

**PERETASAN DATA PRIBADI DAN PEMBERIAN GANTI RUGI
KORBAN TINDAK PIDANA ILLEGAL AKSES DATA ELEKTRONIK
(STUDI PUTUSAN PENGADILAN NOMOR 610/PID.SUS/2022/PN
JKT.SEL)**

Kevin Ferrens Lordy*, A. M. Endah Sri Astuti, R. B. Sularto

Program Studi S1 Hukum, Fakultas Hukum, Universitas Diponegoro

*E-mail: kevinferrens03@gmail.com

Abstrak

Kebocoran data pribadi yang terjadi ditengah perkembangan teknologi yang semakin berkembang pesat ini merupakan efek samping dari perkembangan teknologi. Di tengah meningkatnya fenomena kejahatan siber di Indonesia, yang menempatkan negara ini di peringkat ketiga dunia dalam kasus kebocoran data yang akan menimbulkan efek kerugian serius bagi korban, penelitian ini bertujuan untuk mengkaji pertanggungjawaban pidana pelaku terhadap peretasan data dan perlindungan yang di dapat korban peretasan data pribadi. Penelitian ini bertujuan menganalisis penyelesaian tindak pidana illegal access terhadap data elektronik, mengidentifikasi hambatan dalam penegakan hukum, serta memberikan rekomendasi strategi peningkatan efektivitas penanganan melalui pendekatan hukum, teknologi, dan kolaborasi antar lembaga. Metode yang dipakai di dalam penelitian ini adalah metode penelitian doktrinal, hasil dari penelitian ini menunjukkan bahwa terdakwa terbukti secara sah mengakses sistem elektronik untuk memperoleh data elektronik dan korban dapat mendapatkan ganti rugi dengan cara penggabungan perkara, Meskipun demikian dalam putusan ini Majelis Hakim tidak memuat amar pemberian ganti rugi yang seharusnya dapat diberikan kepada para korban.

Katakunci : Peretasan Data Pribadi; Akses Ilegal; Ganti Rugi Korban; UU ITE; Putusan Pengadilan.

Abstract

The leakage of personal data that occurs amidst the rapid development of technology is a side effect of technological development. Amid the increasing phenomenon of cybercrime in Indonesia, which places this country in the third world ranking in cases of data leaks that will cause serious harm to victims, this study aims to examine the criminal liability of perpetrators for data hacking and the protection received by victims of personal data hacking. This study aims to analyze the resolution of the crime of illegal access to electronic data, identify obstacles in law enforcement, and provide recommendations for strategies to increase the effectiveness of handling through legal approaches, technology, and collaboration between institutions. The method used in this study is the doctrinal research method. The results of this study indicate that the defendant was proven to have legally accessed the electronic system to obtain electronic data and the victims can obtain compensation by consolidating the cases. However, in this decision the Panel of Judges did not include an order to award compensation that should have been given to the victims.

Keywords : Personal Data Hacking; Illegal Access; Victim Compensation; ITE Law; Court Decisions.

I. PENDAHULUAN

Indonesia merupakan negara hukum (Pasal 1 ayat 3 UUD 1945) yang menganut sistem hukum civil law (Romano-Germanik) dengan aturan tertulis sebagai dasar utama. Dalam konteks globalisasi dan Revolusi Industri 4.0 seperti dikemukakan Angela Merkel, muncul tantangan baru berupa digitalisasi dan kejahatan siber (cybercrime) yang kompleks.¹

Perlindungan hukum terhadap data pribadi dan korban kejahatan siber menjadi urgensi penting karena meningkatnya penyalahgunaan informasi pribadi oleh pihak yang tidak bertanggung jawab. UU ITE (No. 11 Tahun 2008 jo. UU No. 19 Tahun 2016) menjadi dasar hukum utama dalam penanganan kasus-kasus cybercrime, seperti ilegal akses, phishing, hacking, penyebaran konten ilegal, hingga penipuan online.² Namun, implementasi dan penegakan hukumnya di lapangan masih menghadapi kendala, terutama dalam pembuktian digital, pembaruan regulasi, dan keterampilan aparat penegak hukum.³

Dalam konsep perlindungan korban, hukum pidana dinilai masih berfokus pada pelaku, sehingga dibutuhkan pendekatan restoratif yang juga memperhatikan hak dan pemulihan bagi korban. Pasal 1365 KUH Perdata menyediakan dasar hukum bagi tuntutan perbuatan melawan hukum dan ganti rugi, baik dalam bentuk uang (kompensasi) maupun pengembalian keadaan semula (restitusi).⁴

Perbandingan dengan sistem hukum Inggris dan Jerman menunjukkan bahwa kedua negara tersebut memiliki regulasi dan lembaga penanganan kejahatan siber yang lebih terperinci dan terkoordinasi, misalnya melalui NCA dan NCCU di Inggris, serta aturan rinci mengenai ganti rugi dalam BGB Jerman. Sementara di Indonesia, kelembagaan dan regulasinya masih perlu diperkuat agar lebih adaptif terhadap perkembangan teknologi dan praktik internasional.

Berbagai kasus di Indonesia seperti tindak illegal access, manipulasi data BPJS, phishing perbankan, hingga putusan Pengadilan Negeri Jakarta Selatan Nomor 610/Pid.Sus/2022/PN JKT.SEL menunjukkan bahwa cybercrime berdampak nyata terhadap masyarakat dan institusi finansial. Kondisi ini menegaskan perlunya pembaruan hukum, peningkatan kapasitas aparat, kerja sama internasional, serta edukasi publik mengenai keamanan digital.

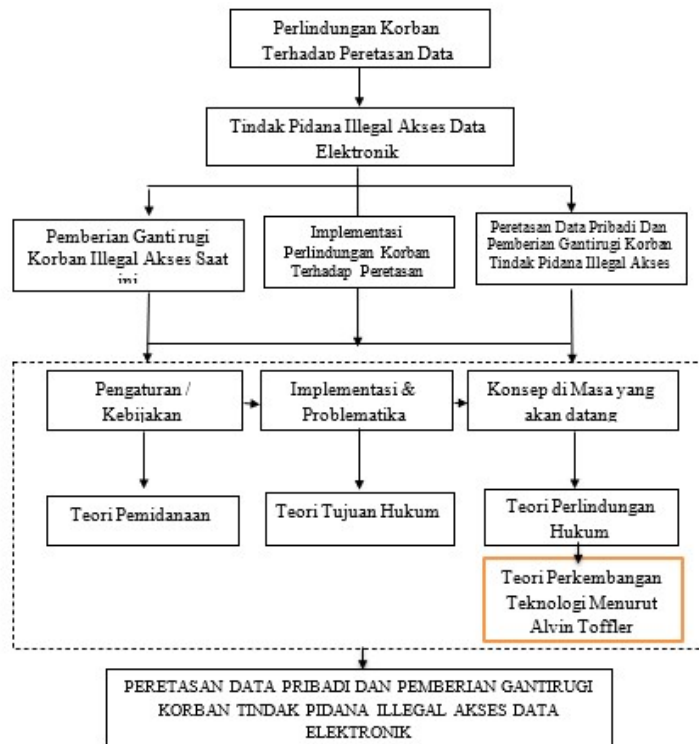
Penelitian ini bertujuan menganalisis penyelesaian tindak pidana *illegal access* terhadap data elektronik, mengidentifikasi hambatan dalam penegakan hukum, serta memberikan rekomendasi strategi peningkatan efektivitas penanganan melalui pendekatan hukum, teknologi, dan kolaborasi antar lembaga.

¹ Huala Adolf. (2002). *Aspek-aspek Negara dalam Hukum Internasional*. Jakarta: Rajawali Press, hlm 3.

² Badan Pembinaan Hukum Nasional. (2012). *Central Authority dan Mekanisme Koordinasi dalam Pelaksanaan Bantuan Timbal Balik dalam Masalah Pidana*, Jakarta: BPHN, hlm 69.

³ Ron Davies. 2015. *Industry 4.0 Digitalisation for Productivity and Growth*, European Parliamentary Research Service, PE 568.337, September.

⁴ M.A. Moegni Djojodirdjo, 1976, *Perbuatan Melawan Hukum*, Jakarta: Pradnya Paramita, Hlm.102



Gambar 1. Kerangka Pemikiran

Berdasarkan uraian latar belakang di atas, maka rumusan masalah yang diteliti adalah bagaimana pertanggungjawaban pidana pelaku peretasan data pribadi dalam putusan no 610/Pid.Sus/2022/PN JKT.SEL; dan bagaimana penerapan kebijakan perlindungan korban peretasan data pribadi atas hak ganti rugi dalam Putusan Nomor 610/Pid.Sus/2022/PN JKT.SEL.

II. METODE PENELITIAN

Metode penelitian yang digunakan dalam penelitian ini adalah metode pendekatan yuridis normatif, khususnya melalui pendekatan perundang-undangan dan pendekatan konsep. Pendekatan perundang-undangan dilakukan dengan cara melakukan inventarisasi hukum positif yang berkaitan dengan pencurian data pribadi, seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), Peraturan Pemerintah tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE), serta peraturan-peraturan Kementerian Komunikasi dan Informatika lainnya.⁵ Sementara itu, pendekatan konsep didasarkan pada Undang-Undang Perlindungan Data Pribadi (UU PDP) yang kemudian dikaitkan dengan pendapat para ahli hukum serta hasil penelitian terdahulu dan sumber dari kamus hukum. Spesifikasi penelitian ini bersifat deskriptif-analitis, yaitu dengan menggambarkan

⁵ Ronny Haniatjo Soemitro. (1990). Metode Penelitian Hukum dan Jurimetri, Jakarta: PT Ghalia Indonesia.hlm. 97-98

peraturan perundang-undangan yang berlaku kemudian dikaitkan dengan teori-teori hukum dan praktik pelaksanaan hukum positif yang relevan dengan permasalahan yang diteliti (Soemitro, 1990). Jenis data yang digunakan dalam penelitian ini terdiri dari data sekunder, yaitu data yang diperoleh dari berbagai sumber yang telah ada. Data sekunder ini dikumpulkan melalui studi kepustakaan, yang mencakup buku-buku, literatur, pendapat ahli hukum, serta berbagai sumber lainnya yang relevan untuk menunjang efektivitas penelitian.⁶

Metode pengumpulan data dilakukan melalui teknik studi pustaka dan studi dokumen. Dalam penelitian ini, data atau bahan hukum dibedakan menjadi tiga kategori, yaitu bahan hukum primer, sekunder, dan tersier. Bahan hukum primer meliputi UU ITE, PP PSTE, KUHP, KUHPA, serta hasil wawancara dengan pihak Direktorat Operasi Keamanan Siber di Badan Siber dan Sandi Negara (BSSN). Bahan hukum sekunder mencakup buku-buku tentang hukum pidana, hukum siber, Undang-Undang Perlindungan Data Pribadi, serta artikel atau makalah yang relevan dengan topik perlindungan data pribadi. Adapun bahan hukum tersier terdiri atas kamus hukum dan ensiklopedia hukum. Analisis data dalam penelitian ini menggunakan metode analisis kualitatif. Analisis dilakukan secara naratif dengan mempertemukan data hasil penelitian dengan teori-teori dan konsep yang relevan, kemudian diolah dan dianalisis menggunakan metode deduktif untuk menghasilkan kesimpulan yang logis dan sistematis.

III. HASIL DAN PEMBAHASAN

A. Pertanggungjawaban pidana pelaku Terhadap Peretasan Data Dalam Putusan Nomor 610/Pid.Sus/2022/PN JKT.SEL

1. Kasus Penyalahgunaan Data Pribadi dan Peretasan

Kasus yang diangkat dalam dokumen ini adalah tindak pidana peretasan dan penyalahgunaan data pribadi nasabah bank oleh seorang pelaku asing bernama Roberts Markarjancs. Pelaku datang ke Indonesia pada bulan April 2022 dengan tujuan melakukan kegiatan scamming, yaitu penipuan melalui skimming data nasabah bank. Skimming adalah tindakan menggandakan informasi dari pita magnetik kartu ATM atau kartu kredit, kemudian menggunakan data tersebut untuk mengambil kendali atas rekening nasabah tanpa izin mereka. Pelaku menggunakan kartu-kartu binance yang dikirim ke tempat tinggalnya, lalu menyalin data nasabah dari aplikasi privnote ke laptop, dan menyalinnya ke kartu-kartu binance melalui mesin encoder. Data yang berhasil disalin digunakan untuk menarik uang dari rekening nasabah melalui ATM, dan hasilnya dikirim ke rekening tujuan sesuai perintah pihak yang tidak dikenal identitasnya. Pelaku mendapatkan komisi sebesar 1,5% dari setiap transaksi yang berhasil dilakukan.

Kejahatan ini terbongkar setelah banyak nasabah melaporkan hilangnya uang di rekening mereka tanpa melakukan transaksi. Investigasi dilakukan oleh tim dari PT. Bank Rakyat Indonesia (BRI) dan kepolisian, yang mengamati rekaman CCTV di mesin ATM dan menemukan ciri-ciri pelaku. Pelaku berhasil ditangkap di

⁶ Sugiyono(2010). Metode Penelitian Kualitatif dan R&D. Bandung: Alfabeta. hlm.205

Depok, dan dari penggeledahan di tempat tinggalnya ditemukan barang bukti berupa kartu ATM, kartu binance, mesin encoder, dan perangkat elektronik lainnya. Dari hasil investigasi, terbukti bahwa pelaku telah melakukan tindak pidana mengakses sistem elektronik tanpa izin, serta melakukan penyalahgunaan data nasabah untuk keuntungan pribadi, sehingga menimbulkan kerugian finansial bagi korban sebesar lebih dari satu miliar rupiah.⁷

2. Aspek Hukum dan Perlindungan Data Pribadi

Dalam kasus ini, pelaku didakwa berdasarkan Pasal 30 ayat 2 Jo Pasal 36 Jo Pasal 51 ayat 2 Undang-Undang RI Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), sebagaimana telah diubah dan ditambah dengan UU Nomor 19 Tahun 2016. Pasal tersebut mengatur tentang akses ilegal terhadap komputer atau sistem elektronik untuk memperoleh informasi elektronik atau dokumen elektronik, yang mengakibatkan kerugian bagi orang lain. Majelis hakim mempertimbangkan bahwa pelaku telah memenuhi seluruh unsur delik, yaitu:⁸

1. Subjek tindak pidana (setiap orang), yaitu pelaku sebagai warga negara asing yang sehat akal dan mampu mempertanggungjawabkan perbuatannya.
2. Niat jahat (dengan sengaja dan tanpa hak), yang terbukti dari bukti bahwa pelaku datang ke Indonesia dengan tujuan melakukan scamming.
3. Akses ilegal terhadap sistem elektronik, yaitu pelaku mengakses data nasabah melalui aplikasi telegram, privnote, dan mesin encoder.
4. Akibat kerugian bagi korban, yaitu hilangnya uang nasabah akibat transaksi ilegal yang dilakukan pelaku.

Pelaku dijatuhi pidana penjara selama 6 tahun dan denda sebesar dua miliar rupiah. Selain itu, barang bukti seperti kartu binance, kartu ATM, dan perangkat elektronik lainnya disita dan ditetapkan sebagai barang bukti dalam perkara ini. Putusan ini menegaskan pentingnya perlindungan data pribadi, karena data pribadi merupakan hak konstitusional warga negara yang wajib dilindungi dan dijaga kerahasiaannya. Kasus ini juga mencerminkan bahwa sistem keamanan dan regulasi di Indonesia masih rentan terhadap kebocoran data, sehingga perlu diperkuat agar tidak terjadi penyalahgunaan data oleh pihak yang tidak bertanggung jawab.

3. Dampak Globalisasi dan Digitalisasi terhadap Hukum

Perkembangan teknologi informasi dan komunikasi (TIK) telah membawa perubahan besar dalam kehidupan sosial, ekonomi, dan hukum di Indonesia. Globalisasi mempercepat arus informasi dan transaksi elektronik, sehingga muncul berbagai bentuk kejahatan baru yang bersifat global dan melampaui batas negara,

⁷ Dian Alan Setiawan, *Perkembangan Modus Operandi Kejahatan Skimming Dalam Pembobolan Mesin ATM Bank Sebagai Bentuk Kejahatan Dunia Maya (Cybercrime)*, Volume 16. No. 2 (Jakarta: 2018, Edisi Oktober), h. 181

⁸ Budi Suhariyanto. *Tindak Pidana Teknologi Informasi (Cybercrime): Urgensi Pengaturan dan Celah Hukumnya*. Jakarta: RajaGrafindo Persada, 2012.

seperti cybercrime, peretasan, dan penyalahgunaan data pribadi. Perkembangan ini juga memunculkan istilah-istilah baru dalam dunia hukum, seperti ICT Law (Hukum Teknologi Informasi dan Komunikasi), yang mengatur aspek-aspek hukum yang berkaitan dengan teknologi digital.

Hukum di Indonesia mengalami transformasi seiring dengan perkembangan sosial dan teknologi. Produk hukum baru dibentuk untuk menangani permasalahan yang muncul akibat digitalisasi, seperti UU ITE yang khusus mengatur kejahatan di bidang informasi dan transaksi elektronik. Selain itu, peran pemerintah diperkuat untuk mencegah penyebaran konten ilegal dan melindungi kepentingan umum dari gangguan akibat penyalahgunaan informasi elektronik. Lembaga peradilan dan penyidik juga diberikan kewenangan untuk meminta informasi dari penyelenggara sistem elektronik demi kepentingan penegakan hukum terhadap kejahatan elektronik.⁹

4. Perlindungan Data Pribadi dan Etika Digital

Perlindungan data pribadi menjadi isu sentral dalam era digital. Data pribadi mencakup informasi yang berkaitan dengan identitas seseorang, seperti Kartu Keluarga, Nomor Induk Kependudukan (NIK), dan lain sebagainya. Indonesia saat ini berada pada peringkat ketiga di dunia dalam kasus kebocoran data terbanyak, sehingga sistem keamanan dan regulasi perlu diperkuat. UU ITE dan UU Perlindungan Data Pribadi (PDP) memberikan sanksi pidana bagi pelaku pencurian data pribadi, yaitu pidana penjara paling lama 4-5 tahun dan denda paling banyak lima miliar rupiah.

Etika digital juga menjadi penting dalam penggunaan media sosial dan teknologi informasi. Masyarakat diharapkan membangun etika yang baik dalam penggunaan media digital agar tidak menimbulkan kerugian bagi orang lain. UU ITE dan UU PDP bertujuan untuk menjamin pengakuan serta penghormatan terhadap hak dan kebebasan orang lain, serta memenuhi tuntutan yang adil sesuai dengan pertimbangan moral, nilai-nilai agama, keamanan, dan ketertiban umum dalam masyarakat yang demokratis.

5. Perkembangan Hukum Perdata dan Pidana terkait Cybercrime

Kejahatan elektronik tidak hanya diatur dalam hukum pidana, tetapi juga dalam hukum perdata. Perbuatan melawan hukum (*onrechtmatige daad*) dalam hukum perdata diatur dalam Pasal 1365 KUHP, yaitu tiap perbuatan yang melanggar hukum dan membawa kerugian kepada orang lain, mewajibkan pelaku untuk mengganti kerugian tersebut. Unsur-unsur perbuatan melawan hukum meliputi adanya perbuatan melawan hukum, adanya kesalahan, adanya sebab akibat antara kerugian dan perbuatan, serta adanya kerugian. Dalam konteks cybercrime, pelaku dapat dituntut secara pidana dan perdata atas kerugian yang ditimbulkan akibat penyalahgunaan data pribadi.¹⁰

⁹ Andi Hamzah, *Asas Asas Hukum Pidana*, Rineka Cipta, 1994, hal.133

¹⁰ Elisabeth Nurhaini Butarbutar, "Hukum Pembuktian (Analisis Terhadap Kemandirian Hakim Sebagai Penegak Hukum Dalam Proses Pembuktian)", CV Nuansa Aulia. Bandung: 2016.

B. Penerapan kebijakan perlindungan yang di dapat korban peretasan data pribadi atas hak ganti rugi dalam putusan nomor 610/Pid.Sus/2022/PN JKT.SEL

Perlindungan data pribadi merupakan hal yang sangat penting di era digital, di mana maraknya kasus kebocoran data pribadi di Indonesia menempatkan Indonesia sebagai salah satu negara dengan insiden kebocoran terbanyak. Data pribadi, seperti Kartu Keluarga, Nomor Induk Kependudukan, dan data nasabah bank, merupakan informasi sensitif yang wajib dijaga kerahasiaannya agar hak konstitusional warga negara terlindungi. Namun, lemahnya sistem keamanan dan regulasi di Indonesia memicu kerentanan penyalahgunaan data ini oleh pihak tidak bertanggung jawab yang kerap memanfaatkan teknologi seperti peretasan dan skimming ATM untuk melakukan kejahatan siber.

Kasus nyata terkait tindak pidana illegal akses dan kebocoran data pribadi dapat dilihat dari peristiwa terdakwa Roberts Markarjancs, warga negara Latvia, yang pada tahun 2022 melakukan peretasan dengan menggunakan aplikasi Telegram dan perangkat encoder untuk mengakses, menyalin, dan memanfaatkan data nasabah bank untuk melakukan transaksi ilegal. Terdakwa dihukum penjara selama enam tahun dan denda 2 miliar rupiah di Pengadilan Negeri Jakarta Selatan atas pelanggaran UU Informasi dan Transaksi Elektronik (UU ITE) Pasal 30 ayat 2 juncto Pasal 36 dan Pasal 51 ayat 2. Kejahatan ini berkontribusi pada kerugian ratusan juta rupiah bagi para korban bank berbasis digital.

Tindak pidana illegal akses tidak hanya mengakibatkan kerugian materiil berupa kehilangan uang digital, tetapi juga kerugian nonmateriil seperti kecemasan, kehilangan privasi, hingga potensi teror fisik terhadap korban. Kerugian psikologis ini sulit diukur dan dijadikan dasar ganti rugi dalam hukum perdata, meskipun secara hukum, pelaku yang melakukan perbuatan melawan hukum wajib mengganti kerugian bagi korban yang dirugikan. Korban dapat memperoleh perlindungan dan pemulihan melalui mekanisme hukum seperti ganti rugi, pendampingan psikososial, serta perlindungan fisik oleh lembaga seperti Lembaga Perlindungan Saksi dan Korban (LPSK) yang berwenang memberikan perlindungan terhadap ancaman yang diderita korban tindak pidana.

Dalam tatanan hukum Indonesia, perlindungan data pribadi diatur dalam beberapa undang-undang yang relevan, termasuk UU ITE, UU Perlindungan Data Pribadi (UU PDP) Nomor 27 Tahun 2022, UU Perlindungan Saksi dan Korban, serta beberapa regulasi lain seperti UU Telekomunikasi dan UU Administrasi Kependudukan. UU PDP secara khusus mengatur tentang hak-hak Subjek Data Pribadi, kewajiban Pengendali Data Pribadi, dan mekanisme ganti kerugian apabila terjadi pelanggaran pemrosesan data pribadi. Namun, implementasi undang-undang ini masih menghadapi kendala besar terutama karena regulasi turunan berupa Peraturan Pemerintah (PP) yang mengatur mekanisme ganti kerugian dan lembaga pengawas administrasi belum terbit, sehingga penegakan hak korban masih terbatas di pengadilan.¹¹

¹¹ Dade, L. L., et al. (2024). Kajian yuridis tentang tindak pidana penyebaran data pribadi melalui internet (doxing) di Indonesia. Lex Privatum, <https://ejournal.unsrat.ac.id/v3/index.php/lexprivatum/article/view/54687>

Salah satu hak penting dalam perlindungan data pribadi adalah hak untuk dilupakan (right to be forgotten, RTBF). Hak ini memungkinkan individu mengajukan permohonan penghapusan data pribadi yang tidak relevan atau disebarkan secara ilegal. Konsep RTBF ini diadopsi dari putusan pengadilan Uni Eropa pada kasus Costeja pada 2014 dan menjadi bagian amandemen UU ITE serta UU PDP di Indonesia. Meskipun demikian, pelaksanaan hak ini menghadapi tantangan karena belum adanya lembaga pengawas yang memberikan sanksi administratif dan mekanisme penghapusan data pribadi secara efektif masih terbatas.¹²

Tantangan perlindungan data pribadi di Indonesia juga terlihat dari rendahnya kesadaran masyarakat untuk menjaga privasi mereka, yang seringkali membagikan informasi sensitif secara terbuka di media sosial. Selain itu, keterbatasan infrastruktur teknologi, penetrasi internet yang belum merata, dan tingginya biaya akses juga menjadi hambatan dalam optimalisasi sistem keamanan data pribadi. Hal ini memperkuat pentingnya regulasi yang kokoh, institusi pengawas yang efektif, serta edukasi publik tentang pentingnya menjaga data pribadi.¹³

Dari perspektif hukum pidana, tindak pidana illegal akses merupakan perbuatan melawan hukum yang merugikan kepentingan hukum publik dan pribadi dengan ancaman pidana penjara, denda, serta pengenaan pidana tambahan seperti pembayaran ganti kerugian. Tujuan pemidanaan menurut KUHP dan UU ITE tidak hanya sebagai koreksi dan resosialisasi pelaku, tetapi juga sebagai bentuk perlindungan dan pengayoman bagi masyarakat luas agar menciptakan rasa aman dan mencegah terulangnya tindak pidana serupa.¹⁴ Putusan hakim dalam perkara illegal akses harus disertai pertimbangan hukum yang jelas untuk menjamin kepastian dan keadilan hukum bagi semua pihak.¹⁵

Kerjasama lintas lembaga seperti aparat penegak hukum, penyedia layanan teknologi dan internet, serta pihak regulator menjadi kunci dalam menangani kejahatan siber secara efektif. Selain itu, karena kejahatan ini kerap bersifat lintas negara, kerja sama internasional melalui perjanjian bantuan hukum timbal balik, pertukaran informasi, dan koordinasi penegakan hukum juga sangat diperlukan untuk memberantas sindikat kejahatan siber yang memanfaatkan yurisdiksi negara-negara berbeda.¹⁶

Sebagai perbandingan global, peraturan perlindungan data pribadi seperti GDPR di Uni Eropa memberikan standar perlindungan tertinggi dengan pengaturan

¹² Budi Suhariyanto. *Tindak Pidana Teknologi Informasi (Cybercrime): Urgensi Pengaturan dan Celah Hukumnya*. Jakarta: RajaGrafindo Persada, 2012.

¹³ Yudiana, T. C., et al. (2022). The urgency of doxing on social media regulation and the implementation of right to be forgotten on related content for the optimization of data privacy protection in Indonesia. *Padjadjaran Journal of Law*, 9(1).

¹⁴ Dade, L. L., et al. (2024). Kajian yuridis tentang tindak pidana penyebaran data pribadi melalui internet (doxing) di Indonesia. *Lex Privatum*, <https://ejournal.unsrat.ac.id/v3/index.php/lexprivatum/article/view/54687>

¹⁵ Widigdo, Z., & Rosando, A. F. (2023). Perlindungan negara terhadap privasi data pribadi dalam layanan SIM card di era digital. *Bureaucracy Journal: Indonesia Journal of Law and Social-Political Governance*, publisher.org/index.php/home/article/view/210

¹⁶ "Suharto, M. A., & Apriyani, M. N. (2021). Konsep Cyber Attack, Cyber Crime, Dan Cyber Warfare Dalam Aspek Hukum Internasional. *Risalah Hukum*, hlm. 98-107,"

yang ketat, hak akses dan koreksi data bagi individu, serta kewajiban pelaporan kebocoran data dalam waktu 72 jam.¹⁷ Negara-negara lain seperti Amerika Serikat dengan CCPA, Singapura melalui PDPA, dan Jepang dengan APPI juga telah mengadopsi regulasi yang ketat untuk melindungi data pribadi warga dan memberikan sanksi tegas bagi pelanggarnya. Indonesia dapat menjadikan standar internasional ini sebagai acuan dalam menguatkan regulasi dan praktik perlindungan data pribadi.¹⁸

Dalam konteks pemulihan hak korban, terdapat tiga mekanisme tuntutan ganti kerugian yaitu administratif, perdata, dan pidana. Melalui mekanisme ini, korban dapat memperoleh kompensasi atas kerugian materiil dan immateriil yang diperoleh. Namun, penilaian besaran ganti kerugian masih menjadi kendala karena belum ada aturan turunan yang mengatur secara rinci. Selain itu, upaya pemulihan juga mencakup dukungan psikososial dan perlindungan fisik bagi korban yang mengalami ancaman nyata akibat pengungkapan data pribadi mereka.¹⁹

Secara teknis, perlindungan data pribadi dapat diperkuat dengan penggunaan teknologi enkripsi, sistem otentikasi multi-faktor, pemantauan keamanan real time, serta audit dan penilaian risiko berkala. Perusahaan dan organisasi yang mengelola data pribadi harus mengadopsi praktik keamanan siber terbaik dan menerapkan teknologi terbaru untuk mencegah terjadinya kebocoran. Upaya preventif ini harus dilengkapi dengan penegakan hukum yang tegas agar memberi efek jera bagi pelaku kejahatan siber.²⁰

Oleh karena itu, perlindungan hak atas data pribadi adalah bagian dari hak asasi manusia dan telah dijamin dalam konstitusi Indonesia. Seiring pesatnya perkembangan teknologi informasi, perlindungan ini harus semakin diperkuat agar tercipta ruang digital yang aman dan bebas dari penyalahgunaan data pribadi. Regulasi yang komprehensif, penerapan teknologi canggih, edukasi masyarakat, dan kerja sama efektif antar lembaga merupakan faktor kunci dalam mewujudkan sistem perlindungan data pribadi yang efektif di Indonesia.²¹

IV. KESIMPULAN

Pertanggungjawaban peretasan data pribadi dalam putusan nomor 610/Pid.Sus/2022/PN JKT.SEL telah terwujud secara yuridis. Terdakwa Robert Markarjancs terbukti secara sah dan meyakinkan bersalah melanggar dakwaan alternatif kesatu, yaitu Pasal 30 Ayat (2) Jo Pasal 36 Jo pasal 51 ayat (2) Undang-Undang RI nomor 11 Tahun 2008 tentang informasi dan Transaksi Elektronik. Majelis Hakim menjatuhkan pidana penjara selama 6 (enam) tahun dan pidana

¹⁷ Sugeng, (2024). Hukum Telematika Indonesia: Edisi Revisi. Prenada Medi, Jakarta.

¹⁸ Satria, M. K., & Yusuf, H. (2024). Analisis Yuridis Tindakan Kriminal Doxing Ditinjau Berdasarkan Undang Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi. Jurnal Intelek Dan Cendekiawan Nusantara, Vol. 1, No. 2, hlm. 2442-2456”

¹⁹ Widigdo, Z., & Rosando, A. F. (2023). Perlindungan negara terhadap privasi data pribadi dalam layanan SIM card di era digital. Bureaucracy Journal: Indonesia Journal of Law and Social-Political Governance, publisher.org/index.php/home/article/view/210

²⁰ “Suharto, M. A., & Apriyani, M. N. (2021). Konsep Cyber Attack, Cyber Crime, Dan Cyber Warfare Dalam Aspek Hukum Internasional. Risalah Hukum, hlm. 98-107,”

²¹ Sugeng, (2024). Hukum Telematika Indonesia: Edisi Revisi. Prenada Medi, Jakarta.

denda sebesar Rp. 2.000.000.000,- (dua miliar rupiah). Pertanggungjawaban ini didasarkan pada terpenuhinya seluruh unsur delik, di mana terdakwa secara sengaja dan tanpa hak mengakses sistem elektronik (laptop, Telegram, Privnote) untuk memperoleh data elektronik (data nasabah BRI) yang mengakibatkan kerugian materiil bagi para korban sekitar Rp 1.250.400.000,-. Dengan demikian Terdakwa sudah bertanggungjawab atas apa yang ia lakukan

Penerapan Kebijakan Korban atas hak ganti rugi dalam putusan Nomor 610/Pid.Sus/2022/PN JKT.SEL tidak dilaksanakan oleh majelis hakim. Meskipun para nasabah PT Bank BRI ini mengalami kerugian finansial yang nyata dan tersedianya mekanisme perlindungan korban baik secara perdata dengan pasal 1365 KUHPperdata, kemudian secara Pidana yaitu dengan penggabungan perkara pada pasal 98 KUHP, dan yang terakhir yaitu dengan cara administratif melalui LPSK dan LPS. Jika dilihat majelis hakim tidak mencantumkan amar putusan yang membebaskan ganti rugi kepada terdakwa. Dengan demikian, Hak ganti rugi korban tidak diterapkan atau tidak terpenuhi dalam putusan ini.

DAFTAR PUSTAKA

- M. A. Suharto dan M. N. Apriyani, "Konsep Cyber Attack, Cyber Crime, dan Cyber Warfare Dalam Aspek Hukum Internasional," *Risalah Hukum* 17, no. 2 (2021): 98–107, <https://doi.org/10.30872/risalah.v17i2.705>.
- Moegni Djodirdjo, 1976, *Perbuatan Melawan Hukum*, Jakarta: Pradnya Paramita, Hlm.102
- Andi Hamzah, *Asas Asas Hukum Pidana*, Rineka Cipta, 1994, hal.133
- Badan Pembinaan Hukum Nasional. (2012). *Central Authority dan Mekanisme Koordinasi dalam Pelaksanaan Bantuan Timbal Balik dalam Masalah Pidana*, Jakarta: BPHN.hlm 69.
- Budi Suhariyanto. *Tindak Pidana Teknologi Informasi (Cybercrime): Urgensi Pengaturan dan Celah Hukumnya*. Jakarta: RajaGrafindo Persada, 2012.
- Budi Suhariyanto. *Tindak Pidana Teknologi Informasi (Cybercrime): Urgensi Pengaturan dan Celah Hukumnya*. Jakarta: RajaGrafindo Persada, 2012.
- Dade, L. L., et al. (2024). *Kajian Yuridis Tentang Tindak Pidana Penyebaran Data Pribadi Melalui Internet (Doxing) di Indonesia*. *Lex Privatum*, Vol.13 No.3 (2024).
<https://ejournal.unsrat.ac.id/v3/index.php/lexprivatum/article/view/54687>
- Dian Alan Setiawan, *Perkembangan Modus Operandi Kejahatan Skimming Dalam Pembobolan Mesin ATM Bank Sebagai Bentuk Kejahatan Dunia Maya (Cybercrime)*, *Era Hukum Jurnal Ilmiah Hukum* Vol. 16. No. 2 (2018), him. 174-181. <https://doi.org/10.24912/erahukum.v16i2.4526>
- Elisabeth Nurhaini Butarbutar, *Hukum Pembuktian (Analisis terhadap Kemandirian Hakim Sebagai Penegak Hukum Dalam Proses Pembuktian)*, CV Nuansa Aulia. Bandung: 2016.



- Huala Adolf. (2002). Aspek-aspek Negara dalam Hukum Internasional. Jakarta: Rajawali Press, hlm 3.
- Ron Davies. 2015. Industry 4.0 Digitalisation for Productivity and Growth, European Parliamentary Research Service, PE 568.337, September.
- Ronny Haniatjo Soemitro. (1990). Metode Penelitian Hukum dan Jurumetri, Jakarta: PT Ghalia Indonesia.hlm. 97-98
- Satria, M. K., & Yusuf, H. (2024). Analisis Yuridis Tindakan Kriminal Doxing Ditinjau Berdasarkan Undang Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi. *Jurnal Intelek Dan Cendekiawan Nusantara*, Vol. 1, No. 2, hlm. 2442-2456
- Sugeng, (2024). Hukum Telematika Indonesia: Edisi Revisi. Prenada Medi, Jakarta.
- Sugiyono(2010). Metode Penelitian Kualitatif dan R&D. Bandung: Alfabeta. hlm.205
- Widigdo, Z. ., & Rosando, A. F. . (2022). Perlindungan Negara terhadap Privasi Data Pribadi Dalam Layanan Sim Card di Era Digital. *Bureaucracy Journal : Indonesia Journal of Law and Social-Political Governance*, 3(1), 679–696. <https://doi.org/10.53363/bureau.v3i1.210>
- Widigdo, Z., & Rosando, A. F. (2023). Perlindungan negara terhadap privasi data pribadi dalam layanan SIM card di era digital. *Bureaucracy Journal: Indonesia Journal of Law and Social-Political Governance*, publisher.org/index.php/home/article/view/210
- Yudiana, T. C., et al. (2022). The urgency of doxing on social media regulation and the implementation of right to be forgotten on related content for the optimization of data privacy protection in Indonesia. *Padjadjaran Journal of Law*, Vol 9, No 1 (2022): 24-45. <https://doi.org/10.22304/pjih.v9n1.a2>