

KEJAHATAN KESEHATAN DI ERA DIGITAL: TINJAUAN HUKUM PIDANA DAN PERDATA ATAS PENYALAHGUNAAN DATA PASIEN DAN TELEMEDISIN YANG TIDAK TERSTANDAR

Gunawan Widjaja

Senior Lecturer, Faculty of Law Universitas 17 Agustus 1945 Jakarta,
widjaja_gunawan@yahoo.com

ABSTRACT

The digitalisation of healthcare services in Indonesia has accelerated significantly since the COVID-19 pandemic, with telemedicine emerging as the primary solution for providing remote access to healthcare. This digital transformation has brought about innovations in healthcare delivery systems that have improved the quality of public services, but has also given rise to new risks of healthcare-related crime, such as the misuse of patient data and non-standardised telemedicine practices. This study employs a normative legal approach using a literature review method to analyse the forms of criminal and civil liability for these two legal issues. The findings indicate that the misuse of patient data constitutes a healthcare offence requiring a comprehensive criminal law approach based on Law No. 27 of 2022 on the Protection of Personal Data and the ITE Law, with criminal penalties of up to 8 years' imprisonment and/or a fine of up to Rp800 million for unauthorised access. Unstandardised telemedicine gives rise to civil liability under Article 1365 of the Civil Code (unlawful acts) and Article 1243 of the Civil Code (breach of contract) when it results in misdiagnosis or inadequate treatment. The interconnection between criminal and civil aspects demonstrates that digital healthcare offences are complex crimes requiring dual law enforcement. Regulatory weaknesses are evident in the absence of technology legislation that explicitly governs telehealth and the lack of comprehensive data protection regulations. There is a need to strengthen regulations on telemedicine service standards, enhance the security of health data systems, oversee digital health platforms, and educate healthcare professionals and the public to reinforce the ecosystem of personal data protection and legal certainty in digital healthcare services.

Keywords: healthcare crime, the digital age, misuse of patient data, non-standardised telemedicine, criminal law, civil law, personal data protection, the Personal Data Protection Act (PDP Act), the Electronic Information and Transactions Act (ITE Act), Article 1365 of the Civil Code

ABSTRAK

Digitalisasi layanan kesehatan di Indonesia mengalami percepatan signifikan sejak pandemi COVID-19 dengan telemedisin menjadi solusi utama dalam menyediakan akses layanan kesehatan jarak jauh. Transformasi digital ini membawa inovasi sistem penyampaian layanan kesehatan yang meningkatkan kualitas pelayanan publik namun juga menimbulkan risiko kejahatan kesehatan baru berupa penyalahgunaan data pasien dan praktik telemedisin yang tidak terstandar. Penelitian ini menggunakan pendekatan hukum normatif dengan metode kajian pustaka untuk menganalisis bentuk pertanggungjawaban pidana dan perdata atas kedua masalah hukum tersebut. Hasil

penelitian menunjukkan bahwa penyalahgunaan data pasien merupakan kejahatan kesehatan yang memerlukan pendekatan hukum pidana komprehensif berdasarkan UU Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi dan UU ITE dengan sanksi pidana penjara maksimal 8 tahun dan/atau denda maksimal Rp800 juta untuk akses ilegal. Telemedisin yang tidak terstandar menimbulkan tanggung jawab perdata berdasarkan Pasal 1365 KUHPerdata (perbuatan melawan hukum) dan Pasal 1243 KUHPerdata (wanprestasi) ketika menyebabkan kesalahan diagnosis atau terapi tidak memadai. Keterkaitan antara aspek pidana dan perdata menunjukkan bahwa kejahatan kesehatan digital merupakan kejahatan kompleks yang memerlukan penegakan hukum ganda. Keterlemahan regulasi terlihat dari ketiadaan undang-undang teknologi yang secara eksplisit mengendalikan telehealth dan regulasi perlindungan data yang belum komprehensif. Diperlukan penguatan regulasi standar layanan telemedisin, peningkatan keamanan sistem data kesehatan, pengawasan terhadap platform digital kesehatan, serta edukasi tenaga kesehatan dan masyarakat untuk memperkuat ekosistem perlindungan data pribadi dan kepastian hukum dalam layanan kesehatan digital.

Kata Kunci: kejahatan kesehatan, era digital, penyalahgunaan data pasien, telemedisin tidak terstandar, hukum pidana, hukum perdata, perlindungan data pribadi, UU PDP, UU ITE, Pasal 1365 KUHPerdata

Pendahuluan

Digitalisasi layanan kesehatan di Indonesia mengalami percepatan signifikan sejak pandemi COVID-19, dengan telemedisin menjadi salah satu solusi utama dalam menyediakan akses layanan kesehatan jarak jauh. Transformasi digital ini membawa inovasi dalam sistem penyampaian layanan kesehatan secara digital yang bertujuan meningkatkan kualitas pelayanan publik. Meskipun telemedisin memiliki potensi revolusioner dalam reformasi sistem kesehatan, layanan ini harus memenuhi standar tinggi yang setara dengan praktik medis konvensional (Ratih et al., 2026). Tingkat kepuasan masyarakat Indonesia terhadap telemedisin secara umum dianggap sukses dengan rata-rata 89%, namun terdapat masalah signifikan dalam aspek keamanan data dan privasi pasien. Tingkat kepuasan di area keamanan data dan privasi pasien berada di bawah ambang batas kritis sebesar 58,30%, yang menunjukkan perlunya perbaikan substansial (Yu & Zhao, 2019). Temuan ini mengindikasikan bahwa perlindungan data pasien belum menjadi prioritas dalam implementasi telemedisin di Indonesia.

Penyalahgunaan data pasien dalam aplikasi layanan kesehatan online menjadi isu hukum yang serius dan memerlukan regulasi khusus. Kasus kebocoran data seperti e-HAC dan rekam medis pasien COVID-19 membuktikan bahwa implementasi praktis masih lemah meskipun terdapat kerangka hukum formal. Regulasi teknis yang tersedia belum memadai untuk mengatasi kompleksitas sistem digital dan kesadaran penyedia layanan terhadap prinsip privasi masih kurang (Zamani et al., 2023).

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi berlaku sebagai landasan hukum, namun belum ada ketentuan khusus yang mengatur

pengamanan data kesehatan pasien dalam telemedisin. Act No. 29 of 2004 concerning medical practice hanya mengatur sanksi tegas terhadap dokter yang melakukan kebocoran data pasien, namun tidak secara langsung mengikat dokter online jika kebocoran data berasal dari aplikasi telemedisin. Informasi transaksi dalam ekosistem layanan digital publik seperti telemedisin rentan terhadap pemanfaatan dan komersialisasi yang disengaja (Tsoulakis et al., 2023).

Ketiadaan hukum privasi data yang komprehensif telah mengurangi potensi Indonesia untuk memimpin dalam pasar kesehatan global yang cost-effective. Kekurangan ini berdampak langsung pada peningkatan pelanggaran hak konstitusional individu dan memerlukan peran negara dalam memastikan pemenuhan kepentingan individu dan negara. Pendekatan ini dapat mengurangi pelanggaran privasi akibat cybercrime, termasuk yang dipicu oleh eksploitasi data pribadi yang ilegal (Truli, 2018).

Indonesia saat ini belum memiliki undang-undang teknologi yang secara eksplisit mengendalikan telehealth atau regulasi perlindungan data yang cocok untuk mengelola volume data masimal dari layanan kesehatan digital. Kesiapan kapasitas Indonesia untuk mewujudkan transformasi digital belum memadai karena perlu mengantisipasi risiko seperti potensi penyalahgunaan data, pelanggaran privasi, dan ancaman cyberattack. Tantangan utama meliputi Orang, Proses, dan Teknologi dalam transformasi digital sektor Kesehatan (Wijaya et al., 2025).

Fenomena digital divide antara pengguna layanan telemedisin di Indonesia menunjukkan kesenjangan akses teknologi yang tidak merata. 82% responden survei berasal dari Jawa, sementara Sumatera 11%, Sulawesi 3%, Kalimantan 2%, Bali dan Nusa Tenggara 2%, dan Papua 0%. Kesenjangan infrastruktur internet di daerah pedesaan dan timur Indonesia menghambat partisipasi masyarakat dalam layanan digital publik (Hamzah, 2024).

Literasi digital dan kesiapan digital di kalangan tenaga kesehatan maupun masyarakat masih rendah sebagai tantangan penerapan telemedisin. Kerangka hukum dan regulasi yang belum memadai terkait perlindungan data dan akuntabilitas menjadi masalah utama. Aspek akuntabilitas hukum dalam kasus dugaan malpraktik melalui layanan telemedicine belum memiliki kejelasan regulasi. Regulasi terkait telemedisin di Indonesia masih dalam tahap perkembangan dan belum sepenuhnya menjawab kebutuhan praktik di lapangan. Landasan hukum melalui Permenkes Nomor 20 Tahun 2019 tentang Penyelenggaraan Telemedisin belum mengatur tanggung jawab hukum antara tenaga medis, fasilitas kesehatan, dan penyedia platform. Pembiayaan telemedisin belum terintegrasi dalam sistem Jaminan Kesehatan Nasional (JKN) (Wijaya et al., 2025).

Penyelesaian pelanggaran dalam praktik telemedisin yang merugikan pasien dapat dilakukan melalui pengaduan ke Majelis Kehormatan Disiplin Kedokteran Indonesia, gugatan perbuatan melawan hukum, serta penyelesaian melalui pengadilan atau di luar pengadilan. Tanggung jawab perdata rekam medis elektronik menuntut

penyelenggara layanan kesehatan bertanggungjawab atas segala kebocoran informasi pribadi pasien (Puspita et al., 2024).

Penyalahgunaan data pasien dalam aplikasi layanan kesehatan online dapat diterapkan sanksi berupa pembayaran ganti rugi, pencabutan izin, hingga sanksi pidana penjara dan denda. Sanksi mencakup UU Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, UU ITE, dan peraturan perundang-undangan terkait. Penyelenggara sistem elektronik termasuk fasilitas pelayanan kesehatan yang melakukan penyalahgunaan data pasien tunduk pada ketentuan sanksi (Vila Seoane, 2021).

Dengan demikian, Kejahatan kesehatan di era digital mencerminkan keresahan publik yang mendalam dan kebutuhan partisipasi lebih besar dalam proses pembuatan kebijakan. Maka dengan itu, kolaborasi antarinstansi menjadi sangat penting dalam mengatasi kejahatan kesehatan di masyarakat di era digital saat ini. Peran instansi lain dalam kolaborasi diperlukan untuk penanganan efektif kejahatan kesehatan.

Metode Penelitian

Penelitian ini menggunakan pendekatan hukum normatif dengan metode kajian pustaka (literature review) yang bersifat deskriptif-analitis. Sumber data diperoleh dari studi literatur atas berbagai bahan hukum primer, sekunder, dan tersier meliputi peraturan perundang-undangan seperti Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Undang-Undang Nomor 36 Tahun 2009 tentang Kesehatan, Undang-Undang Nomor 29 Tahun 2004 tentang Praktik Kedokteran, serta Peraturan Menteri Kesehatan Nomor 20 Tahun 2019 tentang Penyelenggaraan Telemedisin, jurnal nasional dan internasional, buku dan dokumen lainnya. Analisis data dilakukan secara kualitatif dengan mengkaji secara sistematis, logis, dan empiris materi hukum yang diperoleh untuk mengidentifikasi masalah hukum, menganalisis pertanggungjawaban pidana dan perdata, serta memberikan rekomendasi normatif terhadap regulasi yang berlaku (Elijah & Aslan, 2025); .

Hasil dan Pembahasan

Tinjauan Hukum Pidana atas Penyalahgunaan Data Pasien di Era Digital

Penyalahgunaan data pasien dalam era digital merupakan bentuk kejahatan kesehatan yang burgeoning di Indonesia, terutama seiring pesatnya perkembangan telemedisin dan layanan kesehatan berbasis platform digital (Zamani et al., 2023). Data pasien termasuk dalam kategori data pribadi sensitif yang memerlukan perlindungan khusus karena mengandung informasi medis, riwayat kesehatan, dan identitas pribadi yang sangat privasi. Kerahasiaan data pasien dalam aplikasi layanan kesehatan online mengacu pada UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi yang menetapkan data pasien berupa data pribadi dalam rekam medis wajib dilindungi (Yudha et al., 2025).

Bentuk penyalahgunaan data pasien meliputi kebocoran data medis, penjualan data pasien tanpa izin, akses ilegal oleh pihak tidak berwenang, dan perubahan data kronologi kesehatan pasien. Kasus kebocoran data seperti e-HAC dan rekam medis pasien COVID-19 membuktikan bahwa implementasi praktis keamanan data masih lemah meskipun terdapat kerangka hukum formal. Pelayanan kesehatan online yang disalahgunakan menimbulkan risiko serius terhadap privasi dan keamanan informasi medis pasien yang dapat berdampak pada kerugian materiil dan immateriil (Versaci, 2018).

Dasar hukum pidana utama untuk penyalahgunaan data pasien adalah Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi yang berlaku sebagai landasan hukum perlindungan data pribadi di Indonesia. UU PDP mengatur sanksi administratif hingga pidana sesuai Pasal 57 dan Pasal 67 untuk insiden yang terjadi pasca 2022 seperti kasus kebocoran data Halodoc. Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) Nomor 11 Tahun 2008 memberikan ketentuan pidana terkait akses ilegal, perusakan data, dan distribusi informasi elektronik zonder hak (Septiari & Ujianti, 2025).

Unsur tindak pidana dalam penyalahgunaan data pasien mencakup perbuatan melawan hukum dalam pengelolaan data kesehatan, unsur kesengajaan (*mens rea*), dan unsur kelalaian berat dalam pengamanan data. Pasal 30 UU ITE secara tegas melarang akses tanpa izin terhadap sistem elektronik, memperoleh informasi elektronik secara ilegal, dan menjebol sistem pengamanan penegakan hukum akses ilegal. Pasal 32 UU ITE melarang perubahan, penambahan, penghilangan, perusakan, dan transfer informasi elektronik kepada sistem elektronik orang lain yang tidak berhak (Respati, 2024).

Pasal 46 UUIE mengatur sanksi pidana untuk tindak pidana akses ilegal dengan pidana penjara paling lama 6 tahun dan/atau denda paling banyak Rp600 juta untuk Pasal 30 ayat 1, 7 tahun dan Rp700 juta untuk Pasal 30 ayat 2, serta 8 tahun dan Rp800 juta untuk Pasal 30 ayat 3 (Kuspraningrum, 2011). Pelaku yang terbukti melakukan akses tanpa hak, perusakan data, dan pemerasan secara elektronik dapat dijatuhi pidana sesuai asas kesalahan dalam hukum pidana (Respati, 2024). Ancaman hukuman pidana penjara maksimal 8 tahun dan/atau denda maksimal Rp800 juta untuk akses ilegal menunjukkan tingkat seriusitas kejahatan siber dalam sektor kesehatan penegakan hukum akses ilegal.

Fasilitas pelayanan kesehatan memiliki tanggung jawab sebagai penyelenggara sistem elektronik sekaligus pengendali data pribadi dalam pengelolaan data pasien. Dalam ekosistem telemedisin modern, tanggung jawab pidana tidak hanya rests pada individu penyedia layanan kesehatan tetapi juga extends ke fasilitas kesehatan, penyedia platform digital, operator server, dan pihak ketiga yang terlibat dalam proses data. Ketika tanggung jawab pengamanan data gagal dijalankan, penyelenggara sistem

elektronik harus menanggung risiko hukum berupa sanksi administratif, sanksi perdata, bahkan pidana (Taylor, 2020).

Tenaga kesehatan dapat dituntut tanggung jawab pidana jika terjadi kebocoran data akibat perbuatan sadar, kelalaian berat, atau tindakan yang berlawanan dengan standar profesi. Act No. 29 of 2004 concerning medical practice hanya mengatur sanksi tegas terhadap dokter yang melakukan kebocoran data pasien, namun tidak secara langsung mengikat dokter online jika kebocoran data berasal dari aplikasi telemedisin. Penyedia platform telemedisin juga dapat bertanggung jawab secara pidana jika kebocoran data terjadi akibat kelemahan sistem keamanan yang mereka kelola (Ventura & Coeli, 2018).

Platform digital kesehatan sebagai penyelenggara sistem elektronik tunduk pada ketentuan sanksi UU PDP dan UU ITE untuk penyalahgunaan data pasien. Penyelenggara sistem elektronik termasuk fasilitas pelayanan kesehatan yang melakukan penyalahgunaan data pasien harus menanggung sanksi sesuai ketentuan yang diatur. Tanggung jawab pidana platform digital meliputi kegagalan dalam pengamanan data, kelalaian dalam implementasi teknologi keamanan, dan tidak melaporkan insiden kebocoran data kepada otoritas (Truli, 2018).

Penerapan sanksi terhadap aplikasi layanan kesehatan online yang disalahgunakan dilakukan dalam bentuk pembayaran ganti rugi, pencabutan izin, hingga sanksi pidana penjara dan denda. Sanksi mencakup ketentuan dalam UU Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, UU ITE, dan peraturan perundang-undangan terkait lainnya yang menyebutkan secara tegas tentang sanksi. Frontida perdata dapat diterapkan melalui Pasal 1365 KUHPerdata karena tindakan melanggar hak privasi, dilakukan dengan kesengajaan, menimbulkan kerugian immateriil, serta memiliki hubungan kausal dengan akibat yang dialami korban (Xiaying, 2019).

Perbuatan pelaku dalam kasus penyalahgunaan data sudah memenuhi unsur-unsur pasal yang didakwakan sehingga dijatuhi pidana berdasarkan Pasal 67 ayat (3) UU PDP. Selain tanggung jawab pidana, pelaku juga dapat dimintakan pertanggungjawaban hukum secara keperdataan berdasarkan Pasal 1365 KUHPerdata karena melanggar hak privasi dan menimbulkan kerugian (Vila Seoane, 2021). Kombinasi sanksi pidana dan perdata menunjukkan bahwa penyalahgunaan data pasien merupakan kejahatan kompleks yang memerlukan pendekatan hukum ganda.

Studi kasus kebocoran data dari aplikasi kesehatan dan implikasi pidananya menunjukkan bahwa penegakan hukum masih menghadapi tantangan dalam hal identifikasi pelaku, bukti elektronik, dan koordinasi antarinstansi. Implementasi praktis masih lemah meskipun terdapat kerangka hukum formal, dan regulasi teknis yang tersedia belum memadai untuk mengatasi kompleksitas sistem digital. Kesadaran penyedia layanan terhadap prinsip privasi masih kurang dan infrastruktur keamanan data masih lemah di banyak fasilitas kesehatan. Kejahatan kesehatan di era digital mencerminkan keresahan publik yang mendalam dan kebutuhan partisipasi lebih besar

dalam proses pembuatan kebijakan. Kolaborasi antarinstansi menjadi sangat penting dalam mengatasi kejahatan kesehatan di masyarakat di era digital saat ini. Peran instansi lain dalam kolaborasi diperlukan untuk penanganan efektif kejahatan kesehatan termasuk penyalahgunaan data pasien (Truli, 2018).

Tantangan penegakan hukum di era digital meliputi lemahnya infrastruktur keamanan data, literasi digital rendah di kalangan tenaga medis dan pasien, serta kurangnya panduan teknis spesifik. Keterbatasan pengawasan dan penegakan hukum terhadap pelanggaran perlindungan data juga menjadi hambatan utama dalam penanganan kejahatan kesehatan digital. Diperlukan upaya kolaboratif antara pemerintah, penyedia layanan kesehatan, dan masyarakat untuk memperkuat ekosistem perlindungan data pribadi (Yu & Zhao, 2019).

Tinjauan Hukum Perdata atas Telemedisin yang Tidak Terstandar

Telemedisin yang tidak terstandar merupakan praktik layanan kesehatan jarak jauh yang melanggar standar profesi kedokteran dan menimbulkan kerugian bagi pasien secara hukum perdata. Definisi telemedisin mencakup layanan konsultasi medis jarak jauh melalui teknologi telekomunikasi yang menghubungkan pasien dengan tenaga medis tanpa pertemuan fisik langsung. Praktik telemedisin yang tidak terstandar meliputi diagnosis tanpa pemeriksaan memadai, kesalahan terapi berbasis konsultasi online, dan ketiadaan informed consent digital yang sah (Puspita et al., 2024).

Dalam konteks hukum perdata, Pasal 1365 KUHPerdata menyatakan bahwa dokter yang melakukan kesalahan dalam telemedisin dan menyebabkan kerugian pada pasien wajib mengganti kerugian tersebut (Setyo, 2024). Pertanggungjawaban perdata atas kesalahan diagnosis dalam layanan telemedisin dapat dilihat dari dua sudut pandang: tenaga medis tetap memiliki tanggung jawab hukum terhadap pasien apabila terbukti kelalaian menyebabkan kesalahan diagnosis. Pertanggungjawaban juga dapat dilakukan oleh platform layanan telemedisin apabila terbukti bahwa kesalahan diagnosis diakibatkan oleh kesalahan sistem dalam platform tersebut.

Perbuatan melawan hukum (PMH) dalam telemedisin tidak terstandar memenuhi empat syarat Pasal 1365 KUHPerdata: pasien harus mengalami kerugian, ada kesalahan atau kelalaian, ada hubungan kausal antara kerugian dan kesalahan, dan perbuatan melanggar hukum. Dokter yang tidak mengikuti standar profesi dalam telemedisin telah berbuat melawan hukum karena tindakannya bertentangan dengan asas kepatutan, ketelitian, serta sikap hati-hati yang diharapkan. Penerapan Pasal 1365 KUHPerdata untuk PMH dalam malpraktik harus memenuhi empat syarat tersebut (Suyudi et al., 2025).

Bentuk tanggung jawab hukum dokter terhadap pelayanan telemedisin dapat berupa tanggung jawab hukum perdata, hukum pidana, dan hukum administrasi. Dalam hukum perdata, tanggung jawab dokter meliputi wanprestasi (Pasal 1243 KUHPerdata) atau perbuatan melawan hukum (Pasal 1365 KUHPerdata). Pasien yang merasa

dirugikan secara prinsip berhak untuk melakukan tuntutan perdata kepada dokter yang telah lalai, kurang hati-hati, atau melakukan kesalahan tindakan berupa gugatan perbuatan melawan hukum (Setyo, 2024).

Wanprestasi dalam layanan telemedisin terjadi ketika dokter tidak memenuhi perjanjian terapeutik dengan pasien, tidak menjaga rahasia medis, atau tidak memberikan layanan sesuai standar profesi. Perikatan untuk berbuat sesuatu atau untuk tidak berbuat sesuatu apabila si wanprestasi ini pasien harus mempunyai dasar bukti-bukti bahwa benar telah ada perikatan. Pembayaran ganti rugi yang harus dapat dibuktikan oleh pasien bahwa terdapat wanprestasi dalam pelayanan telemedisin (Primavita et al., 2021).

Gangguan teknologi, komunikasi antara pasien dan dokter yang kurang optimal, serta regulasi yang ada belum cukup komprehensif merupakan faktor yang menyebabkan terjadinya kesalahan diagnosis. Faktor tambahan meliputi kesulitan dalam menilai kondisi fisik pasien secara akurat tanpa pemeriksaan langsung dan keterbatasan informasi yang diberikan pasien secara virtual. Kesalahan diagnosis dapat menyebabkan kerugian materiil seperti biaya pengobatan lanjutan dan kerugian immateriil seperti penurunan kualitas hidup (Listyaningrum et al., 2024).

Tanggung jawab perdata rekam medis elektronik menuntut penyelenggara layanan kesehatan bertanggungjawab atas segala kebocoran informasi pribadi pasien. Dalam tele-ICU, tanggung jawab hukum atas kerugian dapat bermanifestasi sebagai liabilitas perdata yang mensyaratkan kompensasi moneter atas kerugian yang ditimbulkan akibat wanprestasi atau perbuatan melawan hukum seperti malapraktik medis. Gugatan perdata ini diajukan untuk memastikan kompensasi moneter atas kerugian, biaya, dan keuntungan yang hilang sebagaimana diatur dalam undang-undang. Tanggung jawab hukum secara perdata atas layanan telemedisin merujuk ke Pasal 66 UU Praktik Kedokteran. Formulasi Pasal 66 menyatakan bahwa setiap orang yang mengetahui atau kepentingannya dirugikan atas tindakan dokter atau dokter gigi saat menjalankan praktik kedokteran maka dapat melakukan pengaduan secara tertulis ke Ketua. Tanggung jawab perdata juga dapat didasarkan pada wanprestasi dan Pasal 38 Ayat (1) UU ITE (Primavita et al., 2021).

Sebagai penyedia layanan kesehatan digital, platform telemedisin dapat bertanggung jawab secara perdata apabila terbukti kesalahan diagnosis diakibatkan oleh kesalahan sistem dalam platform. Sistem elektronik harus diberi batasan hanya mengenai tanggung jawab yang didasarkan pada wanprestasi dan Pasal 38 Ayat (1) UU ITE. Tanggung jawab platform meliputi kegagalan dalam menyediakan sistem yang aman, ketiadaan fitur verifikasi identitas pasien, dan tidak adanya mekanisme mitigasi risiko teknis (Ardiansyah et al., 2024).

Penyelesaian masalah antara pasien dan penyedia layanan konsultasi kesehatan online dapat dilakukan melalui pengaduan ke Majelis Kehormatan Disiplin Kedokteran Indonesia, gugatan perbuatan melawan hukum, serta penyelesaian melalui pengadilan

atau di luar pengadilan. Bentuk tanggung jawab hukum dokter terhadap pelayanan telemedisin pada struktur peraturan perundang-undangan Indonesia dapat berupa tanggung jawab hukum perdata, hukum pidana, dan hukum administrasi. Pasien dapat memilih jalur hukum perdata untuk mendapatkan ganti rugi materiil dan immateriil (Nurdin, 2015).

Bentuk tanggung jawab hukum tenaga medis dan tenaga kesehatan sebagai mitra platform kesehatan digital dalam pelayanan telemedisin di Indonesia meliputi pertanggungjawaban hukum pidana, perdata, dan administratif. Tenaga medis tetap memiliki tanggung jawab hukum personal sebagaimana yang diatur dalam rumusan Pasal 1365 KUHPerdata. Kerugian pasien atas tindakan dokter baik atas kelalaian maupun kesalahan medis akan dipertanggungjawabkan secara personal (Setyo, 2024). Diperlukan penguatan regulasi terkait standar layanan telemedisin guna memberikan kepastian hukum bagi tenaga medis dan perlindungan bagi pasien dalam konteks hukum perdata. Standar profesi yang terukur harus menjadi bagian dari prinsip hukum penggunaan telemedisin baik oleh dokter Indonesia maupun bagi dokter asing. Regulasi yang mengatur mengenai tanggung jawab dokter pada praktik telemedisin belum mengatur secara spesifik tentang standar profesi dalam penggunaan telemedisin (Listyaningrum et al., 2024).

Aspek akuntabilitas hukum dalam kasus dugaan malpraktik melalui layanan telemedisin juga masih belum memiliki kejelasan regulasi. Regulasi yang ada belum sepenuhnya mengatur tanggung jawab hukum antara tenaga medis, fasilitas kesehatan, dan penyedia platform. Pembiayaan telemedisin belum terintegrasi dalam sistem Jaminan Kesehatan Nasional yang juga berdampak pada akses pasien terhadap penyelesaian hukum perdata (Wijaya et al., 2025).

Landasan hukum melalui Permenkes Nomor 20 Tahun 2019 tentang Penyelenggaraan Telemedisin belum mengatur tanggung jawab hukum antara tenaga medis, fasilitas kesehatan, dan penyedia platform. Indonesia saat ini belum memiliki undang-undang teknologi yang secara eksplisit mengendalikan telehealth atau regulasi perlindungan data yang cocok untuk mengelola volume data maksimal dari layanan kesehatan digital (Setyo, 2024). Ketiadaan regulasi spesifik membuat pasien kesulitan dalam membuktikan wanprestasi atau PMH dalam kasus telemedisin tidak terstandar.

Ilustrasi kasus kesalahan diagnosis melalui telekonsultasi yang menyebabkan kerugian pasien menunjukkan perlunya standar layanan yang jelas. Kesalahan diagnosis dapat berakibat pada penatalaksanaan yang tidak tepat, peningkatan kondisi penyakit, dan bahkan kematian pasien. Contoh kasus ini menunjukkan urgensi penguatan regulasi dan standar telemedisin untuk melindungi hak perdata pasien dalam layanan kesehatan digital.

Kesimpulan

Penyalahgunaan data pasien di era digital merupakan kejahatan kesehatan yang memerlukan pendekatan hukum pidana komprehensif berdasarkan UU Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi dan UU ITE. Bentuk penyalahgunaan meliputi kebocoran data medis, penjualan data tanpa izin, dan akses ilegal oleh pihak tidak berwenang yang memenuhi unsur tindak pidana dengan elemen kesengajaan dan kelalaian berat. Fasilitas kesehatan, tenaga medis, dan platform digital kesehatan dapat dituntut tanggung jawab pidana dengan sanksi pidana penjara maksimal 8 tahun dan/atau denda maksimal Rp800 juta untuk akses ilegal, serta pencabutan izin dan pembayaran ganti rugi.

Telemedisin yang tidak terstandar menimbulkan tanggung jawab perdata berdasarkan Pasal 1365 KUHPerdata (perbuatan melawan hukum) dan Pasal 1243 KUHPerdata (wanprestasi) ketika menyebabkan kesalahan diagnosis, terapi tidak memadai, atau ketiadaan informed consent digital yang sah. Pertanggungjawaban perdata dapat dikenakan pada tenaga medis secara personal dan platform telemedisin apabila terbukti kesalahan disebabkan oleh kesalahan sistem platform. Pasien berhak menuntut ganti rugi materiil dan immateriil melalui jalur pengadilan atau di luar pengadilan setelah melakukan pengaduan ke Majelis Kehormatan Disiplin Kedokteran Indonesia.

Keterkaitan antara aspek pidana dan perdata menunjukkan bahwa kejahatan kesehatan digital merupakan kejahatan kompleks yang memerlukan penegakan hukum ganda. Kelemahan regulasi terlihat dari ketiadaan undang-undang teknologi yang secara eksplisit mengendalikan telehealth dan regulasi perlindungan data yang belum komprehensif untuk mengelola volume data masial dari layanan kesehatan digital. Diperlukan penguatan regulasi standar layanan telemedisin, peningkatan keamanan sistem data kesehatan, pengawasan terhadap platform digital kesehatan, serta edukasi tenaga kesehatan dan masyarakat untuk memperkuat ekosistem perlindungan data pribadi dan kepastian hukum dalam layanan kesehatan digital.

References

- Ardiansyah, N. D., Gunawan, B. P., & Siswono, D. (2024). PENERAPAN UU ITE DALAM PENEGAKAN HUKUM SIBER DI INDONESIA Studi Kasus Pada Pasal 27 Hingga Pasal 37. *Jurnal Reformasi Hukum: Cogito Ergo Sum*, 7(2), 17–22. <https://doi.org/10.51804/jrhces.v7i2.16729>
- Eliyah, E., & Aslan, A. (2025). STAKE'S EVALUATION MODEL: METODE PENELITIAN. *Prosiding Seminar Nasional Indonesia*, 3(2), Article 2.
- Hamzah, I. F. (2024). Telekesehatan dan Telemedisin: Perspektif Hukum Kesehatan. *Jurnal Ilmu Sosial Dan Pendidikan*, 2(2), 125–131.
- Kuspraningrum, E. (2011). Keabsahan Kontrak Elektronik Dalam UU ITE Ditinjau Dari Pasal 1320 KUHPerdata dan UNCITRAL Model Law On Electronic Commerce. *Risalah Hukum*, 64–76.

- Listyaningrum, N., Lukman, D. R. K., Alfarizi, L. M., Awaludin, & Sukarno. (2024). Perlindungan Hukum Pasien Telemedicine Yang Menderita Kerugian Akibat Salah Diagnosis Dalam Platform Kesehatan Online. *Unizar Law Review*, 7(2), 185–195. <https://doi.org/10.36679/ulr.v7i2.79>
- Nurdin, M. (2015). PERLINDUNGAN HUKUM TERHADAP PASIEN ATAS KORBAN MALPRAKTEK KEDOKTERAN. *Jurnal Hukum Samudra Keadilan*, 10(1), 92–109.
- Primavita, S., Alawiya, N., & Afwa, U. (2021). TANGGUNG JAWAB HUKUM DOKTER DALAM PELAYANAN TELEMEDICINE. *Soedirman Law Review*, 3(4). <https://doi.org/10.20884/1.slr.2021.3.4.103>
- Puspita, D., Wijayanti, E., & Jaeni, A. (2024). Tanggung Jawab Hukum Perawat pada Pendokumentasian Asuhan Keperawatan dalam Rekam Medis Elektronik (RME). *JURNAL SYNTAX IMPERATIF: Jurnal Ilmu Sosial Dan Pendidikan*, 5(5), 1074–1082. <https://doi.org/10.36418/syntaximperatif.v5i5.520>
- Ratih, R. P. S., Dodi, D. J. W., Ifahda, I. P. H., Deni, D. S., & Eka, E. N. (2026). Blockchain-Based Therapeutic Agreement Model For Patient Legal Protection in Telemedicine. *Jurnal Ius Constituendum*, 11(1), 125–139. <https://doi.org/10.26623/jic.v11i1.13047>
- Respati, A. A. (2024). Reformulasi UU ITE terhadap Artificial Intelligence Dibandingkan dengan Uni Eropa dan China AI Act Regulation. *JURNAL USM LAW REVIEW*, 7(3), 1737–1758. <https://doi.org/10.26623/julr.v7i3.10578>
- Septiari, N., & Ujianti, N. M. P. (2025). Kekuatan hukum perjanjian elektronik dalam perspektif KUH Perdata dan UU ITE. *Indonesian Journal of Law and Justice*, 2(4), 10–10.
- Setyo, F. (2024). Analisis Regulasi Telemedicine: Perlindungan Hukum dan Implikasi bagi Tenaga Kesehatan. *Proceeding Masyarakat Hukum Kesehatan Indonesia*, 1(01), 149–158.
- Suyudi, G. A., Wildana, D. T., Prihatmini, S., & Puspaningrum, G. (2025). Kebijakan Formulasi dan Prospektif Penegakan Hukum Tindakan Kealpaan Tenaga Medis/Tenaga Kesehatan (Dinamika Pertanggungjawaban Pidana dalam Malpraktik Medis). *Jurnal Pembangunan Hukum Indonesia*, 7(2), 228–249. <https://doi.org/10.14710/jphi.v7i2.49-70>
- Taylor, R. D. (2020). “Data localization”: The internet in the balance. *Telecommunications Policy*, 44(8), 102003. <https://doi.org/10.1016/j.telpol.2020.102003>
- Truli, E. (2018). The General Data Protection Regulation and Civil Liability. In M. Bakhoun, B. Conde Gallego, M.-O. Mackenrodt, & G. Surblytė-Namavičienė (Eds.), *Personal Data in Competition, Consumer Protection and Intellectual Property Law: Towards a Holistic Approach?* (pp. 303–329). Springer. https://doi.org/10.1007/978-3-662-57646-5_12
- Tsolakis, N., Schumacher, R., Dora, M., & Kumar, M. (2023). Artificial intelligence and blockchain implementation in supply chains: A pathway to sustainability and data monetisation? *Annals of Operations Research*, 327(1), 157–210. <https://doi.org/10.1007/s10479-022-04785-2>
- Ventura, M., & Coeli, C. M. (2018). Beyond privacy: The right to health information, personal data protection, and governance. *Cadernos de Saúde Pública*, 34, e00106818. <https://doi.org/https://doi.org/10.1590/0102-311X00106818>

- Versaci, G. (2018). Personal Data and Contract Law: Challenges and Concerns about the Economic Exploitation of the Right to Data Protection. *European Review of Contract Law*, 14(4), 374–392. <https://doi.org/10.1515/ercl-2018-1022>
- Vila Seoane, M. F. (2021). Data securitisation: The challenges of data sovereignty in India. *Third World Quarterly*, 42(8), 1733–1750. <https://doi.org/10.1080/01436597.2021.1915122>
- Wijaya, H., Pardede, C. D., & Sinambela, H. (2025). Rekonstruksi Perlindungan Hukum bagi Dokter dalam Praktik Telemedicine: Perspektif Undang-Undang Nomor 17 Tahun 2023 tentang Kesehatan. *Jurnal Hukum Lex Generalis*, 6(12). <https://doi.org/10.56370/jhlhg.v6i12.1889>
- Xiaying, M. (2019). The Legal Attributes of Electronic Data and the Positioning of Data in Civil Law*. *Social Sciences in China*, 40(1), 82–99. <https://doi.org/10.1080/02529203.2018.1519208>
- Yu, X., & Zhao, Y. (2019). Dualism in data protection: Balancing the right to personal data and the data property right. *Computer Law & Security Review*, 35(5), 1053–18. <https://doi.org/10.1016/j.clsr.2019.04.001>
- Yudha, Sahril, I., & Atmadja, D. A. R. W. (2025). Perlindungan Data Pribadi Konsumen, Dokumen dan Tanda Tangan Elektronik yang Dipergunakan oleh Pihak Ketiga dalam Transaksi E-Commerce. *CENDEKIA : Jurnal Penelitian Dan Pengkajian Ilmiah*, 2(2), 173–189. <https://doi.org/10.62335/cendekia.v2i2.897>
- Zamani, E. D., Smyth, C., Gupta, S., & Dennehy, D. (2023). Artificial intelligence and big data analytics for supply chain resilience: A systematic literature review. *Annals of Operations Research*, 327(2), 605–632. <https://doi.org/10.1007/s10479-022-04983-y>
- Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. *Peraturan BPK*.
- Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Perlindungan
- Undang-Undang Republik Indonesia Nomor 29 Tahun 2004 tentang Praktik Kedokteran.
- Undang-Undang Republik Indonesia Nomor 36 Tahun 2009 tentang Kesehatan.