PROSIDING NASIONAL PENELITIAN & PENGABDIAN KEPADA MASYARAKAT

LABEL: Law, Accounting, Business, Economics, and Language

Volume 2, Nomor 1, Agustus 2025

ANALISIS KELEMAHAN DAN KEKUATAN UU NO. 27 TAHUN 2022 DALAM MELINDUNGI DATA PRIBADI PASIEN TELEMEDICINE

Alfred Ariyanto[1], Rezi[2], Maryono[3]

[1] Universitas Duta Bangsa Surakarta, E-mail: alfredariyanto@gmail.com
[2] Universitas Duta Bangsa Surakarta, E-mail: rezi@udb.ac.id
[3] Universitas Kristen Indonesia, E-mail: sebastianusmaryo@gmail.com

ARTICLE INFO

Article History

Received:
Revised:
Published:

Keywords
Telemedicine, Personal Data Protection, Health Law, PDP LAW, GDPR-HIPAA

ABSTRACT

The advancement of information technology in the healthcare sector has encouraged the widespread adoption of telemedicine services. However, the increasing use of such services raises concerns about the protection of patients' personal data, which is often highly sensitive. This study aims to analyze the normative strengths and weaknesses of Law No. 27 of 2022 on Personal Data Protection, particularly in the context of telemedicine services. The method employed is a normative-juridical approach supported by a comparative evaluation of international regulations such as the GDPR and HIPAA. The results indicate that although the PDP Law incorporates strong legal principles, its implementation faces significant challenges, including the absence of implementing regulations, inadequate infrastructure, and the lack of an operational supervisory institution. Comparative evaluation reveals that Indonesia must strengthen technical standards, institutional frameworks, and enforcement mechanisms. Therefore, the protection of patients' personal data in telemedicine services requires a synergy of normative, technical, and institutional aspects to be implemented effectively and credibly.

INFORMASI ARTIKEL

Riwayat Artikel

Diterima:
Direvisi
Dipublikasikan:

Kata Kunci
telemedicine, perlindungan data pribadi, hukum kesehatan, UU PDP, GDPR-HIPAA

ABSTRAK

Perkembangan teknologi informasi di bidang kesehatan telah mendorong pemanfaatan layanan telemedicine secara luas. Namun, meningkatnya penggunaan layanan ini menimbulkan kekhawatiran terhadap perlindungan data pribadi pasien yang sering kali bersifat sensitif. Penelitian ini bertujuan untuk menganalisis kekuatan dan kelemahan normatif dari Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi, khususnya dalam konteks layanan telemedicine. Metode yang digunakan adalah pendekatan yuridis-normatif dengan dukungan evaluasi komparatif terhadap regulasi internasional seperti GDPR dan HIPAA. Hasil penelitian menunjukkan bahwa meskipun UU PDP memiliki prinsip hukum yang kuat, pelaksanaannya masih menghadapi tantangan signifikan, seperti minimnya peraturan pelaksana, lemahnya infrastruktur, dan belum terbentuknya lembaga pengawas yang fungsional. Evaluasi perbandingan menunjukkan bahwa Indonesia masih perlu memperkuat standar teknis, kelembagaan, serta mekanisme penegakan hukum. Dengan demikian, perlindungan data pribadi pasien dalam layanan telemedicine membutuhkan sinergi antara aspek normatif, teknis, dan kelembagaan agar dapat terlaksana secara efektif dan kredibel.

A. Pendahuluan

Perlindungan data pribadi merupakan isu krusial dalam konteks hukum dan teknologi informasi di Indonesia, terlebih dengan diberlakukannya Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Dalam konteks layanan kesehatan digital, khususnya telemedicine, isu perlindungan data menjadi semakin penting karena data pasien bersifat sangat sensitif dan membutuhkan perlakuan yang aman, etis, dan sesuai hukum. Tanpa jaminan perlindungan yang kuat, data kesehatan sangat rentan disalahgunakan, dan hal ini dapat menggerus kepercayaan masyarakat terhadap sistem layanan kesehatan berbasis teknologi.

Asas kepastian hukum dalam UU PDP menjadi fondasi utama untuk menciptakan lingkungan yang aman bagi perlindungan data pribadi. UU ini memberikan kejelasan atas hak individu dan tanggung jawab entitas yang memproses data. Sebagaimana dikemukakan oleh Lazuardiansyah dan Indriati (2023a), kepastian hukum dari UU PDP diharapkan dapat meningkatkan kepercayaan masyarakat terhadap sistem

digital. Kusnadi (2021) memperkuat bahwa hukum yang jelas akan memperkuat hak privasi dan memberikan kepastian bagi pelaku usaha.

Selalin asas kepastian hukum, asas kemanfaatan juga penting dalam konteks ini. Undang-undang ini memberi panduan bagi pelaku usaha untuk mengelola data secara bertanggung jawab. Dalam konteks ini, masyarakat perlu dilibatkan secara aktif dalam menjaga keamanan data mereka. Syailendra dan Fitzgerald (2023) menyatakan bahwa partisipasi aktif masyarakat dalam memahami hak digitalnya dapat menjadi benteng awal terhadap penyalahgunaan data. Kesadaran ini diperkuat melalui edukasi yang berkelanjutan untuk membangun perlindungan data (Siahaan et al., 2024).

Prinsip kepentingan umum sebagaimana terkandung dalam UU PDP menunjukkan bahwa perlindungan data tidak hanya melindungi individu, tetapi juga menjaga stabilitas sosial dari ancaman kejahatan siber. Perlindungan ini bersifat strategis karena menyangkut ketertiban dan keamanan masyarakat digital secara menyeluruh. Pertiwi et al. (2022) menyebutkan bahwa pendekatan kolektif dalam kebijakan perlindungan data memperkuat legitimiasi negara dalam menjaga kepentingan publik. Dengan demikian, kebijakan data pribadi harus menyeimbangkan antara privasi individu dan keamanan digital masyarakat luas (Fitria et al., 2025; Taufik & Zahara, 2024).

Dalam konteks telemedicine, data pribadi pasien menjadi lebih rentan karena transmisi informasi dilakukan secara daring. Transmisi data medis yang dilakukan melalui jaringan digital meningkatkan kemungkinan akses tidak sah, kebocoran data, atau penyalahgunaan informasi. Oleh karena itu, fasilitas kesehatan berkewajiban untuk menjamin keamanan dan kerahasiaan data medis pasien sebagaimana diatur dalam UU PDP dan Permenkes No. 20 Tahun (Lestari, 2021). Data pasien seperti rekam medis harus dikelola dengan standar perlindungan yang tinggi oleh pengendali data (Puspitosari, 2023a). Tak hanya aspek teknis, aspek etis juga menjadi sangat penting dalam telemedicine. Pasien harus diberi informasi yang jelas sebelum data mereka diproses, agar hak mereka sebagai subjek data tetap terlindungi. Nittari et al. (2020) dan Adnan & Pramaningtyas (2021) menegaskan bahwa transparansi ini penting untuk menjamin hak-hak pasien dalam era digital.

Untuk memperkuat efektivitas perlindungan, sanksi administratif dan pidana terhadap pelanggaran data juga diatur dalam UU PDP. Penegakan hukum ini harus dilakukan secara tegas agar menciptakan efek jera serta mendorong kepatuhan terhadap norma hukum (Luthiya et al., 2021a; Yuniarti, 2019). Pemberlakuan sanksi hukum yang tegas juga akan meningkatkan kepercayaan terhadap layanan kesehatan berbasis digital (Devara et al., 2020).

Namun, implementasi UU ini masih menghadapi tantangan besar. Beberapa di antaranya adalah ketidaksiapan infrastruktur, kurangnya pelatihan bagi tenaga medis, serta lemahnya regulasi pelaksana. Ketiadaan standar teknis dan lemahnya edukasi mengenai privasi data menghambat efektivitas UU ini (Dewayanti & Firdaus, 2022; Nittari et al., 2020; Tiolince, 2023).

Jika dengan regulasi internasional seperti GDPR dan HIPAA, Indonesia masih memiliki pekerjaan rumah besar dalam hal kelembagaan dan penegakan hukum. Kusnadi (2021) dan Alkadrie (2023) mencatat bahwa sistem penegakan hukum Indonesia belum seefektif Eropa dan AS, baik dari segi norma maupun kesadaran publik. Kasus-kasus kebocoran data yang terjadi, seperti di Pusat Data Nasional Sementara (PDNS), menunjukkan lemahnya sistem keamanan dan perlindungan hukum terhadap data kesehatan (Febriandy & Wahyutama, 2025; Utomo et al., 2020).

Teknologi seperti blockchain dan smart contract ditawarkan sebagai solusi untuk meningkatkan transparansi dan keamanan (Purwono et al., 2023). Enkripsi, autentikasi ganda, dan teknologi blockchain memberikan lapisan keamanan tambahan (Indriyajati et al., 2023; Maulani et al., 2023; Prayoga et al., 2022) yang akan menjadi alat penting dalam perlindungan data pasien. Akan tetapi, teknologi ini tidak dapat berdiri sendri tanpa disertai dukungan kebijakan, regulasi tambahan, dan literasi digital.

Dengan demikian dapat disimpulkan bahwa UU PDP merupakan tonggak penting dalam membangun kepercayaan publik terhadap layanan telemedicine. Namun, agar peran UU ini optimal, perlu ada sinergi antara teknologi, hukum, edukasi, dan kebijakan. Oleh karena itu, penting untuk menganalisis secara kritis kekuatan dan kelemahan UU No. 27 Tahun 2022 dalam konteks perlindungan data pribadi pasien dalam layanan telemedicine di Indonesia.

Berdasarkan latar belakang yang telah diuraikan, maka rumusan masalah dalam penelitian ini adalah sebagai berikut: Apa saja kekuatan normatif yang dimiliki Undang-Undang No. 27 Tahun 2022 dalam menjamin perlindungan data pribadi pasien pada layanan telemedicine di Indonesia? Bagaimana

kelemahan implementasi Undang-Undang No. 27 Tahun 2022 dalam praktik perlindungan data pribadi pasien dalam sistem telemedicine, terutama dalam aspek teknis, regulatif, dan edukatif? Sejauh mana Undang-Undang No. 27 Tahun 2022 mampu memenuhi standar perlindungan data internasional seperti GDPR dan HIPAA dalam konteks layanan telemedicine di Indonesia?

B. Metode Penelitian

Penelitian ini disusun dengan menggunakan pendekatan metodologis yang sistematis untuk menjawab rumusan masalah secara analitis, sintesis, dan evaluatif. Jenis penelitian yang digunakan adalah penelitian yuridis-normatif, yaitu penelitian hukum yang menelaah norma-norma hukum tertulis, khususnya Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi, serta regulasi dan dokumen hukum yang terkait dengan telemedicine di Indonesia. Pendekatan ini relevan untuk mengkaji kekuatan dan kelemahan normatif dari suatu peraturan perundang-undangan.

Penelitian ini menggunakan beberapa pendekatan:

1. Pendekatan perundang-undangan (statute approach): Mengkaji UU No. 27 Tahun 2022, Permenkes No. 20 Tahun 2019, dan regulasi lain yang relevan.
2. Pendekatan komparatif: Membandingkan UU No. 27 Tahun 2022 dengan GDPR (Uni Eropa) dan HIPAA (Amerika Serikat).
3. Pendekatan konseptual: Menganalisis gagasan atau doktrin hukum terkait perlindungan data pribadi dan hak pasien dalam telemedicine.

Sumber data yang digunakan terdiri dari: Data primer: Peraturan perundang-undangan terkait, seperti UU No. 27 Tahun 2022 dan peraturan pelaksananya. Data sekunder: Literatur akademik, artikel jurnal ilmiah, studi kasus, dan pendapat para ahli hukum serta praktisi teknologi informasi. Sedangkan pengumpulan data dilakukan dengan cara studi kepustakaan (library research), yaitu mengakses jurnal ilmiah, buku, dokumen hukum, dan basis data akademik (scite.ai, Google Scholar, dan repositori hukum). Data yang diperoleh kemudian dianalisis dengan pendekatan kualitatif deskriptif. Penulis akan mengkaji substansi hukum, mengevaluasi kekuatan dan kelemahan regulasi, serta menginterpretasikan efektivitas implementasi UU PDP dalam konteks telemedicine. Analisis tersebut dilakukan secara sistematis untuk menyusun argumen logis dan koheren.

C. Hasil dan Pembahasan

1. Kekuatan Normatif UU No. 27 Tahun 2022 dalam Perlindungan Data Pribadi Pasien Telemedicine

Transformasi digital di sektor kesehatan melalui layanan telemedicine menghadirkan peluang baru dalam pemberian layanan medis, sekaligus membuka potensi risiko terhadap kerahasiaan data pasien. Dalam konteks ini, Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) berfungsi sebagai fondasi yuridis utama yang memperkuat hak individu dan tanggung jawab entitas dalam mengelola data pribadi secara sah. UU ini merupakan wujud respons hukum nasional atas tuntutan global dalam menjamin keamanan dan kedaulatan data pribadi.

a. Asas dan Prinsip Hukum dalam UU PDP

UU PDP dibangun di atas asas kepastian hukum, kemanfaatan, dan kepentingan umum. Asas kepastian hukum menjadi jaminan terhadap hak subjek data yang bersifat pribadi dan sensitif, seperti data medis pasien, agar tidak digunakan secara sewenang-wenang (Lazuardiansyah & Indriati, 2023b). Ketentuan hukum yang tegas mampu menciptakan kepastian bagi pengguna layanan telemedicine mengenai siapa yang bertanggung jawab atas keamanan data mereka (Kusnadi, 2021).

Selain itu, asas kemanfaatan mengarahkan pengelolaan data pribadi kepada fungsi sosialnya, yakni mendukung pelayanan kesehatan yang lebih cepat dan merata, tanpa mengorbankan hak individu (Syailendra & Fitzgerald, 2023). Asas kepentingan umum menjadi dasar untuk menyeimbangkan hak atas privasi dan kebutuhan kolektif dalam menjaga sistem kesehatan nasional dari ancaman digital (Pertiwi et al., 2022).

b. Pengakuan Data Kesehatan sebagai Data Pribadi Spesifik

UU PDP mengklasifikasikan data kesehatan sebagai bagian dari data pribadi yang bersifat spesifik, sebagaimana disebutkan dalam Pasal 3 ayat (2). Ini menunjukkan bahwa data pasien dalam telemedicine tidak hanya dilindungi secara umum, tetapi juga memerlukan langkah-langkah perlindungan ekstra.

Kualifikasi ini menjadi dasar normatif untuk menetapkan pengelolaan data medis sebagai tanggung jawab tinggi yang wajib memenuhi prinsip kehati-hatian dan kehormatan terhadap hak pasien (Puspitosari, 2023).

c. Hak Subjek Data dalam Layanan Telemedicine

UU PDP menjamin berbagai hak yang dimiliki oleh subjek data, yang dalam konteks ini adalah pasien telemedicine. Hak-hak tersebut mencakup hak untuk mengetahui, mengakses, memperbaiki, menghapus, hingga menarik kembali persetujuan atas data yang telah diberikan (Wijaya, 2023). Dalam praktik layanan kesehatan daring, hak-hak ini memberikan kekuatan kontrol terhadap informasi pribadi dan menjadi landasan hukum untuk keberatan jika terjadi penyalahgunaan data (Luthfi, 2022).

Menurut Indriani & Putri (2023), bentuk persetujuan dalam konteks telemedicine dapat berbentuk persetujuan dinamis (dynamic consent), di mana pasien secara aktif dapat mengatur batasan akses, durasi penyimpanan, serta penggunaan data mereka. Hal ini penting untuk mencegah bentuk pemrosesan data yang berlebihan atau melampaui tujuan awal pelayanan.

d. Kewajiban Pengendali dan Prosesor Data

UU PDP menetapkan kewajiban hukum bagi pengendali data (penyedia layanan telemedicine) untuk memastikan perlindungan data pribadi dengan pendekatan teknis dan administratif. Dalam praktik telemedicine, hal ini mencakup penggunaan teknologi enkripsi, pengawasan akses internal, serta dokumentasi pemrosesan data secara berkala (Mahmoud et al., 2022). Menurut Puspitosari (2023), peran Fasilitas Pelayanan Kesehatan (Fasyankes) sebagai pengendali data wajib tunduk pada ketentuan hukum dan melakukan pendaftaran sistem elektroniknya kepada pemerintah.

e. Penegakan Hukum dan Sanksi

Kekuatan normatif UU PDP juga terletak pada keberadaan sanksi administratif dan pidana yang bersifat mengikat. Untuk pelanggaran berat seperti penyebaran data medis pasien tanpa izin, pelaku dapat dijatuhi sanksi pidana berupa denda dan penjara (Yuniarti, 2019). Sedangkan sanksi administratif seperti penghentian sementara dan pencabutan izin berfungsi untuk mendorong kepatuhan jangka panjang. Luthiya et al. (2021)menekankan bahwa pemberlakuan sanksi harus didukung oleh sistem audit reguler untuk memastikan transparansi.

f. Lembaga Pengawasan dan Mekanisme Pengaduan

UU PDP mengatur pembentukan lembaga pengawas independen yang bertugas mengawasi pelaksanaan undang-undang, menerima pengaduan masyarakat, serta menjatuhkan sanksi administratif. Keberadaan lembaga ini menjadi garansi bahwa pengendalian data tidak hanya bergantung pada itikad baik penyelenggara, tetapi juga dapat dipantau oleh institusi yang memiliki kewenangan sah (Devara et al., 2020).

g. Perlindungan Melalui Teknologi

Penguatan norma juga didukung oleh keberadaan teknologi seperti blockchain dan autentikasi ganda yang dapat mengamankan sistem informasi klinis dari potensi peretasan atau kebocoran data (Indriyajati et al., 2023; Syahrial, 2019). Enkripsi ujung-ke-ujung (end-to-end encryption) menjadi praktik baku dalam melindungi komunikasi antara pasien dan dokter dalam sesi telemedicine (Pamungkas et al., 2023).

2. Kelemahan Implementasi UU No. 27 Tahun 2022 dalam Perlindungan Data Pribadi Pasien Telemedicine

Meskipun Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi telah menyediakan kerangka hukum yang kuat, implementasinya dalam konteks layanan telemedicine masih menghadapi berbagai tantangan serius. Tantangan-tantangan ini bukan hanya bersifat teknis, tetapi juga struktural, regulatif, serta berkaitan dengan kesadaran hukum dan kapasitas institusional. Ketimpangan antara norma hukum yang ideal dengan realitas pelaksanaannya menjadi indikator utama lemahnya efektivitas UU PDP di tingkat praktik.

a. Ketidaksiapan Infrastruktur Teknologi

Salah satu hambatan utama dalam penerapan UU PDP pada layanan telemedicine adalah kesenjangan infrastruktur teknologi informasi, khususnya di daerah-daerah dengan keterbatasan akses digital. Telemedicine, yang bergantung pada transmisi data daring dan akses internet stabil, belum dapat dinikmati secara merata di seluruh wilayah Indonesia. Kondisi ini menyebabkan tidak hanya terbatasnya akses terhadap layanan, tetapi juga membuka celah bagi pelanggaran keamanan data yang tidak dapat dideteksi atau ditangani secara cepat (Morgan et al., 2022; Nittari et al., 2020).

Parveen et al. (2025) menekankan bahwa keterbatasan infrastruktur memperburuk kesenjangan layanan kesehatan, yang kemudian berdampak pada ketimpangan perlindungan hukum terhadap data pasien. Dalam kondisi seperti ini, implementasi UU PDP hanya dapat berjalan secara optimal di wilayah perkotaan atau institusi dengan sumber daya teknologi yang mencukupi.

b. Ketiadaan Peraturan Turunan yang Spesifik

Meskipun UU PDP telah disahkan, belum adanya peraturan pelaksana yang spesifik, seperti peraturan pemerintah (PP), peraturan menteri (Permen), atau standar operasional prosedur teknis, menjadi hambatan besar dalam pelaksanaannya. Regulasi pelaksana sangat penting untuk menerjemahkan norma-norma umum dalam UU menjadi panduan teknis bagi penyelenggara layanan.

Dewayanti dan Firdaus (2022) menggarisbawahi bahwa kekosongan regulatif menyebabkan multitafsir terhadap kewajiban pengendali data dan memperlemah daya paksa hukum. Hal ini dapat dilihat dalam praktik telemedicine di Indonesia, di mana beberapa penyedia layanan masih belum memiliki kebijakan privasi yang sesuai dengan prinsip-prinsip UU PDP, bahkan sebagian besar belum mengimplementasikan sistem verifikasi identitas ganda atau audit internal.

c. Rendahnya Literasi Digital dan Kesadaran Hukum

Lemahnya pemahaman masyarakat dan tenaga kesehatan terhadap konsep privasi dan perlindungan data pribadi juga memperparah lemahnya implementasi. Tiolince (2023) menyatakan bahwa sebagian besar penyedia layanan kesehatan masih menggunakan sistem pencatatan manual atau digital non-terenkripsi tanpa memahami risiko yang dapat terjadi. Ini menunjukkan bahwa meskipun instrumen hukum telah tersedia, pemangku kepentingan belum sepenuhnya siap menjalankannya.

Selain itu, Ramirez dan Calimag (2023) mencatat bahwa pelatihan teknologi informasi belum menjadi bagian rutin dalam program pelatihan medis di banyak institusi. Hal ini membuat sebagian tenaga kesehatan masih lebih memilih interaksi langsung karena merasa tidak nyaman atau tidak percaya dengan sistem digital, sehingga pengelolaan data pasien tidak memenuhi standar perlindungan sebagaimana diatur dalam UU PDP.

d. Lemahnya Penegakan Hukum dan Pengawasan

UU PDP memang mengatur sanksi administratif dan pidana yang tegas terhadap pelanggaran, namun penegakan hukum di lapangan masih bersifat lemah dan tidak konsisten. Salah satu penyebabnya adalah belum terbentuknya lembaga pengawas perlindungan data secara independen dan operasional. Akibatnya, tidak ada institusi yang memiliki otoritas penuh untuk mengaudit, memverifikasi, atau menindak pelanggaran yang terjadi dalam penyelenggaraan telemedicine.

Menurut Devara et al. (2020), lemahnya pengawasan ini menyebabkan rendahnya efek jera bagi pelaku pelanggaran data pribadi, serta menciptakan ketidakpastian hukum bagi masyarakat yang ingin mengajukan pengaduan. Selain itu, proses pelaporan dan penanganan kasus sering kali tidak transparan, memperburuk krisis kepercayaan terhadap sistem perlindungan data.

e. Minimnya Perlindungan terhadap Konsumen Layanan Telemedicine Swasta

Layanan telemedicine saat ini tidak hanya disediakan oleh fasilitas kesehatan milik pemerintah, tetapi juga oleh berbagai platform digital swasta. Namun, kewajiban hukum yang diberlakukan kepada penyedia swasta tidak sepenuhnya jelas, terutama yang bersifat startup atau beroperasi lintas negara. Dalam beberapa kasus, data pasien disimpan di server luar negeri tanpa ada mekanisme kontrol atau persetujuan eksplisit dari pasien (Puspitosari, 2023).

Kaplan (2020) dan Paganoni & Simmons (2018) menyebutkan bahwa platform digital cenderung mengutamakan kecepatan dan inovasi, namun mengabaikan aspek etika dan legalitas perlindungan data. Di Indonesia, ketiadaan lembaga verifikasi atau sertifikasi keamanan data terhadap platform semacam ini mengindikasikan adanya celah hukum yang belum ditutup oleh UU PDP maupun Kemenkes.

f. Studi Kasus: Kebocoran Data Kesehatan di PDNS

Salah satu contoh nyata dari lemahnya pelaksanaan perlindungan data di sektor kesehatan adalah kasus kebocoran data di Pusat Data Nasional dan Statistik (PDNS). Febriandy dan Wahyutama (2025) mencatat bahwa kebocoran tersebut mengakibatkan publik meragukan efektivitas sistem keamanan data pemerintah, dan pemerintah hanya mampu memberikan klarifikasi melalui pendekatan komunikasi krisis berbasis Image Repair Theory, bukan melalui mekanisme hukum yang terukur.

Menurut Dewi (2016), lemahnya landasan hukum dalam pengelolaan data berbasis cloud menjadi penyebab utama kebocoran tersebut. Belum adanya sistem audit ketat atau kewajiban pelaporan berkala

dari institusi pengelola data menyebabkan insiden ini terjadi secara berulang. Hal ini mengindikasikan bahwa kekuatan normatif dalam UU PDP belum diterjemahkan menjadi sistem pengawasan yang nyata.

Tabel. 1 Kategori Kelemahan Implementasi UU PDP dalam Telemedicine

Kategori	Uraian Kelemahan	Dampak Langsung terhadap Perlindungan Data Pasien
Teknologi	- Infrastruktur internet tidak merata di wilayah Indonesia - Sistem telemedicine banyak yang belum menggunakan enkripsi end-to-end - Minimnya pemanfaatan teknologi autentikasi dan audit log	- Rentan terhadap peretasan dan kebocoran data - Tidak ada jejak digital atas akses data
Regulasi	- Ketiadaan peraturan turunan teknis (PP, Permen) - Tidak adanya standar teknis minimum layanan telemedicine - Ketidakharmonisan dengan UU sektoral lainnya (UU Kesehatan, UU ITE)	- Ketidakpastian hukum bagi penyedia dan pengguna layanan - Tumpang tindih kewenangan
Sumber Daya Manusia	- Rendahnya literasi digital tenaga medis dan pasien - Tidak adanya pelatihan khusus bagi pengendali/prosesor data - Lemahnya budaya perlindungan data di Fasyankes dan startup	- Pelanggaran tidak disadari dan tidak dilaporkan - Kurang respons terhadap insiden
Pengawasan & Lembaga	- Lembaga pengawas UU PDP belum aktif secara fungsional - Belum tersedia sistem audit perlindungan data nasional - Mekanisme pengaduan publik belum transparan dan efisien	- Tidak ada tindak lanjut atas pelanggaran - Hilangnya kepercayaan terhadap sistem

Sumber: Diadaptasi dan diringkas dari analisis literatur dalam artikel ini, terutama berdasarkan: Dewayanti & Firdaus (2022), Nittari et al. (2020), Tiolince (2023), Puspitosari (2023), Devara et al. (2020), Febriandy & Wahyutama (2025), dan referensi lain dalam pembahasan.

Dari berbagai aspek di atas, terlihat bahwa kelemahan utama implementasi UU PDP dalam konteks telemedicine adalah kesenjangan antara substansi hukum dan kesiapan ekosistem pelaksanaannya. Secara normatif, UU ini telah memuat ketentuan yang kuat; namun secara fungsional, belum tercipta kondisi struktural dan kultural yang mendukung operasionalisasinya.

3. Evaluasi Komparatif dengan GDPR dan HIPAA dalam Perlindungan Data Pribadi Pasien Telemedicine

Perlindungan data pribadi dalam layanan telemedicine tidak dapat hanya dikaji dari perspektif hukum nasional. Evaluasi perbandingan dengan standar internasional seperti General Data Protection Regulation (GDPR) milik Uni Eropa dan Health Insurance Portability and Accountability Act (HIPAA) milik Amerika Serikat menjadi penting, agar UU No. 27 Tahun 2022 tidak berjalan dalam isolasi normatif. Komparasi ini memberikan perspektif global tentang praktik terbaik dalam perlindungan data kesehatan, serta mengidentifikasi area yang perlu diperkuat dalam sistem hukum Indonesia.

a. Prinsip dan Ruang Lingkup Regulasi

GDPR merupakan regulasi komprehensif yang berlaku di seluruh wilayah Uni Eropa dan memiliki jangkauan ekstrateritorial, yakni mengikat entitas mana pun yang memproses data warga negara Uni Eropa, terlepas dari lokasi operasionalnya. GDPR mengatur pemrosesan semua jenis data pribadi, termasuk data kesehatan, yang dikategorikan sebagai "sensitive personal data" dan memerlukan perlindungan tambahan. Di sisi lain, HIPAA berfokus lebih sempit pada data kesehatan yang disebut sebagai Protected Health Information (PHI), dan hanya berlaku untuk entitas kesehatan serta mitra bisnisnya di Amerika Serikat (Alkadrie, 2023).

UU No. 27 Tahun 2022 secara normatif memiliki struktur serupa dengan GDPR dalam hal ruang lingkup, yakni berlaku secara nasional terhadap semua subjek dan pengendali data, baik sektor publik maupun privat. Namun, berbeda dari GDPR, UU PDP belum memiliki efek ekstrateritorial yang jelas, sehingga masih terdapat celah hukum terhadap penyelenggara layanan telemedicine asing yang mengakses data pasien Indonesia (Kusnadi, 2021).

b. Hak Subjek Data dan Konsentrat Perlindungan

GDPR memberikan sejumlah hak kepada subjek data, seperti right to access, right to rectification, right to erasure (right to be forgotten), dan data portability. HIPAA lebih berfokus pada hak akses dan koreksi catatan medis, serta hak untuk memperoleh pemberitahuan atas pelanggaran data. UU PDP memberikan jaminan serupa dengan GDPR, termasuk hak untuk mengakses, memperbaiki, menghapus, serta menarik kembali persetujuan atas data pribadi (Wijaya, 2023).

Namun, masih terdapat kekurangan dari sisi implementasi. Misalnya, meskipun UU PDP telah mengatur hak penghapusan data, prosedur teknis serta batas waktu pemrosesan permintaan belum diatur secara rinci seperti dalam GDPR. Di Indonesia, pasien telemedicine sering kali tidak mengetahui bagaimana menindaklanjuti hak ini, yang menunjukkan perlunya penguatan prosedural dan literasi hukum di tingkat pengguna (Budiman et al., 2023).

c. Kewajiban Pengendali dan Keamanan Teknis

Dalam GDPR dan HIPAA, pengendali dan prosesor data diwajibkan untuk menerapkan langkah-langkah keamanan teknis dan organisasional yang proporsional terhadap risiko pemrosesan data. HIPAA menetapkan Security Rule dan Privacy Rule yang sangat teknis, mencakup kebijakan enkripsi, autentikasi pengguna, serta prosedur audit(Aliza et al., 2022).

UU PDP secara prinsipil juga mewajibkan pengendali data untuk menjamin keamanan dan integritas data pribadi, tetapi belum menetapkan standar teknis minimum secara eksplisit. Perbandingan ini menunjukkan bahwa Indonesia masih membutuhkan peraturan pelaksana yang mengatur detail teknis sebagaimana HIPAA dan GDPR, termasuk penggunaan teknologi seperti end-to-end encryption, multifactor authentication, dan sistem log monitoring (Indriyajati et al., 2023).

d. Penegakan Hukum dan Sanksi

Salah satu kekuatan utama GDPR adalah besarnya sanksi administratif yang dapat dikenakan, yakni hingga €20 juta atau 4% dari pendapatan global tahunan perusahaan. HIPAA juga menetapkan sanksi denda yang tinggi untuk pelanggaran berat, serta memungkinkan tuntutan pidana. Penegakan hukum di kedua yurisdiksi ini didukung oleh lembaga pengawas yang kuat dan prosedur investigasi yang terbuka(Suari & Sarjana, 2023).

Sebaliknya, UU PDP memang mengatur sanksi administratif dan pidana, tetapi mekanisme penegakannya masih dalam tahap transisi. Lembaga pengawas yang dijanjikan dalam undang-undang belum sepenuhnya berfungsi, dan belum ada preseden konkret tentang penerapan denda administratif terhadap pelanggaran data kesehatan (Devara et al., 2020).

e. Transparansi dan Akuntabilitas

GDPR dan HIPAA menempatkan transparansi dan akuntabilitas sebagai fondasi utama dalam pengelolaan data. Dalam praktiknya, entitas diwajibkan untuk menyampaikan kebijakan privasi dalam bahasa yang mudah dipahami, serta menyimpan bukti pemrosesan data yang dapat diaudit sewaktu-waktu. Selain itu, GDPR mewajibkan adanya Data Protection Officer (DPO) untuk organisasi tertentu (Kusnadi, 2021).

UU PDP juga memperkenalkan kewajiban serupa, namun dalam implementasinya, masih banyak penyedia telemedicine yang tidak menyebutkan petugas perlindungan data secara jelas di situs atau aplikasi mereka. Hal ini menunjukkan bahwa konsep akuntabilitas hukum di Indonesia masih lemah secara kultural dan teknis.

f. Pelajaran dan Implikasi untuk Indonesia

Dari perbandingan ini, dapat disimpulkan bahwa UU PDP secara normatif setara dengan GDPR dan HIPAA dalam hal prinsip dasar dan cakupan hak, tetapi masih lemah pada aspek pelaksanaan. Ada beberapa pelajaran penting yang dapat diadopsi Indonesia, yaitu:

1) Efek Ekstrateritorial: Meniru pendekatan GDPR agar penyedia telemedicine asing tunduk pada hukum Indonesia jika memproses data warga negara Indonesia.
2) Standarisasi Teknis: Menetapkan standar keamanan minimum untuk sistem informasi kesehatan sebagaimana dalam HIPAA.
3) Kelembagaan yang Kuat: Membangun lembaga pengawas yang independen dan efektif dalam waktu singkat.
4) Penegakan Hukum yang Konsisten: Menjalankan sanksi administratif dengan tegas dan terbuka untuk menciptakan efek jera.

Tabel 2. Perbandingan UU PDP dengan Standar Uni Eropa dan Amerika Serikat

Aspek	UU PDP (Indonesia)	GDPR (Uni Eropa)	HIPAA (AS)
Cakupan Data	Semua jenis data pribadi	Semua data pribadi, termasuk sensitif	Terbatas pada informasi kesehatan (PHI)
Hak Subjek Data	Akses, koreksi, hapus, tarik consent	Akses, koreksi, hapus, portabilitas	Akses, koreksi
Sanksi	Administratif & pidana, belum teruji	Denda hingga €20 juta / 4% omzet global	Denda & pidana tergantung pelanggaran
Kelembagaan	Belum operasional	Data Protection Authority	OCR (Office for Civil Rights)
Standar Teknis	Umum, butuh peraturan turunan	Wajib enkripsi, DPO, DPIA	Security Rule, Privacy Rule
Efek Ekstrateritorial	Tidak eksplisit	Ya	Tidak

Sumber: Diadaptasi dari ketentuan dalam UU No. 27 Tahun 2022, GDPR (EU 2016/679), HIPAA (1996), serta literatur pendukung: Alkadrie (2023), Kusnadi (2021), Aliza et al. (2022), Suari & Sarjana (2023).

D. Simpulan

Perlindungan data pribadi pasien dalam layanan telemedicine di Indonesia masih berada dalam fase transisi menuju sistem hukum yang matang dan komprehensif. Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) telah menyediakan landasan hukum yang kuat, khususnya dalam menjamin hak-hak subjek data, menetapkan kewajiban pengendali data, dan memperkenalkan sanksi terhadap pelanggaran. Namun, kekuatan normatif tersebut belum sepenuhnya tercermin dalam praktik implementasi.

Kelemahan utama dalam implementasi UU PDP terletak pada empat aspek krusial: pertama, ketidaksiapan infrastruktur teknologi di berbagai daerah; kedua, ketiadaan regulasi pelaksana yang bersifat teknis dan rinci; ketiga, rendahnya literasi digital dan kesadaran hukum di kalangan penyedia dan pengguna layanan kesehatan digital; dan keempat, belum berfungsinya lembaga pengawas perlindungan data secara operasional. Kelemahan-kelemahan ini menyebabkan perlindungan data pasien dalam layanan telemedicine belum dapat terlaksana secara merata dan kredibel.

Evaluasi perbandingan dengan regulasi internasional seperti GDPR di Uni Eropa dan HIPAA di Amerika Serikat menunjukkan bahwa Indonesia masih memerlukan penguatan kelembagaan, standarisasi teknis, serta mekanisme penegakan hukum yang konsisten. Meskipun secara normatif UU PDP telah mengadopsi prinsip-prinsip global, efektivitasnya di lapangan masih tertinggal karena lemahnya dukungan struktural dan rendahnya tingkat kepatuhan para pelaku layanan.

Keberhasilan implementasi UU PDP sangat bergantung pada sinergi antar aktor utama: pemerintah sebagai penyusun regulasi teknis dan pengawas kebijakan; Kementerian Kesehatan dan instansi teknis sebagai penentu standar keamanan informasi kesehatan; lembaga pengawas perlindungan data sebagai penegak hukum; penyedia layanan telemedicine sebagai pelaku pengendali data; serta masyarakat sebagai subjek data yang perlu diberdayakan secara digital.

Oleh karena itu, perlu dilakukan pembenahan sistemik yang menyeluruh. Pemerintah harus segera menyusun peraturan pelaksana yang operasional dan menetapkan standar keamanan informasi secara nasional. Lembaga pengawas perlu diaktifkan secara independen dan profesional, serta diberi kewenangan audit dan penindakan. Literasi digital dan kesadaran hukum masyarakat harus ditingkatkan melalui pendidikan dan kampanye publik yang masif. Selain itu, Indonesia juga perlu memperkuat kerja sama internasional dan mengadopsi praktik terbaik global dalam perlindungan data, serta menjadikan kepatuhan terhadap UU PDP sebagai indikator dalam akreditasi mutu layanan kesehatan digital.

Dengan arah strategis tersebut, perlindungan data pribadi pasien dalam telemedicine tidak hanya menjadi aman secara teknis dan sah secara hukum, tetapi juga berkeadilan secara sosial, inklusif secara digital, dan berkelanjutan secara kelembagaan.

E. Ucapan Terima Kasih

Penulis menyampaikan rasa terima kasih dan apresiasi yang setinggi-tingginya kepada berbagai pihak yang telah memberikan dukungan dalam penyusunan makalah ini. Terutama kepada para narasumber dan peneliti yang karyanya menjadi landasan penting dalam analisis literatur, serta kepada para dosen pembimbing dan rekan sejawat yang telah memberikan masukan konstruktif selama proses penulisan.

Ucapan terima kasih juga disampaikan kepada institusi dan platform akademik yang telah menyediakan akses terhadap literatur ilmiah dan peraturan perundang-undangan yang relevan. Apabila penelitian ini merupakan bagian dari program yang didanai, maka penulis menyampaikan penghargaan kepada lembaga pendanaan atas kepercayaan dan dukungannya.

Semoga segala kontribusi yang diberikan dapat menjadi amal jariyah ilmu pengetahuan dan membawa manfaat bagi pengembangan ilmu hukum dan pelayanan kesehatan digital di Indonesia.

F. Referensi

Adnan, M., & Pramaningtyas, M. D. (2021). Telemedicine Use During Covid-19 Pandemic : Prospects and Challenges. *Jimki Jurnal Ilmiah Mahasiswa Kedokteran Indonesia*, *8*(3), 225–233. https://doi.org/10.53366/jimki.v8i3.247

Aliza, N. O., Prianto, Y., & Rahaditya, R. (2022). Regulasi Proteksi Data Pribadi Pasien Covid-19 Di Indonesia. *Jurnal Muara Ilmu Sosial Humaniora Dan Seni*, *6*(1), 248–255. https://doi.org/10.24912/jmishumsen.v6i1.13462.2022

Alkadrie, S. M. R. R. M. (2023). SIM Card Dengan Identitas Palsu: Melanggar Hukum Atau Area Kelabu Dalam Perlindungan Data Pribadi. *Arus Jurnal Sosial Dan Humaniora*, *3*(3), 207–212. https://doi.org/10.57250/ajsh.v3i3.292

Devara, I. G. D. G., Dewi, A. A. S. L., & Ujianti, N. M. P. (2020a). Perlindungan Hukum Terhadap Data Pribadi Pengguna Jasa Transportasi Online. *Jurnal Preferensi Hukum*, *1*(1), 1–7. https://doi.org/10.22225/jph.1.1.2259.1-7

Dewayanti, I., & Firdaus, S. U. (2022). *Telemedicine in Indonesia: Perspective of Ethic, Discipline and Law*. 3–15. https://doi.org/10.2991/978-2-494069-75-6_2

Dewi, S. (2016). Konsep Perlindungan Hukum Atas Privasi Dan Data Pribadi Dikaitkan Dengan Penggunaan Cloud Computing Di Indonesia. *Yustisia Jurnal Hukum*, *5*(1). https://doi.org/10.20961/yustisia.v5i1.8712

Febriandy, R. K., & Wahyutama. (2025). Kebocoran Data PDNS Analisis Strategi Komunikasi Krisis Pemerintah Berdasarkan Image Repair Theory. *Communcology Jurnal Ilmu Komunikasi*, *12*(2), 325–341. https://doi.org/10.21009/comm.033.09

Fitria, M., Iryani, D., & Setiawan, P. A. H. (2025). Perlindungan Dan Tanggung Jawab Hukum Kebocoran Informasi Data Pribadi Pada Penyelenggara Sistem Elektronik Berdasarkan Perspektif Rahasia Dagang. *Cerdika Jurnal Ilmiah Indonesia*, *5*(1), 1416–1423. https://doi.org/10.59141/cerdika.v5i1.2408

Indriani, M., & Putri, A. A. (2023). Persetujuan Dinamis Sebagai Sarana Optimalisasi Pelindungan Data Pribadi Dan Hak Atas Privasi. *Jurnal Ham*, *14*(2), 105. https://doi.org/10.30641/ham.2023.14.105-122

Indriyajati, F., Jawa, M. M. S. D., & Utomo, H. (2023). Analisis Keamanan Data Electronic Medical Record Digital Transformation Office (DTO) Kementerian Kesehatan Indonesia. *Sanskara Manajemen Dan Bisnis*, *2*(01), 59–66. https://doi.org/10.58812/smb.v2i01.130

Kaplan, B. J. (2020). REVISITING HEALTH INFORMATION TECHNOLOGY ETHICAL, LEGAL, and SOCIAL ISSUES and EVALUATION: TELEHEALTH/TELEMEDICINE and COVID-19. *International Journal of Medical Informatics*, *143*, 104239. https://doi.org/10.1016/j.ijmedinf.2020.104239

Kusnadi, S. A. (2021). Perlindungan Hukum Data Pribadi Sebagai Hak Privasi. *Al Wasath Jurnal Ilmu Hukum*, *2*(1), 9–16. https://doi.org/10.47776/alwasath.v2i1.127

Lazuardiansyah, A. F., & Indriati, N. (2023a). Perlindungan Hak Privasi Atas Data Pribadi Anak Menurut Hukum Internasional Dan Hukum Nasional Indonesia. *SLR*, *5*(3). https://doi.org/10.20884/1.slr.2023.5.3.14192

Lestari, R. D. (2021). Perlindungan Hukum Bagi Pasien Dalam Telemedicine. *Jurnal Cakrawala Informasi*, *1*(2), 51–65. https://doi.org/10.54066/jci.v1i2.150

Luthfi, R. (2022). Perlindungan Data Pribadi Sebagai Perwujudan Perlindungan Hak Asasi Manusia. *Jurnal Sosial Teknologi*, *2*(5), 431–436. https://doi.org/10.36418/jurnalsostech.v2i5.336

Luthiya, A. N., Irawan, B., & Yulia, R. (2021). Kebijakan Hukum Pidana Terhadap Pengaturan Pencurian Data Pribadi Sebagai Penyalahgunaan Teknologi Komunikasi Dan Informasi. *Jurnal Hukum Pidana Dan Kriminologi*, *2*(2), 14–29. https://doi.org/10.51370/jhpk.v2i2.43

Mahmoud, K., Jaramillo, C., & Barteit, S. (2022). Telemedicine in Low- And Middle-Income Countries During the COVID-19 Pandemic: A Scoping Review. *Frontiers in Public Health*, *10*. https://doi.org/10.3389/fpubh.2022.914423

Maulani, I. E., Herdianto, T., Syawaludin, D. F., & Laksana, M. O. (2023). Penerapan Teknologi Blockchain Pada Sistem Keamanan Informasi. *Jurnal Sosial Teknologi*, *3*(2), 99–102. https://doi.org/10.59188/jurnalsostech.v3i2.634

Morgan, A., Goodman, D., Vinagolu-Baur, J., & Cass, I. (2022). Prenatal Telemedicine During COVID-19: Patterns of Use and Barriers to Access. *Jamia Open*, *5*(1). https://doi.org/10.1093/jamiaopen/ooab116

Nittari, G., Khuman, R. S., Baldoni, S., Pallotta, G., Battineni, G., Sirignano, A., Amenta, F., & Ricci, G. (2020). Telemedicine Practice: Review of the Current Ethical and Legal Challenges. *Telemedicine Journal and E-Health*, *26*(12), 1427–1437. https://doi.org/10.1089/tmj.2019.0158

Paganoni, S., & Simmons, Z. (2018). Telemedicine to Innovate Amyotrophic Lateral Sclerosis Multidisciplinary Care: The Time Has Come. *Muscle & Nerve*, *59*(1), 3–5. https://doi.org/10.1002/mus.26311

Pamungkas, D. F., Izzulhaq, M. H., Romadhoni, M. r., & Mukaromah, S. (2023). Paradoks Etika Teknologi Informasi: Kepercayaan Dan Privasi Data Di Era Digital. *Sitasi*, *3*(1), 526–534. https://doi.org/10.33005/sitasi.v3i1.426

Pertiwi, E., Nuraldini, D. D., Buana, G. T., & Arthacerses, A. (2022). Analisis Yuridis Terhadap Penyalahgunaan Data Pribadi Pengguna Media Sosial. *Jurnal Rechten Riset Hukum Dan Hak Asasi Manusia*, *3*(3), 10–16. https://doi.org/10.52005/rechten.v3i3.65

Prayoga, D., Hayati, F., Putra, H. A. Y., Rizki, I. N., & Fitroh, F. (2022). Risiko Keamanan Data Pribadi Pelanggan Dalam Penggunaan Big Data. *Jurnal Nasional Komputasi Dan Teknologi Informasi (Jnkti)*, *5*(3), 459–463. https://doi.org/10.32672/jnkti.v5i3.4381

Purwono, P., Dewi, P., & Dwi, S. K. (2023). Pengembangan Keamanan Sistem Rekam Medis Berbasis Blockchain Dengan Smart Contract. *Smart Comp Jurnalnya Orang Pintar Komputer*, *12*(2). https://doi.org/10.30591/smartcomp.v12i2.5143

Puspitosari, H. (2023). Perlindungan Hukum Terhadap Data Pasien Telemedicine Dalam Menerima Pelayanan Medis Berbasis Online. *Jurnal Syntax Fusion*, *3*(07), 658–668. https://doi.org/10.54543/fusion.v3i07.339

Ramirez, M. F. L., & Calimag, M. M. P. (2023). The Typology of Physicians According to Perspectives on Telemedicine During and Beyond the Covid-19 Pandemic. *Journal of Medicine University of Santo Tomas*, *7*(1), 1090–1111. https://doi.org/10.35460/2546-1621.2023-0018

Siahaan, P. G., Purba, N. R., Ritonga, N., Silalah, E., & Simanjuntak, R. F. N. (2024). Perlindungan Data Pribadi Terhadap Penanggulangan Tindakan Penipuan Online Berbasis Digital. *Fisipublik Jurnal Ilmu Sosial Dan Politik*, *9*(1), 47–58. https://doi.org/10.24903/fpb.v9i1.2881

Suari, K. R. A., & Sarjana, I. M. (2023). Menjaga Privasi Di Era Digital: Perlindungan Data Pribadi Di Indonesia. *Jurnal Analisis Hukum*, *6*(1), 132–142. https://doi.org/10.38043/jah.v6i1.4484

Syahrial, S. (2019). *Keamanan Data Rekam Medis Memanfaatkan Multi-Block Type Blockchain Pada Jaringan Terdistribusi*. https://doi.org/10.31227/osf.io/tpcvg

Syailendra, M. R., & Fitzgerald, S. E. (2023a). Sosialisasi Perlindungan Data Pribadi Bagi Masyarakat Kabupaten Indramayu. *Jsa*, *1*(1), 157–165. https://doi.org/10.24912/jsa.v1i1.23845

Taufik, M., & Zahara, F. (2024). Pengaturan Perlindungan Data Pribadi Dalam E-Commerce Menurut Perspektif Maqashid Syariah (Studi Kasus Marketplace Facebook). *Jurnal Ilmu Hukum Humaniora Dan Politik*, *4*(6), 2378–2392. https://doi.org/10.38035/jihhp.v4i6.2744

Tiolince, T. (2023). Indonesian Telemedicine Regulation to Provide Legal Protection for Patient. *Jsderi*, *1*(2), 75–97. https://doi.org/10.53955/jsderi.v1i2.9

Utomo, H. P., Gultom, E., & Afriana, A. (2020). Urgensi Perlindungan Hukum Data Pribadi Pasien Dalam Pelayanan Kesehatan Berbasis Teknologi Di Indonesia. *Jurnal Ilmiah Galuh Justisi*, *8*(2), 168. https://doi.org/10.25157/justisi.v8i2.3479

Wijaya, E. M. K. (2023). Criminal Law Review of Accident Victims' Personal Data Protection Rights. *Soepra*, *9*(2), 289–305. https://doi.org/10.24167/sjhk.v9i2.11148

Yuniarti, S. (2019). Perlindungan Hukum Data Pribadi Di Indonesia. *Business Economic Communication and Social Sciences (Becoss) Journal*, *1*(1), 147–154. https://doi.org/10.21512/becossjournal.v1i1.6030