdapat pelanggaran yang mengakibatkan kerugian kepada pemilik tanah sertifikat elektronik, pemilik tanah berhak menuntut ganti rugi.

Data-data pribadi yang terdapat dalam sertifikat elektronik terbagi dalam dua, yaitu data umum dan data spesifik. Data umum meliputi informasi pemilik yang berisi nama pemilik tanah, luas tanah, lokasi tanah, dan data yuridis. Data spesifik berisi meliputi nomor identifikasi bidang, jenis hak tanah, gambar bidang tanah dan juga kode unik dokumen yang diterbitkan terhubung

[12] Syarifaatul Hidayah et al., "TANTANGAN DAN PELUANG SERTIFIKAT ELEKTRONIK DALAM REFORMASI PENDAFTARAN TANAH DI ERA DIGITAL," *Jurnal Ilmiah Nusantara (JINU)* 1, no. 6 (November 2024): 186–99, https://doi.org/10.61722/jinu.v1i6.2793.

dengan edisi penerbitan.

Penyelenggara Sistem Elektroik (PSE) bertanggung jawab dalam terkait perlindungan data pribadi pada sertifikat elektronik yang juga terdapat dalam UU PDP dan Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. Penyelenggara Sistem Elektronik adalah setiap orang penyelenggara negara, Badan Usaha, dan masyarakat yang menyediakan, mengelola, dan/atau mengoperasikan Sistem Elektronik, baik secara sendiri-sendiri maupun bersama-sama kepada pengguna Sistem Elektronik untuk keperluan dirinya dan/atau keperluan pihak lain.

Teknologi yang mumpuni juga diperlukan untuk menjaga keamana data, kepatuhan terhadap regulasi bukan hanya sebatas kewajiban hukum akant tetapi membangun sebuah kepercayaan. Teknologi keamanan yang digunakan untuk menjamin keamana data di UU PDP, yaitu:[13]

1) Data Loss Prevention (DLP)
   Teknologi DLP dirancang untuk mendetekai, memantau, dan mencegah kebocran data pribadi secara tiak sengaja maupunn disengaja. DLP dapat diimplementasikan di *endpoint,* jaringan, maupun *email server* untuk memastikan data sensitif tidak keluar dari sistem tanpa otorisasi
2) Identity & Access management (IAM)
   IAM Memastikan bahwa hanya pihak yang berwenang dapat mengakses data pibadi, sesuai prinsip *least privilege.* Dengan autentikasi mulltifaktor dan audit trail, IAM memperkuat kontrol akses berbasis peran untuk mencegah akses yang tidak sah..
3) Encryption & Tokenization
   UU PDP mewajibkan perlindungan data sensitif, dan enkripsi adalah mekanisme utama unntuk itu. Enkripsi dilakukan baik data diam (atrest) maupun saat transit. Tokenisasi membantu dalam *masking* data pribadi dalam aplikasi dan sistem internal.
4) SIEM & Log Management
   Security Infromation and Evemt Management (SIEM) penting untuk mendeteksi dan merespon anomali keamanan, SIEM memungkinkan audit dan analisis aktivitas mencurigakan yang berguna saat investigasi insiden.
5) Privileged Access Management (PAM)
   PAM membatasi akses administrasi ke sistem kritikal. Ini penting untuk mengurangi risiko kebocoran data oleh pihak internal. Teknologi ini memberikan kontrol granular terhadap sesi administratif dan mencatat aktivitas pengguna,
6) Consent Management Platform (CMP)
   UU PDP mewajibkan pencatatan dan pengelolaan persetujuan subjek data. CMP memungkinkan organisasi mengelola siklus *approval* secara transparam ,dapat ditelusuri dan mudah dicabut sesuai hak pengguna.
7) Security Awareness & Training Platform
   Human Error adalah salah satu penyebab utama pelanggaran data. Platform pelatihan keamanan menyediakan pelatihan berskala dan simulasi serangan untuk meningkatkan kesadaran keamanan di seluruh organisasi, ternasuk pengenalan terhadap *phising* dan praktik keamanan siber dasar.
8) Data Recovery & Classification Tools
   Agara data dapat dilindungi, perusahaan harus terlebih dahulu mengetahui lokasi dan jenisnya. *Tools* ini membantu mengindentifikasi dan mengklasifikasikan data pribadi di seluruh IT, memudahkan penerapan kontrol keamanan dan pelaporan.
9) Data Breach Response Platform
   Dalam hal terjadi insiden kebocoran, perusahaan wajib melakukan notifikasi otomatis ke otoritas dan subjek data. Platform ini memfasilitasi orkestrasi respons insiden, pelaporan dan dokumentasi untuk memastikan pemenuhan kewajiban hukum.

Keutuhan data pada sertifikat elektronik terjamin, artinya informasi pemegang hak atas tanah akan selalu utuh, tidak berubah, dan untuk kerahasiaannya telah dilindungi dengan menggunakan teknologi persandian dari Badan Siber dan Sandi Negara (BSSN). Sertifikat elektronik ini mendukung inisiatif *go green* pemerintah dengan mengurangi penggunaan kertas dan tinta, memfasilitasi dan mempercepat proses penandatangan dan pelayanan, serta menerapkan tanda tangan digital yang menjamin otentikasi data, integritas, dan anti penolakan sertifikat tanah. Selain itu mudah dirawat dan dikelola, pengaksesan dapat dilakukan kapan saja dan dimana saja serta menghindari risiko kehilangan, terbakar, kehujanan, dan pencurian dokumen fisik. Nantinya informasi dilindungi dengan kode-kode pengkodean yang rumit sehingga hanya dapat dilihat oleh pihak tertentu dan tidak dapat diakses oleh pihak yang tidak berkepentingan (illegal). Kelemahan keamanan data tergantung pengelola dan pemakai. *Hacker* akan melakukan segala cara untuk mendapatkan data yang dapat menguntungkan bagi *hacker* dengan penjualan data dan merugikan bagi

[13] https://resources.dtrust.co.id/blog/kenali-9-teknologi-keamanan-uu-pdp-nomor-tujuh-sering-diabaikan/?utm_source=chatgpt.com (Diakses 29 Juni 2025)

pemilik data, seperti yang diketahui *hacker* akan mengaku lupa kata sandi dan meminta yang baru dengan cara mengirimkan dan memasukkan data pada link yang diberikan *hacker*. Dengan begitu *hacker* sudah mendapatkan data yang diinginkan maka terjadinyalah kebocoran data pribadi.[14]

Pemerintah memiliki peran yang sangat penting dalam memastikan keberhasilan sistem sertifikat tanah elektronik, baik dalam hal regulasi maupun pengawasan implementasinya. Beberapa langkah yang dapat dilakukan oleh pemerintah untuk memastikan keamanan data dan integritas sistem adalah:[15]

1. Pemerintah bertangggung jawab menetapkan regulasi yang jelas dan tegas. Hal ini meliputi penyusunan kebijakan yang mendukung keamana data, seperti yang diatur dalam UU ITE, UU PDP, dan Peraturan Menteri ATR/BPN Nomor 3 Tahun 2023, yang mengatur standar pelaksanaan sertifikat elektronik. Reguasi ini harus dilengkapi dengan pengawasan ketat terhadap implementasi sistem oleh Kementerian ATR//BPN
2. Pemerintah harus membangun infrastruktur teknologi yang andal dan aman, termasuk sistem penyimpanan data berbasis cloud dengan enkripsi tingkat tinggi untuk melindungi dokumen elektronik dari ancaman peretasan atau manipulasi. Penggunaan teknologi seperti *blockchain* dapat diterapkan untuk memastikan integritas data, karena sifatnya yang transparan, tidak daapt diubah, dan terdistribusi. Teknologi ini mampu melacak setiap perubahan data secara *real-time* dan memastikan setiap transaksi dalam sistem sertifikat tanah elektronik terverifikasi dengan baik.
3. Pemerintah perlu mendorong kolaborasi dengan penyedia teknologi dan ahli keamanan siber untuk mengembangkan sistem keamanan yang adaptif terhadap ancaman baru.
4. Sosialisasi dan Dukungan Teknologi juga harus memberikan dukungan teknologi yang memadai, seperti infrastruktur server yang aman dan kebijakan terkait penggunaan teknologi *blockchain* untuk menciptakan sistem yang transparan dan tidak dapat dimanipulasi.
5. Kemitraan dengan Sektor Swasta. Pemerintah dapat bekerja sama dengan penyedia teknologi swasta dan perusahaan keamanan siber untuk memperkuat sistem pertanahan elektronik agar lebih aman dan dapat dipercaya.
6. Pengembangan sistem pengaawasan dan audit berkala perlu dilakukan untuk memastikan kepatuhan terhadap standar keamana data

Pemerintah dapat membentuk tim khusus atau badan independen yang bertugas melalukan penilaian dan investigasi terkait keamanan data sertifikat elektronik.

Selain itu terdapat sanksi yang diberlakukan sebagai upaya represif, upaya represif adalah tindakan yang dilakukan oleh pemerintah atau aparat keamanan untuk menekan dan menghentikan suatu aksi atau gerakan yang dianggap mengancam stabilitas dan keamanan negara. Menurut Prof. Dr. Andi Hamzah, S.H., M.H., seorang ahli hukum pidana lainnya, upaya represif tetap diperlukan untuk memberikan efek jera bagi pelaku tindak pidana dan menegakkan rasa keadilan di masyarakat. Upaya preventif yanng diberikan berupa sanksi administratif dan sanksi pidana yang sudah diatur dalam UU PDP Pasal 57 dan Pasal 67. Pasal 57 UU PDP berisi sanksi administratif yang diberikan berupa:

a. Peringatan tertulis;
b. Penghentian sementara kegiatan pemrosesan data pribadi;
c. Penghapusan atau pemusnahan data pribadi; dan/atau
d. Denda administratif.

Teguran tertulis resmi diberikan kepada prosesor data. Prosesor data adalah setiap orang, badan publik, dan organisasi internasional yang bertindak sendiri-sendiri atau bersama-sama dalam melakukan pemrosesan data pribadi atas nama pengendali data pribadi. Teguran tertulis diberikan sebagai peringatan awal bagi pengendali data atau prosesor data dengan maksud untuk memberikan kesempatan untuk memperbaiki kesalahan yang telah dilakukan sebelum memberikan sanksi yanng berat. Teguran tertulis juga berguna untuk keperluan audit dan pengawasan dan menjadi bukti bahwa pihak yang memiliki wewenang telah mengambil tiindakan terhadap pelanggaran yang terjadi. Penghentian Sementara Kegiatan Pemrosesan Data Pribadi dilakukan agar tidak terjadi kerugian yang lebih lanjut dan mempengaruhi kepercayaan masyarakat. Denda administratif juga dikenakan kepada pengendali data atau prosesor data yang

[14] Jurnal Preferensi Hukum and | Issn, "PERLINDUNGAN HUKUM TERHADAP PEMEGANG SERTIFIKAT TANAH DIGITAL DIKAITKAN DENGAN KEAMANAN DATA PRIBADI," *Maret* 4, no. 1 (n.d.): 2746–5039, https://doi.org/10.55637/jph.4.1.6590.91-96.

[15] Ach Farhan Arif, Herowati Poesoko, and Miftahul Munir, "Mitigasi Risiko Keamanan Data Dalam Implementasi Sertifikat Tanah Elektronik Untuk Mewujudkan Kepastian Hukum Bagi Pemegang Hak Atas Tanah," *JURNAL HUKUM PELITA* 6, no. 1 (May 16, 2025): 74–89, https://doi.org/10.37366/jhp.v6i1.5674.

melanggar.

Pasal 65 UU PDP dengan tegas melanggar penggunaan data pribadi yang yang bukan miliknya dengan maksud untuk keuntungan pribadi, pengunaan data pribadi tanpa izin merupakan perbuatan melawan hukum dan dapat dikenakan sanksi berupa sanksi pidana yang diatur dalam pasal 67 UU PDP. Pasal tersebut mengatur mengenai Sanksi Pidana yang berbunyi:

(1) Setiap Orang yang dengan sengaja dan melawan hukum memperoleh atau mengumpulkan Data Pribadi yang bukan mililoeya dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian Subjek Data Pribadi sebagaimana dimaksud dalam Pasal 65 ayat (1) dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau pidana denda paling banyak Rp5.000.000.000,00 (lima miliar rupiah).
(2) Setiap Orang yang dengan sengaja dan melawan hukum mengunglapkan Data Pribadi yang bukan miliknya sebagaimana dimaksud dalam Pasal 65 ayat (2) dipidana dengan pidana penjara paling lama 4 (empat) tahun dan/atau pidana denda paling banyak Rp4.000.000.000,00 (empat miliar rupiah).
(3) Setiap Orang yang dengan senqaja dan melawan hukum menggunakan Data

Pribadi yang bukan miliknya sebagaimana dimaksud dalam Pasal 65 ayat (3) dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau pidana denda paling banyak Rp5.000.000.000,00 (lima miliar rupiah).

B. Tantangan Yang Menghambat Perlindungan Data Pemilik Tanah Pada Sertifikat Elektronik

Penjahat siber terus mengembangkan metode baru untuk mengeksploitasi kelemahan sistem keamanan, menyebabkan kerugian finansial dan reputasi yang signifikan bagi individu dan organisasi. Kemajuan teknologi informasi diduga menjadi kekuatan yang dapat memastikan nasib manusia. Dengan adanya internet, aktivitas masyarakat bukan hanya berlaku di dunia nyata namun menjalar ke *cyberspace*, sama halnya atas tindakan criminal.[16]

Upaya pemerintah dalam melindungi data pribadi dengan memberlakukan UU PDP sebagai kerangka hukum terutama setelah diberlakukan sertifikat elektronik sebagai wujud dari modernisasi pertanahan. Kebijakan yang diterapkan memberikan dampak berupa kendala yang menghambat pelaksanaan berupa ancaman siber, kurangnya kesadaran masyarakat maupun regulasi yang belum optimal. Kendala-kendala yang masih menjadi celah yang dapat disalahgunakan terutama pihak yang harusnya bertanggung jawab melindungi akan tetapi memanfaatkan hal tersebut untuk disalahgunakan berupa manipulasi informasi dengan mengubah data yang terdaftar, seperti luas tanah yang tidak sesuai yang bisa berakibat terjadinya sengketa hukum.

Lembaga perlindungan data pribadi bersifat sangat dibutuhkan dan penting mengingat adanya dasar hukum yang kuat pada pasal 58 UU PDP serta melihat kondisi kasus pelanggaran data pribadi di Indonesia yang kian meningkat tiap tahunnya. Lembaga tersebut berperan serta bertugas dalam mengawasi, melindungi dan menegakkan hak privasi individu serta mengawasi penggunaan data pribadi oleh pengendali data pribadi. Bahwa terdapat pesan krusial yang dimiliki oleh lembaga tersebut dalam menjaga keamanan data pribaadi dan memastikan bahwa praktik perlindungan data pribadi di Indonesia sesuai dengan standar yang telah ditetapkan oleh undang-undang terkait, sehingga dapat menumbuhkan kepercayaan masyarakat Indonesia dalam penggunaan data pribadi pada era digital ini khususnya era *society* 5.0 saat ini.[17]

Kewenangan lembaga diatur dalam Pasal 59 UU PDP, yaitu:

a. Merumuskan dan menetapkan kebijakan di bidang Perlindungan
   Data Pribadi;
b. Melakukan pengawasan terhadap kepatuhan Pengendali Data
   Pribadi;
c. Menjatuhkan sanksi administratif atas pelanggaran Perlindungan Data Pribadi yang dilakukan Pengendali Data Pribadi dan/atau
   Prosesor Data Pribadi
d. Membantu aparat penegak hukum dalam penaganan dugaan tindak pidana Data Pribadi sebagaimana dimaksud dalam Undang-Undang
   ini;
e. Bekerja sama dengan lembafa Perlidungan Data Pribadi negara lain dalaam rangka

[16] Citrazalzabilla, R., & Yusuf, H. (2024). Pencurian Data Pribadi Di Internet Dari Sudut Pandang Kriminologi. Jurnal Intelek Dan Cendikiawan …, Query date: 2024-06-05 11:40:45. https://jicnusantara.com/index.php/jicn/article/view/209

[17] Bella Christine and Christine S.T. Kansil, "Hambatan Penerapan Perlindungan Data Pribadi Di Indonesia Setelah Disahkannya Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi," *Syntax Literate ; Jurnal Ilmiah Indonesia* 7, no. 9 (November 6, 2023): 16331–39, https://doi.org/10.36418/syntax-literate.v7i9.13936.

penyelesaian dugaan pelanggaran Perlindungan Data
Pribadi lintas negara;

f. Melakukan penilaian terhadap pemenuhan persyaratan transfer Data
Pribadi ke luar wilayah hukum Negara Republik Indonesia;
g. Memberikan perintah dalam rangka tindak lanjut hasil pengawasan kepada Pengendali Data Pribadi dan/atau Prosesor Data Pribadi;
h. Melakukan publikasi hasil pelaksanaan pengawasan Perlindungan Dara Pribadi sesuai dengan ketentuan peraturan perundang-undangan;
i. Menerima aduan dan/atau laporan tentang dugaan terjadinya pelanggaran Perlindungan Data Pribadi;
j. Melakukan pemeriksaan dan penelurusan atas pengaduan, laporan, dan/atau hasil pengawasan terhadap dugaan Pelanggaran
Perlindungan Data Pribadi;
k. Memanggil dan menghadirkan Setiap orang dan/atau Badan Publik yang terkait dengan dugaan pelanggaran Perlindungan Data Pribadi;
l. Meminta keterangan, data, informasi dan dokumen dari Setiap Orang dan/atau Badan Publik terkait dugaan pelanggaran Perlindungan Data
Pribadi;
m. Memanggil dan menghadirkan ahli yang diperlukan dalam pemeriksaan dan penelusuran terkait dugaam pelanggaran
PerlindunganD Data Pribadi;
n. Melakukan pemeriksaan dan pee=nelusuran terhadap sistem elekronik, sarana, ruang,dan/atau tempat yang digunakan Pengendali Data Pribadi dan/atau Prosesor Data Pribadi, termasuk memperoleh akses terhadap data dan/atau menunjuk pihak ketiga; dan
o. Meminta bantuan hukum kepada kejaksaan dalam penyelesaian sengketa Perlindungan Data Pribadi/

Oleh karena itu, hambatan perlindungan data pribadi di Indonesia juga dipengaruhi karena belum adanya lembaga independen khusus di bidang perlindungan data pribadi. Padahal, pengadaan lembaga tersebut tidak hanya amanat dalam UU PDP melainkan juga berdasarkan interumen hukum internasional di bidang data privasi dan/atau data pribadi. Maka dari itu, terdapat urgensi bagi pemerintah untuk dapat segera menerbitkan serta mengesahkan peraturan pemerintah terkait dengan pembentukan lembaga perlindungan data pribadi sehingga lembaga independen perlindungan data pribadi di Indonesia dapat segera dibentuk dan menjalankan kewenangannya. Lebih lanjut, perlu diingat bahwa hukum seharusnya lebih daripada sekedar seperangkat kaidah sosial saja, hukum juga mencakup lembaga serta proses yang diperlukan untuk mewujudkannya sebagai hukum yang efektif.[18] Seandainya terjadi insiden siber diperlukan lembaga perlindungan data pribadi yang menjadi manajemen yang jelas serta sanksi apa yang lebih dulu diterapkan dalam penyelesaian sengketa.

Kehadiran Lembaga Pengawas PDP memberikan banyak manfaat positif. Pertama, salah satu parameter yang fundamental guna menentukan kesetaraan level *(adequacy of level*) hukum perlindungan data yang dimiliki oleh Indonesia dengan negara lain. menjadi prasyarat penting ketika melakukan transfer data dalam skala internasional, baik yang dilakukan antara pemerintah maupun sektor swasta. Ini penting guna memastikan perlindungan data bagi individu yang data pribadinya sedang diproses, mengingat data tersebut sering kali melewati batas negara (*cross-border).*[19]

Dalam penerapan sanksi pidana dan administratif terdapat garis samar dalam penerapannya, dilansir dari hukumonline Dosen fakultas Hukum Universitas Indonesia (FHUI), Marsya Mutmainah Handayani menyoroti garis samar (batas) antara hukum administratif dan hukum pidana dalam penerapan sanksi dalam dalam Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP). Marsya mengatakan selalu ada garis samar antara penerapan hukum pidana dan hukum administratif. Oleh karena itu, pertimbangan dalam memilih jenis sanksi menjadi sangat penting saat menyusun peraturan perundang-undangan. Dia menekankan dalam menentukan sanksi, penting untuk melihat politik hukum yang berlaku, sifat pelanggaran, serta ketentuan yang digunakan. Faktor lain yang harus dipertimbangkan antara lain, kesalahan pelaku (sengaja atau lalai), keberulangan pelanggaran. Kemudian estimasi manfaat ekonomi dari pelanggaran, dampak dari pelanggaran, kewenangan penegak hukum, hingga situasi ekonomi dan kapasitas pelaku Penegak hukum harus jeli dalam menentukan unsur pelanggaran

[18] *Ibid.*
[19] Juan Matheus and Ariawan Gunadi, "Pembentukan Lembaga Pengawas Perlindungan Data Pribadi Di Era Ekonomi Digital : Kajian Perbandingan Dengan KPPU," *JUSTISI* 10, no. 1 (October 18, 2023): 20–35, https://doi.org/10.33506/jurnaljustisi.v10i1.2757.

dan mekanisme penegakannya.[20]

Ancaman *cybercrime* merupakan ancaman yang sangat serius, penggunaan internet dan perangkat digital yang semakin canggih juga memiliki resiko yang sama tingginya. Metode yang dilakukan berupa serangan *malware* ataupun *phising* akan tetapi teknologi semakin berevolusi terutama penggunaan *Artifical Intelligence* (AI) merupakan kecerdasan buatan bidang illmu komputer yang berfokus pada pengembangan sistem yang dapat melakukan tugas-tugas yang biasanya memerlukan kecerdasan manusia.[21] Salah satu serangan AI yang berbahaya adalah serangan botnet, otnet adalah jaringan komputer yang telah terinfeksi malware dan dikendalikan oleh pihak tertentu, yang dikenal sebagai botmaster atau botherder. Istilah "*botnet*" merupakan gabungan dari kata robot dan network, yang mencerminkan sifat otomatis dan terkoordinasi dari jaringan ini. Komputer yang menjadi bagian dari botnet sering disebut sebagai bot atau zombie computer. Setelah terinfeksi, bot tersebut akan terhubung ke jaringan botnet dan dapat menjalankan perintah yang diberikan oleh botmaster.[22]

Tanpa diketahui pemiliknya, botnet bisa digunakan untuk berbagai aksi ilegal seperti serangan DDoS (*Distributed Denial of Service*), pencurian data, pengiriman malware, serangan *brute force*, dan *phishing*. Jaringan botnet dapat terdiri dari ribuan hingga jutaan perangkat yang rawan terhadap serangan karena infeksi malware. Hal itu kemudian menjadikannya alat yang sangat efektif dalam melakukan kejahatan digital secara masif dan tersembunyi. [23] Badan Siber dan Sandi Negara (BSSN) telah mencatat bahwa *MyloBot Botnet* menominasi anomali trafik di indonesia dengan jumlah 44,62 persen/lebih dari 730 juta anomali pada tahun 2021. *MyloBot* Botnet ini menargetkan sistem operasi windows dengan menyebar melalui spam pada pesan *e-mail* dan file unduhan yang sudah terinfeksi. Setelah botnet terinstall, botnet dapat mematikan windows defender dan menghapus *file.exe* yang dapat menyebabkan hilangnya data.[24]

Kurangnya kesadaran masyarakat merupakan kendala yang dihadapi karenanya kurang kewaspadaan terhadap pesan-pesan yang mencurigakan sehingga resiko serangan terhadap phishing sangat rentan. Banyak pengguna internet yang belum menyadari pentingnya melindungi data pribadi mereka. Ketidaktahuan ini seringkali disebabkan oleh kurangnya edukasi yang memadai mengenai isu-isu privasi dan keamanan data. Sebagian besar pengguna tidak memahami bagaimana data pribadi mereka dapat disalahgunakan atau dieksploitasi oleh pihak yang tidak bertanggung jawab. Misalnya, banyak yang tidak menyadari bahwa informasi yang mereka bagikan di media sosial dapat digunakan untuk mencuri identitas atau melakukan penipuan.[44] Kesulitan mengikuti perkembangan teknologi serta kurangnya literasi mengenai kebijakan privasi yang sangat berpengaruh sehingga terdapat celah-celah yang dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab, masyarakat hanya ikut melakukan pendaftaran sertifikat elektronik tapi tidak mengerti bagaimana cara kerja yang benar.

Diperlukan kampanye dan kolaborasi dengan lembaga pemerintahan maupun non-pemerintahan untuk memberikan informasi yang tepat. Selain kampanye publik, seminar dan pelatihan khusus juga dapat diadakan untuk memberikan pengetahuan yang lebih mendalam dan praktis kepada masyarakat. Seminar yang diadakan di sekolah, universitas, dan komunitas lokal dapat membantu meningkatkan kesadaran sejak dini. Pelatihan khusus untuk pegawai perusahaan, terutama yang bekerja dengan data sensitif, dapat meningkatkan kemampuan mereka dalam mengenali dan mencegah ancaman siber. Dengan pengetahuan yang lebih baik, individu dapat lebih proaktif dalam melindungi data pribadi mereka dan mengurangi risiko kebocoran data. Teknologi juga dapat dimanfaatkan untuk mendukung upaya edukasi ini. Penggunaan aplikasi edukatif dan platform *e-learning* dapat menyediakan akses mudah bagi masyarakat untuk mempelajari praktik-praktik terbaik dalam melindungi data pribadi.[45]

PENUTUP

A. Kesimpulan

1. Jaminan perlindungan data dalam sertifikat elektronik memberikan keutuhan data yang mana pemegang hak atas tanah akan selalu utuh, tidak berubah, dan untuk kerahasiannya telah dilindungi dengan menggunakan teknologi persandian dari Badan Siber dan Sandi Nasional (BSSN). Informasi dilindungi dengan kode-kode rumit dan hanya dapat dilihat oleh pihak-pihak tertentu saja,

[20] https://www.hukumonline.com/berita/a/garis-samar-hukum-administratif-dan-pidana-dalam-uu-pdp-lt67a44c621a07f/?page=2 (Diakses 9 Juli 2025)
[21] https://dif.telkomuniversity.ac.id/kecerdasan-buatan-apa-itu-ai-dan-bagaimana-cara-kerjanya/ (Diakses 1 Juli 2025)
[22] https://cyberhub.id/pengetahuan-dasar/apa-itu-botnet (Diakses 1 Juli 2025)
[23] https://idcloudhost.com/blog/apa-itu-botnet/ (Diakses 1 Juli 2025)
[24] Anastasya Zalsabilla Hermawan et al., "Prosiding Seminar Nasional Teknologi Dan Sistem Informasi (SITASI) 2023 Surabaya," 2023.

penerapan tanda tangan digital menjamin otentikasi data agar tidak terjadi pemalsuan tanda tangan. Jaminan regulasi berupa pemberlakuan Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data yang di dalamnya sudah berisi hak subjek data pribadi dan sanksi yang diterapkan berupa sanksi administratif dalam Pasal 57 Undang-Undang Perlindungan Data Pribadi dan sanksi pidana dalam Pasal 67 Undang-Undang Perlindungan Data Pribadi.

2. Pada praktiknya masih terdapat hambatan yang dihadapi, serangan siber adalah ancaman yang memiliki risiko yang besar. Semakin canggih teknologi maka akan diikuti dengan riisiko yang besar juga, serangan berupa *malware* merupakan risiko yang sering dihadapi. Selain itu, belum terdapat lembaga perlindungan data yang diamanatkan oleh UndangUndang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi Pasal 58. Kuramgnya kesadaran masyarakat juga menjadi faktor penghambat karena kurangnya kewaspadaan dan kurangnya pemahaman mengenai isu-isu penyerangan data pribadi melalui pesan-pesan yang berisi *link phising.*

B. Saran

1. Pemerintah segera menetapkan peraturan turunan Undang-Undang Perlindungan Data Pribadi berupa Peraturan Pemerintah (PP) dan Peraturan Presiden (Pepres). Sesuai dengan amanat Pasal 58 Undang-Undang Perlindungan Data Pribadi menyangkut pembentukan lembaga Perlindungan Data Pribadi melalui aturan Peraturan Presiden, lembaga tersebut akan menjalankan tugas pengawasan terhadap peneyelenggaraan perlindungan data pribadi, penegakan hukum administratif dan pelanggran undang-undang.
2. Penerapan sanksi administratif dan sanksi pidana dalam UU PDP dapat lebih kompleks penerapannya karena dinilai masih rancu dalam hal mengetahui sanksi mana yang di dahulukan jika terjadi pelanggaran. Dalam pemberlakuan sanksi pidana diharapkan menjadi *ultimum remedium* atau upaya terakhir dalam penegakkan hukum. Penumbuhan kesadaran masyarakat menjadi upaya pendukung dengan melakukan edukasi-edukasi melalui platform media *online* dan seminar.

DAFTAR PUSTAKA

Buku

FX. Sumarja, *Hukum Pendaftaran Tanah* (Bandar Lampung; Universitaas Lampung, 2010), hal 40.

Ali Zainudin, 2019, *Metode Penelitian Hukum* Edisi 1 Cetakan ke-11, Jakarta: Sinar Grafika, hal 20.

Dikdik Mansur & Elisa Gultom, *Cyber Law Aspek Hukum Teknologi Informasi* (Bandung: PT Refika Aditama), 2009, hal 7.

Danvrianto Budhijanto, *Hukum Perlindungan Data Pribadi di Indonesia Cyberlaw & Cybersecurity* (Bandung; PT Refika Aditama, 2023), hal 15-16.

Soerjono Soekanto, *Pengantar Penelitian Ilmu Hukum, 2006.*

Jurnal/Artikel

Nur Hidayani Alimuddin, "Implementasi Sertifikat Elektronik Sebagai Jaminan Kepastian Hukum Kepemilikan Hak Atas Tanah di Indonesia," *SASI* 27, no. 3 (7 Oktober 2021): 335, hlm 5. https://doi.org/10.47268/sasi.v27i3.509.

Sapardiyono Sapardiyono dan Sukmo Pinuji, "Konsistensi Perlindungan Hukum Kepemilikan danS Hak Atas Tanah melalui Sertipikat Tanah Elektronik," Widya Bhumi 2, no. 1 (4 Juni 2022): 54–64, hlm 3. https://doi.org/10.31292/wb.v2i1.19.

Dian Aries Mujiburohman dan Sekolah Tinggi Pertanahan Nasional Jalan Tata Bumi No, "BHUMI: Jurnal Agraria dan Pertanahan TRANSFORMASI DARI KERTAS KE ELEKTRONIK: TELAAH YURIDIS DAN TEKNIS SERTIPIKAT TANAH ELEKTRONIK" 7, no. 1 (t.t.): 57–67, hlm 4.

Hanifan Niffari, "PERLINDUNGAN DATA PRIBADI SEBAGAI BAGIAN DARI HAK ASASI MANUSIA ATAS PERLINDUNGAN DIRI PRIBADI (SUATU

TINJAUAN KOMPARATIF DENGAN PERATURAN PERUNDANGUNDANGAN DI NEGARA LAIN)" 7, no. 1 (2020), https://privacyinternational.org

Syarifaatul Hidayah et al., "TANTANGAN DAN PELUANG SERTIFIKAT ELEKTRONIK DALAM REFORMASI PENDAFTARAN TANAH DI ERA DIGITAL," *Jurnal Ilmiah Nusantara (JINU)* 1, no. 6 (November 2024): 186– 99, https://doi.org/10.61722/jinu.v1i6.2793

Fahreza Daniswara & Faiz Rahman. (2018). Perlindungan Data Pribadi: Studi
Komparasi terhadap Praktik di Singapura, Amerika Serikat, dan Malaysia. Center for Digital Society, Universitas Gadjah Mada, hlm 2
Wisnu Prabowo, Satriya Wibawa, and Fuad Azmi, "Perlindungan Data Personal Siber Di Indonesia," Padjadjaran Journal of International Relations 1, no. 3 (February 10, 2020): 218, https://doi.org/10.24198/padjir.v1i3.26194.
Sahat Maruli Tua Situmeang, "PENYALAHGUNAAN DATA PRIBADI SEBAGAI BENTUK KEJAHATAN SEMPURNA DALAM PERSPEKTIF HUKUM SIBER," SASI 27, no. 1 (March 25, 2021): 38, https://doi.org/10.47268/sasi.v27i1.394.
Mirnayanti, "ANALISIS PENGATURAN KEAMANAN DATA PRIBADI DI
INDONESIA ANALYSIS OF PERSONAL DATA SECURITY SETTINGS IN INDONESIA," Jurnal Living Law, vol. 15, 2023, hlm 20.
Grety Putri and Ramadhani Magister Kenotariatan, "ANALISIS YURIDIS
TERHADAP DIBERLAKUKANNYA SERTIPIKAT ELEKTRONIK KAITANNYA SEBAGAI ALAT BUKTI DI PERSIDANGAN,"
Jurnal Preferensi Hukum and | Issn, "PERLINDUNGAN HUKUM TERHADAP PEMEGANG SERTIFIKAT TANAH DIGITAL DIKAITKAN DENGAN KEAMANAN DATA PRIBADI," *Maret* 4, no. 1 (n.d.): 2746–5039, https://doi.org/10.55637/jph.4.1.6590.91-96.
Ach Farhan Arif, Herowati Poesoko, and Miftahul Munir, "Mitigasi Risiko Keamanan Data Dalam Implementasi Sertifikat Tanah Elektronik Untuk
Mewujudkan Kepastian Hukum Bagi Pemegang Hak Atas Tanah," *JURNAL HUKUM PELITA* 6, no. 1 (May 16, 2025): 74–89, https://doi.org/10.37366/jhp.v6i1.5674
Juan Matheus and Ariawan Gunadi, "Pembentukan Lembaga Pengawas Perlindungan Data Pribadi Di Era Ekonomi Digital : Kajian Perbandingan Dengan KPPU," *JUSTISI* 10, no. 1 (October 18, 2023): 20–35, https://doi.org/10.33506/jurnaljustisi.v10i1.2757.
Citrazalzabilla, R., & Yusuf, H. (2024). Pencurian Data Pribadi Di Internet Dari Sudut Pandang Kriminologi. Jurnal Intelek Dan Cendikiawan …, Query date: 2024-06-05 11:40:45. https://jicnusantara.com/index.php/jicn/article/view/209
Bella Christine and Christine S.T. Kansil, "Hambatan Penerapan Perlindungan Data Pribadi Di Indonesia Setelah Disahkannya Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi," *Syntax Literate ; Jurnal Ilmiah Indonesia* 7, no. 9 (November 6, 2023): 16331–39, https://doi.org/10.36418/syntax-literate.v7i9.13936.
Anastasya Zalsabilla Hermawan et al., "Prosiding Seminar Nasional Teknologi Dan Sistem Informasi (SITASI) 2023 Surabaya," 2023.
Ahmad Fachri Yamin Universitas Janabadra Yogyakarta, Annisa Rachmawati Universitas Janabadra Yogyakarta, and Jonathan Kevin Wijaya Universitas Janabadra Yogyakarta, "PERLINDUNGAN DATA PRIBADI DALAM ERA DIGITAL: TANTANGAN DAN SOLUSI," *Rido Aditia Pratama & Jonathan Kevin Wijaya Meraja Journal*, vol. 7, 2024

Peraturan/Perundang-Undangan

Undang-Undang Nomor 5 Tahun 1960 Tentang Peraturan Dasar Pokok-Pokok Agraria.
Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi
Undang -Undang Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-
Undang Nomor 11 Tahun 2008 Tentanng Informasi dan Transaksi Elektronik
Undang-Undang Nomor 36 Tahun 1999 Tentang Telekomunikasi
Peraturan Menteri ATR/BPN Nomor 1 Tahun 2021 Tentang Sertifikat Elektronik
Peraturan Menteri Komunikasi dan Informatika Nomor 11 Tahun 2018 Tentang Penyelenggara Sertifikasi Elektronik
Peraturan Pemerintah Nomor 10 Tahun 1961 Tentang Pendaftaran Tanah
Peraturan Menteri ATR/BPN Nomor 3 Tahun 2024 Tentang Penerbitan Dokumen Elektronik Dalam Kegiatan Pendaftaran Tanah.
Peraturan Pemerintah (PP) Nomor 18 Tahun 2021 tentang Hak Pengelolaan, Hak Atas Tanah, Satuan Rumah Susun dan Pendaftaran Tanah.

Peraturan Pemerintah Nomor 71 Tahun 2019 Tentang Penyelenggara Sistem dan Transaksi Elektronik.

Media Online/Internet

https://www.cnnindonesia.com/teknologi/20250206153253-192-1195388/menkomdigi-peringkat-keamanan-siber-ri-naik-sejajar-as-hinggajepang (Diakses 20 Februari 2025)

https://www.hukumonline.com/berita/a/pertanggungjawaban-hukum-terhadapkebocoran-data-pribadi-lt5f067836b37ef?page=2 (Diakses 3 Maret 2025)

https://www.monitorteknologi.com/apa-itu-ccpa/ (Diakses pada 11 Maret 2025)

https://gdpr.eu/what-is-gdpr/ (Diakses 11 Maret 2025)

https://dif.telkomuniversity.ac.id/kecerdasan-buatan-apa-itu-ai-dan-bagaimanacara-kerjanya/ (Diakses 1 Juli 2025) https://cyberhub.id/pengetahuan-dasar/apa-itu-botnet (Diakses 1 Juli 2025)

https://idcloudhost.com/blog/apa-itu-botnet/ (Diakses 1 Juli 2025)

https://resources.dtrust.co.id/blog/kenali-9-teknologi-keamanan-uu-pdp-nomortujuh-sering-diabaikan/?utm_source=chatgpt.com (Diakses 29 Juni 2025)

https://www.hukumonline.com/berita/a/garis-samar-hukum-administratif-danpidana-dalam-uu-pdp-lt67a44c621a07f/?page=2 (Diakses 9 Juli 2025)