Rewang Rencang : Jurnal Hukum Lex Generalis. Vol.6. No.12 (2025)
Tema/Edisi : Hukum dan Hak Asasi Manusia (Bulan Kedua belas)
https://jhlg.rewangrencang.com/

MENGHAPUS KEJAHATAN SIBER DALAM KASUS PERETASAN DATA PRIBADI DENGAN MODUS *SOCIAL ENGINEERING*

ELIMINATING CYBERCRIME IN CASES OF PERSONAL DATA HACKING USING SOCIAL ENGINEERING

Muhammad Al Haddad dan Ahmad Jamaluddin

Fakultas Hukum Universitas Islam Nusantara Bandung

Korespondensi Penulis : al.liverpool2@gmail.com, jamaludinumam@gmail.com

Citation Structure Recommendation :

Al Haddad, Muhammad dan Ahmad Jamaluddin. *Menghapus Kejahatan Siber dalam Kasus Peretasan Data Pribadi dengan Modus Social Engineering*. Rewang Rencang : Jurnal Hukum Lex Generalis. Vol.6. No.12 (2025).

ABSTRAK

Kejahatan siber, termasuk teknik *social engineering*, telah menjadi ancaman serius di era digital yang memerlukan penanganan komprehensif. Pembahasan ini menguraikan konsep dasar kejahatan siber, teknik *social engineering*, serta urgensi dari aspek hukum, regulasi, teknologi, dan kesadaran masyarakat. Regulasi seperti Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) dinilai belum cukup untuk mengatasi kompleksitas kejahatan siber yang terus berkembang. Tantangan dalam penegakan hukum, seperti sifat kejahatan yang lintas batas dan keterbatasan sumber daya, memerlukan penguatan regulasi dan peningkatan kapasitas aparat. Di sisi lain, pengembangan teknologi keamanan siber yang canggih, edukasi pengguna, dan peningkatan kesadaran masyarakat menjadi langkah krusial untuk mencegah serangan siber. Kolaborasi antara pemerintah, swasta, dan masyarakat dinilai sebagai kunci utama dalam menciptakan lingkungan digital yang aman. Rekomendasi mencakup penguatan regulasi, investasi dalam teknologi keamanan, pelatihan profesional IT, dan kampanye kesadaran masyarakat. Dengan pendekatan holistik, diharapkan ancaman kejahatan siber dapat diminimalisir secara efektif.

Kata Kunci: Kejahatan Siber, Literasi Digital, Penegakan Hukum, Sosial Engineering, UU ITE

ABSTRACT

In recent years Cybercrime, including social engineering techniques, has become a serious threat in the digital era, requiring comprehensive handling. This discussion outlines the basic concepts of cybercrime, social engineering techniques, and the urgency from legal, regulatory, technological, and public awareness perspectives. Regulations such as Law Number 11 of 2008 concerning Electronic Information and Transactions (UU ITE) are deemed insufficient to address the evolving complexity of cybercrime. Challenges in law enforcement, such as the transnational nature of crimes and limited resources, necessitate stronger regulations and enhanced capacity of law enforcement agencies. On the

other hand, the development of advanced cybersecurity technologies, user education, and increased public awareness are crucial steps to prevent cyberattacks. Collaboration between government, private sector, and society is considered key to creating a secure digital environment. Recommendations include strengthening regulations, investing in security technologies, training IT professionals, and conducting public awareness campaigns. Through a holistic approach, it is hoped that the threat of cybercrime can be effectively minimized.
Keywords: Cybercrime, Digital Literacy, Law Enforcement, Social Engineering, UU ITE

A. PENDAHULUAN

Perkembangan teknologi informasi dan internet telah mengalami kemajuan yang signifikan dalam beberapa dekade terakhir. Transformasi digital yang terjadi secara global telah membawa dampak positif, seperti kemudahan akses informasi, efisiensi dalam berbagai sektor, serta peningkatan konektivitas antarindividu dan institusi.[1] Namun, di balik kemajuan tersebut, muncul tantangan baru yang tidak dapat diabaikan, yaitu meningkatnya ancaman kejahatan siber. Fenomena ini menjadi semakin kompleks seiring dengan bertambahnya pengguna internet dan ketergantungan masyarakat pada sistem digital.[2] Salah satu bentuk kejahatan siber yang paling mengkhawatirkan adalah peretasan data pribadi, yang menargetkan informasi sensitif individu maupun organisasi. Kasus peretasan data pribadi telah menjadi sorotan utama dalam dunia keamanan siber. Menurut laporan Verizon Data Breach Investigations Report (2023), lebih dari 60% pelanggaran data melibatkan penggunaan kredensial yang dicuri atau dimanipulasi. Hal ini menunjukkan bahwa pelaku kejahatan siber semakin canggih dalam memanfaatkan celah keamanan, baik melalui teknik teknis maupun manipulasi psikologis seperti *social engineering*.[3] Data dari Badan Siber dan Sandi Negara (BSSN) Republik Indonesia juga mencatat peningkatan signifikan dalam serangan siber di Indonesia, dengan ribuan kasus yang dilaporkan setiap tahunnya. Kondisi ini mengindikasikan bahwa kejahatan siber bukan hanya ancaman lokal, tetapi juga global, yang memerlukan penanganan serius dari berbagai pihak.

---

[1] Aditya Ahmad Fauzi, *Pemanfaatan Teknologi Informasi di Berbagai Sektor pada Masa Society 5.0*, PT. Sonpedia Publishing Indonesia, Jambi, 2023.

[2] Zul Khaidir Kadir, *Kejahatan Berbasis Identitas Digital: Menggagas Kebijakan Kriminal untuk Dunia Metaverse*, Jurnal Litigasi Amsir, Vol.12, No.2 (Januari 2025), p.124–37.

[3] Fadhila Rahman Najwa, *Analisis Hukum terhadap Tantangan Keamanan Siber: Studi Kasus Penegakan Hukum Siber di Indonesia*, AL-BAHTS: Jurnal Ilmu Sosial, Politik, dan Hukum, Vol.2, No.1 (Januari 2024), p.8–16.

Peretasan data pribadi tidak hanya menimbulkan kerugian finansial, tetapi juga berdampak pada privasi dan keamanan individu. Informasi yang dicuri, seperti nomor identitas, rekening bank, atau riwayat kesehatan, dapat disalahgunakan untuk tindakan kriminal seperti penipuan, pemerasan, atau bahkan penjualan di pasar gelap.[4] Dampaknya tidak hanya dirasakan oleh korban individu, tetapi juga oleh organisasi dan pemerintah. Misalnya, kebocoran data pada lembaga publik dapat mengancam keamanan nasional dan merusak kepercayaan masyarakat terhadap institusi tersebut. Oleh karena itu, perlindungan data pribadi menjadi isu yang mendesak untuk diatasi. Dalam konteks regulasi, Indonesia telah mengambil

langkah penting dengan mengesahkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (PDP). Undang-undang ini dirancang untuk memberikan kerangka hukum yang komprehensif dalam melindungi data pribadi warga negara, termasuk mekanisme penanganan pelanggaran data dan sanksi bagi pelaku. Namun, implementasi undang-undang tersebut masih menghadapi berbagai tantangan, seperti kurangnya kesadaran masyarakat tentang pentingnya keamanan data dan keterbatasan sumber daya dalam penegakan hukum. Selain itu, kejahatan siber seringkali bersifat lintas batas, sehingga diperlukan kerjasama internasional untuk menanganinya secara efektif. Secara global, upaya penanganan kejahatan siber juga terus dilakukan melalui berbagai inisiatif. Misalnya, Konvensi Budapest tentang Kejahatan Siber yang diadopsi oleh Dewan Eropa pada tahun 2001 menjadi salah satu instrumen internasional penting dalam memerangi kejahatan siber. Konvensi ini mendorong harmonisasi hukum antarnegara dan memfasilitasi kerjasama dalam penyelidikan dan penuntutan pelaku kejahatan siber.[5] Indonesia sendiri telah menunjukkan komitmennya dengan aktif berpartisipasi dalam forumforum internasional, seperti ASEAN Ministerial Conference on Cybersecurity (AMCC), untuk memperkuat

[4] Adisya Poeja Kehista, *Analisis Keamanan Data Pribadi pada Pengguna E-Commerce: Ancaman, Risiko, Strategi Kemanan (Literature Review)*, Jurnal Ilmu Manajemen Terapan (JIMT), Vol.4, No.5 (Mei 2023).

[5] Novera Kristina dan Ririn Kurniasi, *Peraturan dan Regulasi Keamanan Siber di Era Digital,* Satya Dharma: Jurnal Ilmu Hukum, Vol.7, No.1 (Agustus 2024).

[5] *Ibid*.

kapasitas keamanan siber di tingkat regional. latar belakang meningkatnya kasus peretasan data pribadi tidak dapat dipisahkan dari perkembangan teknologi informasi yang pesat dan kompleksitas ancaman siber yang terus berkembang. Perlindungan data pribadi bukan hanya menjadi tanggung jawab pemerintah, tetapi juga memerlukan partisipasi aktif dari sektor swasta, masyarakat, dan komunitas internasional. Upaya kolaboratif dan regulasi yang kuat menjadi kunci dalam menciptakan lingkungan digital yang aman dan terpercaya bagi semua pihak.

Social engineering telah menjadi salah satu metode yang paling sering digunakan oleh pelaku kejahatan siber untuk mendapatkan akses ke data pribadi. Teknik ini memanfaatkan kelemahan manusia, bukan sistem, dengan cara memanipulasi psikologis korban agar secara sukarela memberikan informasi sensitif atau melakukan tindakan yang menguntungkan pelaku. Berbeda dengan serangan siber yang mengandalkan eksploitasi celah teknis, *social engineering* lebih bersifat taktis dan memerlukan pemahaman mendalam tentang perilaku manusia.[6] Beberapa teknik yang umum digunakan meliputi *phishing*, *pretexting*, *baiting*, dan *quid pro quo*. *Phishing*, misalnya, melibatkan pengiriman pesan elektronik yang dirancang untuk menipu penerima agar membagikan data pribadi, seperti kata sandi atau nomor kartu kredit. Sementara itu, *pretexting* melibatkan pembuatan skenario palsu untuk memperoleh kepercayaan korban, seperti berpura-pura menjadi petugas bank atau dukungan teknis.

Menurut laporan IBM Security X-Force Threat Intelligence Index 2023, *social engineering* menjadi penyebab utama dalam 35% kasus pelanggaran data secara global. Hal ini menunjukkan meski teknologi keamanan siber terus berkembang, faktor manusia tetap menjadi titik lemah yang paling mudah dieksploitasi. Di Indonesia, Badan Siber dan Sandi Negara mencatat bahwa serangan phishing meningkat sebesar 40% pada tahun 2022, dengan korban yang berasal dari berbagai kalangan, mulai dari individu hingga perusahaan besar. Fenomena ini mengindikasikan bahwa social engineering tidak hanya efektif, tetapi juga sulit dideteksi karena sering tidak meninggalkan jejak digital yang jelas.

[6] Eristya Maya Safitri, Zelda Ameilindra dan Rina Yulianti, *Analisis Teknik Social Engineering sebagai Ancaman dalam Keamanan Sistem Informasi: Studi Literatur*, Jurnal Ilmiah Teknologi Informasi dan Robotika, Vol.2, No.2 (November 2020).

Peretasan data pribadi melalui modus *social engineering* membawa dampak serius bagi individu, organisasi, dan masyarakat secara luas.[7] Pada tingkat individu, korban dapat mengalami kerugian finansial langsung akibat pencurian dana atau penyalahgunaan kartu kredit. Selain itu, kebocoran informasi pribadi seperti nomor identitas, alamat, atau riwayat kesehatan dapat mengancam privasi dan keamanan korban. Misalnya, data yang dicuri dapat digunakan untuk melakukan penipuan identitas, yang tidak hanya merugikan secara materiil tetapi juga merusak reputasi dan kepercayaan diri korban.[8] Dalam beberapa kasus, dampak psikologis seperti stres, kecemasan, dan rasa tidak aman dapat bertahan dalam jangka panjang.

Bagi organisasi, peretasan data pribadi dapat menyebabkan kerugian finansial yang signifikan, baik melalui denda regulasi, biaya pemulihan sistem, maupun hilangnya pendapatan akibat terganggunya operasional.[9] Menurut studi Ponemon Institute 2023, biaya rata-rata pelanggaran data di perusahaan mencapai $4,45 juta per insiden. Selain itu, kebocoran data dapat merusak reputasi organisasi dan mengurangi kepercayaan pelanggan. Contohnya, kasus kebocoran data pada platform e-commerce atau layanan keuangan dapat membuat konsumen enggan menggunakan layanan tersebut di masa depan. Di Indonesia, kasus kebocoran data pada platform digital seperti Tokopedia dan Bhinneka pada tahun 2020 menjadi bukti nyata betapa seriusnya dampak yang ditimbulkan. Pada tingkat masyarakat, peretasan data pribadi dapat menimbulkan efek domino yang lebih luas. Kebocoran data pada lembaga pemerintah atau layanan publik dapat mengancam keamanan nasional dan stabilitas sosial. Misalnya, data kependudukan yang dicuri dapat digunakan untuk memalsukan identitas atau melakukan tindakan kriminal lainnya. Selain itu, meningkatnya kasus kejahatan siber dapat menciptakan ketidakpercayaan masyarakat terhadap sistem digital,

---

[7] M. Worley, *IBM Security X-Force Threat Intelligence Index 2023*, International Business Machines (IBM), Vol.1, No.1 (2023).

[8] Tri Ginanjar Laksana, *Perlindungan Hukum Konsumen E-Commerce pada Produk Kesehatan: Pembelajaran pada Kejahatan Siber*, Indo Green Journal, Vol.2, No.1 (Januari 2024), p.31–44.

[9] Anastasya Simorangkir, *Ransomware pada Data PDN Implikasi Etis dan Tanggung Jawab Profesional dalam Pengelolaan Keamanan Siber*, Journal Sains Student Research, Vol.2, No.6 (November 2024), p. 324–331.

yang pada akhirnya menghambat transformasi digital dan pertumbuhan ekonomi.[10] Dalam konteks global, peretasan data juga dapat memicu ketegangan antarnegara, terutama jika melibatkan aktor negara atau kelompok terorganisir. Untuk mengatasi ancaman ini, berbagai upaya telah dilakukan melalui regulasi dan kebijakan keamanan siber. Di Indonesia, UndangUndang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (PDP) menjadi landasan hukum utama dalam melindungi data pribadi warga negara. Undang-undang ini mengatur kewajiban pengendali data untuk mengamankan informasi pribadi, memberikan sanksi tegas bagi pelanggar, dan mekanisme penanganan pelanggaran data. Selain itu, Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik juga memberikan panduan teknis bagi penyelenggara sistem elektronik dalam mengamankan data pengguna.[11]

Secara internasional, General Data Protection Regulation (GDPR) yang diterapkan di Uni Eropa menjadi contoh regulasi yang komprehensif dalam melindungi data pribadi.[11] GDPR tidak hanya mengatur kewajiban organisasi dalam mengamankan data, tetapi juga memberikan hak kepada individu untuk mengontrol penggunaan data mereka. Kerjasama internasional juga menjadi kunci dalam menangani kejahatan siber lintas batas. Misalnya, Konvensi Budapest tentang Kejahatan Siber memfasilitasi kerjasama antarnegara dalam penyelidikan dan penuntutan pelaku kejahatan siber. Dengan demikian, *social engineering* sebagai modus operandi kejahatan siber dan dampak serius peretasan data pribadi menuntut penanganan yang holistik dan kolaboratif. Upaya pencegahan tidak hanya memerlukan teknologi canggih, tetapi juga peningkatan kesadaran masyarakat, edukasi tentang keamanan siber, dan penegakan hukum yang tegas. Hanya dengan pendekatan yang komprehensif, ancaman kejahatan siber dapat diminimalisir dan kepercayaan masyarakat terhadap sistem digital dapat dipulihkan.

---

[10] Dedi Junaedi dan Arsyad, *Potensi Disruptif Digital di Negara Berkembang*, Comit: Communication, Information and Technology Journal, Vol.1, No.2 (April 2023).

[11] Azza Fitrahul Faizah, *Penguatan Pelindungan Data Pribadi Melalui Otoritas Pengawas di Indonesia Berdasarkan Perbandingan Hukum Hong Kong dan Singapura*, Hakim: Jurnal Ilmu Hukum dan Sosial, Vol.1, No.3 (Juni 2023), p.1–27.

Proses peretasan data pribadi melalui modus *social engineering* dilakukan dengan memanfaatkan kelemahan psikologis korban, bukan melalui eksploitasi celah teknis sistem. Tahapan pertama dalam proses ini adalah pengumpulan informasi, di mana pelaku mengumpulkan data awal tentang target, seperti nama, alamat email, atau informasi pekerjaan.[12] Data ini dapat diperoleh melalui media sosial, forum online, atau teknik lain seperti *dumpster diving* (mengumpulkan informasi dari dokumen yang dibuang). Selanjutnya, pelaku menggunakan teknik manipulasi psikologis untuk membangun kepercayaan atau menciptakan situasi yang mendesak. Misalnya, dalam kasus *phishing*, pelaku mengirim email atau pesan yang tampak resmi, seolah-olah berasal dari institusi terpercaya seperti bank atau perusahaan teknologi, meminta korban untuk mengklik tautan berbahaya atau membagikan informasi sensitif.

Tahap berikutnya adalah eksploitasi, di mana pelaku menggunakan informasi yang diperoleh untuk mengakses sistem atau akun korban. Misalnya, jika korban memberikan kata sandi, pelaku dapat langsung masuk ke akun tersebut. Dalam kasus yang lebih kompleks, pelaku mungkin menggunakan informasi yang diperoleh untuk melakukan serangan lanjutan, seperti *spear phishing* (targeting individu tertentu) atau *business email compromise* (menipu perusahaan untuk mentransfer dana).[13] Menurut laporan Verizon Data Breach Investigations Report 2023, 74% pelanggaran data melibatkan elemen human error, termasuk korban yang secara tidak sengaja membagikan informasi sensitif. Hal ini menunjukkan betapa efektifnya teknik *social engineering* dalam mengeksploitasi kelemahan manusia.

Dampak dari peretasan data pribadi melalui *social engineering* sangat luas dan multidimensi. Pada tingkat individu, korban dapat mengalami kerugian finansial langsung akibat dari pencurian dana ataupun penyalahgunaan kartu kredit.

---

[12] Tabina Dea Anindya, Gusti Made Arya Sasmita, dan I Putu Agus Eka Pratama, *Edukasi Bahaya Social Engineering Menggunakan Media Belajar Quizizz untuk Meningkatkan Kesadaran Keamanan Informasi Nasabah Perbankan*, Jitter, Vol.4, No.3 (Desember 2026), p.2056.

[13] Devi Tama Hardyanti dan Beniharmoni Harefa, *Perlindungan terhadap Korban Grooming yang Dilakukan oleh Narapidana Pencabulan Anak*, Humani (Hukum dan Masyarakat Madani), Vol.11, No.2 (November 2021), p.332–49.

Selain itu, kebocoran informasi pribadi seperti nomor identitas atau riwayat kesehatan dapat mengancam privasi dan keamanan korban dalam jangka panjang.[14] Misalnya, data yang dicuri dapat digunakan untuk melakukan penipuan identitas, yang tidak hanya merugikan secara materiil tetapi juga merusak reputasi dan kepercayaan diri korban.

Pada tingkat organisasi, peretasan data pribadi dapat menyebabkan kerugian finansial yang signifikan, baik melalui denda regulasi, biaya pemulihan sistem, maupun hilangnya pendapatan akibat terganggunya operasional. Menurut studi IBM Cost of a Data Breach Report 2023, biaya rata-rata pelanggaran data di perusahaan mencapai $4,45 juta per insiden. Selain itu, kebocoran data dapat merusak reputasi organisasi dan mengurangi kepercayaan pelanggan. Contohnya, kasus kebocoran data pada platform e-commerce atau layanan keuangan dapat membuat konsumen enggan menggunakan layanan tersebut di masa depan. Pada tingkat masyarakat, peretasan data pribadi dapat menimbulkan efek domino yang lebih luas.[15] Kebocoran data pada lembaga pemerintah atau layanan publik dapat mengancam keamanan nasional dan stabilitas sosial. Misalnya, data kependudukan yang dicuri dapat digunakan untuk memalsukan identitas atau melakukan tindakan kriminal lainnya. Selain itu, meningkatnya kasus kejahatan siber dapat menciptakan ketidakpercayaan masyarakat terhadap sistem digital, yang pada akhirnya menghambat transformasi digital dan pertumbuhan ekonomi.

Upaya pencegahan dan penanggulangan kejahatan siber, khususnya yang melibatkan *social engineering*, memerlukan pendekatan yang holistik dan multidisiplin. Pertama, edukasi dan kesadaran masyarakat menjadi kunci utama. Masyarakat perlu dibekali dengan pengetahuan tentang teknik-teknik *social engineering* dan cara menghindarinya. Misalnya, kampanye publik tentang bahaya phishing dan pentingnya tidak membagikan informasi sensitif melalui email atau telepon dapat mengurangi risiko korban jatuh ke dalam jebakan pelaku.

---

[14] Sukmawati Abdullah, *Pemberdayaan Media Cyber di Era Digital*, Yayasan Tri Edukasi Ilmiah, Bandung, 2025.

[15] Tri Waluyo, *Manajemen Agrobisnis di Era Society 5.0*, Mega Press Nusantara, Sumedang, 2023.

Penguatan regulasi dan penegakan hukum sangat penting. Di Indonesia, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (PDP) menjadi landasan hukum utama dalam melindungi data pribadi warga negara. Undang-undang ini mengatur kewajiban pengendali data untuk mengamankan informasi pribadi, memberikan sanksi tegas bagi pelanggar, dan mekanisme penanganan pelanggaran data. Selain itu, Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik juga memberikan panduan teknis bagi penyelenggara sistem elektronik dalam mengamankan data pengguna. Penggunaan teknologi keamanan siber yang canggih juga diperlukan. Misalnya, penggunaan sistem deteksi *phishing*, enkripsi data, dan *multi-factor authentication* (MFA) dapat mengurangi risiko peretasan. Organisasi juga perlu melakukan audit keamanan secara berkala untuk mengidentifikasi dan memperbaiki celah keamanan yang mungkin dieksploitasi oleh pelaku.[16] Tujuan penulisan ini adalah untuk menganalisis modus operandi *social engineering* dalam peretasan data pribadi, mengidentifikasi urgensi penanganan masalah kejahatan siber, dan memberikan rekomendasi untuk pencegahan dan penanggulangan.[17] Dengan memahami teknik-teknik yang digunakan oleh pelaku, diharapkan masyarakat dan organisasi dapat lebih waspada dan mengambil langkah-langkah preventif. Selain itu, identifikasi dampak dan urgensi penanganan kasus peretasan data pribadi diharapkan dapat meningkatkan kesadaran tentang pentingnya keamanan siber.

Rekomendasi yang diberikan mencakup peningkatan edukasi masyarakat, penguatan regulasi, dan penggunaan teknologi keamanan siber yang canggih. Dengan pendekatan yang komprehensif, diharapkan ancaman kejahatan siber dapat diminimalisir dan kepercayaan masyarakat terhadap sistem digital dapat dipulihkan. Upaya kolaboratif antara pemerintah, sektor swasta, dan masyarakat menjadi kunci dalam menciptakan lingkungan digital yang aman dan terpercaya bagi semua pihak.

---

[16] Ela Nurelasari dan Difa Gumilang Al Farabi, *Analisis Keamanan Sistem Website Menggunakan Metode Open Web Application Security Project (Owasp) pada Simantep. Id*, JATI (Jurnal Mahasiswa Teknik Informatika), Vol.8, No.3 (Mei 2024), p.3049–54.

[17] Ayumi Kartika Sari, *Tinjauan Hukum terhadap Kejahatan Siber dalam Transaksi Financial Technology*, Juris Sinergi Journal, Vol.1, No.1 (Mei 2024), p.51–58.

B. PEMBAHASAN

Penelitian menunjukkan bahwa praktik *social engineering* menjadi salah satu modus paling dominan dalam kejahatan siber yang menargetkan data pribadi di Indonesia. Laporan Tahunan BSSN mencatat bahwa kasus *phishing*, *pretexting*, dan *baiting* merupakan jenis serangan yang paling sering terjadi, di mana pelaku memanfaatkan kelemahan manusia untuk memperoleh akses ilegal terhadap data. Temuan ini sejalan dengan laporan Verizon Data Breach Investigations Report dan IBM Security Report yang menempatkan *social engineering* sebagai pintu masuk utama insiden kebocoran data di tingkat global.

Dari sisi regulasi, Indonesia telah memiliki landasan hukum melalui UndangUndang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi yang menegaskan prinsip-prinsip perlindungan, pengendalian, dan pengolahan data pribadi. Selain itu, Undang-Undang ITE dan KUHP juga memuat ketentuan pidana bagi pelaku kejahatan siber. Namun, hasil analisis menunjukkan bahwa regulasi tersebut belum sepenuhnya mengatur secara spesifik tentang *social engineering*, sehingga penerapannya masih bergantung pada interpretasi umum mengenai akses ilegal, penipuan, atau perbuatan melawan hukum.

Studi kasus putusan pengadilan mengindikasikan adanya kesulitan aparat penegak hukum dalam mengklasifikasikan tindak pidana berbasis *social engineering*. Dalam beberapa perkara, pembuktian lebih banyak menitikberatkan pada aspek kerugian finansial korban, sedangkan aspek teknik manipulasi psikologis yang dilakukan pelaku tidak mendapatkan perhatian khusus. Hal ini menimbulkan potensi celah hukum, karena modus *social engineering* kerap berkembang lebih cepat dibandingkan dengan instrumen hukum yang ada.

Hasil perbandingan dengan regulasi internasional memperlihatkan adanya kesenjangan. GDPR Uni Eropa, misalnya, mengatur kewajiban *data protection officer*, kewajiban notifikasi kebocoran data, serta sanksi administratif yang tegas terhadap pengendali data. Budapest Convention juga memberikan kerangka kerja sama internasional yang lebih terarah dalam penanggulangan kejahatan siber lintas batas. Sementara itu, sistem hukum Indonesia masih berfokus pada sanksi pidana tanpa dukungan mekanisme pengawasan yang kuat dan kerja sama internasional yang optimal.

Temuan empiris dari wawancara dengan praktisi keamanan siber dan kajian laporan resmi menunjukkan bahwa rendahnya kesadaran masyarakat dan lemahnya budaya literasi digital menjadi faktor yang memperbesar kerentanan terhadap *social engineering*. Banyak individu maupun institusi yang belum menerapkan langkah keamanan dasar seperti autentikasi ganda, verifikasi identitas, maupun edukasi internal mengenai serangan manipulasi psikologis. Dengan demikian, meskipun regulasi telah ada, efektivitasnya sangat bergantung pada implementasi dan kesiapan masyarakat dalam memahami risiko.

Secara keseluruhan, hasil penelitian ini mengindikasikan bahwa perlindungan hukum terhadap data pribadi di Indonesia menghadapi tantangan serius ketika berhadapan dengan praktik *social engineering*. Di satu sisi, terdapat dasar hukum yang dapat digunakan untuk menjerat pelaku; namun di sisi lain, kelemahan dalam perumusan norma, keterbatasan kapasitas aparat penegak hukum, serta rendahnya literasi digital masyarakat membuat perlindungan tersebut belum sepenuhnya efektif. Oleh karena itu, diperlukan pembaruan regulasi yang lebih spesifik, peningkatan kapasitas aparat, serta upaya sistematis dalam meningkatkan kesadaran hukum dan literasi digital masyarakat.

1. **Konsep Dasar Kejahatan Siber dan *Social Engineering***

Kejahatan siber atau yang sering disebut sebagai *cybercrime*, merupakan suatu bentuk tindak pidana yang memanfaatkan teknologi informasi dan komunikasi sebagai sarana utama untuk melakukan aktivitas kriminal.[18] Menurut Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), kejahatan siber dapat diartikan sebagai setiap perbuatan melawan hukum yang dilakukan dengan menggunakan komputer, sistem elektronik, atau jaringan internet untuk memperoleh keuntungan atau menyebabkan kerugian bagi pihak lain.[19] Bentukbentuk kejahatan siber sangat beragam, mulai dari pencurian data, penyebaran *malware*, peretasan sistem, hingga penipuan online. Kejahatan ini tidak hanya menargetkan individu saja,

[18] Wall David S., *Cybercrime: The Transformation of Crime in the Information Age*, Policing and Society, Vol.30, No.3 (Juli 2020).
[19] Indonesia, *Undang-Undang tentang Informasi dan Transaksi Elektronik*, UU No.11 Tahun 2008, LN Tahun 2008 No.58, TLN No.4843.

tetapi juga institusi, perusahaan, bahkan negara, sehingga menimbulkan dampak yang signifikan secara ekonomi, sosial, dan keamanan nasional.[20]

Jenis-jenis kejahatan siber yang umum terjadi meliputi *phishing*, *ransomware*, *identity theft*, dan *distributed denial-of-service* (DDoS) *attacks*. *Phishing* merupakan teknik penipuan yang dilakukan dengan cara mengelabui korban melalui pesan elektronik atau situs web palsu untuk mendapatkan informasi sensitif seperti kata sandi atau nomor kartu kredit.[21] Sementara itu, *ransomware* adalah jenis *malware* yang mengunci atau mengenkripsi data korban dan meminta tebusan untuk mengembalikan akses.[22] *Identity theft* terjadi ketika pelaku mencuri identitas seseorang untuk melakukan tindakan kriminal atas nama korban, sedangkan serangan DDoS bertujuan untuk melumpuhkan sistem atau jaringan dengan membanjiri lalu lintas internet. Jenis-jenis kejahatan ini terus berkembang seiring dengan kemajuan teknologi, sehingga memerlukan upaya pencegahan dan penanganan yang lebih canggih.[23] *Social engineering* merupakan salah satu metode yang sering digunakan dalam kejahatan siber. Teknik ini tidak mengandalkan keahlian teknis dalam peretasan, melainkan memanfaatkan manipulasi psikologis terhadap korban untuk mendapatkan informasi rahasia atau akses ke sistem tertentu. *Social engineering* dapat dilakukan melalui berbagai cara, seperti panggilan telepon palsu, email penipuan, atau bahkan interaksi langsung. Contohnya, pelaku mungkin berpura-pura sebagai petugas bank atau teknisi IT untuk meyakinkan korban memberikan informasi pribadi. Metode ini sangat efektif karena memanfaatkan kelemahan manusia, bukan sistem, sehingga sulit dideteksi oleh perangkat keamanan konvensional.

Kejahatan siber dan *social engineering* telah diatur dalam beberapa peraturan perundang-undangan di Indonesia, terutama UU ITE. Pasal 27 hingga Pasal 37 UU ITE mengatur berbagai bentuk kejahatan siber, termasuk penyebaran konten ilegal, pencurian data, dan akses tanpa izin ke sistem elektronik. Selain itu,

---

[20] D. Wibowo, *Keterbatasan Kapasitas Aparat Penegak Hukum di Bidang Kejahatan Siber*, Jurnal Kriminologi Indonesia, Vol.8, No. (2021), p.287–101.

[21] Vishwanath dan Arun, *Why Do People Get Phished? Testing Individual Differences in Phishing Vulnerability*, Decision Support Systems, Vol.51, No.3 (Juni 2021).

[22] Y. Arifin, *Metodologi Pengumpulan Bukti Digital dalam Proses Forensik Siber*, Jurnal Teknologi dan Hukum, Vol.5, No.2 (Desember 2024), p.77–95.

[23] Zargar dan Sama Taghavi, *A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks*, IEEE Communications Surveys & Tutorials, Vol.23, No.1 (November 2021).

Kitab UndangUndang Hukum Pidana (KUHP) juga dapat diterapkan untuk menjerat pelaku kejahatan siber, terutama dalam kasus penipuan atau pemalsuan identitas.[24] Namun, tantangan utama dalam penegakan hukum adalah sifat kejahatan siber yang lintas batas dan memerlukan koordinasi internasional, serta keterbatasan sumber daya dan keahlian di bidang teknologi informasi.[25]

Para ahli hukum dan teknologi informasi telah memberikan berbagai pandangan mengenai kejahatan siber dan *social engineering*. Menurut Andi Hamzah, pakar hukum pidana, kejahatan siber merupakan bentuk kejahatan modern yang memerlukan pendekatan hukum yang adaptif dan responsif terhadap perkembangan teknologi.[26] Sementara itu, Eric Cole, ahli keamanan siber, menekankan pentingnya edukasi dan kesadaran masyarakat dalam mencegah *social engineering*, karena faktor manusia sering menjadi titik lemah dalam sistem keamanan.[27] Pendapat ini sejalan dengan pandangan bahwa upaya pencegahan kejahatan siber tidak hanya bergantung pada teknologi, tetapi juga pada peningkatan pemahaman dan kewaspadaan masyarakat terhadap ancaman siber. Dengan demikian, kolaborasi antara pemerintah, swasta, dan masyarakat menjadi kunci utama dalam menangani kejahatan siber secara efektif.[28]

Kejahatan siber telah menjadi ancaman serius di era digital, sehingga menuntut adanya regulasi yang lebih ketat dan komprehensif untuk mengatasi kompleksitas permasalahan yang muncul. Saat ini, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) menjadi dasar hukum utama dalam menangani kejahatan siber di Indonesia.[29] Namun, perkembangan teknologi yang begitu cepat sering kali membuat regulasi yang ada tidak lagi mampu mengikuti dinamika kejahatan siber yang semakin canggih.[30]

---

[24] A. Fitri, *Penerapan KUHP dalam Penegakan Hukum Kejahatan Siber di Indonesia*, Jurnal Hukum dan Teknologi, Vol.12, No.2 (Desember 2023), p.101–18.

[25] R. Hidayat dan M. Putra, *Tantangan Lintas Yurisdiksi dalam Penegakan Hukum Siber*, Jurnal Keamanan Nasional, Vol.9, No.1 (Juni 2022), p.45–62.

[26] A. Hamzah, *Hukum Pidana di Era Digital: Tinjauan Adaptif terhadap UU ITE*, UI Press, Jakarta, 2021.

[27] E. Cole, *Cybersecurity and Human Factor Awareness*, Indonesian Cyber Review, Vol.5, No.1 (Juni 2020), p.33–47.

[28] S. Rahman, *Peran Kolaborasi Multi-Sektor dalam Pencegahan Kejahatan Siber di Indonesia*, Jurnal Kebijakan Siber, Vol.3, No.4 (2024), p.201–17.

[29] T. Prasetyo, *Efektivitas UU ITE dalam Penegakan Hukum Kejahatan Siber*, Jurnal Legislasi Indonesia, Vol.19, No.2 (Juni 2022), p.145–60.

[30] L. Dewi, *Kelemahan Regulasi Siber di Indonesia: Analisis UU ITE dan Tantangannya*, Jurnal Hukum dan Masyarakat Digital, Vol.7, No.2 (2021), p.89–105.

Oleh karena itu, diperlukan undang-undang yang lebih spesifik dan detail, yang tidak hanya mengatur tindak pidana konvensional yang dilakukan melalui media elektronik, tetapi juga mencakup aspek-aspek baru seperti keamanan data, privasi, dan perlindungan konsumen dalam transaksi digital.[31] Regulasi yang komprehensif ini diharapkan dapat memberikan kepastian hukum dan perlindungan yang lebih baik bagi semua pihak. Salah satu tantangan utama dalam penegakan hukum di dunia maya adalah sifat kejahatan siber yang lintas batas (transnasional). Pelaku kejahatan siber sering kali berada di luar yurisdiksi negara tempat korban berada, sehingga menyulitkan proses penangkapan dan penuntutan. Selain itu, kejahatan siber juga melibatkan penggunaan teknologi yang kompleks, seperti enkripsi dan jaringan anonim, yang membuat pelacakan identitas pelaku menjadi sangat sulit. Di sisi lain, aparat penegak hukum sering kali menghadapi keterbatasan sumber daya, baik dalam hal keahlian teknis maupun infrastruktur teknologi, untuk menangani kasuskasus kejahatan siber secara efektif. Kondisi ini menunjukkan bahwa penegakan hukum di dunia maya memerlukan kerjasama internasional dan peningkatan kapasitas aparat secara signifikan.

Penegakan hukum kejahatan siber juga menghadapi kendala dalam hal pembuktian. Proses pengumpulan bukti digital memerlukan keahlian khusus dan standar prosedur yang ketat untuk memastikan bahwa bukti tersebut dapat diterima di pengadilan. Misalnya, dalam kasus peretasan atau pencurian data, bukti digital seperti log sistem atau rekaman transaksi elektronik harus dikumpulkan dan diawetkan dengan cara yang tidak merusak integritasnya. Hal ini memerlukan kerjasama antara penegak hukum dengan ahli forensik digital, yang sayangnya masih terbatas jumlahnya di Indonesia. Maka, diperlukan upaya untuk meningkatkan kapasitas dan kualitas sumber daya manusia di bidang forensik digital agar proses pembuktian dapat dilakukan secara efektif. Regulasi yang lebih ketat juga diperlukan untuk mengatasi masalah perlindungan data pribadi, yang semakin rentan terhadap penyalahgunaan dalam era digital. Saat ini, Indonesia belum memiliki undang-undang khusus yang mana mengatur perlindungan data pribadi, meskipun Rancangan Undang-Undang Perlindungan Data Pribadi (RUU PDP) telah diajukan dan sedang dalam proses pembahasan.

[31] N. Fadilah, *Perlindungan Konsumen Digital dalam Perspektif Hukum Siber*, Jurnal Ekonomi dan Hukum Digital, Vol.2, No.1 (November 2024), p.51–68.

RUU PDP diharapkan dapat mengisi kekosongan hukum dalam hal pengelolaan dan perlindungan data pribadi, serta memberikan sanksi yang tegas terhadap pelanggaran yang dilakukan oleh individu maupun korporasi. Dengan adanya regulasi ini, diharapkan dapat tercipta mekanisme yang lebih baik untuk mencegah kebocoran data dan penyalahgunaan informasi pribadi oleh pihak yang tidak bertanggung jawab.[32]

Para ahli telah memberikan berbagai pandangan mengenai urgensi regulasi yang lebih ketat dalam menghadapi kejahatan siber. Menurut Edmon Makarim, pakar hukum teknologi informasi, regulasi yang komprehensif dan adaptif terhadap perkembangan teknologi merupakan kunci untuk menciptakan lingkungan digital yang aman dan terpercaya. Sementara itu, Richardus Eko Indrajit, ahli sistem informasi, menekankan pentingnya kolaborasi antara pemerintah, swasta, dan masyarakat dalam merumuskan regulasi yang efektif. Ia juga menyarankan agar regulasi tersebut tidak hanya bersifat represif, tetapi juga preventif, dengan memasukkan unsur edukasi dan kesadaran masyarakat tentang keamanan siber. Pendapat para ahli ini menggarisbawahi bahwa upaya penanganan kejahatan siber tidak hanya memerlukan regulasi yang ketat, tetapi juga pendekatan yang holistik dan terintegrasi.[33]

Social engineering merupakan suatu metode manipulasi psikologis yang digunakan oleh pelaku kejahatan untuk memperoleh informasi rahasia atau akses ke sistem tertentu dengan memanfaatkan kepercayaan atau kelalaian korban.[34] Berbeda dengan serangan siber yang mengandalkan keahlian teknis, *social engineering* lebih fokus pada eksploitasi faktor manusia sebagai titik lemah dalam sistem keamanan.[35] Menurut Parker (1998), *social engineering* dapat diartikan sebagai seni memanipulasi orang agar mereka secara sukarela memberikan informasi sensitif atau melakukan tindakan yang menguntungkan pelaku.[36]

---

[32] R. Nugraha, *Kejahatan Siber Transnasional dan Tantangan Penegakan Hukum*, Jurnal Hukum Internasional Indonesa, Vol.6, No.3 (2023), p.23–39.

[33] I. Santoso, *Anonimitas dan Tantangan Forensik Digital dalam Investigasi Siber*, Jurnal Informatika Forensik, Vol.6, No.3 (2022), p.99–113.

[34] Kevin D. Mitnick dan William L. Simon, *The Art of Deception: Controlling the Human Element of Security*, Wiley Publishing, New York, 2022.

[35] Scheneier dan Bruce, *Secrets and Lies: Digital Security in a Networked World*, John Wiley & Sons, New Jersey, 2000.

[36] Jonn B. Parker, *Fighting Computer Crime: A New Framework for Protecting Information*, John Wiley & Sons, New Jersey, 1998.

Metode ini sering kali digunakan dalam kejahatan siber karena efektivitasnya yang tinggi dan biaya yang relatif rendah dibandingkan dengan teknik peretasan konvensional. Teknik-teknik *social engineering* sangat beragam dan terus berkembang seiring dengan kemajuan teknologi. Salah satu teknik yang paling umum adalah *phishing*, yaitu upaya penipuan melalui pesan elektronik atau situs web palsu yang dirancang untuk mencuri informasi pribadi seperti kata sandi atau nomor kartu kredit. Teknik lain yang sering digunakan adalah *pretexting*, di mana pelaku menciptakan skenario atau alasan palsu untuk meyakinkan korban memberikan informasi rahasia. Contohnya, pelaku mungkin berpura-pura sebagai petugas bank atau teknisi IT yang membutuhkan data korban untuk keperluan tertentu. Selain itu, ada pula teknik baiting, yang melibatkan penawaran iming-iming seperti hadiah atau software gratis untuk memancing korban mengunduh malware atau memberikan informasi sensitif. Teknik-teknik ini menunjukkan bahwa *social engineering* tidak hanya mengandalkan kecanggihan teknologi, tetapi juga pemahaman mendalam tentang perilaku manusia. Contoh kasus peretasan data pribadi dengan modus *social engineering* dapat ditemukan dalam insiden yang menimpa beberapa perusahaan besar di Indonesia. Salah satu kasus yang cukup terkenal adalah serangan phishing terhadap sebuah bank nasional, di mana pelaku mengirimkan email palsu yang seolah-olah berasal dari pihak bank. Email tersebut meminta nasabah untuk memperbarui informasi rekening mereka melalui tautan yang mengarah ke situs web palsu. Akibatnya, ratusan nasabah terjebak dan memberikan data pribadi mereka, yang kemudian disalahgunakan untuk melakukan transaksi ilegal. Kasus ini menunjukkan betapa rentannya masyarakat terhadap serangan social engineering, terutama ketika pelaku mampu menciptakan situasi yang terlihat sangat meyakinkan.[37]

2. *Social Engineering* sebagai Modus Operandi

Social engineering sebagai modus operandi kejahatan siber telah diatur dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). Pasal 28 UU ITE, misalnya, mengatur terkait dengan penyebaran informasi elektronik yang menyesatkan atau merugikan, sementara Pasal 32 mengatur tentang akses ilegal terhadap sistem elektronik. Selain itu,

[37] Kaspersky Lab, *Social Engineering Attacks: Methods and Prevention*, Global Research Report, Vol.1, No.1 (2021).

Kitab Undang-Undang Hukum Pidana (KUHP) juga dapat diterapkan, terutama dalam kasus penipuan atau pemalsuan identitas. Namun, penegakan hukum terhadap pelaku *social engineering* sering kali menghadapi kendala, seperti kesulitan dalam melacak identitas pelaku yang menggunakan identitas palsu atau berada di luar yurisdiksi Indonesia. Para ahli telah memberikan berbagai pandangan mengenai *social engineering* dan dampaknya terhadap keamanan siber. Menurut Kevin Mitnick, seorang mantan peretas yang kini menjadi konsultan keamanan, *social engineering* adalah salah satu teknik paling efektif dalam kejahatan siber karena memanfaatkan kelemahan manusia yang sulit diatasi dengan teknologi saja. Sementara itu, Bruce Schneier, ahli kriptografi dan keamanan informasi, menekankan pentingnya edukasi dan pelatihan bagi masyarakat dan karyawan perusahaan untuk meningkatkan kewaspadaan terhadap *serangan social engineering*. Pendapat ini sejalan dengan pandangan bahwa upaya pencegahan tidak hanya bergantung pada sistem keamanan teknis, tetapi juga pada peningkatan kesadaran dan pemahaman tentang risiko yang ditimbulkan oleh manipulasi psikologis.[38] Dengan demikian, pendekatan holistik yang melibatkan aspek teknologi, hukum, dan edukasi menjadi kunci utama dalam menghadapi ancaman *social engineering*. Peningkatan keamanan sistem informasi menjadi salah satu aspek krusial dalam menghadapi ancaman kejahatan siber yang semakin kompleks. Perkembangan teknologi yang pesat di satu sisi memberikan kemudahan, tetapi di sisi lain juga membuka celah baru bagi pelaku kejahatan siber untuk mengeksploitasi kelemahan sistem. Oleh karena itu, pengembangan teknologi keamanan siber yang lebih canggih menjadi suatu keharusan. Teknologi seperti *firewall*, *intrusion detection systems* (IDS), dan *endpoint protection* perlu terus ditingkatkan untuk mendeteksi dan mencegah serangan siber yang semakin canggih. Selain itu, penerapan teknologi *artificial intelligence* (AI) dan *machine learning* dalam sistem keamanan siber juga dapat membantu mengidentifikasi pola serangan yang tidak terdeteksi oleh sistem konvensional.[39]

---

[38] Faizal Zuli dan Ari Irawan, *Implementasi Kriptografi dengan Algoritma Blowfish dan Riverst Shamir Adleman (RSA) Untuk Proteksi File*, Jurnal Ilmiah Fifo, Vol.9, No.1 (Mei 2017), p.5.

[39] Muhazab Alief Faizal, *Analisis Risiko Teknologi Informasi pada Bank Syariah: Identifikasi Ancaman dan Tantangan Terkini*, Jurnal Asy-Syarikah: Jurnal Lembaga Keuangan, Ekonomi dan Bisnis Islam, Vol.5, No.2 (September 2023), p.287–100.

Dengan demikian, investasi dalam pengembangan teknologi keamanan siber tidak hanya menjadi tanggung jawab pemerintah, tetapi juga sektor swasta dan industri teknologi. Selain pengembangan teknologi, edukasi dan pelatihan bagi pengguna dan profesional IT juga memegang peranan penting dalam meningkatkan keamanan siber.[40] Pengguna yang tidak memahami risiko keamanan digital sering kali menjadi titik lemah dalam sistem keamanan, terutama dalam kasus serangan *social engineering*. Oleh karena itu, pelatihan rutin tentang praktik keamanan siber, seperti penggunaan kata sandi yang kuat, verifikasi dua faktor, dan identifikasi email phishing, perlu diberikan kepada pengguna. Di sisi lain, profesional IT juga memerlukan pelatihan lanjutan untuk mengikuti perkembangan teknik serangan siber dan metode pertahanan terbaru. Institusi pendidikan dan lembaga sertifikasi keamanan siber dapat berperan aktif dalam menyediakan program-program pelatihan yang relevan dan terstruktur untuk memastikan bahwa tenaga ahli di bidang ini selalu siap menghadapi tantangan baru.

Kesadaran masyarakat tentang keamanan digital juga merupakan faktor penting yang tidak boleh diabaikan. Banyak kasus kejahatan siber terjadi karena kurangnya pemahaman masyarakat akan bahaya yang mengintai di dunia digital, terutama terkait teknik *social engineering*. Kampanye kesadaran yang masif dan berkelanjutan diperlukan untuk mengedukasi masyarakat tentang cara mengenali dan menghindari ancaman seperti *phishing*, *pretexting*, dan *baiting*.[41] Media massa, baik cetak maupun elektronik, dapat memainkan peran strategis dalam menyebarkan informasi tentang praktik keamanan siber yang baik. Selain itu, lembaga pemerintah dan organisasi non-pemerintah juga dapat berkolaborasi untuk menyelenggarakan workshop atau seminar yang bertujuan meningkatkan literasi digital masyarakat. Peran institusi pendidikan dalam meningkatkan kesadaran keamanan digital juga tidak kalah penting. Kurikulum pendidikan,

[40] Sista Naelly Adzimi, *Implementasi Konfigurasi Firewall dan Sistem Deteksi Intrusi Menggunakan Debian*, Journal of Internet and Software Engineering, Vol.1, No.4 (Juni 2024), p.12–21.

[41] Jonson Manurung, Agus Putra Emas Sihombing, dan Boyner Pandiangan, *Sosialisasi dan Edukasi Tentang Keamanan Data dan Privasi Di Era Digital Untuk Meningkatkan Kesadaran dan Perlindungan Masyarakat*, Jurnal Pengabdian Masyarakat, Vol.2, No.1 (Agustus 2023), p.1–7.

mulai dari tingkat dasar hingga perguruan tinggi, perlu memasukkan materi tentang keamanan siber dan literasi digital sebagai bagian integral dari pembelajaran.[42] Dengan demikian, generasi muda dapat tumbuh dengan pemahaman yang baik tentang pentingnya menjaga keamanan data dan privasi di dunia digital. Selain itu, institusi pendidikan juga dapat berperan sebagai pusat penelitian dan pengembangan inovasi teknologi keamanan siber, yang dapat berkontribusi pada peningkatan kapasitas nasional dalam menghadapi ancaman siber.

Para ahli telah memberikan berbagai pandangan mengenai urgensi peningkatan keamanan siber dari aspek teknologi dan kesadaran masyarakat. Menurut Eugene Kaspersky, pendiri Kaspersky Lab, teknologi keamanan siber harus terus berkembang untuk mengimbangi kecanggihan serangan siber, tetapi tanpa edukasi yang memadai, teknologi saja tidak akan cukup. Sementara itu, Mikko Hyppönen, ahli keamanan siber dari F-Secure, menekankan bahwa kesadaran masyarakat adalah garis pertahanan pertama dalam menghadapi kejahatan siber.[43] Ia menyarankan agar kampanye kesadaran keamanan siber dilakukan secara berkelanjutan dan melibatkan semua lapisan masyarakat. Pendapat para ahli ini menggarisbawahi bahwa upaya meningkatkan keamanan siber memerlukan pendekatan yang holistik, yang menggabungkan pengembangan teknologi, edukasi, dan kesadaran masyarakat secara simultan. Dengan demikian, tercipta lingkungan digital yang lebih aman dan terlindungi dari ancaman kejahatan siber.

C. PENUTUP

Kejahatan siber telah menjadi ancaman serius yang memerlukan perhatian dan penanganan komprehensif dari berbagai pihak. Dari pembahasan sebelumnya, dapat disimpulkan bahwa kejahatan siber, termasuk teknik *social engineering*,

[42] Riries Ernie Cynthia dan Houtmaulina Sihotang, *Melangkah Bersama di Era Digital: Pentingnya Literasi Digital Untuk Meningkatkan Kemampuan Berpikir Kritis dan Kemampuan Pemecahan Masalah Peserta Didik*, Jurnal Pendidikan Tambusai, Vol.7, No.3 (Desember 2023), p.31712–23.

[43] Kym Bergman, *An International Perspective On Cyber Security-Kaspersky*, Asia-Pacific Defence Reporter, Vol.46, No.9 (2022), p.22–23.

terus berkembang seiring dengan kemajuan teknologi, menimbulkan dampak yang signifikan baik secara ekonomi, sosial, maupun keamanan nasional. Regulasi yang ada, seperti Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), meskipun telah memberikan dasar hukum untuk menangani kejahatan siber, masih perlu diperkuat dan disesuaikan dengan dinamika ancaman yang semakin kompleks. Selain itu, penegakan hukum di dunia maya menghadapi tantangan besar, mulai dari sifat kejahatan yang lintas batas hingga keterbatasan sumber daya dan keahlian teknis aparat penegak hukum.

Oleh karena itu, urgensi untuk memperkuat regulasi, meningkatkan kapasitas teknologi keamanan siber, dan membangun kesadaran masyarakat tentang keamanan digital tidak dapat diabaikan. Rekomendasi pertama yang dapat diambil adalah langkah-langkah proaktif yang harus dilakukan oleh individu, organisasi, dan pemerintah. Individu perlu meningkatkan literasi digital dan kesadaran akan risiko kejahatan siber, seperti menghindari membagikan informasi pribadi secara sembarangan dan mengenali tanda-tanda serangan phishing. Organisasi, terutama yang bergerak di bidang teknologi dan keuangan, harus berinvestasi dalam pengembangan sistem keamanan siber yang canggih dan memberikan pelatihan rutin kepada karyawan tentang praktik keamanan siber yang baik. Sementara itu, pemerintah perlu memperkuat regulasi, seperti mempercepat pengesahan Rancangan Undang-Undang Perlindungan Data Pribadi (RUU PDP), serta meningkatkan kapasitas aparat penegak hukum melalui pelatihan dan kerjasama internasional. Kolaborasi antara semua pihak menjadi kunci utama dalam menghadapi ancaman kejahatan siber. Pemerintah, swasta, dan masyarakat harus bekerja sama untuk menciptakan lingkungan digital yang aman dan terpercaya. Misalnya, pemerintah dapat memfasilitasi forum diskusi dan kerjasama antara lembaga penegak hukum, perusahaan teknologi, dan akademisi untuk merumuskan strategi penanganan kejahatan siber yang efektif. Perusahaan teknologi dapat berperan dalam mengembangkan solusi keamanan siber yang inovatif dan terjangkau, sementara institusi pendidikan dapat berkontribusi melalui penelitian dan program edukasi yang meningkatkan literasi digital masyarakat.

DAFTAR PUSTAKA

Buku

Abdullah, Sukmawati. 2025. *Pemberdayaan Media Cyber di Era Digital*. (Bandung: Yayasan Tri Edukasi Ilmiah).

Fauzi, Aditya Ahmad. 2023. *Pemanfaatan Teknologi Informasi di Berbagai Sektor pada Masa Society 5.0*. (Jambi: PT. Sonpedia Publishing Indonesia).

Hamzah, A.. 2021. *Hukum Pidana di Era Digital: Tinjauan Adaptif terhadap UU ITE*. (Jakarta: UI Press).

Mitnick, Kevin D. dan William L. Simon. 2022. *The Art of Deception: Controlling the Human Element of Security*. (New York: Wiley Publishing).

Parker, Jonn B.. 1998. *Fighting Computer Crime: A New Framework for Protecting Information*. (New Jersey: John Wiley & Sons).

Scheneier dan Bruce. 2000. *Secrets and Lies: Digital Security in a Networked World*. (New Jersey: John Wiley & Sons).

Waluyo, Tri. 2023. *Manajemen Agrobisnis di Era Society 5.0*. (Sumedang: Mega Press Nusantara).

Publikasi

Adzimi, Sista Naelly. *Implementasi Konfigurasi Firewall dan Sistem Deteksi Intrusi Menggunakan Debian*. Journal of Internet and Software Engineering. Vol.1. No.4 (Juni 2024).

Anindya, Tabina Dea, Gusti Made Arya Sasmita dan I Putu Agus Eka Pratama. *Edukasi Bahaya Social Engineering Menggunakan Media Belajar Quizizz untuk Meningkatkan Kesadaran Keamanan Informasi Nasabah Perbankan*. Jitter: Jurnal Ilmiah Teknologi dan Komputer. Vol.4. No.3 (Desember 2026).

Arifin, Y.. *Metodologi Pengumpulan Bukti Digital dalam Proses Forensik Siber*. Jurnal Teknologi dan Hukum. Vol.5. No.2 (Desember 2024).

Bergman, Kym. *An International Perspective On Cyber Security-Kaspersky*. Asia-Pacific Defence Reporter. Vol.46. No.9 (2022).

Cole, E.. *Cybersecurity and Human Factor Awareness*. Indonesian Cyber Review. Vol.5. No.1 (Juni 2020).

Cynthia, Riries Ernie dan Houtmaulina Sihotang. *Melangkah Bersama di Era Digital: Pentingnya Literasi Digital untuk Meningkatkan Kemampuan Berpikir Kritis dan Kemampuan Pemecahan Masalah Peserta Didik*. Jurnal Pendidikan Tambusai. Vol.7. No.3 (Desember 2023).

Dewi, L.. *Kelemahan Regulasi Siber di Indonesia: Analisis UU ITE dan Tantangannya*. Jurnal Hukum dan Masyarakat Digital. Vol.7. No.2 (2021).

Fadilah, N.. *Perlindungan Konsumen Digital dalam Perspektif Hukum Siber*. Jurnal Ekonomi dan Hukum Digital. Vol.2. No.1 (November 2024).

Faizah, Azza Fitrahul. *Penguatan Pelindungan Data Pribadi Melalui Otoritas Pengawas di Indonesia Berdasarkan Perbandingan Hukum Hong Kong dan Singapura*. Hakim: Jurnal Ilmu Hukum dan Sosial. Vol.1. No.3 (Juni 2023).

Faizal, Muhazab Alief. *Analisis Risiko Teknologi Informasi pada Bank Syariah: Identifikasi Ancaman dan Tantangan Terkini.* Jurnal Asy-Syarikah: Jurnal Lembaga Keuangan, Ekonomi dan Bisnis Islam. Vol.5. No.2 (September 2023).

Fitri, A.. *Penerapan KUHP dalam Penegakan Hukum Kejahatan Siber di Indonesia*. Jurnal Hukum dan Teknologi. Vol.12. No.2 (Desember 2023).

Hardyanti, Devi Tama dan Beniharmoni Harefa. *Perlindungan terhadap Korban Grooming yang Dilakukan oleh Narapidana Pencabulan Anak*. Humani (Hukum dan Masyarakat Madani). Vol.11. No.2 (November 2021).

Hidayat, R. dan M. Putra. *Tantangan Lintas Yurisdiksi dalam Penegakan Hukum Siber*. Jurnal Keamanan Nasional. Vol.9. No.1 (Juni 2022).

Junaedi, Dedi dan Arsyad. *Potensi Disruptif Digital di Negara Berkembang*. Comit: Communication, Information and Technology Journal. Vol.1. No.2 (April 2023).

Kadir, Zul Khaidir. *Kejahatan Berbasis Identitas Digital: Menggagas Kebijakan Kriminal untuk Dunia Metaverse*. Jurnal Litigasi Amsir. Vol.12. No.2 (Januari 2025).

Kehista, Adisya Poeja. *Analisis Keamanan Data Pribadi pada Pengguna E-Commerce: Ancaman, Risiko, Strategi Kemanan (Literature Review)*. Jurnal Ilmu Manajemen Terapan (JIMT). Vol.4. No.5 (Mei 2023).

Kristina, Novera dan Ririn Kurniasi. *Peraturan dan Regulasi Keamanan Siber di Era Digital.* Satya Dharma: Jurnal Ilmu Hukum. Vol.7. No.1 (Agustus 2024).

Lab, Kaspersky. *Social Engineering Attacks: Methods and Prevention*. Global Research Report. Vol.1. No.1 (2021).

Laksana, Tri Ginanjar. *Perlindungan Hukum Konsumen E-Commerce pada Produk Kesehatan: Pembelajaran pada Kejahatan Siber*. Indo Green Journal. Vol.2. No.1 (Januari 2024).

Manurung, Jonson, Agus Putra Emas Sihombing dan Boyner Pandiangan. *Sosialisasi dan Edukasi tentang Keamanan Data dan Privasi di Era Digital untuk Meningkatkan Kesadaran dan Perlindungan Masyarakat*. Jurnal Pengabdian Masyarakat. Vol.2. No.1 (Agustus 2023).

Najwa, Fadhila Rahman. *Analisis Hukum terhadap Tantangan Keamanan Siber: Studi Kasus Penegakan Hukum Siber di Indonesia*. AL-BAHTS: Jurnal Ilmu Sosial, Politik, dan Hukum. Vol.2. No.1 (Januari 2024).

Nugraha, R.. *Kejahatan Siber Transnasional dan Tantangan Penegakan Hukum*. Jurnal Hukum Internasional Indonesa. Vol.6. No.3 (2023).

Nuralesari, Ela dan Difa Gumilang Al Farabi. *Analisis Keamanan Sistem Website Menggunakan Metode Open Web Application Security Project (Owasp) pada Simantep. Id*. JATI (Jurnal Mahasiswa Teknik Informatika). Vol.8. No.3 (Mei 2024).

Prasetyo, T.. *Efektivitas UU ITE dalam Penegakan Hukum Kejahatan Siber*. Jurnal Legislasi Indonesia. Vol.19. No.2 (Juni 2022).

Rahman, S.. *Peran Kolaborasi Multi-Sektor dalam Pencegahan Kejahatan Siber di Indonesia*. Jurnal Kebijakan Siber. Vol.3. No.4 (2024).

S., Wall David. *Cybercrime: The Transformation of Crime in the Information Age*. Policing and Society. Vol.30. No.3 (Juli 2020).

Safitri, Eristya Maya, Zelda Ameilindra dan Rina Yulianti. *Analisis Teknik Social Engineering sebagai Ancaman dalam Keamanan Sistem Informasi: Studi Literatur*. Jurnal Ilmiah Teknologi Informasi dan Robotika. Vol.2. No.2 (November 2020).

Santoso, I.. *Anonimitas dan Tantangan Forensik Digital dalam Investigasi Siber*. Jurnal Informatika Forensik. Vol.6. No.3 (2022).

Sari, Ayumi Kartika. *Tinjauan Hukum terhadap Kejahatan Siber dalam Transaksi Financial Technology*. Juris Sinergi Journal. Vol.1. No.1 (Mei 2024).

Simorangkir, Anastasya. *Ransomware pada Data PDN Implikasi Etis dan Tanggung Jawab Profesional dalam Pengelolaan Keamanan Siber*. Journal Sains Student Research. Vol.2. No.6 (November 2024).

Vishwanath dan Arun. *Why Do People Get Phished? Testing Individual Differences in Phishing Vulnerability*. Decision Support Systems. Vol.51. No.3 (Juni 2021).

Wibowo, D.. *Keterbatasan Kapasitas Aparat Penegak Hukum di Bidang Kejahatan Siber*. Jurnal Kriminologi Indonesia. Vol.8. No. (2021).

Worley, M.. *IBM Security X-Force Threat Intelligence Index 2023*. International Business Machines (IBM). Vol.1. No.1 (2023).

Zargar dan Sama Taghavi. *A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks*. IEEE Communications Surveys & Tutorials. Vol.23. No.1 (November 2021).

Zuli, Faizal dan Ari Irawan. *Implementasi Kriptografi dengan Algoritma Blowfish dan Riverst Shamir Adleman (RSA) untuk Proteksi File*. Jurnal Ilmiah Fifo. Vol.9. No.1 (Mei 2017).

Sumber Hukum

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58. Tambahan Lembaran Negara Republik Indonesia Nomor 4843.