Sibatik Journal
Jurnal Ilmiah Bidang Sosial, Ekonomi, Budaya, Teknologi, dan Pendidikan
E-ISSN: 2809-8544

ANALISIS HUKUM TINDAK PIDANA *CYBER DATA BREACH* DI ERA DIGITAL BERDASARKAN UNDANG-UNDANG INFORMASI DAN TRANSAKSI ELEKTRONIK (STUDI PUTUSAN NOMOR 2447/PID.SUS/2024/PN MDN)

LEGAL ANALYSIS OF CYBERDATA BREACH IN THE DIGITAL ERA BASED ON THE ELECTRONIC INFORMATION AND TRANSACTIONS LAW (STUDY OF DECISION NUMBER 2447/PID.SUS/2024/PN MDN)

Ririn Silvana Silalahi[1]*, Mahmud Mulyadi[2], Wessy Trisna[3]
Universitas Sumatera Utara, Indonesia
Email: ririnsilvanasilalahi02@gmail.com[1]*, Mahmumulyadi.dr@gmail.com[2], wessy_trisna@yahoo.com[3]

Abstract

The rapid development of information technology has brought convenience to people's lives but also presents new challenges in the form of cybercrime, particularly Cyber Data breach which has serious impacts on personal data protection and individual privacy rights. Specifically, this research analyzes Cyber Data breach crimes from the perspective of Indonesian criminal law using normative juridical methods with statutory and case study approaches to Decision Number 2447/Pid.Sus/2024/PN Mdn, which shows that legal regulations regarding Cyber Data breach are still general and scattered across various regulations, especially the ITE Law and PDP Law, thus requiring crucial integration between these two laws so that prevention can be carried out comprehensively from both preventive and repressive aspects, where the panel of judges has applied the provisions of the ITE Law normatively and proportionally by using Article 30 paragraph (3) in conjunction with Article 46 paragraph (3) of the ITE Law as the legal basis for imposing imprisonment and fines on defendants who carried out unauthorized electronic information transfer.

Keywords: Legal Analysis, Cyber Data Breach Crime, ITE Law.

Abstrak

Perkembangan teknologi informasi yang pesat telah menghadirkan kemudahan dalam kehidupan masyarakat namun juga membawa tantangan baru berupa kejahatan siber, khususnya Cyber Data breach yang berdampak serius terhadap perlindungan data pribadi dan hak privasi individu. Secara khusus, penelitian ini menganalisis tindak pidana Cyber Data breach dalam perspektif hukum pidana Indonesia menggunakan metode yuridis normatif dengan pendekatan perundang-undangan dan studi kasus terhadap Putusan Nomor 2447/Pid.Sus/2024/PN Mdn, yang menunjukkan bahwa pengaturan hukum terhadap Cyber Data breach masih bersifat umum dan tersebar dalam berbagai regulasi terutama UU ITE dan UU PDP, sehingga diperlukan integrasi yang krusial antara kedua undang-undang tersebut agar penanggulangan dapat dilakukan secara komprehensif baik dari aspek preventif maupun represif, dimana majelis hakim telah menerapkan ketentuan UU ITE secara normatif dan proporsional dengan menggunakan Pasal 30 ayat (3) jo. Pasal 46 ayat (3) UU ITE sebagai dasar hukum dalam menjatuhkan pidana penjara dan denda kepada terdakwa yang melakukan pemindahan informasi elektronik secara tidak sah.

Kata kunci: *Analisis Hukum, Tindak Pidana Cyber Data Breach, Undang-Undang ITE.*

PENDAHULUAN

Kriminalisasi (*criminalization*) merupakan objek studi hukum pidana materiil (*substantive criminal law*) yang membahas penentuan suatu perbuatan sebagai tindak pidana (perbuatan pidana atau kejahatan) yang diancam dengan sanksi pidana tertentu. Perbuatan

DOI: https://doi.org/10.54443/sibatik.v4i9.3249

tercela yang sebelumnya tidak dikualifikasikan sebagai perbuatan terlarang dijustifikasi sebagai tindak pidana yang diancam dengan sanksi pidana.

Kriminalisasi merupakan hukum pidana materiil yang sebagai objek studi penentuan suatu tindakan sebagai delik atau tindak pidana dengan ancaman pidana tertentu. Perbuatan yang tidak terpuji yang awalnya tidak termasuk dalam perbuatan terlarang dikualifikasikan sebagai delik dengan ancaman sanksi pidana. Pendapat Soerjono Soekamto tingkah laku atau tindakan yang ditetapkan oleh penguasa yang dianggap oleh golongan atau oleh masyarakat sebagai nggapan perbuatan yang dapat pidana menjadi perbuatan pidana atau kriminal yang dpat dipidana oleh lembaga yang berwenang.

Teknologi komputer telah membawa suatu inovasi baru dalam kehidupan saat ini, yakni internet. Keberadaan internet kini menjadi sangat vital bagi manusia di seluruh dunia. Beberapa jenis bisnis bahkan tidak dapat beroperasi tanpa keterlibatan internet. Manusia semakin merasa nyaman menjalani aktivitas sehari-hari, dan mereka yang telah terbiasa dengan internet merasa tidak nyaman jika aksesnya terhambat. Fenomena internet dan digitalisasi memberikan dampak yang signifikan terhadap kehidupan manusia, membawa perubahan paradigmatik dalam berbagai sektor, termasuk kegiatan ekonomi, sosial, dan politik. Meskipun teknologi membawa kemudahan dan inovasi, namun kemajuan ini juga diiringi dengan tantangan baru, seperti maraknya kejahatan siber. Kejahatan siber telah menjadi ancaman global yang melintasi batas negara dan merugikan individu, perusahaan, serta pemerintahan.

Dalam pertimbangan Undang-Undang Nomor 11 Tahun 2008, disebutkan bahwa pesatnya perkembangan Teknologi Informasi telah mengakibatkan perubahan signifikan dalam kehidupan manusia di berbagai bidang, yang secara langsung mempengaruhi munculnya bentuk-bentuk perbuatan hukum baru. Teknologi informasi dan komunikasi telah mengubah perilaku masyarakat serta peradaban manusia secara global. Selain itu, kemajuan teknologi dan informasi telah menghapus batas-batas (*borderless*) di dunia, menyebabkan perubahan sosial yang terjadi dengan sangat cepat. Teknologi informasi kini menjadi alat dua sisi, memberikan kontribusi positif terhadap kesejahteraan dan kemajuan manusia, tetapi juga menjadi sarana efektif untuk tindakan melawan hukum. Sementara menciptakan peluang baru dalam kehidupan masyarakat, internet juga membuka peluang baru bagi tindak kejahatan. Di dunia maya, orang melakukan berbagai perbuatan jahat yang tidak dapat dilakukan di dunia nyata. Tindak kejahatan ini dilakukan dengan menggunakan komputer sebagai alat pelaksananya. Kejahatan di bidang telematika ini merupakan dampak negatif dari kemajuan teknologi yang berdampak luas pada berbagai aspek kehidupan modern saat ini. Indonesia memiliki peraturan utama yang mengatur informasi dan transaksi elektronik, yaitu Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, yang kemudian direvisi menjadi Undang-Undang Nomor 19 Tahun 2016. Undang-Undang ITE ini mengandung ketentuan-ketentuan yang melarang melakukan tindakan tertentu yang dapat dikenakan sanksi pidana. Di dalamnya, terdapat perbuatan-perbuatan yang dianggap sebagai tindak pidana komputer dengan sanksi yang telah ditetapkan.

DOI: https://doi.org/10.54443/sibatik.v4i9.3249

Munculnya teknologi internet menyebabkan munculnya golongan tindakan ilegal yang biasa disebut dengan *cybercrime* atau pelanggaran yang dilakukan melalui jaringan internet. Phishing merupakan contoh penting dari kejahatan dunia maya. Phishing dikategorikan sebagai jenis serangan *cyber* di mana penyerang berusaha memperoleh informasi pribadi atau rahasia secara tidak sah dari individu atau entitas dengan menyamar sebagai bisnis yang dapat dipercaya. Pelaku biasanya menggunakan strategi yang menipu, seperti membuat komunikasi elektronik, pesan teks, atau situs web palsu yang sangat mirip dengan platform sah, untuk menyesatkan individu yang tidak menaruh curiga agar mengungkapkan informasi sensitif, seperti kata sandi, rincian kartu kredit, atau data keuangan penting lainnya. Phishing adalah praktik umum yang bertujuan melakukan pencurian identitas, melakukan tindakan penipuan terkait informasi keuangan, atau secara tidak sah memperoleh akses tidak sah ke akun dan data korban.

Menurut Barda Nawawi Arief, upaya pencegahan tindak pidana, khususnya dalam hal tindak pidana siber, menunjukkan fokus kebijakan pada pembaharuan undangundang. Meskipun pembaharuan undangundang merupakan langkah yang penting, kompleksitas masalah tindak pidana siber menuntut pendekatan integral. Selain reformasi hukum, pendekatan ini juga melibatkan reformasi sosial, ekonomi, politik, budaya, moral, dan administratif.

Pemberantasan tindak pidana sering kali menggunakan sanksi pidana sebagai cara yang umum. Hingga saat ini, penerapan sanksi pidana terhadap tindak pidana siber dianggap sebagai metode yang diharapkan dapat memberantasnya. Dalam Rancangan KUHP tahun 2015, terdapat perubahan dalam ketentuan mengenai sistem pemidanaan, termasuk jenis dan ukuran pidana. Sistem double track diterapkan untuk pidana dan tindakan, sementara ukuran pidana mencakup minimum dan maksimum. Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) menjadi landasan hukum utama dalam menangani kejahatan siber di Indonesia. Namun, implementasi dan efektivitas UU ITE dalam penegakan hukum masih menghadapi berbagai kendala. Perubahan cepat dalam metode kejahatan siber, kurangnya kesadaran masyarakat terhadap ancaman digital, serta tuntutan regulasi yang terus berkembang menjadi faktor-faktor yang mempengaruhi penegakan hukum. Oleh karena itu, penelitian ini dilakukan untuk mengidentifikasi kendalakendala tersebut dan merumuskan upaya penanggulangan kejahatan siber yang lebih efektif di masa depan. Oleh karena itu, pola pemidanaan dalam Undang-Undang ITE perlu disesuaikan dengan pola pemidanaan yang diusulkan dalam konsep Rancangan KUHP terbaru ini. Efek dari sanksi pidana merupakan masalah empiris, karena persepsi manusia terhadap sanksi tersebut dapat bervariasi. Beberapa pihak berpendapat bahwa peningkatan kriminalitas disebabkan oleh sanksi atau hukuman yang terlalu ringan, sementara yang lain berpendapat bahwa sanksi yang terlalu ringan tidak akan memberikan efek jera yang cukup.

Dalam era globalisasi yang terus berkembang, kemajuan teknologi informasi, beserta pembentukan hukum teknologi informasi, memerlukan langkah-langkah antisipatif dari aparat penegak hukum. Langkah ini diperlukan agar tercapai keseimbangan dan tata pergaulan di tengah-tengah kehidupan kelompok, golongan, ras, dan suku, serta masyarakat

DOI: https://doi.org/10.54443/sibatik.v4i9.3249

di dalam negeri maupun dalam konteks hubungan regional dan internasional. Hal ini diharapkan dapat menciptakan perlindungan yang optimal dan kesejahteraan bagi masyarakat Indonesia, sesuai dengan tujuan nasional yang tercantum dalam alinea keempat UUD 1945, sekaligus sebagai elemen dasar penyelenggaraan negara hukum di Indonesia.

Namun, penerapan kebijakan kriminalisasi dalam UU ITE sering kali menimbulkan perdebatan, terutama terkait dengan ketentuan-ketentuan yang dianggap multitafsir dan berpotensi menimbulkan kriminalisasi yang berlebihan. Beberapa pasal dalam UU ITE, seperti yang mengatur tentang pencemaran nama baik dan ujaran kebencian, kerap menjadi kontroversi dalam praktik penegakan hukumnya. Oleh karena itu, diperlukan kajian lebih lanjut mengenai efektivitas kebijakan kriminalisasi dalam UU ITE dalam menanggulangi tindak pidana siber di era digital.

Ketidakoptimalan dalam penegakan hukum terhadap kejahatan siber disebabkan oleh kurangnya sarana dan fasilitas yang memadai. Penanggulangan kejahatan siber memerlukan alat karena kejahatan ini dapat dilakukan dengan berbagai perangkat, baik berwujud maupun tidak berwujud. Waktu dan tempat terjadinya kejahatan siber ditentukan oleh efektivitas alat yang digunakan, sehingga analisis telematika menjadi penting untuk mengungkap kejahatan tersebut. Onno W. Purbo menjelaskan bahwa cara untuk menelusuri, mendeteksi, dan menanggulangi kejahatan siber sangat bergantung pada aplikasi dan topologi jaringan yang digunakan. Beberapa aplikasi yang gnacktrack dan digunakan backtrack. termasuk Hal ini menunjukkan bahwa sarana dan fasilitas yang memadai memiliki peran krusial dalam penegakan hukum. Tanpa sarana atau fasilitas tertentu, penegakan hukum akan kesulitan mencapai tujuannya. Sarana dan fasilitas yang dibutuhkan meliputi tenaga manusia yang terdidik dan trampil, organisasi yang efisien, peralatan yang memadai, keuangan yang mencukupi, dan sebagainya. Jika hal-hal tersebut tidak terpenuhi, penegakan hukum tidak dapat berjalan dengan lancar.

METODE

Penelitian ini menggunakan metode penelitian hukum normatif dengan pendekatan yuridis normatif yang bersifat preskriptif untuk menganalisis pencemaran nama baik melalui media massa dari perspektif hukum. Sumber data yang digunakan adalah data sekunder berupa bahan hukum primer (UUD 1945, UU ITE, UU Perlindungan Data Pribadi, dan KUHP), bahan hukum sekunder (buku, artikel, jurnal), dan bahan hukum tersier (kamus hukum, ensiklopedia). Teknik pengumpulan data dilakukan melalui studi kepustakaan dan media elektronik, kemudian dianalisis menggunakan teknik analisis kualitatif normatif dengan mengkaji substansi KUHP tentang delik pencemaran nama baik, melakukan sinkronisasi horizontal terhadap undang-undang terkait, dan memperkuat interpretasi dengan doktrin-doktrin hukum yang relevan.

HASIL DAN PEMBAHASAN

Pengaturan Hukum Tindak Pidana *Cyber Data breach* Di Era Digital Berdasarkan Undang-Undang Informasi Dan Transaksi Elektronik

DOI: https://doi.org/10.54443/sibatik.v4i9.3249

Data breach adalah insiden di mana data pribadi atau informasi penting lainnya diakses, diungkapkan, atau dicuri oleh pihak yang tidak berwenang. Dalam konteks *cyber*, insiden ini biasanya terjadi karena serangan siber (*cyber*attack), kebocoran sistem, atau kelalaian pengelola data.

Cyber Data breach memiliki konsekuensi hukum karena menyangkut:

1. Hak atas privasi individu,
2. Kewajiban perlindungan data oleh penyelenggara sistem elektronik (PSE),
3. Potensi kerugian finansial dan reputasi.

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) ini adalah regulasi utama yang secara eksplisit mengatur pelanggaran data pribadi di Indonesia. Ketentuan penting, Pasal 39 ayat (1) pengendali data wajib memberitahukan subjek data pribadi jika terjadi kegagalan dalam pelindungan data pribadi. Pasal 58 pelanggaran terhadap ketentuan ini dapat dikenai sanksi administratif, termasuk denda maksimal 2% dari pendapatan tahunan. Pasal 67-70 ketentuan pidana (pidana penjara dan denda) jika kebocoran terjadi karena perbuatan melawan hukum, seperti memperoleh atau mengungkapkan data pribadi tanpa hak.

Undang-Undang Nomor 11 Tahun 2008 jo. UU No. 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE), undang – undang ini mengatur aspek kejahatan di dunia digital termasuk akses ilegal dan gangguan sistem elektronik. Ketentuan relevan Pasal 30-32 larangan akses tanpa hak ke sistem elektronik, manipulasi data, atau pengambilalihan data. Pasal 46 ancaman pidana penjara dan/atau denda bagi pelaku. Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE), aturan teknis untuk penyelenggara sistem elektronik. Ketentuan terkait Pasal 14-15 PSE wajib menjaga keandalan, keamanan, dan tanggung jawab atas sistem elektronik. Pasal 20 kewajiban PSE untuk menjaga kerahasiaan, keutuhan, dan ketersediaan data pribadi.

Peraturan Otoritas Jasa Keuangan dan BI (khusus sektor keuangan) POJK No. 11/POJK.03/2022 menyebut bahwa lembaga keuangan harus memiliki sistem keamanan informasi untuk mencegah insiden siber dan kebocoran data. Peraturan Bank Indonesia No. 23/6/PBI/2021 tentang perlindungan konsumen termasuk perlindungan data pribadi di sektor sistem pembayaran.

Pendekatan Pidana Digunakan apabila terdapat niat jahat (mens rea), pelanggaran dilakukan dengan sengaja untuk mendapatkan keuntungan, ada akibat yang menimbulkan kerugian pada korban. Contoh: Hacker membobol sistem e-commerce dan menjual data pelanggan. Pendekatan Administratif**,** PSE yang lalai melindungi data dapat dikenai sanksi administratif (teguran, denda, pembekuan izin). Mekanisme ini lebih menitikberatkan pada kepatuhan (*compliance*) daripada penjeraan. Tantangan Implementasi di Indonesia antara lain:

1. Minimnya kesadaran PSE terhadap pentingnya keamanan siber.
2. Ketidakjelasan definisi teknis dalam UU PDP dan UU ITE soal apa yang dimaksud sebagai "*Data breach*."
3. Kurangnya kesiapan teknologi dan infrastruktur pelindung data.

DOI: https://doi.org/10.54443/sibatik.v4i9.3249

4. Koordinasi antar lembaga yang belum optimal (Kominfo, BSSN, OJK, Kepolisian).
5. Budaya melaporkan insiden masih rendah dan banyak PSE menyembunyikan kebocoran karena takut reputasi buruk.

Cyber Data breach di Indonesia memiliki dasar hukum yang cukup lengkap, terutama setelah lahirnya UU PDP. Namun, penegakan hukumnya masih dalam tahap awal dan menghadapi tantangan dari sisi teknis, budaya pelaporan, dan kepatuhan. Ke depannya, penguatan kelembagaan dan edukasi publik menjadi kunci dalam meningkatkan efektivitas perlindungan data di era digital.

Perkembangan teknologi selain mambawa banyak manfaat dan keuntungan berupa semakin dipermudahnya hidup manusia, akan tetapi juga membawa nilainilai negatif misalnya sedemikain mudahnya para criminal melakukan tindak kejahatannya. Teknologi juga memberikan pengaruh yang cukup besar dalam pemahaman mengenai kejahatan terutama terhadap paham-paham dalam kriminologi yang menitikberatkan pada faktor manusia baik secara lahir maupun batin. Perkembangan teknologi merupakan salah satu faktor yang dapat menimbulakan terjadinya kejahatan, sedangkan kejahatan itu sendiri telah ada dan timbul sejak kejahatan itu sendiri ada.

Kejahatan sendiri merupakan perbuatan antisosial, tidak hanya terjadi dilingkungan masyarakat atau negara yang sedang berkembang, tetapi juga masyarakat atau negara yang sudah maju. Kejahatan terjadi tidak hanya terdapat dalam dunia nyata. Tetapi juga terdapat dalam dunia maya dengan formulasi yang berbeda dengan kejahatan konvensional karena semakin canggihnya teknologi. Meskipun belum ada kesepahaman mengenai definisi kejahatan teknologi informasi (*cyber crime*), namun ada kesamaan pengertian universal mengenai kejahatan komputer, hal ini dapat dimengerti karena kehadiran komputer yang sudah mengglobal mendorong terjadinya universalisasi aksi dan akibat yang dirasakan dari kejahatan komputer tersebut.secara umum yang dimaksud kejahatan komputer atau kejahatan didunia *cyber* adalah upaya untuk memasuki dan atau menggunakan fasilitas komputer atau jaringan komputer tanpa ijin dan dengan melawan hukum dengan atau tanpa menyebabkan perubahan dan atau kerusakan pada fasilitas komputer yang dimasuki atau diguakan tersebut.

Indra Safitri mengemukakan kejahatan dunia maya adalah jenis-jenis kejahatan yang berkaitan dengan pemanfaat sebuah teknologi informasi tanpa batas serta memiliki karakteristik yang kuat dengan sebuah rekayasa teknologi yang mengandalkan kepada tingkat keamanan yang tinggi dan kredibilitas dari sebuah informasi yang disampaikan dengan diakses oleh pelanggan internet. Dengan demikian jelaslah bahwa jika seseorang menggunakan komputer atau bagian dari jaringan komputer tanpa seijin yang berhak, tindakan tersebut sudah tergolong pada kejahatan komputer.

Kejahatan teknologi informasi yaitu komputer dan internet pada masa ini memang telah mewarnai pergaulan globalisasi kehidupan manusia. Kejahatan tersebut dapat timbul dari komputer maupun dari internet yang kita gunakan semagai media informasi dan kejahatan-kejahatan ini mengunakan teknologi informasi sebagai sasaran utama untuk mewujudkan niat tersebut.

DOI: https://doi.org/10.54443/sibatik.v4i9.3249

Kebijakan Hukum Pidana Terhadap Tindak Pidana Siber *Data Breach*

Kebijakan aplikasi (yudisial) adalah bagian dari kebijakan penegakan hukum (*law enforcement policy*) yang berfokus pada tahapan penerapan hukum oleh lembaga peradilan, terutama kepolisian, kejaksaan, dan pengadilan, dalam menindak pelanggaran hukum. Dalam konteks tindak pidana *Cyber Data breach*, kebijakan aplikasi mencakup:

1. Penyidikan oleh aparat penegak hukum (APH),
2. Penuntutan oleh jaksa,
3. Pemeriksaan dan pemidanaan oleh pengadilan,
4. Pelaksanaan putusan (eksekusi pidana).

Cyber Data breach adalah tindakan ilegal berupa: Akses tanpa hak ke sistem elektronik (hacking), pencurian dan penyebaran data pribadi, perusakan atau manipulasi data elektronik. Jenis kejahatan ini bersifat Transnasional, anonim, memerlukan keahlian teknis dalam digital forensics.

Tahapan Kebijakan Yudisial dalam Penanganan *Cyber Data breach* yaitu Penyidikan oleh Kepolisian (Direktorat Tindak Pidana Siber Bareskrim Polri**),** digital forensic terhadap perangkat dan jaringan, pelacakan log IP, geolokasi, metadata, Koordinasi dengan PSE (Google, Meta, ISP). Penuntutan oleh Kejaksaan Jaksa menilai kelengkapan berkas penyidikan, menentukan kelayakan pembuktian, menyusun surat dakwaan berdasarkan UU ITE atau UU PDP. Pemeriksaan dan Pemidanaan oleh Pengadilan Contoh putusan Putusan No. 2447/Pid.Sus/2024/PN Mdn

1. Terdakwa: Herbert
2. Delik: Transfer data elektronik tanpa hak (Pasal 32 ayat (2) jo Pasal 46 ayat (2) UU ITE)
3. Putusan: Pidana penjara 7 tahun dan denda Rp 50 juta
4. Pertimbangan hakim: Tindakannya membahayakan kerahasiaan sistem keuangan digital nasabah.

Eksekusi Putusan dilakukan oleh kejaksaan setelah putusan inkracht (berkekuatan hukum tetap). Arah Penguatan Kebijakan Aplikasi Yudisial yaitu Peningkatan kapasitas SDM Pelatihan forensik digital bagi aparat penegak hukum (Polri, Kejaksaan, Hakim). Pembaruan hukum acara pidana digital yaitu Penyusunan RUU Acara Pidana Khusus Kejahatan Siber. Kerja sama lintas sektor dan internasional yaitu Interpol, *ASEAN Cybercrime Initiative, Budapest Convention* (meski belum diratifikasi). Pemanfaatan alat bukti digital yaitu legalisasi penggunaan log, jejak audit sistem, metadata, dan bukti digital sebagai alat bukti sah.

Kebijakan aplikasi yudisial terhadap tindak pidana *Cyber Data breach* di Indonesia telah memiliki fondasi hukum yang memadai, tetapi menghadapi tantangan serius dalam hal kapasitas teknis, kerangka pembuktian, dan koordinasi antar lembaga. Oleh karena itu, dibutuhkan:

1. Reformasi hukum acara,
2. Pembentukan lembaga pengawasan data (otoritas PDP),
3. Penguatan sinergi antar penegak hukum dan sektor swasta,
4. Respons yudisial yang progresif dan adaptif terhadap perkembangan teknologi.

DOI: https://doi.org/10.54443/sibatik.v4i9.3249

Cybercrime merupakan salah satu sisi gelap dari kemajuan teknologi yang mempunyai dampak negatif sangat luas bagi seluruh bidang kehidupan modern saat ini. *Cybercrime* sebagai salah satu bentuk atau dimensi baru dari kejahatan masa kini yang mendapat perhatian masyarakat luas di dunia internasional. Kemajuan teknologi informasi dimanfaatkan sebagian orang dengan sangat mudah memasuki ruang lingkup kejahatan hanya dengan mengandalkan kemampuannya untuk menggerakkan sistem teknologi.

Kebijakan hukum pidana merupakan kebijakan dari negara melalui badan-badan yang berwenang untuk menerapkan peraturan-peraturan yang dikehendaki yang diperkirakan bisa digunakan dalam mengekspresikan apa yang terkandung dalam masyarakat dan untuk mencapai apa yang dicitacitakan. Kebijakan dan usaha untuk membuat peraturan hukum pidana yang baik hakikatnya tidak bisa dilepaskan dari tujuan penanggulangan kejahatan. Teknologi informasi diyakini membawa keuntungan yang besar bagi negara- negara di dunia. Lahirnya suatu rezim hukum baru ini dikenal dengan hukum *cyber*, diambil dari kata *cyber* law yaitu istilah hukum yang berkaitan dengan pemanfaatan teknologi informasi.

Terkait dengan hal tersebut, peraturan perundang-undangan yang mengatur tentang *cyber*crime di Indonesia bisa dibilang kita masih sangat tertinggal. Banyak yang menganggap bahwa keberadaan Kitab UndangUndang Hukum Pidana (KUH Pidana) tidak mampu menjangkau kejahatan baru tersebut, baru satu peraturan yang mengatur secara spesifik tentang *cyber*crime, yaitu Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Tentang Transaksi Elektronik yang telah diubah dengan Undang-Undang No. 19 Tahun 2016 tentang Perubahan Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Tentang Transaksi Elektronik (UU ITE). Namun adanya undang-undang itu belum dapat menekan keberadaan *cyber*crime karena masih terdapat kekurangan dalam undang-undang tersebut. Mengingat *cyber*crime merupakan suatu kejahatan mayantara yang bisa dilakukan tanpa mengenal batas ruang dan waktu, diperlukan suatu upaya pencegahan untuk menanggulanginya. Aktivitas pokok dari *cybercrime* yaitu penyerangan terhadap computer system dan communication system milik orang lain atau umum di dalam *cyberspace.*

Perubahan paradigma tersebut juga diikuti perubahan cara pandang baru, yaitu dokumentasi yang semula paper based menjadi *electronic based.* Transaksi online dalam proses keseluruhannya serba berbasis elektronik, misalnya digital signature, e-mail. Teknologi informasi tersebut membawa dampak bagi masyarakat secara luas, baik dampak positif maupun negatif. Dampak positifnya yaitu memperoleh berbagai kemudahan informasi, baik dari dalam maupun luar negeri, transaksi jarak jauh. Dampak negatifnya yaitu memberikan peluang melakukan berbagai kejahatan *cyber*, seperti pencurian, penipuan, pencemaran nama baik, perjudian, keasusilaan, perusakan, pengancaman, dan teror yang seluruhnya dikenal dengan *cybercrime*.

Cybercrime merupakan kejahatan yang bisa dilakukan oleh seseorang, sekelompok orang dan korporasi atau badan hukum dengan cara menggunakan atau dengan sasaran komputer atau sistem komputer atau jaringan komputer. Kejahatan ini terjadi di dunia maya sehingga mempunyai karakteristiknya berbeda dengan kejahatan tradisional. Fenomena *cybercrime* memang harus diwaspadai karena kejahatan ini berbeda dengan kejahatan lain

DOI: https://doi.org/10.54443/sibatik.v4i9.3249

pada umumnya, karena dapat dilakukan tanpa mengenal batas teritorial dan tidak memerlukan interaksi langsung antara pelaku dengan korban kejahatan.

Upaya penanggulangan *cybercrime* dalam perspektif hukum pidana dapat dilihat dari berbagai aspek, antara lain aspek kebijakan kriminalisasi (formulasi tindak pidana), aspek pertanggungjawaban pidana atau pemidanaan (aspek pembuktian dan alat bukti), dan aspek yurisdiksi. Terkait dengan hal tersebut, KUH Pidana masih bersifat konvensional, belum dikaitkan dengan erkembangan *cyber*crime secara langsung. Dengan demikian mengandung kelemahan dan keterbatasan dalam menghadapi perkembangan teknologi dan kejahatan berteknologi tinggi yang sangat bervariasi.

Usaha penanggulangan kejahatan dengan hukum pidana pada hakikatnya merupakan bagian dari usaha penegakan hukum (khususnya penegakan hukum pidana). Politik hukum pidana merupakan bagian dari kebijakan penegakan hukum. Penggunaan upaya hukum termasuk hukum pidana, sebagai salah satu upaya mengatasi masalah sosial termasuk dalam bidang kebijaksanaan penegakan hukum. Disamping itu bertujuan mencapai kesejahteraan masyarakat pada umumnya, maka kebijaksanaan penegakan hukum ini pun termasuk dalam kebijaksanaan sosial, yaitu segala usaha yang rasional untuk mencapai kesejahteraan masyarakat. Di dalam konstelasi hukum pidana Indonesia, tindak pidana *cyber* termasuk ke dalam kategori tindak pidana khusus meskipun dengan unsur yang utamanya dapat dipadankan dengan beberapa pasal-pasal di dalam KUH Pidana, namun dilakukan dengan cara-cara (modus) yang baru, sehingga dalam memerangi kejahatan ini dibutuhkan suatu instrumen hukum yang lebih jelimet. Seperti yang diterangkan Soerjono Soekanto bahwa salah satu faktorfaktor yang mempengaruhi penegakan hukum adalah sarana dan prasarana atau fasilitas yang mendukung penegakan hukum, karena faktor tersebut juga merupakan tolak ukur daripada efektivitas penegakan hukum.

Penegakan hukum kejahatan dunia maya di Indonesia menghadapi banyak tantangan yang sulit diatasi karena kejahatan dunia maya terus berkembang dan dinamis. Beberapa tantangan utama yang dihadapi dalam penanggulangan kejahatan dunia maya antara lain: Kurangnya Peraturan yang Memadai: Meskipun Indonesia memiliki Undang-Undang Informasi dan Transaksi Elektronik (ITE) yang dimaksudkan untuk mengontrol aktivitas dunia maya, undangundang tersebut sering dianggap tidak efektif dalam memerangi berbagai bentuk *cyber*crime yang semakin kompleks. UU ITE, yang disahkan pada tahun 2008, bertujuan untuk mengawasi transaksi elektronik dan melindungi data pribadi. Namun, undang-undang tersebut tidak sepenuhnya mengantisipasi kemajuan pesat dalam teknologi digital, seperti penggunaan blockchain, cryptocurrency, dan kecerdasan buatan (AI).

Peraturan saat ini perlu diperbarui untuk menangani jenis *cyber*crime baru yang memanfaatkan teknologi canggih ini. Pengumpulan Bukti Digital yang Rumit: Pengumpulan dan penyelidikan bukti digital dalam kasus *cyber*crime juga merupakan masalah yang signifikan. Data yang tersimpan di perangkat komputer, server, atau cloud seringkali merupakan informasi penting dalam penyidikan, tetapi dapat dengan mudah diubah atau dihapus. Selain itu, bukti digital biasanya tersebar di banyak tempat di dalam dan luar negeri, membuat pengumpulan bukti lebih sulit. Untuk menangani bukti elektronik ini secara sah

DOI: https://doi.org/10.54443/sibatik.v4i9.3249

dan efisien, penegak hukum membutuhkan perangkat forensik digital yang sangat canggih serta keterampilan teknis yang tinggi.

Sifat *Cybercrime* yang Lintas Negara: Sifat ini adalah lintas negara. Pelaku kejahatan dunia maya biasanya beroperasi dari luar negeri, yang membuat penegakan hukum di Indonesia sangat sulit. Ini membutuhkan kerja sama global yang lebih erat. Selain itu, perbedaan peraturan hukum di setiap negara sering menghambat proses ekstradisi pelaku *cybercrime* yang berada di luar negeri. Oleh karena itu, diperlukan mekanisme yang lebih efektif di tingkat internasional untuk memerangi kejahatan dunia maya yang mencakup lebih dari satu negara.

Keterbatasan Sumber Daya Manusia dan Infrastruktur: Kekurangan sumber daya manusia yang terlatih di bidang teknologi digital dan forensik komputer terus menjadi kendala yang signifikan bagi upaya Indonesia untuk memerangi *cyber*crime. Banyak penegak hukum tidak memiliki kemampuan untuk menangani kasus *cyber*crime yang kompleks. Selain itu, infrastruktur yang ada saat ini masih terbatas. Ini termasuk sistem pelacakan kejahatan dunia maya dan laboratorium forensik digital. Hal ini menyebabkan proses penanganan kasus kejahatan internet menjadi lebih lama dan tidak efisien. Untuk mengantisipasi perkembangan kejahatan yang terjadi melalui media teknologi informasi (internet), semenjak akhir Maret 2008, DPR RI telah mengesahkan Rancangan Undang-Undang Informasi dan Transaksi Elektronik (ITE) menjadi undang-undang. Regulasi yang telah dirancang sejak tahun 1999 secara umum dapat menjadi instrumen hukum yang memiliki akselerasi yang baik terhadap perkembangan kejahatan dunia maya. Namun, undang-undang ini juga memiliki permasalahan dalam beberapa hal tertentu, baik dari aspek non hukum maupun dari aspek hukumnya.

Penegak hukum di Indonesia mengalami kesulitan dalam menghadapi merebaknya *cyber*crime. Hal ini dilatarbelakangi masih sedikitnya aparat penegak hukum yang memahami seluk-beluk teknologi informasi (internet), di samping itu aparat penegak hukum di daerah pun belum siap dalam mengantisipasi maraknya kejahatan ini karena masih banyak aparat penegak hukum yang gagap teknologi "gaptek" hal ini disebabkan oleh masih banyaknya institusi-institusi penegak hukum di daerah yang belum didukung dengan jaringan Internet.

Tindak pidana siber memiliki karakteristik tersendiri yang berdampak pada kebijakan aplikatif, seperti: Lokus dan tempus delicti yang bisa tersebar di berbagai tempat dan waktu, pelaku bisa anonim atau menggunakan identitas palsu, barang bukti berupa data elektronik yang mudah dihapus atau dimodifikasi. Maka, kebijakan aplikatif dalam konteks ini mencakup:

1. Tahap Penyidikan oleh Kepolisian (terutama Direktorat Siber Bareskrim Polri) Pelacakan dan identifikasi pelaku menggunakan alat digital forensik, penyitaan data elektronik sebagai barang bukti (sesuai UU ITE Pasal 43 dan UU No. 8 Tahun 1981 tentang KUHAP), bekerjasama dengan ISP (Internet Service Provider) untuk memperoleh data log, IP address, dan metadata, penanganan kasus dilakukan oleh Tim Siber karena memerlukan spesialisasi teknis.

DOI: https://doi.org/10.54443/sibatik.v4i9.3249

2. Tahap Penuntutan oleh Jaksa**,** penuntut umum menyusun dakwaan berdasarkan hasil penyidikan dan menetapkan pasal yang relevan dari UU ITE dan/atau KUHP. Tantangan: mengkonkretkan unsur-unsur delik digital ke dalam logika hukum pidana klasik. Dalam praktik, jaksa juga mempertimbangkan nilai-nilai keadilan, kepentingan umum, dan kadang menggunakan pendekatan *restorative justice.*
3. Tahap Persidangan oleh Hakim**,** hakim menilai sah atau tidaknya alat bukti elektronik, termasuk apakah diperoleh secara sah. Hakim juga harus memahami bukti digital, jejak digital, dan analisis teknis yang diajukan oleh ahli digital forensik. Penggunaan keterangan ahli sangat krusial untuk membuktikan tindak pidana siber.

Tantangan dalam Kebijakan Aplikatif Penegakan Hukum Siber, minimnya kompetensi teknis aparat penegak hukum, terutama di daerah, dalam memahami seluk-beluk kejahatan digital. Keterbatasan perangkat digital forensik dan infrastruktur penunjang. Batas yurisdiksi dalam kejahatan siber lintas negara (cross-border *cyber*crime). Overkriminalisasi terhadap warganet karena pasal-pasal multitafsir dalam UU ITE. Ancaman terhadap kebebasan berekspresi, misalnya penggunaan Pasal 27 ayat (3) untuk membungkam kritik terhadap pejabat publik.

Upaya Peningkatan Kualitas Kebijakan Aplikatif Penguatan Kapasitas Aparat Penegak Hukum**.** Pelatihan dan pendidikan intensif di bidang digital forensik, keamanan siber, dan hukum teknologi informasi. Penempatan penyidik dan jaksa khusus untuk menangani kejahatan siber. Kolaborasi Lintas Sektor**,** kerja sama antara Polri, Kominfo, BSSN, PPATK, dan operator seluler. Kerja sama internasional dengan INTERPOL, ASEAN *Cyber*crime Working Group, dan negara-negara mitra dalam kasus cross-border. Penguatan SOP dan Pedoman Teknis**,** SOP tentang tata cara penyitaan bukti digital, prosedur penanganan konten ilegal, dan mitigasi siber. Penegakan hukum berbasis prinsip kehati-hatian (*due process of law*) agar tidak menimbulkan kriminalisasi. Pendekatan Restoratif**,** penggunaan pendekatan *restorative justice* untuk kasus ringan, seperti pencemaran nama baik non-struktural. Mempertemukan korban dan pelaku agar tercipta penyelesaian yang adil dan tidak membebani sistem peradilan.

Analisis Terhadap Pertimbangan Hakim Dalam Penanggulangan Tindak Pidana Siber Di Era Digital Berdasarkan Undang-Undang Informasi Dan Transaksi Elektronik Dalam Putusan Pengadilan Nomor Studi Putusan Nomor 2447/Pid.Sus/2024/PN Mdn

Tindakan Herbert dikualifikasikan sebagai tindak pidana berdasarkan: Pasal 32 ayat (2) jo. Pasal 48 ayat (2) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE), sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016, yang berbunyi:

Pasal 32 ayat (2):

"Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun memindahkan dan/atau mentransfer Informasi Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik orang lain yang tidak berhak."

Pasal 48 ayat (2):

DOI: https://doi.org/10.54443/sibatik.v4i9.3249

"Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32 ayat (2) dipidana dengan pidana penjara paling lama 9 (sembilan) tahun dan/atau denda paling banyak Rp3.000.000.000,00 (tiga miliar rupiah)."

Analisis Unsur Delik:

1. "Dengan sengaja" Herbert melakukannya dengan niat (dolus), bukan karena kelalaian (culpa). "Tanpa hak atau melawan hukum" Tidak ada hak atau izin dari pemilik sistem elektronik yang datanya dipindahkan.
2. "Dengan cara apa pun memindahkan atau mentransfer informasi elektronik" Termasuk penggunaan software, akses jarak jauh, atau teknik digital lainnya untuk mengalihkan data secara tidak sah.
3. "Kepada sistem elektronik orang lain yang tidak berhak" Herbert memindahkan data ke sistem yang seharusnya tidak mengakses atau menyimpan informasi tersebut.

Majelis Hakim menyatakan bahwa semua unsur delik terpenuhi secara sah dan meyakinkan. Oleh karena itu, Herbert dinyatakan bersalah. Putusan ini menunjukkan keseriusan hukum dalam melindungi data dan sistem elektronik serta mendukung kebijakan nasional terkait keamanan siber dan privasi informasi.

Hakim harus mampu merefleksikan setiap teks pasal yang terkait dengan fakta kejadian yang ditemukan di persidangan ke dalam putusan hakim yang mengandung nilai-nilai Pancasila dan nilai-nilai konstitusi dasar dalam UUD 1945, sehingga setiap putusan hakim memancarkan pertimbangan nilai filosofis tinggi, konkretnya ditandai oleh karakter putusan yang berketuhanan, berperikemanusiaan, menjaga persatuan, penuh kebajikan, dan berkeadilan sosial bagi seluruh rakyat Indonesia. Filsafat harus masuk membantu pikiran hakim menyusun pertimbangan putusannya, sehingga putusan hakim mengandung nilai nilai keadilan filosofis. Putusan hakim yang baik harus mengandung 3 (tiga) pokok pertimbangan meliputi pertimbangan keadilan filosofis, pertimbangan keadilan sosiologis, dan pertimbangan keadilan yuridis. "Demi Keadilan Berdasarkan Ketuhanan Yang Maha Esa", Agar putusan tersebut dapat dilaksanakan, karena dengan demikian putusan akan mempunyai kekuatan eksekutorial dan memberi kekuasaan untuk dapat dilaksanakan.

Putusan ini mencerminkan penerapan prinsip *"nullum crimen sine lege*" dan pentingnya kriminalisasi terhadap kejahatan siber, sejalan dengan: Pendekatan Penal Hukum Pidana: Memberikan efek jera Pendekatan Non-Penal: Mendorong kesadaran publik akan keamanan siber Aspek Preventif: Mengantisipasi penyalahgunaan sistem informasi di era digital.

Unsur-unsur Pidana yang Dipenuhi Perbuatan dengan sengaja dan tanpa hak atau melawan hukum Terdakwa melakukan akses dan pemindahan data secara sadar tanpa otorisasi. Memindahkan atau mentransfer informasi elektronik Herbert mentransfer data dari satu sistem elektronik ke sistem lain. Kepada sistem elektronik orang lain yang tidak berhak Tindakan diarahkan pada sistem elektronik yang tidak dimiliki atau dikuasai oleh terdakwa. Hakim dalam pertimbangannya menyatakan bahwa semua unsur dalam Pasal 32 ayat (2) telah terpenuhi, sehingga terdakwa dijatuhi pidana penjara dan/atau denda sebagaimana diatur dalam Pasal 48 ayat (2).

DOI: https://doi.org/10.54443/sibatik.v4i9.3249

Analisis dari Perspektif *Cyber*law Perlindungan Data Elektronik *Cyber*law Indonesia menekankan pentingnya hak atas privasi digital dan integritas sistem elektronik. Herbert telah melanggar prinsip-prinsip ini dengan mengakses dan memindahkan data tanpa izin. Amanat UU ITE merupakan manifestasi dari *cyber*law nasional yang mengatur kejahatan berbasis teknologi. Dalam konteks ini, pemindahan data tanpa hak adalah bentuk pelanggaran terhadap integritas dan keamanan siber. Penguatan Peran Negara, melalui UU ITE dan aparat penegak hukum, menunjukkan bahwa pelanggaran terhadap hak-hak digital merupakan tindak pidana yang serius dan layak untuk dikriminalisasi.

Analisis dari Pendekatan Hukum Pidana Kebijakan Kriminalisasi tindakan Herbert masuk dalam kategori perbuatan yang telah dikriminalisasi secara tegas. Ini menunjukkan bahwa legislator telah menerapkan kebijakan penal untuk memberikan efek jera dan perlindungan hukum.

1. Tujuan Pemidanaan Pemidanaan terhadap Herbert tidak semata-mata untuk menghukum, tetapi juga memiliki dimensi preventif dan edukatif, baik bagi pelaku maupun masyarakat umum.
2. Penerapan Asas Legalitas Putusan tersebut mencerminkan penerapan asas *nullum delictum nulla poena sine lege* (tidak ada perbuatan pidana tanpa ketentuan pidana terlebih dahulu), yang menjadi asas fundamental dalam hukum pidana.

Implikasi terhadap Sistem Hukum Penerapan *Cyber*law dalam Praktik Peradilan Putusan ini merupakan preseden penting bagi penegakan hukum siber di Indonesia, memperlihatkan bahwa hukum mampu mengikuti dinamika kejahatan digital. Tantangan Penegakan Kendala teknis seperti pembuktian digital, kebutuhan digital forensik, dan kapasitas SDM masih menjadi hambatan dalam proses pembuktian dan pengadilan perkara siber. Urgensi Harmonisasi Regulasi Ke depan, perlu ada harmonisasi antara UU ITE dengan RKUHP serta penguatan aspek internasional dalam menanggulangi kejahatan siber lintas negara.

Putusan Nomor 2447/Pid.Sus/2024/PN Mdn memperlihatkan bahwa kriminalisasi terhadap pemindahan data elektronik secara ilegal telah memiliki dasar hukum yang kuat dalam sistem hukum Indonesia. Dari sudut pandang *cyber*law, perbuatan Herbert merusak tatanan hukum digital yang melindungi hak dan privasi. Sementara dari sudut hukum pidana, kriminalisasi dan pemidanaan terhadap perbuatan ini merupakan bentuk pertanggungjawaban hukum yang adil, sejalan dengan asas dan teori hukum pidana.

KESIMPULAN

Penelitian ini menyimpulkan bahwa pengaturan hukum terhadap tindak pidana *Cyber Data breach* di Indonesia masih bersifat umum dan tersebar dalam berbagai regulasi, terutama UU ITE dan UU PDP, dengan penegakan hukum yang masih menghadapi tantangan serius akibat keterbatasan kapasitas aparat, minimnya alat bukti elektronik, dan hambatan yurisdiksi lintas negara. Kebijakan hukum pidana saat ini belum memadai dalam aspek formulasi, aplikasi, dan eksekusi karena masih bersifat reaktif dan parsial tanpa mengatur mekanisme pertanggungjawaban pidana secara khusus terhadap pelaku kebocoran

DOI: https://doi.org/10.54443/sibatik.v4i9.3249

data digital. Analisis terhadap Putusan Nomor 2447/Pid.Sus/2024/PN Mdn menunjukkan bahwa hakim telah menerapkan UU ITE secara normatif dan proporsional dengan mempertimbangkan dampak sosial kejahatan siber, namun masih diperlukan peningkatan kapasitas aparat penegak hukum dan harmonisasi regulasi. Oleh karena itu, penelitian ini merekomendasikan evaluasi dan pembaruan regulasi UU ITE secara berkala, pembuatan pedoman nasional baku (SOP) untuk seluruh tahap penegakan hukum, serta peningkatan pelatihan berkala mengenai *cybercrime* dan digital forensik bagi aparat penegak hukum agar dapat menangani kasus serupa dengan lebih komprehensif dan efektif di masa depan.

DAFTAR PUSTAKA

Aldo, Dasril. *Pengantar Teknologi Informasi*. Jakarta: Insan Cendikia Mandiri, 2020.

Alamsyah, Firdaus. *Cybercrime dan Hukum di Indonesia: Analisis Perkembangan dan Tantangan*. Jakarta: Sinar Grafika, 2018.

Arief, Barda Nawawi. *Masalah Penegakan Hukum Dan Kebijakan Hukum Pidana Dalam Penanggulangan Kejahatan*. Ed. 1. Jakarta: Kencana Predana Media Group, 2008.

--------. *Pembaharuan Hukum Pidana dalam Perspektif Kajian Perbandingan*. Bandung: Pranamedia Group, 2005.

--------. *Tindak Pidana Mayantara: Perkembangan Kajian Cyber crime di Indonesia*. Jakarta: PT RajaGrafindo Persada, 2006.

Bahri, Idik Saeful. *Cyber crime Dalam Sorotan Hukum Pidana*. Jakarta: Bahasa Rakyat, 2020.

Casey, Eoghan. *Digital Evidence and Computer Crime*. London: A Harcourt Science and Technology Company, 2001.

Fitri, J. "Pengaruh Internet Banking dan Cyber crime Terhadap ke percayaan Nasabah di Perbankan Syariah." Skripsi S1 Universitas Islam ArRaniry Banda Aceh, 2021.

Golose, Petrus Reinhard. "Perkembangan Cybercrime dan Upaya Penanganannya di Indonesia Oleh Polri." Makalah pada Seminar Nasional tentang "Penanganan Masalah Cybercrime di Indonesia dan Pengembangan Kebijakan Nasional yang Menyeluruh Terpadu", diselenggarakan oleh Deplu. BI, dan DEPKOMINFO, Jakarta, 10 Agustus 2006.

Gulo, Ardi Saputro, Sahuri Lasmadi, dan Kabib Nawawi. "Cyber crime dalam Bentuk Phising Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik." *Pampas Journal Law Criminal Law* Vol. 1, No. 2 (2020).

Harahap, M. Yahya. *Pembuktian dan Penyidikan dalam Tindak Pidana Siber*. Jakarta: Sinar Grafika, 2020.

Hariyono, A. G., dan F. Simangunsong. "Perlindungan Hukum Korban Pencurian Data Pribadi (Phising Cybercrime) dalam Perspektif Kriminologi." *Jurnal of Law and Social-Political Governance* Vol. 3, No. 1 (2023).

Julianti, Lis, dan Anak Agung Putu Wiwik Sugiantar. "Tanggung Jawab Hukum Perbankan Dalam Pencurian Data Pribadi Nasabah Dengan Tekhnik "Phising" Pada Transaksi

DOI: https://doi.org/10.54443/sibatik.v4i9.3249

Perbankan." *PROSIDING SEMINAR NASIONAL FH UNMAS DENPASAR* Vol. 1 (2021).

Manthovani, Reda. *Problematika & Solusi Penanganan Kejahatan Cyber di Indonesia*. Jakarta: Malibu, 2006.

Mansur, Dikdik M. Arief, dan Elisatris Gultom. *Cyber Law: Aspek Hukum Teknologi Informasi*. Bandung: Refika Aditama, 2005.

Ohoitimur, Johanis. "Disrupsi: Tantangan bagi Perkembangan Ilmu Pengetahuan dan Peluang bagi Lembaga Pendidikan Tinggi." *Jurnal Respons* Vol. 23, No. 02 (2018).

Prasetyo, Teguh. *Kriminalisasi dalam Hukum Pidana*. Yogyakarta: Nusa Media, 2016.

Pratama, Ali. *Cyber Law: Aspek Hukum dan Regulasi dalam Dunia Digital di Indonesia*. Jakarta: Rajawali Pers, 2022.

Ramli, Ahmad M. *Cyber Law & HAKI Dalam Sistem Hukum Indonesia*. Ed. 1. Bandung: Refika Aditama, 2024.

Shiefti, Alyusi Dyah. *Media Sosial Interaksi, Identitas, dan Modal Sosial*. Jakarta: Prenada Media, 2019.

Soekanto, Soerjono. *Faktor-faktor yang Mempengaruhi Penegakkan Hukum*. Jakarta: Raja Grafindo Persada, 2007.

----------. *Sosiologi Suatu Pengantar*. Jakarta: Rajawali Press, 2005.

Subagyo, Agus. *Evolusi Hukum Pidana Siber di Indonesia: Tinjauan Historis dan Konseptual*. Jakarta: Penebar Swadaya, 2021.

Suhariyanto, Budi. *Tindak Pidana Teknologi Informasi (Cybercrime) Urgensi Pengaturan dan Celah Hukumnya*. Depok: Rajagrafindo Persada, 2013.

Susanto, Hadi. *Hukum dan Teknologi Informasi: Kajian Hukum Pidana Siber*. Bandung: CV Putra Media Nusantara, 2022.

Wahib, Abdul, dan Mohammad Labib. *Kejahatan Mayantara (Cyber crime)*. Bandung: Refika Aditama, 2005.

Wignjosoebroto, Soetandyo. "Kriminalisasi Dan Dekriminalisasi: Apa Yang Dibicarakan Sosiologi Hukum Tentang Hal Ini." Disampaikan dalam Seminar Kriminalisasi Dan Dekriminalisasi Dalam Pebaruan Hukum Pidana Indonesia, Fakultas Hukum UII, Yogyakarta, 15 Juli 1993.Pengukuhan Jabatan Guru Besar Tetap, Universitas Sumatera Utara, 2006.

DOI: https://doi.org/10.54443/sibatik.v4i9.3249