Rewang Rencang : Jurnal Hukum Lex Generalis. Vol.6. No.7 (2025)
Tema/Edisi : Hukum Pidana (Bulan Ketujuh)
https://jhlg.rewangrencang.com/

ANALISIS KRITIS PENEGAKAN HUKUM KEJAHATAN SIBER *DATA BREACH* DALAM PERSPEKTIF HUKUM PIDANA INDONESIA

CRITICAL ANALYSIS OF LAW ENFORCEMENT OF CYBER CRIME DATA BREACH FROM THE PERSPECTIVE OF INDONESIAN CRIMINAL LAW

Raden Andhitya dan Jamaludin Umam

Universitas Islam Nusantara Bandung Indonesia

Korespondensi Penulis : radenandhitya@uninus.ac.id, jamaludinumam@gmail.com

Citation Structure Recommendation :

Andhitya, Raden dan Jamaludin Umam. *Analisis Kritis Penegakan Hukum Kejahatan Siber Data Breach dalam Perspektif Hukum Pidana Indonesia*. Rewang Rencang : Jurnal Hukum Lex Generalis. Vol.6. No.7 (2025).

ABSTRAK

Majunya teknologi dibarengi dampak negatif yang ditimbulkan, seperti kejahatan *data breach.* Menindaklanjuti hal tersebut, Indonesia telah memiliki kerangka hukum dalam mengatasinya meski dalam implementasinya dihadapkan dengan tantangan. Tujuan penelitian ini untuk menganalisis kerangka hukum serta mengevaluasi penanganan tindak kejahatan *data breach* di Indonesia. Penelitian ini berjenis penelitian kualitatif dengan metode deskriptif analistis yang didasarkan atas data studi kepustakaan. Hasil penelitian ini disimpulkan bahwa, kerangka hukum normatif yang digunakan dalam penanganan kejahatan *data breach* di Indonesia adalah Undang-Undang ITE dan PDP. Dalam implementasinya, ketentuan ini dihadapkan dengan tantangan diantaranya dalam pengumpulan bukti digital, keterbatasan pemahaman aparat, serta kurangnya koordinasi antar lembaga.

Kata Kunci: Data Breach, Hukum Pidana, Penegakan Hukum, Siber

ABSTRACT

Advances in technology are accompanied by negative impacts, such as data breach crimes. In response to this, Indonesia has established a legal framework to address this issue, although its implementation faces challenges. The purpose of this study is to analyze the legal framework and evaluate the handling of data breach crimes in Indonesia. This research is qualitative in nature, using a descriptive analytical method based on literature review. The findings of this study conclude that the normative legal framework used in addressing data breach crimes in Indonesia is the ITE Law and the PDP. In its implementation,these provisions face challenges, including in the collection of digital evidence, limited understanding among law enforcement officials, and a lack of coordination between institutions.

Keywords: Criminal Law, Cyber, Data Breach, Law Enforcement

A. PENDAHULUAN

Globalisasi dipandang memiliki dampak yang pesat terhadap perkembangan teknologi. Bahkan, globalisasi sebagai katalis utamanya yang mendorong kemajuan ini. Akibat pengaruh daripada globalisasi, Indonesia mengalami berbagai perkembangan pesat salah satunya dalam pengadopsian serta penerapan teknologi canggih yang diterapkan di berbagai sektor. Hal ini menunjukkan bahwa Indonesia telah memasuki era digital dengan serta adanya kemajuan teknologi tersebut. Menurut data Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), tercatat penertrasi teknologi internet telah mencapai 78% dari total populasi di Indonesia pada tahun 2023.[1] Berbanding lurus dengan realitas, telah tampak mayoritas masyarakat di Indonesia dalam kesehariannya selalu bergantung pada layanan internet seperti *mobile banking, e-commerce,* hingga media sosial. Tentu dengan adanya kemajuan teknologi (internet) satu sisi berdampak positif dan memudahkan masyarakat dalam menjalankan kesehariannya sebagai sarana perbankan transaksi, jual beli, hingga komunikasi dan bahkan masih banyak lainnya dari dampak positif adanya kemajuan teknologi ini. Namun meski teknologi memiliki banyak dampak positif yang memudahkan masyarakat dalam berbagai pekerjaan dan keseharian, tentu saja justru atas dampak positif ini dibarengi dengan dampak negatif yang ditimbulkan dan tidak bisa dihindari.

Dampak negatif atas kemajuan teknologi yang dimaksud seperti meningkatnya modus operandi tindak kejahatan-kejahatan di dunia maya salah satunya adalah tindak kejahatan siber di Indonesia. Sejalan dengan pernyataan ini, Barda Nawawi Arief pakar hukum pidana dari Universitas Diponegoro menyatakan bahwa kejahatan di Indonesia terus berevolusi dengan modus operandi yang semakin caggih dan kompleks. Berdasarkan catatan dari Badan Siber dan Sandi Negara (BSSN) telah terjadi lebih dari 1,2 miliar serangan siber yang terjadi di Indonesia sepanjang tahun 2022.

---

[1] Bisnis.com, *Survei APJII Pengguna Internet di Indonesia Tembus 215 Juta Orang*, diakses dari *https://apjii.or.id/berita/d/survei-apjii-pengguna-internet-di-indonesia-tembus-215-juta-orang#:~:text=Survei APJII Pengguna Internet di Indonesia Tembus,dari total populasi yang sebesar 275.773.901 jiwa*, diakses pada 31 Agustus 2025.

Akibat dari serangan siber itulah, Indonesia mengalami kerugian ditaksir mencapai triliunan rupiah.[2] Berbagai bentuk kejahatan serangan siber sebagai dampak dari majunya teknologi yang semakin canggih, antaranya pencurian data, peretasan sistem, penyebaran *malware,* hingga penipuan online. Menindaklanjuti hal tersebut, perlu kiranya diciptakan perlindungan dan penegakan hukum yang tegas serta ruang digital yang aman dan terpercaya guna melindungi masyarakat dari ancaman kejahatan-kejahatan siber tersebut.[3]

Sebagaimana disebutkan sebelumnya atas pengadopsian dan kemajuan teknologi di era digital ini memberikan tantangan tersendiri khususnya berkenaan bagaimana kita menyikapi dan memanfaatkan kemajuan teknologi tersebut dengan benar dan bijak. Atas kemajuan teknologi ini, tidak sedikit justru sebagian oknum memanfaatkannya untuk melakukan suatu tindakan-tindakan yang tidak bijak dan tidak benar, seperti halnya melakukan tindak kejahatan di dunia maya. Tindak kejahatan di dunia maya ini merupakan bentuk kejahatan yang terjadi dalam dimensi tidak biasa seumpama kejahatan umumnya yang terjadi, hal ini kian mengundang banyak sorot perhatian masyarakat luas nasional hingga internasional. Salah satu bentuk tindak kejahatan dunia maya yang dimaksud adalah tindak kejahatan siber. Berdasarkan laporan tahunan profil keamanan siber Indonesia yang dirilis oleh Badan Siber dan Sandi Negara (BSSN) bahwa sepanjang tahun 2023 telah tercatat sebanyak 1.318.296.114 serangan siber yang terjadi di Indonesia.

Angka tersebut mengalami peningkatan yang signifikan dengan sebelumnya dari jumlah insiden kejahatan siber di Indonesia. Salah satu bentuk kejahatan siber yang terjadi di Indonesia diantaranya adalah *data breach*. *Data breach* merupakan insiden kebocoran data pribadi dalam skala besar. Fenomena kebocoran data bersakala besar atau *data breach* ini menjadi ancaman yang serius dan nyata termasuk bagi Indonesia. Fenomena kejahatan *data breach* yang dilakukan oleh oknum yang tidak bertanggung jawab, sebelumnya terjadi di Indonesia yang menimpa aplikasi bernama eHAC *(electronic-Health Alert Card)*

---

[2] Sri Adningsih, *Transformasi Ekonomi Berbasis Digital di Indonesia: Lahirnya Tren Baru Teknologi, Bisnis, Ekonomi, dan Kebijakan di Indonesia*, Gramedia Pustaka Utama, Jakarta, 2019, p.12.

[3] Taufiq A. Gani, *Kedaulatan Data Digital untuk Integritas Bangsa*, Syiah Kuala University Press, Banda Aceh, 2023.

yang merupakan aplikasi milik Kementerian Kesehatan yang berfungsi untuk membuat kartu kewaspadaan kesehatan elektronik. Dilansir dari BBC News, kebocoran data bersakala besar atau *data breach* pada aplikasi eHAC tersebut terjadi pada tahun 2021 dimana sekitar 1.3 juta data pengguna aplikasi bocor dan dijual di *dark web*.[4] Dampak yang ditimbulkan atas insiden kebocoran data pada aplikasi eHAC tersebut tentu sangatlah merugikan masyarakat luas khususnya masyarakat Indonesia. Diantara dampak akibat atas peretasan atau kebocoran data bersakala besar atau *data breach* korban dapat mengalami kerugian finansial, pencemaran nama baik, gangguan psikologis, hingga pencurian identitas. Tindak kejahatan *data breach* ini seperti dilansir pada kasus eHAC, dapat merusak kepercayaan publik terhadap sistem digital khususnya pemerintah selebihnya dapat menghambat perkembangan ekonomi di Indonesia.

Tindak kejahatan *data breach* yang merupakan salah satu bentuk tindak kejahatan siber yang terjadi di era digital ini seringkali menjadi suatu masalah yang pelik terselesaikan. Bahkan, tindak kejahatan semacam kejahatan siber ini tidak mengenal batas wilayah teritorial suatu negara, ini terjadi karena sifatnya yang transnasional sehingga dalam penangannnya perlu koordinasi dan kerjasama antar negara dalam pemberantasannya. Menghadapi ancaman tindak kejahatan siber ini, dalam teritorialnya negara Indonesia telah menyusun kerangka hukum guna menghadapi kasus semacam ini. Kerangka hukum ini diciptakan dan dimaksudkan untuk menciptakan suatu kondisi yang diharapkan. Sebagaimana tujuan hukum itu sendiri adalah untuk menjaga suatu keadaan sesuai harapan, memastikan akan ketertiban, keamanan, kepercayaan, dan keadilan. Misalnya dalam menghadapi ancaman tindak kejahatan *data breach* yang merupakan bentuk tindak kejahatan siber ini, pemerintah Indonesia telah menyusun Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), beserta perubahannya dalam UU Nomor 19 Tahun 2016, menjadi payung hukum utama dalam menangani kejahatan siber, termasuk *data breach*. UU ITE mengatur berbagai aspek kejahatan siber, mulai dari akses ilegal, intersepsi ilegal, modifikasi data, penyebaran konten ilegal, hingga penipuan online.

[4] BBC News, *Data eHAC Milik 1,3 Juta Penggunanya Dilaporkan Bocor, 'Keamanan Data Tidak Prioritas*, diakses dari *https://www.bbc.com/indonesia/indonesia-58393345*, diakses pada 31 Agustus 2025.

Kendati Undang-Undang Informasi dan Transaksi Elektronik telah disusun sebagai kerangka dan patung hukum guna menghadapi dan menangani tindak kejahatan siber salah satunya adalah kejahatan *data breach.* Namun dalam implementasinya menghadapi dan menangani kejahatran data breach ini¸ditemukan masih menghadapi sejumlah tantangan sehingga dalam prosesnya cukup pelik untuk diselesaikan. Salah satu tantangan utama adalah kurangnya pemahaman aparat penegak hukum tentang teknologi informasi dan modus operandi kejahatan siber yang semakin kompleks. Hal ini menyebabkan kesulitan dalam penyelidikan, pengumpulan bukti digital, dan pembuktian di persidangan. Selain itu, terdapat juga permasalahan dalam koordinasi antar instansi penegak hukum, seperti kepolisian, kejaksaan, dan pengadilan. Kurangnya sinkronisasi dan standar operasional prosedur yang jelas dapat menghambat proses penegakan hukum terhadap kasus *data breach*. Putusan pengadilan yang belum memberikan efek jera juga menjadi sorotan. Hukuman yang ringan bagi pelaku kejahatan siber dikhawatirkan tak akan mencegah kejahatan serupa berulang di kemudian hari.[5]

Berangkat dari kerangka hukum yang ada dan tantangan yang harus dihadapi, analisis terhadap kerangka normatif dan impelementasinya dalam sistem peradilan pidana terhadap penanganan tindak kejahatan siber menjadi urgen untuk dikaji ulang. Hal ini juga menjadi bentuk evaluasi yang komprehensif untuk mengukur efektivitas pemberlakuan dan penanganan hukum terhadap tindak kejahatan siber, khususnya kasus tindak kejahatan *data breach*. Penelitian ini diharapkan dapat memberikan kontribusi dalam mengidentifikasi kelemahan dan merumuskan rekomendasi perbaikan bagi sistem peradilan pidana di Indonesia.[6]

Sehubungan dengan kajian dalam penelitian ini yaitu berkenaan penegakan hukum atas penanganan kejahatan *data breach*, terdapat beberapa hasil penelitian terdahulu yang masih berkaitan dan relevan dengan penelitian ini, di antaranya sebagai berikut: *pertama,* penelitian yang dilakukan oleh I Gusti Ayu Suanti Karnadi Singgi dalam judul penelitiannya "*Penegakan Hukum terhadap Tindak Pidana Peretasan Sebagai Bentuk Kejahatan Mayantara (Cyber Crime)".*

[5] Ervina Chintia, *Kasus Kejahatan Siber Yang Paling Banyak Terjadi di Indonesia dan Penanganannya*, Journal Information Engineering And Educational Technology, Vol.2, No.1 (Februari 2019), p.25.

[6] Ahmad Ziruddin, *Merawat Negara Hukum*, Guepedia, Surabaya, 2023, p.164.

Adapun inti dari penelitian yang dilakukan oleh I Gusti yaitu bertujuan untuk mendeskripsikan penegakan dan penanganan terhadap tindak pidana kejahatan mayantara (*cyber crime*). Hasil penelitian yang ditemukan bahwa menurutnya penegakan hukum tindak pidana mayantara (*cyber crime*) menerapkan atau mengacu pada Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik. Serta dalam upaya penanganan yang dilakukan terhadap tindak pidana mayantara (*cyber crime)* dilakukan dengan dua tahap yakni upaya preventif seperti pemblokiran, mengedukasi, dan hal lainnya guna mencegah tindak pidana kejahatan ini terjadi. Upaya lain yang dilakukan adalah upaya refresif seperti penjatuhan sanksi pidana kepada pelaku (pasca tindak pidana terjadi).[7]

Kedua, penelitian yang dilakukan oleh Sinta Sukma Ayu dalam judul penelitiannya *"Analisis Kebocoran Data Privacy pada e-Commerce Tokopedia"*. Inti dari penelitian yang dilakukan oleh Sinta Sukma Ayu yaitu bertujuan menganalisis sistem keamanan data *privacy pada e-commerce* Tokopedia. Adapun hasil yang ditemukan dalam penelitiannya bahwa *e-commerce* Tokopedia tidak menguatamakan perlindungan terhadap data *privacy* penggunanya, sehingga atas kelalain tersebut sistem keamanan pada *e-commerce* Tokopedia dapat dibobol dengan mudah oleh oknum yang tidak bertanggungjawab.[8]

Ketiga, penelitian yang dilakukan oleh Miftakhur Rohmah Habibi Isnatul Liviani dalam judul penelitiannya *"Kejahatan Teknologi Informasi (Cyber Crime) dan Penanggulangannya dalam Sistem Hukum Indonesia"*. Inti dari penelitian yang dilakukan oleh Miftakhur Rohmah bertujuan untuk mengkaji ulang pemahaman berkenaan dengan kejahatan *cyber crime* yang terjadi di dunia maya. Berdasar hasil kajiannya, dihasilkan suatu simpulan dalam penelitian ini bahwa *cyber crime* adalah tindakan seseorang atau beberapa orang dalam keahliannya di bidang komputer yang menggunakannya dengan penyalahgunaan dan tidak bijak untuk melakukan suatu tindakan kejahatan *cyber crime* di dalam dunia maya.

---

[7] I Gusti Ayu Suanti Karnadi, *Penegakan Hukum terhadap Tindak Pidana Peretasan Sebagai Bentuk Kejahatan Mayantara (Cyber Crime)*, Jukonhum: Jurnal Kontruksi Hukum, Vol.1, No.2 (Oktober 2020), p.335.

[8] Sinta Sukma Ayu, *Analisis Kebocoran Data Privacy Pada e-Commerce Tokopedia,* JUEB: Jurnal Ekonomi dan Bisnis, Vol.2, No.3 (September 2023), p.21.

Adapun sifat daripada kejahatan ini memiliki dua bentuk yaitu *cyber crime* sebagai tindakan kriminal dan *cyber crime* sebagai tindakan abu-abu.

Berdasar atas hasil penelitian-penelitian terdahulu yang dilakukan oleh peneliti sebelumnya, dirasa relevan dan memeiliki keterhubungan dengan penelitian ini. Adapun penelitian ini nantinya dapat digunakan sebagai landasan untuk merumuskan kebijakan dan strategi yang lebih tepat dalam meningkatkan kapasitas dan efektivitas kerangka hukum dan sistem peradilan pidana di Indonesia. Sistem peradilan pidana yang responsif dan adaptif terhadap perkembangan kejahatan siber merupakan keharusan di era digital. Hal ini penting untuk menjamin penegakan hukum yang adil dan memberikan perlindungan yang maksimal bagi masyarakat dari ancaman kejahatan siber.[9] Penelitian ini bertujuan untuk memberikan gambaran yang lebih jelas serta dalam kajiannya memfokuskan mulai dari kajian terhadap kerangka normatif dalam penanganan kejahatan *data breach* hingga evaluasi sistem peradilan pidana dalam penanganan tindak kejahatan ini dalam perspektif hukum pidana di Indonesia.

Penelitian ini digunakan pendeketana penelitian kualitatif yang tidak berdasarkan rumus atau perhitungan melainkan berupa data-data tulisan non angka yang dideskripsikan menggunakan metode deskriptif analistis terhadap kerangka hukum normatif pada suatu peraturan perundang-undangan yang menjadi dasar hukum penegakan dan penanganan tindak kejahatan *data breach.* Sehubungan hal tersebut penelitian ini juga merupakan penelitian hukum normatif yang didasarkan dari data kualitatif yang bersumber dari sumber primer berupa peraturan perundang-undangan dan sukender berupa jurnal ilmiah atau buku-buku lain yang relevan dengan penelitian ini. Mendasar dari sumber data yang digunakan tersebut, dikumpulkan dengan teknik studi kepustakaan (*library recearch)*. Selanjutnya, data-data yang dikumpulkan tersebut diidentifikasi, diklasifikasi Serta penganalisisan sehingga didapatkan hasil simpulan dan pemahaman yang kritis sistematik.[10]

---

[9] Siswanto Sunarso, *Viktimologi dalam Sistem Peradilan Pidana*, Sinar Grafika, Jakarta, 2022, p.334.

[10] Muhaimin, *Metode Penelitian Hukum*, Mataram Universty Press, Mataram, 2020, p.60.

B. PEMBAHASAN

1. Kerangka Normatif Penanganan *Data Breach* dalam Sistem Peradilan Pidana Indonesia

Dalam konteks hukum pidana Indonesia, kejahatan dunia maya, seperti *data breach*, semakin relevan seiring dengan pesatnya perkembangan teknologi informasi dan komunikasi (TIK). Dengan meningkatnya ketergantungan individu terhadap sistem elektronik, baik dalam konteks pribadi, pemerintahan, maupun bisnis, kejahatan siber dapat menimbulkan dampak yang signifikan terhadap perlindungan data pribadi serta kerahasiaan informasi. Keamanan data pribadi merupakan hak asasi yang harus dilindungi, mengingat informasi ini menyangkut identitas, privasi, dan kehidupan sosial individu.[11] Oleh karena itu, menjadi sangat penting untuk mengevaluasi sejauh mana hukum pidana di Indonesia, terutama dalam Kitab Undang-Undang Hukum Pidana (KUHP) dan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), dapat mengidentifikasi dan menangani kejahatan-kejahatan tersebut secara efektif. Salah satu aspek yang perlu dibahas adalah apakah pasal-pasal yang ada sudah cukup memadai untuk menjerat pelaku *data breach*, jenis kejahatan yang sering kali terjadi di dunia maya dan sangat berisiko terhadap keamanan informasi.

Data breach, yang mengacu pada kebocoran atau penyalahgunaan data pribadi, menjadi salah satu kejahatan yang perlu mendapat perhatian serius dalam kerangka hukum pidana Indonesia. Meskipun istilah *data breach* tidak diatur secara eksplisit dalam UU ITE, kebocoran data yang terjadi akibat akses yang tidak sah atau kelalaian dapat dikategorikan sebagai tindak pidana yang melanggar ketentuan perlindungan data pribadi dan sistem elektronik.[12] Dalam hal ini, beberapa pasal dalam UU ITE dapat dijadikan dasar hukum untuk menjerat pelaku yang terlibat dalam insiden kebocoran data. Pasal 26 UU ITE mengatur tentang penyebaran informasi elektronik yang merugikan pihak lain, termasuk informasi pribadi.

---

[11] Edi Saputra Hasibuan dan Elfirda Ade Putri, *Perlindungan Keamanan atas Data Pribadi di Dunia Maya*, Jurnal Hukum Sasana, Vol.10, No.1 (Juni 2024), p.121.

[12] Herol Hansen Samin, *Perlindungan Hukum terhadap Kebocoran Data Pribadi oleh Pengendali Data melalui Pendekatan Hukum Progresif*, Jurnal Ilmiah Recearh Student, Vol.1, No.3 (Desember 2024), p.261.

Jika kebocoran data pribadi terjadi akibat pengelolaan yang tidak hati-hati atau kelalaian, pasal ini bisa digunakan untuk menuntut pihak yang bersangkutan. Selain itu, Pasal 32 UU ITE mengatur tentang pengaksesan tanpa izin terhadap sistem atau data elektronik, yang relevan jika kebocoran terjadi akibat peretasan atau serangan dari pihak yang tidak berwenang. Pasal-pasal lain, seperti Pasal 33 dan Pasal 34, juga mencakup tentang penyalahgunaan sistem elektronik yang dapat merusak data atau sistem, yang bisa diterapkan dalam kasus data breach yang terjadi akibat serangan siber yang merusak integritas data. Namun, meskipun UU ITE memberikan landasan hukum untuk menangani kasus data breach, penerapan pasal-pasal tersebut dalam praktik masih menghadapi sejumlah tantangan. Salah satu tantangan terbesar adalah pembuktian pelanggaran yang terjadi, khususnya dalam hal pengaksesan atau penyebaran data tanpa izin. Pembuktian dalam kasus *data breach* membutuhkan bukti digital yang sah, yang sering kali sulit didapatkan tanpa dukungan infrastruktur forensik digital yang memadai.

Di sisi lain, dalam banyak kasus, pelaku *data breach* seringkali menggunakan teknik yang canggih, seperti peretasan yang memanfaatkan celah dalam sistem atau aplikasi, yang membuat identifikasi pelaku dan cara akses data menjadi lebih rumit. Hal ini menunjukkan bahwa meskipun UU ITE telah menyediakan dasar hukum yang cukup, penguatan implementasi hukum, terutama dalam hal perolehan dan pengelolaan bukti digital, masih diperlukan untuk memastikan proses peradilan yang adil dan transparan. Meskipun *data breach* dapat dijerat dengan pasal-pasal yang ada dalam UU ITE, masih terdapat kekurangan dalam hal pengaturan yang lebih spesifik mengenai kewajiban pengamanan data pribadi oleh penyelenggara sistem elektronik. Pengaturan ini menjadi penting, mengingat banyak kasus *data breach* yang terjadi akibat kelalaian dalam menjaga kerahasiaan data oleh pihak yang memiliki akses terhadap data tersebut.[13] Oleh karena itu, kehadiran Undang-Undang Perlindungan Data Pribadi (UU PDP) yang baru disahkan pada tahun 2022 dapat menjadi langkah penting dalam memberikan perlindungan lebih jauh terhadap data pribadi.

[13] Herol Hansen Samin, *Perlindungan Hukum terhadap Kebocoran Data Pribadi oleh Pengendali Data melalui Pendekatan Hukum Progresif*, p.275.

Meskipun UU PDP menawarkan kewajiban yang lebih ketat bagi pengendali data dalam hal pengamanan dan perlindungan data pribadi, implementasi dari undang-undang ini masih memerlukan pengawasan dan pemahaman yang mendalam dari berbagai pihak terkait. Peningkatan kapasitas teknis dan hukum dalam menangani kasus data breach akan sangat mendukung keberhasilan penegakan hukum di ranah ini. Pasal-pasal dalam UU ITE dapat digunakan untuk menjerat pelaku data breach, terdapat sejumlah tantangan dalam penerapannya yang perlu diatasi melalui perbaikan infrastruktur hukum, penguatan forensik digital, dan peningkatan kesadaran tentang pentingnya pengamanan data pribadi.

KUHP maupun UU ITE menyediakan pasal-pasal yang dapat digunakan untuk menjerat pelaku kejahatan siber seperti *data breach*. Namun, ada beberapa kritik dari ahli hukum dan praktisi yang menunjukkan bahwa pasal-pasal yang ada belum sepenuhnya memadai dalam menangani kompleksitas kejahatan dunia maya yang terus berkembang. Salah satu masalah utama adalah ketidakjelasan dalam mendefinisikan kejahatan-kejahatan dunia maya secara lebih terperinci. Meskipun UU ITE memberikan dasar hukum untuk mengatasi pelanggaran terkait *data breach*, pasal-pasalnya belum mencakup secara rinci tentang semua aspek teknis yang terkait dengan kejahatan dunia maya. Misalnya, pasal-pasal tentang data breach lebih berfokus pada penyalahgunaan atau pengaksesan data tanpa izin, tetapi belum secara eksplisit mengatur tentang kewajiban penyelenggara sistem elektronik dalam hal pengamanan data pribadi, yang seharusnya menjadi tanggung jawab utama dalam menghindari kebocoran data.

Pendekatan hukum terhadap *data breach* dalam hukum Indonesia menunjukkan adanya perbedaan yang signifikan, terutama dalam hal teknik dan tujuan pelanggaran. Data breach lebih berfokus pada pelanggaran terhadap integritas data dan sistem informasi, dengan pendekatan yang lebih teknis dan berbasis pada pengamanan data.[14] Pendekatan hukum terhadap *data breach* cenderung lebih terfokus pada perangkat hukum yang mengatur sistem elektronik dan pengelolaan data pribadi, seperti UU ITE dan UU PDP (Undang-Undang Perlindungan Data Pribadi), yang memberi perhatian khusus pada pengamanan data dan tanggung jawab penyelenggara sistem elektronik.

[14] Eristya Maya Safitri, *Analisis Teknik Social Enginering Sebagai Ancaman dalam Keamanan Sistem Informasi*, Studi Literatur, Vol.2, No.2 (Desember 2020), p.10.

Meskipun pasal-pasal yang ada dalam KUHP dan UU ITE dapat diterapkan untuk menangani kedua jenis kejahatan ini, penguatan dalam hal pengaturan teknis dan kewajiban penyelenggara sistem elektronik untuk mencegah kejahatan dunia maya perlu menjadi perhatian lebih lanjut. Seiring dengan berkembangnya teknologi, peraturan perundang-undangan juga harus terus diperbarui agar dapat mengimbangi dinamika kejahatan siber yang semakin kompleks.

Tindak pidana *data breach* dalam konteks hukum pidana Indonesia memiliki unsur-unsur yang saling terkait dengan peraturan yang ada, seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan Undang-Undang Perlindungan Data Pribadi (UU PDP), serta Kitab Undang-Undang Hukum Pidana (KUHP). Meskipun termasuk dalam kategori kejahatan dunia maya, setiap jenis kejahatan tersebut memiliki karakteristik yang berbeda, dan unsur-unsur pembuktian yang harus dipenuhi pun berbeda. Unsur Tindak Pidana Data Breach sebagai insiden kebocoran data pribadi atau informasi sensitif yang terjadi karena akses yang tidak sah atau kelalaian dalam menjaga kerahasiaan data. Perbuatan (*Actus Reus*) Unsur perbuatan dalam data breach meliputi pengaksesan, penyebaran, atau pengubahan data pribadi tanpa izin atau otorisasi yang sah. Perbuatan ini bisa terjadi baik melalui tindakan peretasan (*hacking*), kesalahan dalam pengelolaan data oleh penyelenggara sistem elektronik, atau bahkan penyalahgunaan akses oleh pihak yang sudah memiliki hak akses tetapi melanggar ketentuan yang ada.[15]

Dalam konteks UU ITE, pasal-pasal yang relevan adalah Pasal 32, yang mengatur tentang pengaksesan sistem elektronik tanpa izin, serta Pasal 33 yang mengatur tentang penyalahgunaan sistem elektronik yang dapat merusak data. Selain itu, pasal 26 UU PDP juga memberi ketentuan yang berkaitan dengan pengelolaan dan pengamanan data pribadi yang harus dilakukan oleh pengendali data. Niat Jahat (*Mens Rea*), untuk membuktikan niat jahat dalam *data breach*, harus dilihat apakah pelaku dengan sengaja melakukan pengaksesan atau penyebaran data tanpa izin, ataukah hal tersebut terjadi diakibatkan kelalaian.

[15] Padrisan Jamba dan Irene Svinarky, *Pertanggungjawaban Pidana dalam Penyebaran Data Pribadi: Tinjauan Hukum Pidana Saat Ini*, Prosiding Seminar Nasional Ilmu Sosial dan Teknologi, Vol.5, No.5 (September 2023), p.498.

Apabila pelaku sengaja melakukan kejahatan untuk keuntungan pribadi (misalnya, untuk mencuri identitas atau menjual data pribadi), maka *mens rea* dapat dianggap jelas. Dalam hal ini, niat jahat ini akan tercermin dari tujuan pelaku dalam melanggar sistem atau mengambil data dengan cara yang tidak sah.

Beberapa ahli hukum berpendapat bahwa pembuktian *mens rea* dalam kasus data breach dapat sangat bergantung pada rekaman aktivitas digital (*digital footprints*), yang membuktikan niat pelaku untuk mengakses data secara ilegal. Oleh karena itu, proses forensik digital menjadi sangat penting untuk mengidentifikasi langkah-langkah yang diambil pelaku, serta mengetahui apakah akses dilakukan dengan itikad buruk atau hanya sebagai akibat dari kelalaian dalam sistem keamanan. Dengan teknologi forensik digital yang canggih, bukti-bukti ini dapat memberikan gambaran yang jelas tentang cara pelaku mengakses data dan apakah ada unsur kesengajaan dalam tindakannya, yang sangat krusial untuk membuktikan mens rea dalam konteks hukum pidana. Pembuktian Mens Rea dan Actus Reus dalam Kasus *Data Breach* Dalam jenis kejahatan ini, pembuktian unsur tindakan (*actus reus*) dan niat jahat (*mens rea*) sering kali menjadi tantangan utama dalam proses peradilan. Untuk data breach, pembuktian tindaka (*actus reus*) dapat dilakukan melalui bukti digital yang menunjukkan adanya akses atau pengelolaan data yang tidak sah. Hal ini bisa melibatkan log akses (*access logs*), rekaman sistem, serta bukti lainnya yang menunjukkan bahwa data telah dibuka, disalin, atau disebarkan tanpa izin.

Penanganan Kasus *Data Breach* oleh Peradilan Indonesia, Keamanan data pribadi dalam peraturan Indonesia semakin diatur dengan adanya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), yang memberikan dasar hukum yang lebih kuat untuk perlindungan data pribadi warga negara Indonesia. Namun, meskipun UU PDP telah disahkan, penerapan hukum terhadap pelanggaran data pribadi yang melibatkan data breach masih dalam tahap pengembangan, dengan beberapa keputusan pengadilan yang dapat dijadikan referensi dalam menangani kasus semacam ini. Salah satu kasus yang relevan dalam konteks *data breach* adalah perkara yang melibatkan kebocoran data pribadi yang disebabkan oleh kelalaian dalam pengelolaan data oleh penyelenggara sistem elektronik.

Meskipun tidak selalu disebutkan dengan jelas sebagai *data breach*, beberapa kasus pelanggaran perlindungan data pribadi yang masuk ke ranah hukum sering kali melibatkan pasal-pasal dalam UU ITE yang mengatur tentang pengaksesan data tanpa izin atau penyalahgunaan sistem elektronik. Dalam perkara ini, peradilan Indonesia lebih banyak merujuk pada ketentuan dalam UU ITE Pasal 32 yang mengatur tentang pengaksesan tanpa izin terhadap sistem elektronik yang dapat mencederai kerahasiaan data. Sebagai contoh, meskipun belum ada putusan pengadilan yang secara eksplisit merujuk pada data breach seperti yang dikenal di dunia internasional, terdapat beberapa kasus yang berhubungan dengan pelanggaran data pribadi yang merujuk pada ketentuan hukum tentang penyalahgunaan data dan sistem. Salah satunya adalah putusan PN Jakarta Selatan dalam perkara No. 232/Pid.Sus/2018/PN.Jkt.Sel, yang melibatkan kasus kebocoran data melalui media sosial yang disebarkan tanpa izin oleh pihak ketiga. Dalam putusan tersebut, pelaku dijatuhi hukuman berdasarkan ketentuan UU ITE yang mengatur tentang penyalahgunaan informasi dan transaksi elektronik. Meski bukan kasus *data breach* dalam pengertian yang lebih luas, perkara ini memberi gambaran bahwa peradilan Indonesia mulai menilai pelanggaran terhadap pengelolaan data pribadi dengan serius, meski belum ada hukum yang sepenuhnya terperinci dalam hal ini. Di sisi lain, dalam praktik pengadilan Indonesia, salah satu kendala utama dalam penanganan data breach adalah kesulitan dalam memperoleh bukti digital yang sah dan dapat diterima di pengadilan. Oleh karena itu, dalam kasus-kasus yang melibatkan kejahatan siber, bukti-bukti yang diperoleh melalui forensik digital sering kali menjadi kunci dalam membuktikan adanya pelanggaran terhadap integritas data.

2. Evaluasi Sistem Peradilan Pidana dalam Menangani *Data Breach* Perspektif Penegakan Hukum

Adapun kasus *data breach* sendiri memberikan tantangan signifikan bagi penegak hukum karena sifat unik dari bukti dan modus kejahatan siber. Bukti digital dalam kasus-kasus ini bersifat volatil, mudah hilang atau dimanipulasi, sehingga segera membutuhkan tindakan cepat dan metode penanganan khusus.[16]

[16] Yedija Otniel Purba, *Kejahatan Siber dan Kebijakan Identitas Kependudukan Digital: Sebuah Studi tentang Potensi Pencurian Data Online*, Jcic: Jurnal Cic Lembaga Riset dan Konsultan Sosial, Vol.5, No.2 (September 2023), p.55-66.

Selain itu, tingkat kompleksitas teknis dalam menganalisis bukti digital sangat tinggi, mengingat data tersebar di berbagai perangkat dan sistem yang berbeda. Tantangan ini juga diperburuk oleh anonimitas pelaku, yang seringkali menggunakan jaringan anonim, proxy, atau VPN untuk menyembunyikan identitas.[17] Dalam forensik digital, cepatnya pengamanan bukti sangatlah vital, terutama selama "*golden hour*," yaitu periode kritis setelah insiden terjadi ketika bukti sangat rentan mengalami perubahan. Semakin cepat bukti diamankan, semakin tinggi peluang memperoleh data yang akurat dan lengkap, dengan dokumentasi "*chain of custody*" yang ketat untuk menjaga integritas bukti sepanjang proses. Keahlian tim investigasi juga memainkan peran penting, terutama ketika terdiri dari anggota multidisiplin, termasuk ahli komputer, analis data, dan ahli hukum. Dalam hal ini, perangkat lunak forensik harus fleksibel untuk menangani berbagai format data dan mampu melakukan analisis mendalam, seperti pemulihan data yang terhapus dan analisis jaringan. Selain itu, standarisasi prosedur menjamin konsistensi dan kualitas hasil investigasi, sementara etika dan hukum menuntut agar privasi tetap terjaga dan setiap tindakan sesuai dengan peraturan yang berlaku. Dokumentasi yang memadai juga diperlukan, termasuk laporan investigasi yang detail dan bukti sah untuk persidangan. Namun, tantangan tetap ada, seperti perkembangan teknologi yang cepat yang mengharuskan penegak hukum terus beradaptasi, serta volume data yang besar yang membuat proses analisis semakin kompleks.[18]

Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) berfungsi sebagai landasan hukum utama yang mengatur berbagai aspek terkait transaksi elektronik dan informasi di Indonesia. UU ini mencakup definisi transaksi elektronik, tanda tangan elektronik, hingga berbagai jenis kejahatan siber seperti *hacking*, pencurian data, dan penyebaran konten negatif. Meskipun UU ITE telah memberikan kerangka hukum yang relatif komprehensif, praktik penerapannya sering kali menimbulkan perbedaan interpretasi, terutama terkait pasal-pasal yang bersifat ambigu, seperti pasal penghinaan dan pencemaran nama baik, yang berpotensi menimbulkan ketidakpastian hukum dan penyalahgunaan. Di sisi lain,

[17] Nurul Aini, *Tantangan Pembuktian dalam Kasus Kejahatan Siber*, Judge: Jurnal Hukum, Vol.5, No.2 (Juli 2024), p.55-63.

[18] W.N.D.K. Aji, *Pengaruh Kompetensi Auditor, Penggunaan Analitik Big Data, dan Penggunaan Forensik Digital terhadap Kualitas Audit Investigatif*, Akurasi, Vol.6, No.2 (2023).

Kitab Undang-Undang Hukum Acara Pidana (KUHAP) berperan sebagai prosedur umum dalam penyidikan semua tindak pidana, termasuk kejahatan siber. Namun, prosedur ini sering kali tidak cukup spesifik untuk menangani kompleksitas kasus digital. Tantangan dalam pembuktian digital juga sangat besar, terutama terkait dengan autentikasi bukti yang mudah dimanipulasi, serta pentingnya menjaga rantai bukti (*chain of custody*) untuk menghindari keberatan dari terdakwa.[19] Selain itu, persidangan kasus siber membutuhkan saksi ahli yang kompeten di bidang teknologi informasi untuk menjelaskan bukti-bukti digital secara ilmiah. Sebagaimana disebutkan sebelumnya, perbedaan interpretasi hukum terhadap UU ITE seringkali menjadi isu dalam persidangan.[20] Oleh karena itu, peningkatan literasi digital di kalangan masyarakat dan penguatan regulasi yang lebih jelas dan terperinci menjadi langkah penting untuk memberikan kepastian hukum yang lebih baik dalam menghadapi tantangan kejahatan siber.

Peningkatan kapasitas aparat penegak hukum dalam forensik digital mencakup beberapa aspek penting. *Pertama*, diperlukan spesialisasi dalam bidang forensik digital agar setiap anggota tim dapat fokus pada bidang keahliannya masing-masing. Hal ini didukung dengan pembangunan laboratorium forensik digital yang tersebar di berbagai wilayah untuk memudahkan akses dan mempercepat penanganan kasus. Selain itu, standarisasi prosedur operasional harus diperkuat dengan dokumentasi yang jelas melalui Dokumen Prosedur Tetap (DPT) yang menjadi pedoman bagi seluruh tim. DPT ini perlu ditinjau secara berkala dan diperbarui sesuai perkembangan teknologi dan regulasi. Dalam menjalankan tugasnya, aparat penegak hukum juga harus menyeimbangkan penegakan hukum dengan perlindungan data pribadi melalui prinsip proporsionalitas, di mana tindakan yang diambil harus sebanding dengan ancaman yang dihadapi, serta transparansi dan akuntabilitas dalam proses investigasi. Pengawas independen juga diperlukan untuk memastikan hak-hak warga negara tetap terlindungi sepanjang proses tersebut.

---

[19] Aisyah Putri Nabila, *Peran Hukum Internasional Dalam Menanggulangi Cyber Crime Pada Kejahatan Transnasional*, Indonesian Journal of Law, Vol.1, No.1 (Januari 2024), p.26-33.

[20] Fegie Yoanti Wattimena, *Inovasi Digital dalam Pemerintahan: Meningkatkan Keterbukaan dan Efisiensi dengan AI, IOT, dan Blockchain*, Kaizan Media Publishing, Bandung, 2024, p.45.

Aparat penegak hukum memiliki peran yang sangat penting dalam menangani kasus *data breach*, terutama di tengah pesatnya perkembangan teknologi informasi. Dalam hal ini, Kepolisian sebagai garda terdepan bertugas untuk melakukan penyelidikan awal, mengumpulkan bukti digital, dan menangkap pelaku kejahatan. Tugas ini memerlukan ketelitian dan keahlian khusus, mengingat bukti digital sering kali bersifat kompleks dan mudah hilang jika tidak ditangani dengan baik.[21] Selain itu, Kejaksaan memiliki tanggung jawab untuk menuntut pelaku di pengadilan, di mana peran jaksa sangat krusial dalam memastikan bahwa semua bukti yang dikumpulkan dapat diterima dan cukup kuat untuk mendukung dakwaan. Pengadilan, pada gilirannya, bertugas untuk memutus perkara berdasarkan bukti yang ada dan memberikan putusan yang adil, yang memerlukan pemahaman mendalam tentang teknologi informasi dari para hakim.[22]

Dalam penanganan kejahatan siber, aparat penegak hukum memerlukan keahlian teknis yang spesifik dan keterampilan pendukung lainnya. Pemahaman bahasa pemrograman sangat penting untuk menganalisis kode malware dan jejak digital pelaku, sementara pengetahuan mendalam tentang jaringan komputer membantu melacak lalu lintas data, mengidentifikasi sumber serangan, dan menganalisis infrastruktur jaringan yang diretas. Keahlian dalam kriptografi juga diperlukan agar aparat dapat memahami dan memecahkan kode enkripsi yang mungkin melindungi data bukti. Selain keahlian teknis, keterampilan *soft skill* seperti kemampuan analisis diperlukan untuk memahami data kompleks dan mengidentifikasi pola yang relevan. Kemampuan komunikasi efektif, baik lisan maupun tertulis, mendukung koordinasi dengan saksi, ahli, dan pihak terkait lainnya. Peran laboratorium forensik digital yang dilengkapi dengan peralatan dan perangkat lunak khusus sangat krusial dalam proses analisis bukti, ditambah akses ke database informasi terkait, seperti database pelaku, modus operandi, dan indikator kompromi (IoC), yang memperkuat penyelidikan. Di tengah perkembangan teknologi yang pesat, penegak hukum harus terus memperbarui

[21] Pramawi Nicolas Huliselan, *Peran Inteijen Kepolisian Sebagai Tindakan Preventif Dalam Menanggulangi Tindak Pidana Cyber Crime*, Paulus Law Journal, Vol.5, No.1 (September 2023), p.67-87.

[22] Januri, *Upaya Kepolisian dalam Penanggulangan Kejahatan Cyber Terorganisir*, Jurnal Penelitian Hukum, Vol.1, No.2 (Juli 2022), p.100.

pengetahuan dan keterampilan mereka agar dapat menghadapi berbagai ancaman baru. Selain itu, upaya penegakan hukum harus tetap seimbang dengan perlindungan data pribadi, sehingga hak privasi tetap terlindungi.

Aparat penegak hukum menghadapi berbagai tantangan dalam menangani kejahatan siber. Perkembangan teknologi yang pesat membuat para pelaku kejahatan sering memanfaatkan celah keamanan terbaru yang sulit diantisipasi oleh aparat. Selain itu, kurangnya keahlian khusus di bidang teknologi informasi dan forensik digital menyebabkan kesulitan dalam proses pengumpulan, analisis, dan penyajian bukti digital di pengadilan. Anonimitas pelaku, yang sering kali memanfaatkan jaringan anonim seperti Tor, VPN, atau *cryptocurrency*, semakin mempersulit proses penyelidikan. Bukti digital yang mudah dimanipulasi menambah tantangan dalam menjaga keaslian dan integritas data.[23] Kejahatan siber yang bersifat transnasional juga memerlukan kolaborasi internasional yang kompleks, sementara perbedaan sistem hukum antarnasional menjadi hambatan tersendiri. Pengembangan regulasi yang komprehensif dan *up to date*, serta harmonisasi aturan terkait kejahatan siber dengan negara lain, menjadi langkah penting dalam mengatasi tantangan ini. Dalam konteks hukum, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) merupakan landasan hukum yang penting dalam penanganan kejahatan siber di Indonesia. UU ini mencakup pasal-pasal yang mengatur tentang perbuatan yang dilarang, ancaman pidana bagi pelaku kejahatan komputer, serta prosedur pembuktian dalam perkara elektronik. Selain UU ITE, Kitab Undang-Undang Hukum Acara Pidana (KUHAP) juga mengatur prosedur penanganan perkara pidana secara umum, termasuk dalam konteks kejahatan siber. Peraturan pemerintah dan peraturan menteri yang terkait dengan pelaksanaan UU ITE menjadi tambahan penting dalam penegakan hukum di bidang ini.

Kesiapan aparat penegak hukum dalam menghadapi kejahatan siber masih menghadapi tantangan besar, terutama karena perkembangan teknologi yang cepat membuat sulit bagi aparat untuk mengikuti tren terbaru. Pembentukan unit *cyber crime* khusus menjadi Langkah yang strategis untuk mengatasi tantangan ini,

[23] Masduki Khamdan Muchamad, *Kejahatan Siber Ancaman dan Permasalahannya: Tinjauan Yuridis pada Upaya Pencegahan dan Pemberantasannya di Indonesia*, Syiah Kuala University Press, Aceh, 2023, p.78.

karena melalui unit ini dapat difokuskan untuk menangani kasus-kasus kejahatan siber secara lebih efektif dan efisien. Selain itu, koordinasi yang baik antar unit, seperti reserse kriminal dan intelijen, sangat penting untuk memastikan setiap aspek penanganan kasus berjalan secara sinergis, sehingga informasi dari berbagai unit dapat saling melengkapi dan memperkuat proses penyelidikan.[24] Walaupun berbagai upaya telah dilakukan, penanganan kejahatan siber masih menghadapi tantangan besar ke depan, termasuk munculnya jenis-jenis kejahatan siber baru yang semakin kompleks, perubahan perilaku pelaku yang terus mengembangkan taktik baru untuk menghindari deteksi, serta kebutuhan untuk mengembangkan teknologi yang efektif dalam mendeteksi dan mencegah kejahatan siber.

Penanganan kasus *data breach* menghadirkan tantangan signifikan, mengingat pelaku yang seringkali sulit dilacak, bukti digital yang rentan untuk dimanipulasi, serta dampaknya yang luas bagi korban. Dalam menghadapi tantangan ini, peningkatan kapasitas aparat penegak hukum menjadi hal yang sangat krusial, terutama dalam hal pengetahuan mengenai teknologi, forensik digital, dan hukum siber. Selain itu, diperlukan regulasi yang komprehensif dan jelas untuk mengatur ruang digital serta memberikan perlindungan hukum yang memadai bagi korban kejahatan siber. Pengembangan teknologi juga memainkan peranan penting dalam mendeteksi dan mencegah kejahatan siber, sehingga penanganannya dapat lebih efektif.[25] Oleh karena itu, penanganan kasus-kasus ini memerlukan pendekatan yang komprehensif dan berkelanjutan, di mana sinergi antara berbagai pihak akan berkontribusi pada pembangunan sistem keamanan siber yang lebih kuat dan efektif.

Kasus *data breach* adalah bentuk kejahatan siber yang kompleks dan sering terjadi. Dalam proses persidangan, kasus-kasus ini sering kali menghadapi hambatan dari segi hukum acara pidana dan teknis. Tantangan ini mencakup keabsahan bukti digital, keterbatasan ahli, perbedaan yurisdiksi lintas negara, hingga laju perkembangan teknologi yang sulit diimbangi oleh sistem hukum.[26]

---

[24] Muladi, *Kompleksitas Perkembangan Tindak Pidana Dan Kebijakan Kriminal*, Penerbit Alumni, Bandung, 2021, p.57.

[25] Afifah Rizki Widianingrum, *Analisis Implementasi Kebijakan Hukum terhadap Penanganan Kejahatan Siber di Era Digital*, Journal Jurista, Vol.2, No.2 (Juli 2024), p.90-102.

[26] Rachelya Putri, *Kendala Penerapan Pembuktian Dokumen Elektronik dalam Pemeriksaan di Pengadilan*, Causa, Vol.6, No.6 (Oktober 2024), p.61-70.

Oleh karena itu, aparat penegak hukum dan instansi terkait perlu terus beradaptasi dan meningkatkan kapasitas agar dapat menangani kasus-kasus kejahatan siber ini dengan lebih efektif dan komprehensif. Dalam konteks hukum acara pidana, salah satu hambatan utama adalah volatilitas bukti digital yang dapat dengan mudah dimanipulasi. Keabsahan bukti digital sangat bergantung pada autentifikasi yang kuat, sedangkan menjaga rantai bukti dari saat pengumpulan hingga persidangan juga menimbulkan tantangan tersendiri.[27] Di samping itu, belum adanya standar pembuktian yang baku untuk bukti digital memperumit proses pembuktian di pengadilan. Keberlanjutan dan keandalan proses pembuktian menjadi penting untuk memastikan bahwa bukti digital dapat diterima dan dipertimbangkan oleh hakim. Perkembangan teknologi yang pesat telah memberi peluang bagi pelaku kejahatan siber untuk terus berinovasi dan memanfaatkan teknologi terbaru, seringkali membuat mereka satu langkah lebih maju dibandingkan penegak hukum dalam hal teknis. Anonimitas menjadi salah satu keunggulan yang dimanfaatkan oleh para pelaku, yang kerap menggunakan jaringan anonim seperti TOR, VPN, atau mata uang kripto untuk menyembunyikan identitas mereka dan menyulitkan pelacakan. Selain itu, bukti digital yang menjadi dasar investigasi forensik juga rentan dimanipulasi atau dihapus, sehingga menjaga keaslian dan integritas bukti digital menjadi tantangan tersendiri dalam upaya menegakkan hukum terhadap kejahatan siber.

Perkembangan teknologi yang pesat menjadi salah satu tantangan utama dalam penegakan hukum pidana, khususnya dalam konteks kejahatan siber. Hukum acara pidana yang berlaku saat ini sering kali menghadapi kesulitan dalam menyesuaikan diri dengan perkembangan teknologi baru yang terjadi dengan cepat, mengingat sifat perubahan tersebut yang sangat dinamis dan kompleks. Di sisi lain, para pelaku kejahatan siber terus berinovasi, menciptakan modus operandi yang semakin canggih dan sukar diprediksi, seperti pemanfaatan teknologi enkripsi untuk menyembunyikan identitas dan aktivitas mereka, serta eksploitasi kelemahan sistem dan perangkat yang terhubung dalam jaringan digital. Kondisi ini memperburuk ketidakseimbangan antara kapasitas aparat penegak hukum dan potensi kejahatan yang terus berkembang.

[27] Imam Yuadi, *Forensik Digital dan Analisis Citra*, Media Grafika, Magetan, 2023, p.80.

Pentingnya pembaruan regulasi hukum untuk menghadapi ancaman ini sangatlah mendesak. Peraturan yang ada harus mampu merespons perubahan yang terjadi begitu cepat dalam dunia digital, serta menyusun kerangka hukum yang lebih adaptif untuk mencakup jenis-jenis kejahatan yang terus berkembang. Salah satu langkah yang dapat diambil adalah dengan melakukan evaluasi terhadap regulasi yang ada, seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), agar dapat mengakomodasi fenomena baru dalam kejahatan siber. Hal ini termasuk, namun tidak terbatas pada, isu-isu yang muncul seiring dengan perkembangan teknologi terkini, seperti *Internet of Things* (IoT), *blockchain*, dan *cloud computing*.

Sejalan dengan itu, pembaruan hukum acara pidana merupakan langkah yang sangat relevan untuk mengatasi tantangan kejahatan siber. Mengingat bahwa hukum acara pidana yang berlaku saat ini belum sepenuhnya mencakup karakteristik spesifik dari kejahatan siber, pembaruan tersebut sangat mendesak untuk memberikan kerangka hukum yang lebih kokoh dalam menangani kasus-kasus yang terkait dengan kejahatan siber. Beberapa hal yang harus diperhatikan dalam pembaruan ini meliputi pengakuan bukti digital sebagai bukti yang sah di hadapan pengadilan, penyusunan prosedur yang jelas dan cepat dalam penyitaan bukti digital, serta upaya untuk menyeimbangkan penegakan hukum dengan perlindungan terhadap hak privasi, terutama dalam konteks penyadapan komunikasi elektronik.[28] Dengan adanya komitmen yang kuat dari pemerintah dan aparat penegak hukum, pembaruan ini dapat memperkuat sistem peradilan yang ada dan meningkatkan efektivitas dalam menghadapi perkembangan kejahatan siber yang semakin kompleks.

Badan Siber dan Sandi Negara (BSSN) memegang peran sentral sebagai pusat koordinasi dalam penanganan ancaman keamanan siber di Indonesia. Dengan kemampuan untuk mengumpulkan informasi dari berbagai sumber, menganalisis ancaman secara mendalam, dan mengkoordinasikan respons, BSSN mampu memberikan respon yang cepat dan tepat terhadap insiden keamanan siber.

---

[28] Eddy Army, *Bukti Elektronik dalam Praktik Peradilan*, Sinar Grafika, Jakarta, 2020, p.53.

Dukungan tim ahli dan teknologi canggih yang dimiliki BSSN memungkinkan dilakukannya analisis forensik digital yang komprehensif, yang sangat penting untuk mengungkap pelaku kejahatan siber dan memahami modus operandi mereka.[29] Selain itu, BSSN berperan penting dalam merumuskan kebijakan dan regulasi terkait keamanan siber, menciptakan kerangka hukum yang jelas dan melindungi kepentingan nasional. Mengingat perkembangan teknologi yang begitu pesat, tantangan dalam menjaga keamanan siber semakin kompleks, dengan pelaku kejahatan siber yang terus berinovasi dan mengembangkan taktik baru untuk menghindari deteksi. Dalam menghadapi dinamika tersebut, BSSN, dengan dukungan berbagai pihak, dapat semakin efektif dalam menjaga stabilitas dan keamanan siber nasional.

Kejahatan siber, khususnya yang melibatkan kasus *data breach*, telah berkembang pesat dan memerlukan adaptasi yang sigap dari sistem peradilan pidana di Indonesia. Karakteristik kejahatan ini yang terus berubah dan kompleks, ditambah dengan bukti digital yang sulit untuk dijaga integritasnya, menuntut pendekatan baru dalam penyidikan dan pengadilan. Selain itu, kurangnya ahli forensik digital yang memadai dalam sistem peradilan juga menjadi tantangan besar. Oleh karena itu, peningkatan kapasitas serta perbaikan regulasi sangat diperlukan agar aparat penegak hukum mampu menangani kejahatan siber secara lebih efektif. Pembangunan laboratorium forensik digital yang modern dan tersebar di berbagai wilayah memainkan peran krusial dalam mempercepat penanganan kasus kejahatan siber. Fasilitas ini memungkinkan analisis bukti digital dilakukan dengan lebih efisien dan akurat, yang pada gilirannya memperkuat integritas proses penyelidikan. Salah satu keuntungan utama dari keberadaan laboratorium tersebut adalah peningkatan akurasi hasil analisis, yang didukung oleh peralatan mutakhir dan prosedur operasional yang terstandarisasi, sehingga hasilnya dapat dipertanggungjawabkan secara ilmiah. Selain itu, laboratorium forensik digital juga berkontribusi atas efisiensi waktu, mempercepat proses penyidikan, dan menyelaraskan prosedur kerja (SOP) antar laboratorium, yang memungkinkan perbandingan hasil analisis secara konsisten. Di sisi lain,

[29] Damar Apri, *Strategi Badan Siber dan Sandi Negara (BSSN) dalam Menghadapi Ancaman Siber di Indonesia*, Journal Kajian Strategic Ketahanan Nasional, Vol.2, No.1 (Januari 2019), p.7.

sistem manajemen kasus yang terintegrasi dengan laboratorium ini akan mempermudah pengelolaan data dan pemantauan perkembangan kasus dari tahap penyelidikan hingga persidangan, serta meningkatkan efisiensi operasional dan transparansi dalam penanganan kasus. Akses yang diperluas ke berbagai database terkait kejahatan siber juga mendukung proses penyidikan dengan menyediakan intelijen yang lebih relevan dan memungkinkan identifikasi pola-pola kejahatan yang sedang berkembang.[30] Oleh karena itu, keberadaan laboratorium forensik digital yang modern dan sistem manajemen yang terintegrasi akan memperkuat upaya penegakan hukum dalam mengatasi kompleksitas kejahatan siber.

Perbaikan regulasi juga dibutuhkan, terutama dengan merevisi Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) untuk menyesuaikan dengan perkembangan teknologi. Revisi ini penting agar undang-undang tersebut dapat memberikan definisi yang lebih jelas dan komprehensif mengenai berbagai jenis kejahatan siber. Di samping itu, harmonisasi peraturan di berbagai undang-undang terkait diperlukan untuk menghindari tumpang tindih atau ketidakjelasan hukum yang dapat menghambat proses peradilan. Memperkuat perlindungan terhadap korban kejahatan siber, baik dari sisi hukum maupun dukungan psikologis, juga harus menjadi prioritas. Pembentukan forum koordinasi khusus untuk membahas isu kejahatan siber secara berkala adalah langkah strategis yang memungkinkan berbagai pihak untuk bertukar informasi, berbagi praktik terbaik, dan merumuskan strategi bersama. Dalam forum ini, Badan Siber dan Sandi Negara (BSSN) memiliki peran sentral, dengan fokus pada keamanan siber, dukungan teknis, analisis ancaman, dan koordinasi penanganan insiden siber. Aparat penegak hukum, seperti kepolisian, kejaksaan, dan pengadilan, juga memiliki peran penting dalam proses hukum terhadap pelaku kejahatan siber, di mana koordinasi antar lembaga sangat krusial untuk mempercepat penyidikan dan penuntutan. Namun, kejahatan siber yang bersifat lintas batas menghadirkan tantangan yurisdiksi, karena pelaku sering kali berada di negara berbeda dari korban.[31] Oleh karena itu, sinergi internasional, seperti perjanjian ekstradisi, pertukaran informasi, dan peningkatan kapasitas kolektif, menjadi sangat penting.

[30] Sugeng, *Hukum Telematika Indonesia*, Prenadamedia, Jakarta, 2020, p.94.
[31] Appryan Anggara, *Hacker Bjorka: Pihak yang Berperan dalam Mencegah Kebocoran Data*, Jorunal Hukum Magnum, Vol.6, No.1 (2023), p.13.

Organisasi internasional, seperti Interpol dan Europol, juga berperan dalam memfasilitasi kolaborasi ini, meskipun perbedaan regulasi antarnasional terkadang menjadi kendala. Di sisi lain, teknologi yang terus berkembang menuntut aparat penegak hukum dan lembaga terkait untuk selalu beradaptasi dalam menghadapi modus kejahatan siber yang semakin canggih.[32]

Urgensi pembentukan unit khusus yang berfokus pada penanganan kejahatan siber menjadi penting. Unit ini dianggap sangat penting untuk meningkatkan efektivitas dalam menangani kasus-kasus siber yang terus meningkat dalam hal jumlah dan kompleksitas. Selain itu, beliau juga menyoroti perlunya revisi terhadap Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) agar regulasi tersebut dapat selaras dengan perkembangan teknologi yang semakin pesat.[33] Penyempurnaan undang-undang ini diharapkan tidak hanya mencakup aspek teknis, tetapi juga dapat mengakomodasi berbagai modus kejahatan baru yang seringkali tidak dapat dijangkau oleh regulasi yang ada. Dengan dukungan unit khusus yang kompeten dan regulasi yang mutakhir, penanganan kejahatan siber akan menjadi lebih terarah, terkoordinasi, serta memberikan kepastian hukum yang lebih kuat bagi pihak-pihak yang terlibat. Pendekatan yang berkelanjutan dan kolaboratif sangat diperlukan dalam menangani kejahatan siber, mengingat perkembangan teknologi yang pesat dan terus berubah. Kejahatan siber tidak hanya bersifat dinamis, tetapi juga melibatkan berbagai aspek yang memerlukan sinergi antara pemerintah, sektor swasta, akademisi, dan berbagai pihak terkait untuk mencapai hasil yang optimal. Dalam konteks ini, reformasi sistem peradilan pidana sangat penting agar dapat mengikuti perkembangan teknologi digital, termasuk pembaruan regulasi, prosedur penyelidikan, dan proses persidangan yang mengakomodasi bukti digital. Selain itu, penguatan infrastruktur teknologi yang memadai, seperti penyediaan peralatan forensik digital canggih dan sistem manajemen kasus yang terintegrasi, akan mendukung proses penyelidikan yang lebih efisien. Pembaruan regulasi juga diperlukan untuk menyesuaikan dengan kemajuan teknologi tanpa menghambat inovasi, dan memberikan perlindungan yang memadai bagi individu.

---

[32] Joseps Teguh, *Teknologi Keamanan Siber (Cyber Security)*, Penerbit Yayasan Prima, Jakarta, 2023, p.87.

[33] *Ibid.,* p.17.

Perlindungan data pribadi, yang menjadi isu krusial dalam era digital, harus didorong dengan adanya regulasi yang kuat. Selain itu, penerapan etika dalam dunia siber harus terus ditekankan guna mencegah penyalahgunaan teknologi yang dapat merugikan individu atau pihak lain.

C. PENUTUP

Data breach merupakan tindak kejahatan kebocoran dan penyalahgunaan data bersakala besar. Tindak kejahatan *data breach* ini menjadi perhatian serius dalam kerangka hukum pidana Indonesia. Undang-Undang Informasi dan Teknologi Elektronik serta Undang-Undang Perlindungan Data Pribadi menjadi dasar hukum untuk menjerat pelaku yang terlibat dalam insiden tindak kejahatan kebocoran data yakni *data breach.* Akan tetapi, hal ini masih menghadapi tantangan signifikan dalam penerapannya. Kesulitan dalam pengumpulan dan pembuktian bukti digital, kurangnya pemahaman aparat hukum terhadap modus operandi kejahatan siber yang terus berkembang, serta terbatasnya koordinasi antar lembaga penegak hukum, menjadi penghambat utama dalam efektivitas penegakan hukum. Meskipun beberapa ketentuan UU ITE sudah dapat digunakan untuk menjerat pelaku, masih diperlukan penyempurnaan regulasi terkait keamanan data pribadi yang selaras dengan kemajuan teknologi. Implementasi UU PDP juga membutuhkan dukungan infrastruktur yang kuat dan peningkatan kapasitas teknis untuk menunjang investigasi yang efektif. Pendekatan adaptif, peningkatan keahlian forensik digital, dan harmonisasi regulasi menjadi langkah penting agar sistem peradilan pidana dapat secara responsif menangani kejahatan siber dan memberikan perlindungan yang optimal bagi masyarakat di era digital.

DAFTAR PUSTAKA

Buku

Adningsih, Sri. 2019. *Transformasi Ekonomi Berbasis Digital di Indonesia: Lahirnya Tren Baru Teknologi, Bisnis, Ekonomi, dan Kebijakan di Indonesia*. (Jakarta: Gramedia Pustaka Utama).

Army, Eddy. 2020. *Bukti Elektronik dalam Praktik Peradilan*. (Jakarta: Sinar Grafika).

Gani, Taufiq A.. 2023. *Kedaulatan Data Digital Untuk Integritas Bangsa*. (Banda Aceh: Syiah Kuala University Press).

Muchamad, Masduki Khamdan. 2023. *Kejahatan Siber Ancaman dan Permasalahannya: Tinjauan Yuridis pada Upaya Pencegahan dan Pemberantasannya di Indonesia*. (Aceh: Syiah Kuala University Press).

Muhaimin. 2020. *Metode Penelitian Hukum*. (Mataram: Mataram Universty Press).

Muladi. 2021. *Kompleksitas Perkembangan Tindak Pidana Dan Kebijakan Kriminal*. (Bandung: Penerbit Alumni).

Sugeng. 2020. *Hukum Telematika Indonesia*. (Jakarta: Prenadamedia).

Sunarso, Siswanto. 2022. *Viktimologi dalam Sistem Peradilan Pidana*. (Jakarta: Sinar Grafika).

Teguh, Joseps. 2023. *Teknologi Keamanan Siber (Cyber Security)*. (Jakarta: Penerbit Yayasan Prima).

Wattimena, Fegie Yoanti. 2024. *Inovasi Digital dalam Pemerintahan: Meningkatkan Keterbukaan dan Efisiensi dengan AI, IOT, dan Blockchain*. (Bandung: Kaizan Media Publishing).

Yuadi, Imam. 2023. *Forensik Digital dan Analisis Citra*. (Magetan: Media Grafika).

Publikasi

Aggara, Appryan. *Hacker Bjorka: Pihak yang Berperan dalam Mencegah Kebocoran Data*. Jorunal Hukum Magnum. Vol.6. No.1 (2023).

Aini, Nurul. *Tantangan Pembuktian dalam Kasus Kejahatan Siber*. Judge: Jurnal Hukum. Vol.5. No.2 (Juli 2024).

Aji, Wahyu Nugroho Dwi Kuncoro. *Pengaruh Kompetensi Auditor, Penggunaan Analitik Big Data, dan Penggunaan Forensik Digital terhadap Kualitas Audit Investigatif*. Akurasi: Jurnal Riset Akuntansi dan Keuangan. Vol.6. No.2 (November 2023).

Apri, Damar. *Strategi Badan Siber dan Sandi Negara (BSSN) dalam Menghadapi Ancaman Siber di Indonesia*. Journal Kajian Strategic Ketahanan Nasional. Vol.2. No.1 (Januari 2019).

Ayu, Sinta Sukma. *Analisis Kebocoran Data Privacy Pada e-Commerce Tokopedia.* JUEB: Jurnal Ekonomi dan Bisnis. Vol.2. No.3 (2023).

Chintia, Ervina. *Kasus Kejahatan Siber Yang Paling Banyak Terjadi di Indonesia dan Penanganannya*. Journal Information Engineering And Educational Technology. Vol.2. No.1 (Februari 2019).

Hasibuan, Edi Saputra, dan Elfirda Ade Putri, *Perlindungan Keamanan atas Data Pribadi di Dunia Maya*. Jurnal Hukum Sasana. Vol.10. No.1 (Juni 2024).

Huliselan, Pramawi Nicolas. *Peran Inteijen Kepolisian Sebagai Tindakan Preventif Dalam Menanggulangi Tindak Pidana Cyber Crime*. Paulus Law Journal. Vol.5. No.1 (September 2023).

Jamba, Padrisan, dan Irene Svinarky. *Pertanggungjawaban Pidana dalam Penyebaran Data Pribadi: Tinjauan Hukum Pidana Saat Ini*. Prosiding Seminar Nasional Ilmu Sosial dan Teknologi. Vol.5. No.5 (September 2023).

Januri. *Upaya Kepolisian dalam Penanggulangan Kejahatan Cyber Terorganisir*. Jurnal Penelitian Hukum. Vol.1. No.2 (Juli 2022).

Karnadi, I Gusti Ayu Suanti. *Penegakan Hukum terhadap Tindak Pidana Peretasan Sebagai Bentuk Kejahatan Mayantara (Cyber Crime)*. Jukonhum: Jurnal Kontruksi Hukum. Vol.1. No.2 (Oktober 2020).

Nabila, Aisyah Putri. *Peran Hukum Internasional Dalam Menanggulangi Cyber Crime pada Kejahatan Transnasional*. Indonesian Journal of Law. Vol.1. No.1 (Januari 2024).

Purba, Yedija Otniel. *Kejahatan Siber dan Kebijakan Identitas Kependudukan Digital: Sebuah Studi tentang Potensi Pencurian Data Online*. Jcic: Jurnal Cic Lembaga Riset dan Konsultan Sosial. Vol.5. No.2 (September 2023).

Putri, Rachelya. *Kendala Penerapan Pembuktian Dokumen Elektronik dalam Pemeriksaan di Pengadilan*. Causa: Jurnal Hukum dan Kewarganegaraan. Vol.6. No.6 (Oktober 2024).

Safitri, Eristya Maya. *Analisis Teknik Social Enginering Sebagai Ancaman dalam Keamanan Sistem Informasi*. Studi Literatur: Jurnal Ilmiah Teknokogi Informasi dan Robotika. Vol.2. No.2 (Desember 2020).

Samin, Herol Hansen. *Perlindungan Hukum terhadap Kebocoran Data Pribadi oleh Pengendali Data melalui Pendekatan Hukum Progresif*. Jurnal Ilmiah Recearh Student. Vol.1. No.3 (Desember 2024).

Widianingrum, Afifah Rizki. *Analisis Implementasi Kebijakan Hukum terhadap Penanganan Kejahatan Siber di Era Digital*. Journal Jurista. Vol.2. No.2 (Juli 2024).

Ziruddin, Ahmad. *Merawat Negara Hukum*. (Surabaya: Guepedia).

Website

BBC News. *Data eHAC milik 1,3 juta penggunanya dilaporkan bocor, 'keamanan data tidak prioritas*, diakses dari *https://www.bbc.com/indonesia/indonesia-58393345*.

Bisnis.com. *Survei APJII Pengguna Internet di Indonesia Tembus 215 Juta Orang*, diakses dari *https://apjii.or.id/berita/d/survei-apjii-pengguna-internet-di-indonesia-tembus-215-juta-orang#:~:text=Survei APJII Pengguna Internet di Indonesia Tembus,dari total populasi yang sebesar 275.773.901 jiwa*.

Sumber Hukum

Undang-Undang Nomor 1 Tahun 1946 tentang Peraturan tentang Hukum Pidana.

Undang-Undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana.

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

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