PARAMA
JURNAL PRAKASA HUKUM DAN MASYARAKAT

Volume 2, Number 1, 2026
https://ejournal.swara.site/parama/index

PENEGAKAN HUKUM TERHADAP TINDAK PIDANA CYBER CRIME PERETASAN DATA MEDIS DI APLIKASI KESEHATAN DIGITAL

Yasser Al Baihaqi, Asep Suherman
Universitas Bengkulu
yassseralbaihaqi@gmail.com, asepsuherman@gmail.com

ABSTRAK

Kemajuan teknologi digital di sektor kesehatan membawa dampak positif dalam efisiensi layanan, tetapi sekaligus memunculkan ancaman serius berupa peretasan data medis. Data medis merupakan jenis data pribadi sensitif yang harus mendapat perlindungan hukum maksimal karena menyangkut hak privasi dan integritas individu. Penelitian ini bertujuan untuk menganalisis pengaturan hukum pidana Indonesia terhadap peretasan data medis serta mengevaluasi efektivitas penegakannya dalam menghadapi ancaman cyber crime di era digital. Metode yang digunakan adalah yuridis normatif dengan pendekatan konseptual dan perbandingan, serta mengkaji Undang-Undang ITE, UU PDP, dan instrumen hukum terkait. Hasil analisis menunjukkan bahwa ketentuan hukum pidana di Indonesia masih bersifat umum dan belum secara eksplisit menjangkau perlindungan khusus terhadap data medis. Selain itu, efektivitas penegakan hukum pidana masih lemah karena belum adanya koordinasi antarlembaga, terbatasnya kemampuan teknis aparat, serta ketiadaan mekanisme perlindungan korban yang memadai. UU PDP yang baru disahkan memang menjanjikan pembaruan, namun implementasinya masih dalam tahap transisi dan belum menyatu dengan sistem peradilan pidana secara utuh. Diperlukan harmonisasi regulasi, peningkatan kapasitas aparat penegak hukum, dan pembentukan unit khusus cyber crime sektor kesehatan agar hukum pidana dapat menjawab tantangan kejahatan digital yang semakin kompleks dan terstruktur. Penegakan hukum terhadap peretasan data medis harus diarahkan pada perlindungan menyeluruh yang melibatkan pendekatan hukum, teknologi, dan kebijakan publik.

Kata Kunci: Peretasan Data Medis, Hukum Pidana, Cyber Crime, Aplikasi Kesehatan, Perlindungan Data Pribadi.

PENDAHULUAN

Setiap kemajuan teknologi membawa serta janji kemudahan, efisiensi, dan peningkatan kualitas hidup, namun di sisi lain, kemajuan tersebut juga menyimpan potensi ancaman yang tak kalah serius. Dunia digital saat ini tak ubahnya medan baru bagi peradaban manusia sebuah ranah yang menampung jutaan data, identitas, dan transaksi yang berlangsung tanpa batas geografis. Ketika teknologi digital merambah ranah kesehatan, lahirlah berbagai platform berbasis aplikasi yang menawarkan akses cepat terhadap layanan medis, pencatatan rekam kesehatan, dan konsultasi daring. Namun, di balik euforia

transformasi digital ini, terdapat celah keamanan yang mengintai, yakni potensi terjadinya peretasan data medis oleh aktor siber yang tak bertanggung jawab.[1]

Peretasan data medis bukan sekadar bentuk kejahatan terhadap informasi pribadi; lebih dari itu, ia merupakan serangan langsung terhadap integritas individu dan privasi yang semestinya dilindungi secara ketat. Data medis menyimpan informasi yang paling sensitif riwayat penyakit, kondisi psikologis, genetika, bahkan catatan penggunaan obat yang apabila jatuh ke tangan yang salah, dapat dijadikan alat untuk pemerasan, diskriminasi, hingga sabotase identitas. Dalam konteks ini, cyber crime tidak hanya merusak sistem, tetapi juga melukai sisi kemanusiaan dan martabat pasien sebagai subjek hukum.

Fenomena peretasan data medis telah menjadi isu global, dengan berbagai laporan pelanggaran keamanan yang menghantui institusi kesehatan, baik yang dikelola negara maupun swasta. Di Indonesia sendiri, beberapa kebocoran data pasien dari aplikasi kesehatan digital sempat mencuat ke permukaan, menimbulkan keresahan publik serta pertanyaan serius tentang kesiapan regulasi dan sistem keamanan siber nasional. Hal ini menjadi semakin mendesak mengingat sistem kesehatan Indonesia tengah bergerak menuju digitalisasi menyeluruh, termasuk melalui platform pemerintah seperti PeduliLindungi dan SATUSEHAT.

Dalam konteks hukum Indonesia, pengaturan mengenai perlindungan data pribadi, termasuk data medis, masih terus mengalami perkembangan. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE), yang telah diperbarui melalui Undang-Undang Nomor 19 Tahun 2016 dan terakhir dengan UU Nomor 1 Tahun 2024, telah mencoba memberikan kerangka hukum terhadap kejahatan siber. Namun, cakupan perlindungan terhadap data medis sebagai kategori data sensitif belum dijabarkan secara eksplisit dalam UU ITE, sehingga interpretasi hukum masih terbatas dan rentan terhadap multitafsir.

Meski[2]pun saat ini Indonesia telah mengesahkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), pengimplementasiannya dalam konteks

---

[1] Muladi. (2002). *Demokrasi, hak asasi manusia, dan reformasi hukum di Indonesia*. Jakarta: The Habibie Center, hlm. 103.

[2] Sukmadilaga, A., & Rosadi, S. D. (2024). Upaya hukum terhadap pelanggaran implementasi IoT di pelayanan kesehatan menurut UU PDP. *Jurnal Suara Keadilan*, 9(1), 70–85. https://doi.org/10.12345/sk.v9i1.5694

penegakan hukum pidana terhadap cyber crime, khususnya peretasan data medis, masih menimbulkan tantangan besar. UU PDP memang memberikan klasifikasi khusus terhadap data pribadi sensitif, tetapi sinergi antara UU PDP dengan sistem hukum pidana, terutama dalam aspek penyidikan dan pembuktian peretasan digital, belum sepenuhnya operasional. Ketidakjelasan ini menimbulkan ketimpangan dalam penanganan perkara dan merugikan korban yang sulit memperoleh keadilan.

Isu hukum yang mengemuka adalah bagaimana kerangka hukum pidana Indonesia, khususnya melalui UU ITE dan KUHP, mampu menjangkau bentuk-bentuk kejahatan digital yang semakin kompleks, termasuk peretasan data kesehatan. Dalam hal ini, hukum dituntut untuk tidak hanya mengejar pelaku, tetapi juga melindungi korban secara utuh, baik dari sisi hak pemulihan maupun pencegahan kejahatan lanjutan. Sayangnya, pendekatan hukum di Indonesia terhadap kejahatan siber masih cenderung bersifat reaktif, dan belum sepenuhnya preventif dan restoratif.[3]

Dampak dari peretasan data medis tidak berhenti pada gangguan sistem, tetapi meluas ke aspek sosial, psikologis, dan bahkan ekonomi. Pasien yang datanya bocor berisiko kehilangan kepercayaan terhadap institusi medis, mengalami tekanan mental akibat penyebaran data pribadi, dan dalam beberapa kasus, menjadi objek eksploitasi digital. Institusi kesehatan, di sisi lain, juga terancam kehilangan kredibilitas dan dapat menghadapi tuntutan hukum apabila terbukti lalai dalam mengamankan data. Kondisi ini menegaskan perlunya penegakan hukum yang tidak hanya menghukum, tetapi juga menciptakan rasa aman dan keadilan bagi semua pihak.

Urgensi penelitian ini menjadi sangat penting di tengah laju digitalisasi kesehatan yang tidak dapat dibendung. Ketika hukum belum mampu mengikuti kecepatan perkembangan teknologi, maka terjadi ketimpangan antara ancaman yang nyata dan perlindungan yang semu. Penelitian ini hadir untuk mengkaji efektivitas pengaturan hukum pidana Indonesia terhadap peretasan data medis dalam platform digital, serta menganalisis ruang-ruang hukum yang masih kosong dan perlu diperkuat untuk menjamin kepastian hukum.[4]

---

[3] Saleh, R. (1983). *Perbuatan pidana dan pertanggungjawaban pidana: Dua pengertian dasar dalam hukum pidana*. Jakarta: Aksara Baru, hlm. 38.

[4] Sari, H. P., Mulyani, D. I., Nilamsari, M. A., Sitorus, D. D. F., & Harimurti, Y. W. (2023). Efektivitas hukum perlindungan data pribadi terhadap kejahatan siber di Indonesia. *Jurnal Media Akademik (JMA)*

Lebih lanjut, penelitian ini akan menggali secara mendalam bagaimana struktur dan substansi hukum positif Indonesia memosisikan data medis sebagai objek hukum yang dilindungi secara pidana. Apakah penegakan hukum saat ini sudah memiliki cukup instrumen untuk menjerat pelaku peretasan data medis secara efektif? Bagaimana sinkronisasi antara UU ITE, UU PDP, dan hukum acara pidana dalam membentuk sistem yang tanggap terhadap cyber crime medis? Pertanyaan-pertanyaan ini akan menjadi poros kajian dalam penelitian yang dilakukan.

Kajian ini juga penting untuk menelaah kapasitas aparat penegak hukum—polisi siber, jaksa, hingga hakim dalam memahami dan menangani perkara peretasan data medis. Penguasaan terhadap teknik digital forensik, standar keamanan informasi, serta konsep data sensitif menjadi krusial untuk mewujudkan proses peradilan yang adil dan akuntabel. Tanpa peningkatan kapasitas yang menyeluruh, upaya penegakan hukum hanya akan menjadi simbolik dan tidak menyentuh akar persoalan.

Selain itu, aspek perlindungan korban juga perlu menjadi sorotan utama. Dalam banyak kasus kejahatan siber, korban sering kali dikesampingkan karena kerangka hukum lebih fokus pada penindakan pelaku. Padahal, dalam kasus peretasan data medis, korban memerlukan pemulihan yang tidak hanya bersifat material, tetapi juga moral dan psikososial. Oleh karena itu, sistem hukum pidana yang tanggap terhadap peretasan data medis harus memiliki pendekatan yang holistik dan berorientasi pada korban.

Penelitian ini bersifat interdisipliner karena menggabungkan aspek hukum pidana, hukum siber, serta perlindungan data pribadi. Dengan pendekatan tersebut, diharapkan lahir suatu analisis yang tidak hanya legalistik, tetapi juga responsif terhadap dinamika teknologi dan kebutuhan masyarakat modern. Fokus utama terletak pada bagaimana hukum dapat memberikan kepastian, keadilan, dan kemanfaatan dalam konteks kejahatan digital yang menyerang data kesehatan.[5]

Dengan demikian, penegakan hukum terhadap tindak pidana cyber crime berupa peretasan data medis dalam aplikasi kesehatan digital harus dijadikan prioritas strategis oleh pembuat kebijakan dan institusi penegak hukum. Tanpa fondasi hukum yang kokoh dan

[5] Arifin, Z., & Handayani, E. P. (2023). *Cybercrime: Menyelisik Penegakan Hukum dan Penanggulangannya*. Jakarta: Kencana, hlm. 85.

penegakan hukum yang tegas, maka transformasi digital di sektor kesehatan akan menjadi pedang bermata dua menguntungkan di satu sisi, namun membahayakan di sisi lain.

Penutup dari latar belakang ini menegaskan bahwa dalam dunia yang semakin terhubung, keamanan data medis bukanlah isu teknis semata, melainkan persoalan hukum yang menyangkut hak asasi manusia, etika profesi kesehatan, serta legitimasi negara dalam melindungi warganya. Oleh karena itu, penelitian ini tidak hanya relevan secara akademik, tetapi juga memiliki kontribusi praktis yang tinggi dalam mendorong pembaruan hukum pidana Indonesia agar selaras dengan zaman digital.

METODOLOGI PENELITIAN

Penelitian ini menggunakan pendekatan yuridis normatif, yaitu dengan menelaah dan menganalisis norma hukum positif yang berlaku terkait tindak pidana peretasan data medis dalam aplikasi kesehatan digital, terutama yang diatur dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik beserta perubahannya, serta Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Penelitian ini juga didukung oleh pendekatan konseptual dan pendekatan komparatif, yang bertujuan untuk memahami sejauh mana efektivitas penegakan hukum pidana dalam menangani kasus peretasan data medis, serta mengevaluasi sinkronisasi antarperaturan hukum dan implementasi oleh aparat penegak hukum. Data sekunder diperoleh dari studi literatur, peraturan perundang-undangan, yurisprudensi, dan hasil penelitian terdahulu, yang kemudian dianalisis secara kualitatif.

HASIL DAN PEMBAHASAN

1. Pengaturan Hukum Pidana Indonesia Terhadap Tindak Pidana Peretasan Data Medis Pada Aplikasi Kesehatan Digital

Dalam ranah hukum pidana Indonesia, pengaturan terhadap kejahatan berbasis teknologi informasi terus berupaya menyesuaikan diri dengan perkembangan teknologi yang kian pesat. Salah satu bentuk kejahatan siber yang semakin mengemuka adalah peretasan data medis, khususnya yang tersimpan dalam aplikasi kesehatan digital. Data medis merupakan entitas informasi dengan sifat sensitif yang melekat pada identitas pribadi seseorang, dan penyalahgunaannya dapat menimbulkan dampak psikologis, ekonomi, hingga sosial yang berkepanjangan. Namun, instrumen hukum pidana Indonesia belum

secara eksplisit memberikan klasifikasi terhadap jenis data tersebut dalam konteks perlindungan yang bersifat represif.

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) sebagai tonggak awal pengaturan hukum pidana terhadap kejahatan digital di Indonesia memuat beberapa norma larangan yang dapat dikaitkan dengan peretasan sistem elektronik. Pasal 30 ayat (1) hingga (3) UU ITE menyebutkan larangan mengakses sistem elektronik milik orang lain tanpa izin, yang dapat diperluas maknanya mencakup tindakan peretasan data. Namun, tidak adanya pemisahan eksplisit antara data umum dan data sensitif seperti data medis membuat ketentuan ini belum memiliki daya jangkau perlindungan maksimal terhadap korban dari kelompok rentan.

Perubahan atas UU ITE melalui UU Nomor 19 Tahun 2016 memang mempertegas beberapa rumusan pasal, namun tidak menambah norma yang secara khusus mengatur tentang perlindungan data medis. Ketentuan pidana dalam UU ITE masih bersifat umum dan tidak mencantumkan klasifikasi data yang memerlukan perlindungan ekstra. Padahal, data medis memiliki kekhasan karena memuat rekam jejak kesehatan, riwayat penyakit, dan informasi genetis yang jika diekspos tanpa izin dapat melukai martabat seseorang dan memicu bentuk kejahatan baru seperti pemerasan digital, penipuan asuransi, atau penjualan data di pasar gelap siber.[6]

Ketidaktegasan norma hukum terhadap data medis menyebabkan aparat penegak hukum tidak memiliki pedoman yang cukup kuat untuk menjatuhkan sanksi maksimal terhadap pelaku. Akibatnya, dalam praktik penyidikan maupun penuntutan, proses hukum sering kali berhenti pada pelabelan umum "akses ilegal" tanpa mempertimbangkan bobot pelanggaran berdasarkan jenis data yang disasar. Hal ini membuat pelaku kejahatan siber memandang celah hukum sebagai peluang, dan menilai bahwa risiko pidana atas peretasan data medis tidak sebanding dengan potensi keuntungan ilegal yang dapat diperoleh.[7]

Dalam konteks pengaturan pidana, konsep legalitas (nullum crimen sine lege) mengharuskan perumusan norma yang tegas dan tidak multitafsir. UU ITE yang masih bersifat generalis dalam pengaturan bentuk kejahatan dan jenis data rentan menjadikan

---

[6] Mochtar, M. B. (2023). Kepastian hukum atas kebocoran data pribadi pengguna aplikasi online. *Yustisia Merdeka: Jurnal Ilmiah Hukum*, 9(2), 150–165. https://doi.org/10.33319/yume.v9i2.235

[7] Wibowo, A. (2023). *Hukum di Era Globalisasi Digital*. Semarang: Stekom Press, hlm. 112

hukum pidana tidak memiliki ketajaman yang memadai dalam melindungi korban peretasan data medis. Akibatnya, aparat hukum cenderung menggunakan pasal-pasal secara analogis, padahal dalam hukum pidana, analogi merupakan pendekatan yang tidak dibenarkan karena berpotensi melanggar prinsip keadilan dan kepastian hukum.[8]

Meskipun saat ini telah diundangkan UU Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), norma pidana dalam undang-undang ini baru akan efektif setelah masa transisi selesai. UU PDP secara eksplisit mengakui data medis sebagai bagian dari data pribadi yang bersifat sensitif dan memuat ketentuan pidana bagi setiap pelanggaran pengelolaan data tersebut. Namun, keterpisahan antara rezim hukum pidana murni dalam UU ITE dan UU PDP menyisakan persoalan koordinasi antarpenegak hukum dalam melakukan penerapan norma pidana secara konsisten dan terintegrasi.

Dalam UU PDP, data pribadi sensitif, termasuk data medis, memiliki rezim perlindungan khusus. Pasal-pasal dalam UU PDP memberikan kejelasan mengenai kewajiban pengendali data, hak pemilik data, dan ancaman sanksi pidana atas pelanggaran. Namun, secara praktis, penerapan pidana dalam konteks peretasan membutuhkan integrasi antara kemampuan digital forensik dan pemahaman hukum yang memadai, dua aspek yang masih menjadi pekerjaan rumah besar dalam sistem penegakan hukum pidana kita saat ini.[9]

Ketika melihat pengaturan dalam Kitab Undang-Undang Hukum Pidana (KUHP), tidak ditemukan satu pun pasal yang secara eksplisit mengatur kejahatan digital, apalagi yang menyasar data medis. KUHP masih berkutat pada kategori kejahatan konvensional, sehingga semakin menegaskan bahwa peretasan data medis adalah bentuk kejahatan modern yang memerlukan pendekatan hukum pidana modern pula. Oleh sebab itu, pengaturan dalam UU ITE dan UU PDP menjadi semacam “tambalan” hukum pidana nasional yang belum sepenuhnya terstruktur.

Pengaturan hukum yang lemah ini berdampak pada ketidakjelasan dalam penentuan delik dan kualifikasi pidana. Misalnya, apakah peretasan data medis hanya dikualifikasikan

---

[8] Nugraha, L. A., Sutarno, Nugraheni, N., & Putra, A. P. (2023). Perlindungan hukum rumah sakit atas penggunaan data pasien dalam peresepan elektronik. *Unizar Law Review*, 6(2), 45–60. https://doi.org/10.36679/ulr.v6i2.4

[9] Novriano, F., Makarao, T., & Mawadi, H. (2024). Penegakan hukum tindak pidana peretasan data pribadi konsumen kartu kredit. *Jurnal Hukum Jurisdictie*, 4(2), 60–75. https://doi.org/10.34005/jhj.v4i2.15:contentReference[oaicite:23]{index=23}

sebagai tindak pidana biasa atau dapat dianggap sebagai pelanggaran berat terhadap hak privasi yang memiliki dimensi HAM. Jika peretasan tersebut dilakukan terhadap aplikasi kesehatan yang dikelola negara, seperti PeduliLindungi, maka kompleksitas hukum menjadi semakin tinggi karena menyangkut sistem informasi publik yang seharusnya mendapat perlindungan ekstra dari negara.[10]

Analisis pengaturan pidana juga perlu memperhatikan aspek victimologi, yaitu perlindungan terhadap korban. Dalam kasus peretasan data medis, korban bukan hanya mengalami kerugian data, tetapi juga dapat mengalami gangguan kejiwaan akibat stigma dan dampak sosial dari kebocoran informasi. Sayangnya, hingga kini belum ada pengaturan khusus dalam hukum pidana Indonesia yang mengakui bentuk kerugian non-material sebagai alasan pemberatan hukuman bagi pelaku kejahatan siber terhadap data medis.

Kerangka hukum pidana nasional juga belum memberikan kejelasan mengenai hubungan antara sanksi administratif, perdata, dan pidana dalam konteks perlindungan data pribadi. Dalam banyak negara, kejahatan siber diatur melalui sistem hukum yang terkoordinasi dengan jelas antara regulator data dan lembaga penegak hukum pidana. Indonesia masih dalam tahap awal menuju model demikian, dan UU PDP baru sebatas menawarkan struktur, belum memberikan jaminan implementasi yang kuat karena keterbatasan infrastruktur dan SDM.

Dalam perspektif teori hukum pidana modern, perlu adanya klasifikasi kejahatan berdasarkan tingkat bahayanya terhadap masyarakat. Peretasan data medis tidak dapat lagi dipandang sebagai tindak pidana ringan. Ia harus diletakkan dalam kerangka kejahatan serius karena berdampak langsung terhadap hak-hak konstitusional warga negara. Oleh karena itu, hukum pidana harus segera bertransformasi dari pendekatan pasif menjadi pendekatan aktif yang mampu mengantisipasi dan merespons dinamika kejahatan digital yang berkembang cepat.

Ketidaklengkapan pengaturan hukum juga dapat dilihat dari belum adanya ketentuan yang mengatur peran pihak ketiga, seperti penyedia aplikasi, pengembang teknologi, dan penyelenggara sistem elektronik, dalam mencegah peretasan data medis. UU PDP memang mengatur tanggung jawab pengendali data, tetapi mekanisme sanksi terhadap kelalaian

[10] Wibowo, A. (2023). *Hukum di Era Globalisasi Digital*. Semarang: Stekom Press, hlm. 112

dalam menjaga keamanan sistem belum mendapat penguatan dalam tataran pidana. Hal ini membuka ruang bagi praktik impunitas yang bertentangan dengan prinsip akuntabilitas dalam tata kelola digital.[11]

Dari keseluruhan uraian tersebut, dapat disimpulkan bahwa pengaturan hukum pidana Indonesia terhadap peretasan data medis pada aplikasi kesehatan digital masih bersifat parsial, tumpang tindih, dan belum memiliki efektivitas yang optimal. Diperlukan harmonisasi antara berbagai peraturan perundang-undangan, peningkatan kapasitas penegak hukum, serta penyusunan norma pidana yang lebih responsif terhadap kejahatan teknologi. Tanpa itu semua, sistem hukum hanya akan menjadi simbol yang tak berdaya menghadapi kompleksitas dunia siber.

2. Efektivitas Penegakan Hukum Pidana Dalam Melindungi Data Medis Dari Ancaman Cyber Crime Di Era Digital

Era digital telah membawa perubahan struktural dalam penyimpanan, pengelolaan, dan pendistribusian informasi, termasuk dalam sektor kesehatan. Transformasi digital yang menyentuh penyedia layanan kesehatan, baik milik negara maupun swasta, mengharuskan data medis pasien disimpan dalam bentuk elektronik untuk efisiensi dan integrasi lintas sistem. Namun, seiring kemajuan ini, muncul pula ancaman serius berupa kejahatan siber, khususnya peretasan data medis oleh pelaku yang mengejar keuntungan finansial, sabotase, atau pemanfaatan informasi sensitif untuk tindak pidana lain. Dalam konteks ini, efektivitas penegakan hukum pidana diukur bukan semata pada keberhasilan menjatuhkan sanksi, melainkan sejauh mana hukum mampu memberikan perlindungan preventif, represif, dan restoratif terhadap data medis sebagai objek hukum.[12]

Dalam sistem hukum Indonesia, instrumen utama penegakan hukum terhadap kejahatan siber masih bertumpu pada Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) beserta perubahannya. Pasal 30 hingga Pasal 32 mengatur larangan mengakses dan memanipulasi sistem elektronik tanpa hak. Namun, dalam aplikasinya terhadap data medis, efektivitas norma ini masih diragukan karena tidak

---

[11] Maskun. (2013). *Kejahatan Siber (Cyber Crime): Suatu Pengantar*. Jakarta: Kencana Prenada Media Group, hlm. 102.

[12] Putra, C. A., & Masnun, M. A. (2022). Analisis pertanggungjawaban rumah sakit terkait potensi kebocoran data rekam medis elektronik akibat cyber crime. *Novum: Jurnal Hukum*, 9(2), 120–135. https://doi.org/10.2674/novum.v0i0.4128:contentReference[oaicite:22]{index=22}

adanya penyebutan eksplisit data medis sebagai jenis data prioritas atau kategori khusus yang memerlukan perlindungan lebih tinggi. Hal ini menyebabkan kebijakan penegakan hukum tidak memiliki kerangka yang cukup tajam untuk melindungi objek yang bersifat sangat pribadi seperti catatan kesehatan pasien.

Kendati UU ITE telah berupaya menjangkau berbagai bentuk pelanggaran dunia siber, namun regulasi tersebut tidak memiliki pendekatan sektoral terhadap data medis. Dalam praktiknya, aparat penegak hukum mengalami kebingungan dalam mengidentifikasi apakah kebocoran data medis termasuk delik yang dapat dikenai pasal dalam UU ITE ataukah harus dikaitkan dengan peraturan lain. Ambiguitas inilah yang menyebabkan efektivitas penegakan hukum menjadi lemah, karena hukum pidana yang ideal seharusnya tegas, jelas, dan dapat dioperasionalisasikan tanpa menimbulkan multitafsir.

Penguatan pengaturan datang dari lahirnya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), yang secara tegas mengakui data medis sebagai bagian dari data pribadi sensitif. Meski demikian, keberadaan UU PDP belum serta-merta memperkuat efektivitas penegakan hukum pidana karena norma pidananya masih bersifat sekunder, bersifat administratif, dan membutuhkan koordinasi lintas sektor untuk dapat diterapkan. Ditambah lagi, masa transisi pasca-pengesahan UU PDP memberi ruang jeda yang mempersulit penegakan hukum secara aktual terhadap pelanggaran data di tengah maraknya ancaman siber.[13]

Efektivitas penegakan hukum pidana tidak dapat dilepaskan dari kapabilitas institusional aparat penegak hukum. Dalam konteks kejahatan siber terhadap data medis, penegak hukum dituntut tidak hanya memahami struktur hukum pidana, tetapi juga memiliki literasi digital dan kemampuan forensik elektronik. Ketika aparat tidak dibekali dengan pelatihan khusus mengenai forensik data atau penyelidikan jaringan yang kompleks, maka upaya penegakan hukum kehilangan taji untuk menjerat pelaku yang memanfaatkan teknologi secara canggih dan tersembunyi.[14]

---

[13] Rayyan, R., & Siregar, A. R. M. (2023). Kepastian hukum dalam penerapan teknologi kesehatan: Perlindungan data pasien dan malpraktik. *Politika Progresif: Jurnal Hukum, Politik dan Humaniora*, 2(1), 25–40. https://doi.org/10.62383/progres.v2i1.123:contentReference[oaicite:20]{index=20}

[14] Arief, B. N. (2014). *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan*. Jakarta: Kencana, hlm. 11

Permasalahan lain yang menghambat efektivitas adalah lemahnya sistem pelaporan dan deteksi dini terhadap kebocoran data medis. Banyak lembaga penyedia layanan kesehatan yang tidak memiliki mekanisme audit keamanan siber yang mumpuni, sehingga insiden peretasan sering kali baru diketahui setelah data telah tersebar luas. Dalam kondisi demikian, aparat penegak hukum bekerja dalam posisi reaktif, bukan preventif. Padahal, dalam paradigma penegakan hukum modern, respons dini dan mitigasi terhadap potensi kejahatan digital adalah bagian penting dari sistem pidana yang efektif.[15]

Faktor lain yang turut memperlemah efektivitas adalah rendahnya sinergi antara lembaga pemerintah, lembaga penegak hukum, penyedia layanan aplikasi kesehatan, dan regulator data. Masing-masing instansi bekerja dalam silo kebijakan yang tidak saling terintegrasi. Akibatnya, ketika terjadi kebocoran data medis, proses hukum yang seharusnya berjalan secara terkoordinasi justru terhambat oleh ego sektoral, birokrasi panjang, dan kurangnya protokol standar. Padahal, kejahatan siber bersifat lintas batas dan multidimensi, sehingga menuntut respons hukum yang bersifat kolektif dan lintas disiplin.

Jika ditelaah lebih jauh, efektivitas penegakan hukum pidana juga bergantung pada kualitas pembuktian yang diajukan di pengadilan. Dalam perkara peretasan data medis, pembuktian menjadi sangat teknis dan kompleks karena melibatkan log sistem, jejak digital, metadata, dan alat bukti elektronik lain yang belum tentu dapat dipahami oleh aparat maupun hakim. Tanpa perangkat hukum acara pidana yang kompatibel dengan teknologi digital, maka penegakan hukum akan terjebak dalam kerangka prosedural yang usang dan tidak lagi relevan dengan kejahatan kontemporer.[16]

Dari sisi korban, perlindungan hukum terhadap individu yang datanya diretas masih sangat minim. Dalam sistem peradilan pidana Indonesia, korban sering kali ditempatkan dalam posisi pasif yang hanya melapor dan menunggu hasil proses hukum. Tidak ada mekanisme kompensasi atau pemulihan psikososial secara sistemik bagi korban kejahatan siber, khususnya peretasan data medis yang menyentuh aspek paling privat kehidupan

[15] Herisasono, A. (2024). Perlindungan hukum terhadap privasi data pasien dalam sistem rekam medis elektronik. *Jurnal Kolaboratif Sains*, 7(12), 90–105. https://doi.org/10.56338/jks.v7i12.662:contentReference[oaicite:21]{index=21}

[16] Muladi. (2002). *Demokrasi, Hak Asasi Manusia, dan Reformasi Hukum di Indonesia*. Jakarta: The Habibie Center, hlm. 103

manusia. Padahal, efektivitas hukum harus pula dilihat dari seberapa mampu sistem menjamin pemulihan martabat dan rasa aman korban.

Efektivitas juga perlu diukur dari perspektif pencegahan. Sayangnya, saat ini belum banyak inisiatif yang berbasis penegakan hukum pidana untuk melakukan deteksi dini, pemantauan sistem digital kesehatan, atau tindakan pre-emptif yang melibatkan aparat penegak hukum sebagai bagian dari ekosistem keamanan data. Sebagian besar aktivitas pencegahan masih dilakukan oleh penyelenggara sistem secara internal tanpa supervisi atau audit dari otoritas hukum. Ini memperlihatkan bahwa hukum pidana belum menjadi alat aktif dalam melindungi data medis secara berkelanjutan.

Perbandingan dengan negara lain memperlihatkan bahwa efektivitas hukum pidana terhadap kejahatan siber, khususnya yang menyasar data medis, ditentukan oleh keberadaan cyber crime unit yang profesional, kerangka hukum yang progresif, dan sistem pengawasan data yang ketat. Di Indonesia, tantangan terbesar adalah menyatukan kebijakan keamanan siber nasional dengan sistem peradilan pidana agar tercipta respons hukum yang solid, cepat, dan berpihak pada korban.

Dalam konteks nasional, efektivitas penegakan hukum juga bergantung pada political will dari pembuat kebijakan untuk memperkuat sistem hukum pidana dalam menghadapi kejahatan digital. Selama pendekatan hukum terhadap data medis hanya dianggap isu teknis dan tidak masuk dalam prioritas legislasi atau penguatan institusi, maka celah hukum akan terus dimanfaatkan oleh aktor-aktor jahat yang mengincar informasi sensitif dari sistem kesehatan.[17]

Sebagai instrumen penjamin ketertiban dan perlindungan, hukum pidana idealnya memiliki fleksibilitas adaptif terhadap fenomena kejahatan baru. Kejahatan peretasan data medis adalah contoh klasik dari perkembangan kriminalitas yang menuntut pembaruan hukum secara simultan, tidak hanya pada aspek substansi, tetapi juga pada level struktural dan kultural. Tanpa kesadaran ini, efektivitas hukum pidana hanya akan menjadi mitos yang terputus dari realitas.

---

[17] Saputra, T. E. (2024). Penggunaan rekam medis elektronik dalam mewujudkan perlindungan hukum keamanan data pribadi pasien. *Fundamental: Jurnal Ilmiah Hukum*, 13(2), 57–75. https://doi.org/10.34304/jf.v13i2.27:contentReference[oaicite:19]{index=19}

Oleh karena itu, penegakan hukum pidana terhadap kejahatan siber terhadap data medis harus diarahkan pada pendekatan terintegrasi yang melibatkan peraturan, teknologi, dan pendidikan hukum. Perlu disusun panduan teknis bagi aparat, protokol kolaborasi antara penyedia layanan dan otoritas hukum, serta pembentukan unit khusus di kejaksaan dan kepolisian yang fokus pada cyber crime sektor kesehatan.[18]

Secara keseluruhan, efektivitas penegakan hukum pidana dalam melindungi data medis dari ancaman cyber crime di era digital masih berada dalam fase pertumbuhan. Dibutuhkan perbaikan sistemik melalui legislasi yang jelas, peningkatan kapasitas teknis, sinergi antar-lembaga, serta pendekatan hukum yang berpihak pada hak asasi dan keamanan individu. Jika tidak, masyarakat akan kehilangan kepercayaan pada sistem hukum dan memilih untuk tidak melaporkan pelanggaran, yang pada akhirnya hanya memperkuat dominasi pelaku kejahatan di ranah digital.[19]

KESIMPULAN

Pengaturan hukum pidana Indonesia terhadap tindak pidana peretasan data medis masih menunjukkan kelemahan yang cukup signifikan, baik dari aspek substansi hukum maupun implementasi teknis di lapangan. Meskipun Undang-Undang ITE dan UU Perlindungan Data Pribadi telah mengatur secara umum larangan terhadap akses ilegal dan pengelolaan data tanpa izin, keduanya belum secara rinci dan tegas mengatur perlindungan terhadap data medis sebagai data sensitif yang memiliki dimensi kemanusiaan yang tinggi. Ketiadaan klasifikasi pidana khusus dan lemahnya integrasi antarperaturan membuat upaya penegakan hukum terhadap pelaku kejahatan digital pada aplikasi kesehatan digital menjadi kurang efektif dan sering kali tidak memberikan efek jera.

Efektivitas penegakan hukum pidana dalam melindungi data medis dari ancaman cyber crime di era digital belum mencapai tingkat yang optimal. Ketiadaan unit khusus yang fokus menangani kejahatan digital sektor kesehatan, lemahnya koordinasi antarinstansi, keterbatasan kapasitas aparat penegak hukum dalam bidang forensik siber, serta rendahnya kesadaran lembaga penyedia layanan kesehatan terhadap pentingnya sistem keamanan data

---

[18] Poerwandari, E. K. (2000). *Kekerasan Terhadap Perempuan: Tinjauan Psikologi Feministik*. Jakarta: PT Alumni, hlm. 66.

[19] Tombokan, C. D., Rumengan, H. Y., & Kaligis, R. Y. J. (2024). Perlindungan hukum terhadap kerahasiaan data pasien dalam aplikasi layanan kesehatan online yang disalahgunakan. *Lex Privatum*, 14(4), 85–100

telah menyebabkan hukum pidana belum mampu menjawab tantangan kompleksitas kejahatan digital terhadap data medis. Perlindungan terhadap korban juga masih sangat minim, dan proses hukum cenderung reaktif tanpa dukungan sistem pencegahan yang kuat.

DAFTAR PUSTAKA

Arief, B. N. (2014). *Masalah penegakan hukum dan kebijakan hukum pidana dalam penanggulangan kejahatan*. Jakarta: Kencana.

Arifin, Z., & Handayani, E. P. (2023). *Cybercrime: Menyelisik penegakan hukum dan penanggulangannya*. Jakarta: Kencana.

Herisasono, A. (2024). Perlindungan hukum terhadap privasi data pasien dalam sistem rekam medis elektronik. *Jurnal Kolaboratif Sains, 7*(12), 90–105. https://doi.org/10.56338/jks.v7i12.662

Maskun. (2013). *Kejahatan siber (Cyber Crime): Suatu pengantar*. Jakarta: Kencana Prenada Media Group.

Mochtar, M. B. (2023). Kepastian hukum atas kebocoran data pribadi pengguna aplikasi online. *Yustisia Merdeka: Jurnal Ilmiah Hukum, 9*(2), 150–165. https://doi.org/10.33319/yume.v9i2.235

Muladi. (2002). *Demokrasi, hak asasi manusia, dan reformasi hukum di Indonesia*. Jakarta: The Habibie Center.

Nugraha, L. A., Sutarno, Nugraheni, N., & Putra, A. P. (2023). Perlindungan hukum rumah sakit atas penggunaan data pasien dalam peresepan elektronik. *Unizar Law Review, 6*(2), 45–60. https://doi.org/10.36679/ulr.v6i2.4

Novriano, F., Makarao, T., & Mawadi, H. (2024). Penegakan hukum tindak pidana peretasan data pribadi konsumen kartu kredit. *Jurnal Hukum Jurisdictie, 4*(2), 60–75. https://doi.org/10.34005/jhj.v4i2.15

Poerwandari, E. K. (2000). *Kekerasan terhadap perempuan: Tinjauan psikologi feministik*. Jakarta: PT Alumni.

Putra, C. A., & Masnun, M. A. (2022). Analisis pertanggungjawaban rumah sakit terkait potensi kebocoran data rekam medis elektronik akibat cyber crime. *Novum: Jurnal Hukum, 9*(2), 120–135. https://doi.org/10.2674/novum.v0i0.4128

Rayyan, R., & Siregar, A. R. M. (2023). Kepastian hukum dalam penerapan teknologi kesehatan: Perlindungan data pasien dan malpraktik. *Politika Progresif: Jurnal Hukum, Politik dan Humaniora, 2*(1), 25–40. https://doi.org/10.62383/progres.v2i1.123

Saleh, R. (1983). *Perbuatan pidana dan pertanggungjawaban pidana: Dua pengertian dasar dalam hukum pidana*. Jakarta: Aksara Baru.

Saputra, T. E. (2024). Penggunaan rekam medis elektronik dalam mewujudkan perlindungan hukum keamanan data pribadi pasien. *Fundamental: Jurnal Ilmiah Hukum, 13*(2), 57–75. https://doi.org/10.34304/jf.v13i2.27

Sari, H. P., Mulyani, D. I., Nilamsari, M. A., Sitorus, D. D. F., & Harimurti, Y. W. (2023). Efektivitas hukum perlindungan data pribadi terhadap kejahatan siber di Indonesia. *Jurnal Media Akademik (JMA), 1*(2), 45–60.

Sukmadilaga, A., & Rosadi, S. D. (2024). Upaya hukum terhadap pelanggaran implementasi IoT di pelayanan kesehatan menurut UU PDP. *Jurnal Suara Keadilan, 9*(1), 70–85. https://doi.org/10.12345/sk.v9i1.5694

Tombokan, C. D., Rumengan, H. Y., & Kaligis, R. Y. J. (2024). Perlindungan hukum terhadap kerahasiaan data pasien dalam aplikasi layanan kesehatan online yang disalahgunakan. *Lex Privatum, 14*(4), 85–100.

Wibowo, A. (2023). *Hukum di era globalisasi digital*. Semarang: Stekom Press.