E-ISSN: 3031-8521
P-ISSN: 3032-1867
Halaman 3504-3518
Volume 3 Nomor 4 Tahun 2026

ANALISIS YURIDIS TERHADAP KEKABURAN NORMA PERTANGGUNGJAWABAN PIDANA DALAM PENGGUNAAN SOFTWARE BAJAKAN YANG MENGAKIBATKAN PERETASAN DATA

Andre Samson Del Agung[1], Aksi Sinurat[2], Rosalind Angel Fanggi[3]

[1,2,3]Fakultas Hukum, Universitas Nusa Cendana, Indonesia.
E-mail: andreagung90@gmail.com[1], aksi.sinurat@staf.undana.ac.id[2], rosalind_fanggi@yahoo.com[3]

Abstrak

Perkembangan teknologi informasi telah mendorong meningkatnya penggunaan sistem elektronik dalam berbagai sektor kehidupan, termasuk pemerintahan, pelayanan publik, dan kegiatan bisnis. Seiring dengan perkembangan tersebut, ancaman terhadap keamanan siber juga semakin meningkat, salah satunya berupa peretasan data yang sering kali dipicu oleh penggunaan software bajakan. Perangkat lunak bajakan memiliki tingkat kerentanan yang tinggi karena tidak memperoleh pembaruan keamanan (*security update*) serta berpotensi disisipi malware yang dapat dimanfaatkan oleh pelaku untuk memperoleh akses tanpa hak ke dalam sistem elektronik. Kondisi ini telah mengakibatkan berbagai kasus kebocoran data skala nasional di Indonesia yang berdampak pada terganggunya kerahasiaan, integritas, dan ketersediaan data pribadi. Meskipun Indonesia telah memiliki Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik beserta perubahannya, Undang-Undang Nomor 28 Tahun 2014 tentang Hak Cipta, dan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, pengaturan mengenai pertanggungjawaban pidana atas penggunaan software bajakan yang mengakibatkan peretasan data masih menunjukkan adanya kekaburan norma dan ketidaksinkronan antarperaturan. Oleh karena itu, diperlukan analisis yuridis terhadap pengaturan tersebut guna mewujudkan kepastian hukum dan memperkuat perlindungan data nasional.

Kata Kunci: *software bajakan, peretasan data, pertanggungjawaban pidana, perlindungan data pribadi, hukum pidana siber.*

Abstract

The development of information technology has driven the increasing use of electronic systems across various sectors of society, including government, public services, and business activities. Alongside these developments, cybersecurity threats have also increased, one of which is data hacking, frequently triggered by the use of pirated software. Pirated software is highly vulnerable to security threats because it does not receive security updates and may contain embedded malware that can be exploited by perpetrators to gain

unauthorized access to electronic systems. This situation has resulted in various cases of large-scale data breaches in Indonesia, affecting the confidentiality, integrity, and availability of personal data. Although Indonesia has enacted Law Number 11 of 2008 concerning Electronic Information and Transactions, as amended, Law Number 28 of 2014 concerning Copyright, and Law Number 27 of 2022 concerning Personal Data Protection, the legal framework governing criminal liability for the use of pirated software that results in data hacking still reveals legal ambiguities and inconsistencies among related regulations. Therefore, a juridical analysis of these regulations is necessary to establish legal certainty and strengthen national data protection.

Keywords: *Pirated software, data hacking, criminal liability, personal data protection, cybercrime law.*

LATAR BELAKANG

Pemanfaatan teknologi informasi telah menjadi komponen esensial dalam menunjang berbagai aktivitas masyarakat modern di Indonesia, mulai dari penyelenggaraan pemerintahan, kegiatan ekonomi, hingga pelayanan kesehatan. Peningkatan ketergantungan terhadap infrastruktur digital tersebut diikuti oleh tantangan serius pada aspek keamanan informasi berupa berkembangnya tindak pidana siber (*cybercrime*) dengan berbagai modus operandi. Peredaran serta penggunaan perangkat lunak tanpa lisensi yang sah (*software* bajakan) menjadi persoalan krusial karena perangkat lunak ilegal umumnya tidak memperoleh pembaruan keamanan (*security update*) secara berkala dari pengembang resmi serta berpotensi disisipi kode berbahaya. Kerentanan sistemik yang muncul akibat praktik tersebut membuka celah eksploitasi bagi pihak tidak bertanggung jawab untuk mengakses data pribadi maupun informasi strategis milik institusi negara secara tidak sah.

Praktik penggunaan *software* bajakan di Indonesia tergolong tinggi dan telah menjadi kebiasaan umum di berbagai lapisan masyarakat maupun lingkungan kerja. Faktor utama yang mendorong maraknya pelanggaran ini meliputi rendahnya kesadaran hukum dan literasi digital, serta tingginya harga lisensi perangkat lunak resmi. Laporan *Business Software Alliance* (BSA) mencatat bahwa sekitar 83% perusahaan di Indonesia masih menggunakan perangkat lunak tanpa lisensi. Perangkat lunak ilegal tersebut sering kali dimodifikasi oleh pihak tidak berwenang dan disusupi *malware*, *trojan*, atau *ransomware* yang mampu mencuri, merusak, maupun mengenkripsi data pengguna. Badan Siber dan Sandi Negara (BSSN) turut mengonfirmasi bahwa pemanfaatan perangkat lunak ilegal merupakan faktor utama yang memperbesar potensi ancaman siber nasional, sejalan dengan temuan 403.990.813 anomali trafik siber di Indonesia sepanjang tahun 2023. Kondisi empiris tersebut menggarisbawahi urgensi penguatan sistem keamanan digital, khususnya pada infrastruktur sistem elektronik yang dikelola oleh instansi pemerintah maupun penyelenggara layanan publik.

Urgensi perlindungan terhadap data nasional semakin nyata apabila mencermati rentetan insiden kebocoran data berskala masif di Indonesia dalam beberapa tahun terakhir. Publik dikejutkan oleh dugaan kebocoran 4,7 juta data aparatur sipil negara pada sistem Satu Data ASN serta terungkapnya 6,6 juta data Nomor Pokok Wajib Pajak (NPWP) pada Agustus 2024. Serangan *ransomware* LockBit 3.0 terhadap Pusat Data Nasional Sementara (PDNS) 2

pada 17 Juni 2024 bahkan melumpuhkan operasional ratusan instansi pemerintahan dan layanan publik strategis. Insiden serupa juga pernah melanda sektor swasta dan layanan dasar masyarakat, seperti dugaan kebocoran 15 juta data pengguna Tokopedia pada 2020, kebocoran data 279 juta peserta BPJS Kesehatan pada 2021, serta kebocoran 1,3 miliar data registrasi kartu SIM pada 2022. Rangkaian peristiwa tersebut memperlihatkan bahwa kelemahan pengamanan sistem elektronik berdampak langsung terhadap kerahasiaan, integritas, dan ketersediaan data masyarakat luas. Pembuktian keterkaitan antara insiden kebocoran data dan penggunaan *software* bajakan menuntut evaluasi menyeluruh terhadap bentuk perbuatan, unsur kesalahan, serta hubungan kausalitas melalui pendekatan hukum yang mengintegrasikan rezim hak kekayaan intelektual, pengamanan sistem elektronik, dan pelindungan data pribadi.

Persoalan yuridis tersebut melibatkan tiga instrumen hukum positif di Indonesia, yakni Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah terakhir dengan Undang-Undang Nomor 1 Tahun 2024 (UU ITE), Undang-Undang Nomor 28 Tahun 2014 tentang Hak Cipta (UU Hak Cipta), serta Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP). Perbedaan fokus dan ruang lingkup pengaturan di antara ketiga undang-undang tersebut memunculkan ketidaksinkronan norma dalam menetapkan pertanggungjawaban pidana atas penggunaan *software* bajakan yang memicu peretasan data. Pasal 9 ayat (1) huruf a dan Pasal 113 UU Hak Cipta berorientasi pada perlindungan hak eksklusif pencipta atas penggandaan program komputer, Pasal 30 ayat (1) UU ITE melarang tindakan akses tanpa hak terhadap sistem elektronik milik orang lain, sementara Pasal 35 hingga Pasal 39 UU PDP mewajibkan pengendali data pribadi menjamin keamanan pemrosesan data dari akses ilegal. Ketiadaan norma eksplisit yang menjembatani pelanggaran penggunaan *software* ilegal dengan akibat lanjutan berupa peretasan data menciptakan kekaburan norma (*vague norm*). Kekaburan norma ini menyulitkan penegak hukum dalam menentukan subjek pertanggungjawaban pidana bagi pengguna maupun pengelola sistem elektronik yang lalai (*culpa*) menjaga standar keamanan sistem sehingga memfasilitasi terjadinya kebocoran data.

Kondisi kekaburan norma tersebut menimbulkan ketegangan terhadap asas-asas fundamental dalam hukum pidana. Penerapan asas legalitas terhambat karena belum terdapat rumusan delik yang secara spesifik mengkualifikasikan kelalaian penggunaan *software* bajakan sebagai faktor pemicu peretasan data. Penerapan asas kepastian hukum turut terganggu akibat tumpang tindih kewenangan dan sanksi antarundang-undang, sedangkan dari sisi asas kemanfaatan, hukum positif belum mampu memberikan efek jera maupun perlindungan optimal bagi keamanan data nasional. Rendahnya literasi digital masyarakat memperburuk keadaan karena pengguna umumnya memandang instalasi *software* bajakan sekadar pelanggaran hak cipta biasa tanpa menyadari posisinya yang rentan menjadi korban sekaligus fasilitator dalam rantai kejahatan siber. Kajian mengenai hubungan kausalitas antara penyebaran serta penggunaan *software* bajakan dan peretasan data skala nasional dalam perspektif hukum pidana siber masih jarang dielaborasi secara komprehensif. Penelitian-penelitian terdahulu, seperti karya Deny Budiyanto dan Muhammad Mabruri maupun studi Dewi Chirzah dan Rizqy Akbar Ramadhan, lebih menitikberatkan pada pembangunan sistem keamanan siber nasional dan ancaman *cyber war* secara umum tanpa mengaitkannya dengan

faktor teknis penggunaan *software* ilegal. Demikian pula kajian Hani Puspita Sari dkk. mengenai efektivitas UU PDP, riset edukatif A. C. Sari dkk. terkait alternatif *freeware*, serta skripsi Gusti Wisnu Wibisono mengenai tinjauan pidana hak cipta atas *software* ilegal belum menyentuh konstruksi pertanggungjawaban pidana atas kebocoran data berskala nasional.

Bertolak dari kesenjangan normatif dan kekosongan kajian tersebut, penelitian ini berfokus pada dua permasalahan utama, yakni bagaimana konstruksi pertanggungjawaban pidana terhadap kekaburan norma hukum dalam penggunaan *software* bajakan yang secara tidak langsung mengakibatkan peretasan data ditinjau dari ketidaksinkronan peraturan perundang-undangan di Indonesia, serta bagaimana upaya pembaruan hukum pidana siber yang diperlukan guna memperjelas batas pertanggungjawaban hukum dan memperkuat perlindungan data nasional. Penelitian ini bertujuan menganalisis secara yuridis bentuk kekaburan norma dalam ketidaksinkronan antara UU ITE, UU Hak Cipta, dan UU PDP terkait pertanggungjawaban pidana pengguna *software* bajakan, sekaligus merumuskan rekomendasi pembaruan hukum pidana siber yang adaptif dan harmonis. Secara teoritis, hasil penelitian ini diharapkan memperkaya khazanah ilmu hukum pidana siber dan hukum pelindungan data pribadi, khususnya dalam mengelaborasi penerapan asas legalitas, asas kepastian hukum, dan asas kemanfaatan sebagai landasan integrasi norma. Secara praktis, kajian ini diharapkan menjadi rujukan strategis bagi pembentuk undang-undang, pemerintah, dan aparat penegak hukum dalam menyusun standar keamanan sistem elektronik yang tegas, serta meningkatkan kesadaran hukum masyarakat akan risiko keamanan siber di balik penggunaan perangkat lunak ilegal.

METODE

Penelitian ini merupakan penelitian hukum normatif (*juridical normative research*) yang menitikberatkan pada penelaahan terhadap norma hukum positif, doktrin hukum, serta asas-asas hukum yang relevan dengan permasalahan pertanggungjawaban pidana atas penggunaan *software* bajakan yang memicu peretasan data. Pelaksanaan kajian ini memadukan tiga pendekatan utama, yaitu pendekatan perundang-undangan (*statute approach*), pendekatan konseptual (*conceptual approach*), dan pendekatan kasus (*case approach*). Pendekatan perundang-undangan dilakukan dengan menginventarisasi dan menganalisis sinkronisasi regulasi terkait kejahatan siber, hak kekayaan intelektual, dan pelindungan data pribadi. Pendekatan konseptual digunakan untuk membedah konstruksi teoretis mengenai keamanan siber, peretasan data, kesalahan (*schuld*), hubungan kausalitas, serta kepastian hukum. Pendekatan kasus diterapkan guna menelaah berbagai insiden kebocoran data skala nasional di Indonesia, seperti insiden pada BPJS Kesehatan, data registrasi kartu SIM, hingga serangan terhadap Pusat Data Nasional Sementara, sebagai gambaran empiris kerentanan sistem elektronik.

Sumber bahan hukum dalam kajian normatif ini diklasifikasikan ke dalam tiga kategori utama, meliputi bahan hukum primer, bahan hukum sekunder, dan bahan hukum tersier. Bahan hukum primer mencakup peraturan perundang-undangan yang memiliki kekuatan mengikat secara yuridis, yakni Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik beserta perubahannya, Undang-Undang Nomor 28 Tahun 2014 tentang Hak Cipta, serta Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.

Bahan hukum sekunder terdiri atas literatur hukum, buku referensi, artikel jurnal ilmiah nasional, hasil penelitian terdahulu, serta pandangan para ahli hukum yang memberikan eksplanasi mendalam terhadap bahan hukum primer. Bahan hukum tersier berfungsi memberikan petunjuk maupun informasi penunjang, meliputi kamus hukum, ensiklopedia hukum, serta laporan statistik dan berita kredibel mengenai keamanan siber.

Pengumpulan seluruh bahan hukum tersebut dilakukan melalui teknik studi kepustakaan (*library research*) dengan cara menelusuri, menginventarisasi, dan mengklasifikasikan dokumen hukum dari perpustakaan, pangkalan data peraturan perundang-undangan, serta repositori jurnal ilmiah. Bahan hukum yang telah terkumpul diolah dan dianalisis secara deskriptif-kualitatif melalui penafsiran sistematis dan gramatikal terhadap pasal-pasal terkait. Proses analisis dilakukan dengan mengonstruksikan argumentasi yuridis secara logis guna mengidentifikasi kekaburan norma dan ketidaksinkronan antarundang-undang, sekaligus merumuskan pembaruan hukum pidana siber yang harmonis dan memberikan kepastian hukum dalam pelindungan data nasional.

HASIL DAN PEMBAHASAN

Pertanggungjawaban Pidana terhadap Kekaburan Norma Hukum dalam Penggunaan Software Bajakan yang Secara Tidak Langsung Mengakibatkan Peretasan Data

Kemajuan teknologi informasi telah memengaruhi berbagai bidang kehidupan, termasuk dalam penyelenggaraan pelayanan publik dan aktivitas sektor swasta. Pemanfaatan sistem elektronik semakin luas untuk menunjang proses pengumpulan, penyimpanan, pengolahan, serta pengelolaan informasi, termasuk data pribadi masyarakat. Meskipun penerapan teknologi tersebut dapat meningkatkan efisiensi dan mempermudah akses terhadap informasi, penggunaannya juga menghadirkan tantangan dalam aspek keamanan data. Risiko tersebut dapat meningkat apabila sistem elektronik yang digunakan tidak dilengkapi dengan mekanisme pengamanan yang memadai, sehingga berpotensi menimbulkan kerentanan terhadap akses tanpa hak maupun penyalahgunaan informasi. Penerapan sistem elektronik dengan mekanisme keamanan yang memadai merupakan salah satu langkah penting untuk mengurangi risiko akses tanpa hak terhadap data yang tersimpan maupun diproses di dalamnya. Dalam kaitannya dengan perlindungan hak privasi, Sinta Dewi menjelaskan bahwa pelindungan data pribadi merupakan bagian dari upaya menjamin hak setiap individu atas informasi yang berkaitan dengan dirinya, sehingga data tersebut tidak digunakan atau disalahgunakan oleh pihak lain tanpa dasar persetujuan yang sah. Dengan demikian, pengelolaan data melalui sistem elektronik harus dilakukan dengan memperhatikan aspek keamanan sistem yang digunakan.

Permasalahan keamanan sistem elektronik menjadi semakin kompleks dengan adanya praktik penggunaan perangkat lunak bajakan dalam berbagai institusi. Penggunaan perangkat lunak yang tidak memiliki lisensi resmi tidak hanya menimbulkan pelanggaran terhadap hak kekayaan intelektual, tetapi juga dapat menimbulkan kerentanan keamanan sistem yang berpotensi dimanfaatkan oleh pelaku kejahatan siber untuk melakukan peretasan data. Pelindungan data pribadi merupakan salah satu bentuk penegakan hak atas privasi yang dimaksudkan untuk menjamin keamanan informasi pribadi setiap individu, sehingga penggunaannya tidak dilakukan secara sewenang-wenang oleh pihak lain tanpa persetujuan

atau dasar hukum yang sah. Perlindungan tersebut menjadi semakin penting seiring dengan berkembangnya penggunaan teknologi informasi dalam berbagai aktivitas masyarakat, khususnya dalam pengolahan data melalui sistem elektronik. Pengaturan mengenai perlindungan data pribadi di Indonesia secara khusus tercantum dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Peraturan tersebut menjadi landasan hukum bagi pelaksanaan pemrosesan data pribadi sekaligus menetapkan tanggung jawab pengendali data dalam melindungi data yang dikelolanya. Dalam penerapannya, keamanan sistem elektronik memiliki keterkaitan erat dengan perlindungan data pribadi, mengingat pemrosesan data pada era digital umumnya memanfaatkan teknologi informasi sebagai sarana utama. Oleh karena itu, penerapan pengamanan sistem elektronik menjadi salah satu aspek penting dalam upaya menjaga data pribadi dari risiko penyalahgunaan maupun akses yang tidak sah.

Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) turut mengatur tanggung jawab penyelenggara sistem elektronik dalam menjaga keamanan sistem yang berada di bawah pengelolaannya. Tanggung jawab tersebut meliputi kewajiban untuk menyelenggarakan sistem elektronik secara andal, aman, dan bertanggung jawab dengan berpedoman pada ketentuan hukum yang berlaku. Penerapan standar keamanan yang memadai diperlukan untuk menjaga data yang disimpan maupun diproses oleh suatu instansi, serta mengurangi kemungkinan terjadinya gangguan operasional, akses ilegal, dan kerugian yang dapat berdampak pada para pengguna sistem elektronik. Perangkat lunak atau *software* merupakan komponen utama dalam sistem komputer yang berfungsi untuk menjalankan berbagai proses pengolahan data. Dalam praktiknya, penggunaan perangkat lunak harus memperhatikan ketentuan hukum yang berlaku, terutama yang berkaitan dengan hak kekayaan intelektual. Program komputer termasuk salah satu ciptaan yang memperoleh perlindungan hukum berdasarkan ketentuan hak cipta. Oleh karena itu, penggunaan maupun penggandaan perangkat lunak tanpa kewenangan atau izin yang diwajibkan oleh pemegang hak cipta berpotensi menimbulkan akibat hukum. Pengenaan sanksi terhadap pelaku bergantung pada terpenuhinya unsur-unsur pelanggaran sebagaimana ditetapkan dalam peraturan perundang-undangan yang berlaku.

Penggunaan perangkat lunak bajakan tidak hanya menimbulkan permasalahan dari sisi pelanggaran hak cipta, tetapi juga berpotensi menimbulkan risiko terhadap keamanan sistem elektronik. Banyak kejahatan siber terjadi karena adanya celah keamanan pada sistem teknologi informasi yang tidak terlindungi dengan baik. Dalam konteks ini, perangkat lunak bajakan sering kali tidak mendapatkan pembaruan keamanan dari pengembang resmi sehingga lebih rentan terhadap serangan siber. Pemanfaatan perangkat lunak dalam penyelenggaraan sistem elektronik tidak semata-mata menyangkut pemenuhan ketentuan hukum di bidang hak cipta, tetapi juga mencakup aspek keamanan sistem dalam menunjang proses penyimpanan, pengolahan, dan pengelolaan data. Oleh karena itu, penggunaan perangkat lunak perlu memperhatikan aspek legalitas sekaligus standar keamanan yang diperlukan untuk meminimalkan risiko terhadap data yang dikelola. Peretasan sistem elektronik merupakan salah satu jenis kejahatan siber yang semakin mendapat perhatian seiring dengan berkembangnya penggunaan teknologi digital. Tindakan tersebut dapat berupa akses ke dalam sistem komputer tanpa kewenangan yang sah, sehingga pelaku berpotensi

memperoleh informasi atau data yang tersimpan di dalam sistem tersebut. Menurut Maskun, *cybercrime* merupakan tindak kejahatan yang memanfaatkan komputer dan jaringan internet sebagai media untuk melakukan perbuatan yang bertentangan dengan hukum. Pada praktiknya, pelaku kejahatan siber dapat memanfaatkan kelemahan keamanan pada sistem elektronik milik suatu instansi untuk memasuki sistem tanpa izin atau melakukan tindakan yang berpotensi mengancam kerahasiaan dan keamanan data serta informasi yang tersimpan di dalamnya.

Ketentuan mengenai larangan akses ilegal terhadap sistem elektronik diatur dalam Pasal 30 Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). Pasal tersebut menetapkan larangan bagi setiap orang yang dengan sengaja dan tanpa hak atau secara melawan hukum memasuki komputer maupun sistem elektronik milik pihak lain melalui cara-cara yang ditentukan dalam ketentuan tersebut. Pengaturan ini menunjukkan bahwa hukum pidana memberikan perlindungan terhadap sistem elektronik dengan menetapkan batasan hukum atas tindakan mengakses sistem tanpa kewenangan yang sah. Walaupun peraturan perundang-undangan telah menetapkan kewajiban bagi penyelenggara sistem elektronik untuk memastikan keamanan sistem yang dikelolanya, masih terdapat persoalan mengenai kejelasan standar pengamanan yang wajib diterapkan. Situasi tersebut memunculkan persoalan mengenai kecukupan pengaturan hukum yang ada dalam memberikan kejelasan pedoman bagi penyelenggara sistem elektronik untuk melaksanakan kewajiban perlindungan dan pengamanan sistem yang dikelolanya. Perumusan norma hukum yang jelas dan tegas merupakan unsur penting dalam mewujudkan kepastian hukum, sehingga masyarakat dapat memahami ketentuan yang berlaku serta mengetahui hak dan kewajiban yang harus dipenuhi. Norma yang terlalu umum dapat menimbulkan berbagai penafsiran yang berbeda dalam penerapannya.

Keadaan tersebut menunjukkan bahwa hukum pidana nasional masih menghadapi kesulitan dalam mengikuti perkembangan teknologi informasi. Meningkatnya *cybercrime* merupakan konsekuensi dari pesatnya perkembangan teknologi, sedangkan hukum pidana sering kali tertinggal sehingga diperlukan pembaruan hukum (*ius constituendum*) agar mampu mengakomodasi bentuk-bentuk kejahatan baru. Pengaturan mengenai pertanggungjawaban pidana terhadap penggunaan *software* bajakan yang menjadi sarana peretasan data perlu dirumuskan secara lebih jelas agar memberikan kepastian hukum bagi aparat penegak hukum maupun masyarakat. Dalam hal perlindungan sistem elektronik, ketentuan hukum yang berlaku cenderung menekankan kewajiban penyelenggara untuk menjaga keamanan sistem yang dikelolanya, tetapi belum tentu menguraikan secara terperinci tolok ukur keamanan yang wajib diterapkan. Keadaan ini dapat menimbulkan persoalan ketika kebocoran data terjadi akibat kelemahan sistem, terutama dalam menilai ruang lingkup kewajiban serta menentukan bentuk pertanggungjawaban hukum pihak yang bertanggung jawab atas pengelolaan sistem tersebut.

Seiring dengan kemajuan teknologi informasi, sistem elektronik semakin berperan penting sebagai media untuk menyimpan dan mengolah beragam informasi, termasuk data pribadi masyarakat yang bersifat sensitif dan memiliki nilai strategis. Kondisi ini menuntut penerapan mekanisme perlindungan yang memadai untuk mengurangi risiko penyalahgunaan informasi serta akses ilegal terhadap sistem oleh pihak yang tidak memiliki kewenangan.

Dengan demikian, diperlukan pengaturan hukum yang memberikan kejelasan mengenai persyaratan dan standar pengamanan sistem elektronik agar perlindungan terhadap data pribadi masyarakat dapat terlaksana secara efektif. Upaya pengamanan sistem elektronik memiliki keterkaitan yang erat dengan penerapan prinsip-prinsip perlindungan data pribadi. Prinsip-prinsip tersebut menjadi landasan dalam memastikan bahwa data pribadi dikelola secara tepat serta terlindungi dari risiko penyalahgunaan maupun akses yang tidak sah, yang meliputi pembatasan pengumpulan data (*collection limitation*), pemeliharaan kualitas data (*data quality*), penentuan tujuan penggunaan data (*purpose specification*), pembatasan pemanfaatan data (*use limitation*), penerapan mekanisme pengamanan (*security safeguards*), transparansi dalam pengelolaan data (*openness*), pemberian kesempatan kepada individu untuk berpartisipasi dalam pengelolaan data pribadinya (*individual participation*), serta kewajiban untuk mempertanggungjawabkan pengelolaan data (*accountability*).

Dalam konteks penelitian ini, prinsip *security safeguards* menegaskan bahwa setiap data pribadi wajib dilindungi melalui langkah-langkah pengamanan yang memadai agar terhindar dari kehilangan, penyalahgunaan, perubahan maupun akses yang tidak sah. Dengan demikian, penggunaan *software* bajakan yang tidak memperoleh pembaruan keamanan bertentangan dengan prinsip perlindungan data pribadi karena meningkatkan kerentanan sistem elektronik terhadap serangan siber. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi telah menjadi dasar hukum dalam penyelenggaraan perlindungan dan pengelolaan data pribadi di Indonesia. Meskipun demikian, penerapannya masih menghadapi persoalan terkait pengaturan standar keamanan sistem elektronik yang digunakan untuk memproses data pribadi, yang berkaitan dengan ketentuan undang-undang yang masih dirumuskan secara umum sehingga belum menguraikan secara spesifik mengenai bentuk dan standar pengamanan sistem elektronik yang harus dipenuhi oleh pengendali data pribadi. Permasalahan tersebut menjadi semakin penting apabila dikaitkan dengan praktik penggunaan perangkat lunak bajakan dalam lingkungan kerja yang mengelola sistem elektronik yang berisi data masyarakat, di mana penggunaan perangkat lunak bajakan tidak hanya menimbulkan pelanggaran terhadap hukum hak cipta, tetapi juga berpotensi menimbulkan kerentanan keamanan sistem karena perangkat lunak tersebut tidak memperoleh pembaruan keamanan dari pengembang resmi, sehingga meningkatkan risiko serangan siber yang berpotensi menyebabkan kebocoran data pribadi dalam skala besar.

Pertanggungjawaban pidana menjadi dasar untuk menilai apakah suatu perbuatan yang melanggar hukum dapat dibebankan kepada seseorang sebagai bentuk kesalahan yang dapat dipidana. Penilaian tersebut berlandaskan asas *geen straf zonder schuld*, yang menegaskan bahwa penjatuhan pidana harus didasarkan pada adanya kesalahan pada diri pelaku. Prinsip tersebut menegaskan bahwa pemidanaan terhadap seseorang hanya dapat dilakukan apabila unsur kesalahan yang dipersyaratkan dalam hukum pidana terbukti terpenuhi. Kesalahan secara umum diklasifikasikan ke dalam dua kategori, yakni kesengajaan (*dolus*) dan kealpaan (*culpa*), di mana kesengajaan merujuk pada keadaan ketika seseorang secara sadar menghendaki atau mengetahui perbuatan yang dilakukannya, sedangkan kealpaan berkaitan dengan tidak terpenuhinya kewajiban untuk bertindak secara hati-hati sebagaimana yang sewajarnya diharapkan dalam situasi tersebut. Pertanggungjawaban pidana merupakan unsur penting dalam menganalisis berbagai tindak pidana yang berkaitan

dengan penggunaan teknologi informasi. Pada sistem elektronik yang digunakan untuk mengelola data masyarakat, pihak yang memiliki tanggung jawab atas pengoperasian dan pengelolaan sistem berkewajiban memastikan bahwa langkah-langkah pengamanan yang diterapkan telah memadai, dan apabila kewajiban tersebut diabaikan, perlu dilakukan penelaahan lebih lanjut untuk menentukan apakah terdapat unsur kelalaian dalam pengelolaan sistem elektronik yang berpotensi mengakibatkan kerugian bagi pihak lain.

Dalam hukum pidana, kealpaan merupakan bentuk kesalahan yang dapat terjadi ketika seseorang tidak melaksanakan tindakan pencegahan yang sepatutnya dilakukan untuk menghindari timbulnya kerugian, yang umumnya berkaitan dengan tidak dipenuhinya kewajiban untuk bertindak secara hati-hati sesuai dengan standar yang semestinya diterapkan dalam suatu kegiatan. Dalam konteks penggunaan perangkat lunak bajakan, kelalaian dapat terjadi apabila suatu instansi atau pihak yang bertanggung jawab terhadap pengelolaan sistem elektronik menggunakan perangkat lunak yang tidak memiliki lisensi resmi dan tidak mendapatkan pembaruan keamanan dari pengembang perangkat lunak tersebut, sehingga meningkatkan risiko terjadinya kerentanan keamanan dalam sistem elektronik yang digunakan. Kerentanan sistem elektronik tersebut dapat dimanfaatkan oleh pelaku kejahatan siber untuk memperoleh akses tidak sah terhadap sistem komputer, mengingat kejahatan siber pada umumnya memanfaatkan kelemahan sistem keamanan yang terdapat dalam suatu sistem teknologi informasi. Oleh karena itu, penggunaan perangkat lunak yang tidak resmi berpotensi meningkatkan risiko terjadinya peretasan sistem elektronik.

Kejahatan siber (*cybercrime*) dapat diartikan sebagai tindak pidana yang melibatkan pemanfaatan teknologi, komputer, maupun jaringan internet, yang mencakup berbagai perbuatan seperti akses tanpa hak (*unauthorized access*), perubahan atau penghapusan data secara tidak sah (*unauthorized alteration or destruction of data*), sabotase siber (*cyber sabotage*), pelanggaran hak kekayaan intelektual, serta tindakan yang melanggar privasi seseorang. Dengan demikian, penyebaran *software* bajakan yang telah dimodifikasi dengan *malware* tidak hanya merupakan pelanggaran hak cipta, tetapi juga dapat menjadi sarana terjadinya *unauthorized access* terhadap sistem elektronik yang berujung pada peretasan data. Penggunaan perangkat lunak bajakan dalam suatu sistem elektronik yang mengelola data penting dapat menimbulkan persoalan hukum apabila penggunaan perangkat lunak tersebut menyebabkan terjadinya kerentanan sistem yang kemudian dimanfaatkan oleh pelaku kejahatan siber. Kausalitas memiliki peranan penting dalam hukum pidana untuk menilai keterkaitan antara suatu tindakan dan akibat yang ditimbulkannya, di mana keberadaan hubungan sebab-akibat tersebut diperlukan dalam proses pembuktian guna menentukan apakah kerugian yang terjadi dapat dikaitkan dengan perbuatan yang dilakukan oleh seseorang.

Pembuktian hubungan sebab-akibat dalam hukum pidana dapat menjadi kompleks, khususnya pada perkara yang melibatkan teknologi informasi karena beragamnya faktor teknis yang memengaruhi pengoperasian sistem elektronik. Dalam kondisi tertentu, penggunaan perangkat lunak bajakan yang tidak memperoleh pembaruan keamanan atau memiliki perlindungan yang memadai berpotensi menimbulkan celah keamanan yang dapat dimanfaatkan oleh pelaku kejahatan siber untuk melakukan peretasan data, meskipun untuk menetapkan adanya hubungan kausalitas secara hukum, tetap diperlukan pembuktian bahwa

kerentanan tersebut berkaitan dengan terjadinya serangan yang dimaksud. Hubungan kausalitas antara penggunaan perangkat lunak bajakan dengan terjadinya peretasan data dapat dianalisis dengan melihat apakah kerentanan sistem yang disebabkan oleh penggunaan perangkat lunak tersebut menjadi salah satu faktor yang memungkinkan terjadinya akses tidak sah atau peretasan terhadap sistem elektronik, di mana menurut doktrin hukum pidana, suatu tindakan dapat dinilai sebagai penyebab timbulnya akibat tertentu apabila terdapat keterkaitan yang memadai antara tindakan yang dilakukan dan akibat yang ditimbulkan.

Pemanfaatan perangkat lunak tanpa lisensi yang sah dapat menimbulkan persoalan hukum berdasarkan ketentuan hak cipta di Indonesia, di mana Undang-Undang Nomor 28 Tahun 2014 tentang Hak Cipta mengatur perlindungan terhadap program komputer sebagai salah satu bentuk ciptaan, termasuk pembatasan atas tindakan penggandaan atau pemanfaatannya yang melanggar hak pemegang hak cipta guna menjaga kepentingan ekonomi pencipta sekaligus memberikan perlindungan terhadap karya intelektual. Penggunaan perangkat lunak bajakan juga dapat menimbulkan risiko keamanan terhadap sistem elektronik yang digunakan karena umumnya tidak memperoleh pembaruan keamanan dari pengembang resmi sehingga memiliki tingkat kerentanan yang lebih tinggi terhadap berbagai bentuk serangan siber, yang berpotensi memberikan kesempatan kepada pelaku kejahatan siber untuk mengeksploitasi kelemahan keamanan pada sistem elektronik yang menjalankan perangkat lunak tersebut. Pemanfaatan perangkat lunak bajakan dapat menjadi indikasi bahwa aspek pertanggungjawaban (*accountability*) dalam perlindungan data pribadi belum diterapkan secara optimal, mengingat prinsip ini menuntut pengendali data untuk bertanggung jawab atas kegiatan pemrosesan data yang dilakukannya, termasuk memastikan bahwa sistem elektronik yang digunakan memiliki mekanisme pengamanan yang sesuai untuk melindungi data pribadi. Oleh karena itu, apabila suatu instansi tetap menggunakan perangkat lunak ilegal yang diketahui memiliki risiko keamanan tinggi, maka tindakan tersebut dapat dipandang sebagai bentuk pengabaian terhadap kewajiban kehati-hatian (*duty of care*) dalam pengelolaan sistem elektronik.

Pertanggungjawaban hukum atas suatu perbuatan perlu mempertimbangkan adanya keterkaitan sebab-akibat antara tindakan yang dilakukan dan konsekuensi yang muncul, di mana dalam hukum pidana, hubungan kausalitas berfungsi untuk menilai apakah akibat tertentu dapat dikaitkan dengan perbuatan seseorang sehingga dapat menjadi dasar dalam menentukan pertanggungjawaban atas akibat tersebut. Jika penggunaan perangkat lunak bajakan menimbulkan kerentanan pada sistem elektronik yang selanjutnya dieksploitasi oleh pelaku kejahatan siber untuk meretas data, kondisi tersebut dapat dinilai sebagai salah satu faktor yang turut berkontribusi terhadap terjadinya kebocoran data. Penetapan hubungan sebab-akibat secara hukum tetap memerlukan pembuktian bahwa kerentanan tersebut berkaitan dengan insiden peretasan yang terjadi, sementara pihak yang bertanggung jawab dalam pengelolaan sistem elektronik sendiri dapat dipandang telah melakukan kelalaian dalam menjaga keamanan sistem yang digunakan untuk mengelola data masyarakat. Kelalaian dalam hukum pidana dikenal sebagai *culpa*, yaitu keadaan di mana seseorang tidak melakukan kehati-hatian yang seharusnya dilakukan sehingga menimbulkan akibat yang merugikan.

Apabila suatu instansi yang mengelola data masyarakat menggunakan perangkat lunak bajakan yang memiliki risiko keamanan yang tinggi, maka penggunaan perangkat lunak tersebut dapat dipandang sebagai bentuk kelalaian dalam menjaga keamanan sistem elektronik, yang dapat menimbulkan tanggung jawab hukum apabila kerentanan sistem yang disebabkan oleh penggunaan perangkat lunak bajakan tersebut kemudian dimanfaatkan oleh pihak lain untuk melakukan peretasan data. Dalam proses penegakan hukum sendiri masih terdapat kesulitan dalam menentukan pertanggungjawaban hukum dalam kasus kebocoran data yang disebabkan oleh kelemahan sistem keamanan, yang berkaitan dengan belum terperincinya pengaturan dalam peraturan perundang-undangan Indonesia mengenai tolok ukur keamanan sistem elektronik yang wajib diterapkan oleh setiap penyelenggara sistem elektronik sehingga menyebabkan adanya kekosongan norma dalam menentukan batas tanggung jawab hukum pihak yang mengelola sistem elektronik apabila terjadi kebocoran data. Dengan demikian, dapat disimpulkan bahwa penggunaan perangkat lunak bajakan dalam sistem elektronik yang mengelola data masyarakat berpotensi menimbulkan pertanggungjawaban hukum apabila penggunaan perangkat lunak tersebut menyebabkan kerentanan sistem yang kemudian dimanfaatkan oleh pelaku kejahatan siber untuk melakukan peretasan data, sehingga diperlukan pengaturan hukum yang lebih jelas mengenai standar keamanan sistem elektronik agar dapat memberikan kepastian hukum dalam menentukan tanggung jawab pihak yang mengelola sistem elektronik yang menyimpan data pribadi masyarakat.

Solusi atau Upaya Pembaruan Hukum Pidana Siber untuk Memperjelas Pertanggungjawaban Hukum serta Memperkuat Perlindungan Data Nasional

Penggunaan perangkat lunak bajakan dalam sistem elektronik yang mengelola data pribadi masyarakat membawa implikasi hukum yang signifikan, di mana perbuatan tersebut tidak sekadar bersinggungan dengan pelanggaran hak cipta, melainkan berpotensi menimbulkan tanggung jawab hukum apabila penggunaan perangkat lunak tersebut menyebabkan kerentanan sistem yang kemudian dimanfaatkan oleh pelaku kejahatan siber untuk melakukan peretasan data. Penggunaan perangkat lunak bajakan dalam sistem elektronik dapat meningkatkan risiko keamanan karena perangkat lunak tersebut pada umumnya tidak memperoleh pembaruan keamanan resmi dari pengembang serta berpotensi mengandung *malware* atau program berbahaya, yang dapat membuka celah bagi pelaku kejahatan siber untuk memperoleh akses terhadap sistem elektronik yang menyimpan data masyarakat. Apabila kerentanan sistem tersebut mengakibatkan terjadinya kebocoran atau peretasan data pribadi, maka pihak yang bertanggung jawab dalam pengelolaan sistem elektronik dapat dimintai pertanggungjawaban hukum atas kelalaian dalam menjaga keamanan sistem yang digunakan.

Dalam perspektif pelindungan data pribadi, pengendali data memiliki kewajiban untuk memastikan bahwa sistem elektronik yang digunakan dalam pemrosesan data pribadi memiliki tingkat keamanan yang memadai, sehingga penggunaan perangkat lunak bajakan yang memiliki risiko keamanan tinggi dapat dipandang sebagai bentuk kelalaian dalam memenuhi kewajiban tersebut. Meskipun demikian, keberadaan perangkat lunak bajakan tidak serta-merta membuktikan bahwa perangkat lunak tersebut menjadi penyebab tunggal terjadinya

peretasan, melainkan hubungan antara penggunaan perangkat lunak, kerentanan sistem, dan terjadinya peretasan tetap harus dibuktikan melalui pemeriksaan teknis dan pembuktian hukum.

Permasalahan utama yang ditemukan dalam penelitian ini adalah belum terintegrasinya pengaturan mengenai hak cipta, penyelenggaraan sistem elektronik, dan pelindungan data pribadi dalam menentukan batas pertanggungjawaban hukum ketika penggunaan perangkat lunak bajakan berhubungan dengan terjadinya peretasan data. Undang-Undang Nomor 28 Tahun 2014 tentang Hak Cipta memberikan perlindungan terhadap program komputer, Pasal 15 ayat (1) Undang-Undang Informasi dan Transaksi Elektronik mewajibkan penyelenggaraan sistem elektronik secara andal dan aman, serta Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi memberikan kewajiban kepada pengendali data pribadi untuk melindungi data yang berada dalam penguasaannya. Ketiga peraturan tersebut memiliki ruang lingkup yang berbeda namun saling berkaitan, sehingga ketika penggunaan perangkat lunak bajakan diduga menjadi salah satu faktor yang menyebabkan kerentanan sistem dan berujung pada peretasan data, diperlukan harmonisasi peraturan perundang-undangan agar tidak berjalan secara terpisah. Berdasarkan teori *Stufenbau des Recht* yang dikemukakan oleh Hans Kelsen, harmonisasi tersebut diperlukan untuk membentuk kesatuan sistem hukum berjenjang yang tidak menimbulkan ketidakpastian dalam menentukan pertanggungjawaban.

Selain harmonisasi peraturan, pembaruan hukum perlu diarahkan pada penegasan standar keamanan sistem elektronik yang dijabarkan secara lebih konkret guna menjadi pedoman penegakan hukum. Penegasan standar keamanan tersebut mencakup kewajiban pemeriksaan keaslian perangkat lunak, keharusan melakukan pembaruan keamanan secara berkala, pembatasan hak akses pengguna, pelaksanaan audit keamanan sistem secara berkala, serta kepemilikan kebijakan internal mengenai penggunaan perangkat lunak pada perangkat kerja. Pengaturan mengenai standar keamanan tersebut juga harus disesuaikan dengan ketentuan Pasal 35 hingga Pasal 39 UU PDP yang mewajibkan pengendali data pribadi melakukan pencegahan terhadap risiko keamanan melalui penggunaan sistem elektronik yang andal dan aman. Dengan demikian, penggunaan perangkat lunak yang tidak jelas keabsahannya dalam sistem pengolahan data pribadi perlu ditempatkan sebagai bagian dari penilaian kepatuhan terhadap kewajiban pengamanan dan prinsip kehati-hatian (*duty of care*).

Penentuan batas pertanggungjawaban pidana terhadap pihak-pihak yang terlibat dalam pengelolaan sistem elektronik harus dilakukan secara selektif dengan memperhatikan kewenangan, tugas, pengetahuan, serta bentuk keterlibatan masing-masing pihak. Pegawai yang menggunakan perangkat lunak bajakan belum tentu memiliki kewenangan menentukan jenis perangkat lunak instansi, sehingga penentuan pertanggungjawaban wajib berlandaskan asas *geen straf zonder schuld* dan pembuktian unsur kesalahan baik kesengajaan (*dolus*) maupun kealpaan (*culpa*). Penilaian kealpaan didasarkan pada kewajiban kehati-hatian, kemampuan memperkirakan risiko, serta tindakan yang secara wajar dapat dilakukan untuk mencegah akibat, sehingga pertanggungjawaban pidana perlu dibedakan secara tegas dari tanggung jawab administratif atau kewajiban pelindungan data pribadi.

Upaya pembaruan hukum juga harus diiringi dengan penguatan tata kelola keamanan informasi di lingkungan penyelenggara sistem elektronik melalui kebijakan tertulis pengadaan perangkat lunak, pelaksanaan audit sistem secara berkala, evaluasi terhadap pihak ketiga, serta penyediaan alternatif perangkat lunak sumber terbuka (*open source*) yang sah dan aman. Apabila terjadi kegagalan pelindungan data pribadi, pengendali data wajib menyampaikan pemberitahuan tertulis paling lambat 3×24 jam kepada subjek data pribadi dan lembaga berwenang sebagaimana diatur dalam Pasal 46 dan Pasal 47 UU PDP, serta melakukan prosedur penanganan insiden termasuk pengumpulan bukti digital forensik. Terakhir, berdasarkan pemikiran Lon L. Fuller mengenai prinsip-prinsip legalitas dan moralitas hukum, pembaruan norma hukum siber harus dirumuskan secara jelas, konsisten, dan terarah agar mampu berfungsi sebagai pedoman perilaku yang efektif, mewujudkan kepastian hukum, serta memperkuat pelindungan data nasional secara optimal.

SIMPULAN

Pengaturan hukum positif terhadap penggunaan *software* bajakan yang berimplikasi pada peretasan data skala nasional masih mengandung kekaburan norma, yang diakibatkan oleh ketidaksinkronan substansial antara Undang-Undang Informasi dan Transaksi Elektronik, Undang-Undang Hak Cipta, dan Undang-Undang Pelindungan Data Pribadi. Ketiga instrumen hukum tersebut belum secara eksplisit mengatur korelasi kausal antara penggunaan perangkat lunak ilegal dan akibat lanjutan berupa kebocoran data, sehingga menciptakan ketidakpastian hukum dalam mematok batas pertanggungjawaban pidana, khususnya terhadap subjek hukum yang melakukan kealpaan (*culpa*).

Solusi strategis dan upaya pembaruan hukum pidana siber guna memperjelas pertanggungjawaban hukum serta memperkuat pelindungan data nasional wajib ditempuh melalui harmonisasi legislatif antara ketiga rezim undang-undang tersebut. Harmonisasi ini berfungsi untuk menyelaraskan parameter penggunaan perangkat lunak yang sah, mempertegas kewajiban pengamanan sistem elektronik, menetapkan standar keamanan yang konkret dan terukur, serta memetakan batasan pertanggungjawaban pidana berdasarkan kedudukan, kewenangan, unsur kesalahan, dan hubungan kausalitas masing-masing pihak. Dengan demikian, pembaruan hukum siber tidak hanya berorientasi pada aspek penegakan hukum yang represif dan berkeastian, melainkan turut mendorong efektivitas pencegahan melalui penguatan tata kelola keamanan sistem elektronik demi mewujudkan pelindungan data pribadi masyarakat secara optimal.

DAFTAR PUSTAKA

A. C. Sari, M. A. Syahputra, M. Irfansyahfalah, M. Y. Qardhawi, N. R. Maulana, P. D. L. Santoso, R. D. Fajri, R. Maulana, T. R. M. Zaki, W. Maeylani, dan S. Rinusantoro, “Edukasi Bahaya Software Bajakan serta Pengenalan Aplikasi Freeware sebagai Alternatif,” *Jurnal Kreativitas Mahasiswa Informatika*, Vol. 2, No. 2, 2021, hlm. 301–303.

Adami Chazawi, *Pelajaran Hukum Pidana*, Jakarta: Rajawali Pers, 2011.

Andi Hamzah, *Asas-Asas Hukum Pidana di Indonesia*, Jakarta: Rineka Cipta, 2010.

Ayik Teteki, Bambang Muryanto, dan Gilang Adikara, *Handbook Digital Safety*, Yogyakarta: Yayasan LKiS, 2023.

Barda Nawawi Arief, *Bunga Rampai Kebijakan Hukum Pidana*, Jakarta: Kencana, 2011.

Budi Suhariyanto, *Tindak Pidana Teknologi Informasi (Cybercrime)*, Jakarta: Rajawali Pers, 2012.

Chief Executive, "Almost 90% of Cyber Attacks Are Caused by Human Error Behavior".

CNN Indonesia, "83 Persen Perusahaan Indonesia Pakai Software Bajakan".

CNN Indonesia, "BSSN Bongkar Pemerintah Termasuk Software Bajakan," CNN Indonesia, 3 November 2023.

Danrivanto Budhijanto, *Cybersecurity Law: Pelindungan Data Virtual dan Infrastruktur Informasi Vital*, Bandung: Refika Aditama, 2022.

Danrivanto Budhijanto, *Hukum Telekomunikasi, Penyiaran dan Teknologi Informasi*, Bandung: Refika Aditama, 2013.

Deny Budiyanto dan Muhammad Mabruri, "Pentingnya Keamanan Siber dalam Era Digital: Tinjauan Global dan Kondisi di Indonesia," *Prosiding Seminar Nasional Sains dan Teknologi "SainTek"*, Vol. 2, No. 1, 2025.

Dewi Chirzah dan Rizqy Akbar Ramadhan, "Cyber War: Ancaman pada Keamanan Nasional," *The Journal Implementation of Data Science*, Vol. 1, No. 1, 2023.

Eddy Damian, *Hukum Hak Cipta*, Bandung: Alumni, 2014.

Edmon Makarim, *Pengantar Hukum Telematika*, Jakarta: Rajawali Pers, 2017.

Fadhila Rahman Najwa, "Analisis Hukum terhadap Tantangan Keamanan Siber: Studi Kasus Penegakan Hukum Siber di Indonesia," *AL-BAHTS: Jurnal Ilmu Sosial, Politik, dan Hukum*, Vol. 2, No. 1, 2024, hlm. 8–16.

Fortune Indonesia, "Kominfo Tanggapi Kebocoran Data 1,3 Miliar Kartu SIM di Situs Gelap," Fortune Indonesia, 1 September 2022.

Hanafi, *Dasar Cyber Security dan Forensic*, Yogyakarta: Deepublish, 2022.

Hani Puspita Sari, dkk., "Efektivitas Hukum Perlindungan Data Pribadi terhadap Kejahatan Siber di Indonesia," *Jurnal Media Akademik (JMA)*, Vol. 2, No. 12, 2024.

Husamuddin MZ, *Hukum Acara Pidana dan Pidana Cyber*, Jakarta: Prenadamedia Group, 2024.

IDN Times, "Data 279 Juta Penduduk Bocor, Ini Hasil Temuan Investigasi Kominfo," IDN Times, 21 Mei 2021.

Indriana Firdaus, "Upaya Perlindungan Hukum Hak Privasi terhadap Data Pribadi dari Kejahatan Peretasan," *Jurnal Rechten: Riset Hukum dan Hak Asasi Manusia*, Vol. 4, No. 2, 2022, hlm. 23–33.

Jurnaltinta.com, "Bukan Infrastruktur, Peretasan Pusat Data Nasional Bisa Dibol Diduga Karena Human Error, Sangat Besar".

Kompas Tekno, "5 Faktor Penyebab Kebocoran Data Menurut Pengamat".

Maskun, *Kejahatan Siber (Cyber Crime)*, Jakarta: Kencana, 2013.

Muhammad Fajrin, "Pertanggungjawaban Pidana terhadap Pelaku Tindak Pidana Peretasan (Hacker) dalam Undang-Undang Nomor 19 Tahun 2016 tentang Undang-Undang Informasi dan Transaksi Elektronik," *Jurnal Ilmu Hukum Fakultas Hukum Universitas Malikussaleh*, Vol. 5, No. 2, 2021.

Reuters, “Indonesia President Orders Audit of Data Centres After Cyberattack,” Reuters, 28 Juni 2024.

Sinta Dewi, *Konsep Perlindungan Data Pribadi*, Bandung: Refika Aditama, 2016.

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) beserta perubahannya.

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.

Undang-Undang Nomor 28 Tahun 2014 tentang Hak Cipta.