REAL: Journal of Religion Education Accounting and Law
E-ISSN: XXXX-XXXX P-ISSN: XXXX-XXXX
Vol. 2 No. 1 Maret 2025

Studi Yuridis Peran Hacker Dalam Cyber Crime dan Pengaruhnya Terhadap Keamanan Sistem Elektronik

Bambang Hartono[1] Suta Ramadan[2] Salsabila Brillianti Sarenc[3]
Program Studi Ilmu Hukum, Universitas Bandar Lampung, Kota Bandar Lampung, Provinsi Lampung, Indonesia[1,2,3]
Email: brillianty.sarenc@gmail.com[3]

Abstrak

Perkembangan teknologi informasi dan komunikasi yang pesat telah membawa dunia digital menjadi bagian integral dalam berbagai aspek kehidupan manusia, mulai dari komunikasi hingga layanan kesehatan. Namun, kemajuan ini juga memunculkan ancaman serius berupa kejahatan siber yang melibatkan hacker sebagai aktor utama dalam serangan digital yang merugikan individu, organisasi, dan negara. Penelitian ini bertujuan untuk mengkaji peran hacker dalam kejahatan siber serta dampaknya terhadap keamanan digital melalui perspektif yuridis. Metode yang digunakan adalah studi literatur dengan mengumpulkan dan menganalisis sumber-sumber tertulis yang relevan, seperti buku, jurnal, laporan riset, dan peraturan perundang-undangan. Hasil penelitian menunjukkan bahwa hacker dengan berbagai motivasi memiliki pengaruh besar dalam meningkatkan risiko serangan siber, sehingga upaya pencegahan dari individu, organisasi, dan pemerintah sangat diperlukan. Implementasi teknologi keamanan, penguatan regulasi hukum, serta edukasi masyarakat menjadi langkah strategis dalam memitigasi ancaman tersebut. Penelitian ini merekomendasikan adanya kolaborasi yang lebih kuat antara sektor publik dan swasta untuk memperkuat ketahanan digital melalui pelatihan, peningkatan kesadaran, dan penerapan kebijakan yang adaptif terhadap perkembangan teknologi.
Kata Kunci: Kejahatan Siber, Hacker, Keamanan Digital, Penegakan Hukum.

Abstract

The rapid development of information and communication technology has made the digital world an integral part of various aspects of human life, from communication to healthcare services. However, this advancement also brings a serious threat in the form of cybercrime, with hackers playing a central role in digital attacks that harm individuals, organizations, and nations. This study aims to examine the role of hackers in cybercrime and their impact on digital security from a juridical perspective. The research method used is literature study, gathering and analyzing relevant written sources such as books, journals, research reports, and legal regulations. The findings show that hackers, driven by various motivations, have a significant influence in increasing the risk of cyberattacks. Therefore, preventive efforts by individuals, organizations, and governments are essential. The implementation of security technology, strengthening legal regulations, and public education are strategic steps in mitigating these threats. This study recommends stronger collaboration between the public and private sectors to enhance digital resilience through training, awareness-building, and the application of adaptive policies in response to technological advancements.
Keywords: *Cybercrime, Hacker, Digital Security, Law Enforcement*

PENDAHULUAN

Di tengah pesatnya perkembangan teknologi informasi dan komunikasi, dunia digital telah menjadi bagian yang tidak terpisahkan dari berbagai aspek kehidupan manusia. Aktivitas sehari-hari, mulai dari komunikasi, transaksi keuangan, pendidikan, hingga layanan kesehatan, kini bergantung pada sistem digital yang terhubung secara global. Namun, kemajuan ini diiringi oleh tantangan besar dalam hal keamanan data dan informasi. Salah satu ancaman terbesar yang muncul adalah kejahatan siber, di mana hacker berperan sebagai aktor utama dalam

melakukan serangan yang dapat merugikan individu, organisasi, bahkan negara. UUD 1945 adalah konstitusi Negara Kesatuan Republik Indonesia.[1] Hacker, dengan kemampuan teknis yang tinggi, mampu mengeksploitasi kerentanan sistem untuk mendapatkan akses ilegal, mencuri data, atau bahkan melumpuhkan infrastruktur digital. Meski sebagian hacker berperan positif dalam memperkuat keamanan sistem, tidak sedikit yang memanfaatkan keahliannya untuk tujuan kriminal yang berdampak luas.

Peran hacker dalam kejahatan siber semakin kompleks seiring berkembangnya teknologi dan meningkatnya ketergantungan masyarakat pada layanan digital. Teknik serangan yang digunakan pun semakin beragam, mulai dari malware, ransomware, phishing, hingga serangan Distributed Denial of Service (DDoS) yang dapat melumpuhkan sistem secara keseluruhan.[2] Dampak dari serangan ini tidak hanya menyebabkan kerugian finansial yang besar, tetapi juga mengancam reputasi perusahaan, keamanan data pribadi, dan stabilitas sektor penting seperti perbankan, pemerintahan, dan layanan publik. Selain itu, faktor-faktor yang mendorong seseorang menjadi hacker, seperti motivasi finansial, ideologi, hingga tantangan teknis, turut memperkuat dinamika kejahatan siber yang sulit diprediksi dan diatasi. Kondisi ini menuntut upaya yang lebih serius dan berkelanjutan untuk memahami serta mengantisipasi berbagai bentuk ancaman siber yang terus berkembang.

Oleh karena itu, penelitian ini penting dilakukan untuk mencapai tiga tujuan utama. Pertama, mengidentifikasi dan menganalisis teknik serta metode yang digunakan oleh hacker dalam melakukan serangan siber. Pemahaman ini diperlukan untuk mengenali pola serangan dan mengembangkan sistem pertahanan yang lebih efektif. Kedua, menilai dampak kejahatan siber terhadap keamanan digital di berbagai sektor, sehingga dapat diketahui sejauh mana ancaman ini memengaruhi stabilitas ekonomi, sosial, dan politik. Ketiga, merumuskan langkah-langkah preventif dan responsif yang dapat diterapkan untuk meningkatkan keamanan digital, baik melalui penguatan infrastruktur teknologi, kebijakan keamanan yang adaptif, maupun peningkatan kesadaran masyarakat terhadap risiko siber. Dengan tercapainya tujuan-tujuan tersebut, diharapkan penelitian ini dapat memberikan kontribusi nyata dalam upaya pencegahan dan penanggulangan kejahatan siber yang semakin kompleks di era digital.

Permasalahan dalam penelitian ini berfokus pada semakin kompleksnya ancaman kejahatan siber yang dilakukan oleh hacker, di tengah pesatnya perkembangan teknologi dan meningkatnya ketergantungan masyarakat pada sistem digital. Hacker dengan kemampuan teknis yang tinggi memanfaatkan berbagai metode serangan seperti malware, ransomware, phishing, dan DDoS untuk mengeksploitasi kerentanan sistem, mencuri data, atau melumpuhkan infrastruktur digital yang penting. Hal ini menyebabkan dampak yang luas, mulai dari kerugian finansial, ancaman terhadap keamanan data pribadi, hingga gangguan pada sektor-sektor strategis seperti perbankan, pemerintahan, dan layanan publik. Namun, belum ada pemahaman yang mendalam tentang pola serangan hacker, dampak kejahatan siber secara komprehensif di berbagai sektor, serta strategi pencegahan dan penanganan yang efektif untuk mengatasi ancaman yang terus berkembang ini.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan studi literatur (library research) dengan tujuan untuk mengkaji secara mendalam peran hacker dalam kejahatan siber dan pengaruhnya terhadap keamanan digital melalui tinjauan yuridis. Studi literatur dipilih sebagai metode penelitian karena fokus penelitian ini adalah pada analisis konsep, teori, dan peraturan hukum

[1] Retno Wulansari, I Ketut Seregig, Suta Ramadan. 2022. *Pertimbangan Hakim Terhadap Pelaku Tindak Pidana Pembakaran Polsek Candipuro Lampung Selatan (Studi Putusan Nomor: 285/Pid. Sus/2021/PN. KLA)*. Yustisia Tirtayasa, Vol. 2, No. 2, hlm. 28.
[2] Sriwulan. 2023. *Tinjauan Yuridis Tindak Pidana Cyber Crime Di Indonesia.* Diss. Institut Agama Islam Negeri Palopo.

yang ada dalam kaitannya dengan kejahatan siber dan peran hacker. Dengan demikian, penelitian ini akan mengandalkan berbagai sumber tertulis yang relevan, baik berupa buku, artikel jurnal, laporan riset, serta peraturan perundang-undangan yang berkaitan dengan aspek hukum kejahatan siber dan perlindungan data. Dalam mengumpulkan data, peneliti akan mengkaji literatur yang relevan terkait dengan teori-teori tentang keamanan digital, kejahatan siber, dan hukum yang mengaturnya. Referensi yang digunakan dalam penelitian ini akan mencakup buku-buku hukum, jurnal akademik, artikel-artikel hukum, serta keputusan-keputusan pengadilan yang relevan dengan isu kejahatan siber. Selain itu, kajian terhadap peraturan-peraturan seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), serta konvensi internasional tentang kejahatan siber, akan menjadi bagian penting dari analisis untuk melihat bagaimana hukum menangani peran hacker dan dampaknya terhadap keamanan digital.

HASIL PENELITIAN DAN PEMBAHASAN

Dampak Kejahatan Siber terhadap Keamanan Digital

Kejahatan siber memiliki dampak yang sangat besar terhadap keamanan digital, dengan efek yang meresap ke berbagai sektor dan aspek kehidupan. Salah satu dampak yang paling mencolok adalah kerugian finansial yang dialami oleh individu, organisasi, maupun negara.[3] Kejahatan siber yang melibatkan pencurian data atau serangan ransomware, misalnya, dapat menyebabkan kerugian yang sangat besar. Perusahaan dapat kehilangan jutaan dolar akibat serangan yang merusak sistem atau mencuri data sensitif, seperti informasi kartu kredit, data pelanggan, atau rahasia dagang.[4] Selain itu, serangan seperti ransomware sering kali mengarah pada pemerasan, di mana hacker meminta uang tebusan untuk mengembalikan data yang terkunci atau untuk mencegah penyebaran informasi yang telah dicuri. Selain itu, biaya pemulihan yang dikeluarkan oleh perusahaan setelah serangan siber—baik untuk mengganti perangkat keras, memperbaiki sistem, maupun menanggulangi dampak hukum dan regulasi—dapat menyebabkan beban finansial yang berat dan mempengaruhi stabilitas ekonomi organisasi tersebut. KUHP di Indonesia telah mengatur tindak pidana dan sanksi pidana sesuai dengan kejahatan atau pelanggaran yang dilakukan.[5]

Selain dampak finansial, kejahatan siber juga memiliki dampak serius terhadap reputasi organisasi atau institusi yang menjadi korban serangan. Ketika data pelanggan atau informasi sensitif lainnya terekspos akibat serangan, kepercayaan publik terhadap organisasi tersebut dapat hancur dalam sekejap.[6] Reputasi adalah aset berharga yang dibangun bertahun-tahun, dan serangan siber dapat merusak citra perusahaan dalam waktu singkat.[7] Pelanggan dan mitra bisnis yang sebelumnya percaya pada keamanan sistem perusahaan mungkin mulai meragukan kemampuan organisasi untuk melindungi informasi mereka, yang bisa berujung pada penurunan jumlah pelanggan, berkurangnya pendapatan, dan bahkan kerugian lebih lanjut melalui tindakan hukum atau peraturan yang lebih ketat. Di sisi lain, institusi pemerintahan yang menjadi korban kejahatan siber juga dapat mengalami hilangnya kepercayaan dari masyarakat, yang dapat merusak legitimasi dan kredibilitas pemerintah tersebut, terlebih jika data pribadi atau informasi sensitif terkait kebijakan negara terungkap.

Ancaman terhadap infrastruktur kritis juga menjadi salah satu dampak kejahatan siber yang sangat mengkhawatirkan, terutama dalam sektor-sektor yang memiliki peran penting

[3] Budiyanto. 2025. *Pengantar Cybercrime dalam Sistem Hukum Pidana di Indonesia.* Sada Kurnia Pustaka.
[4] Kapoyos, Jeremiah Marvin. 2023. "Pentingnya Cybersecurity di Era Society 5.0." *Nusantara Journal of Multidisciplinary Science* 1.5: 1347.
[5] Suta Ramadan, I Ketut Seregig, Deta Merly Oktavianti. 2022. *Analisis Pertimbangan Hakim dalam Menjatuhkan Sanksi Pidana Terhadap Pelaku Tindak Pidana Penggelapan dalam Jabatan*. PAMPAS: Journal of Criminal Law, Vol. 3, No. 1, hlm. 105.
[6] Tamhidah, Mas Atsilah Rahmah. 2023. "Pengaruh Media Sosial Terhadap Penyebaran Informasi Palsu dan Kejahatan Siber." *Innovative: Journal Of Social Science Research* 3.6: 9142.
[7] Mardiansyach, Dewo. 2023. *Implikasi Delik Pidana Khusus Cybercrime Praktik Perjudian Online.* Diss. Universitas Islam Sultan Agung Semarang.

dalam menjaga kelangsungan hidup masyarakat, seperti perbankan, pemerintahan, dan sektor kesehatan. Serangan siber yang menargetkan sistem keuangan atau perbankan dapat mengganggu sistem pembayaran global, mencuri dana, atau merusak operasi bank yang dapat menyebabkan krisis ekonomi. Serangan terhadap infrastruktur pemerintahan dapat menghambat penyelenggaraan layanan publik, merusak sistem pemilu, atau mengakses data sensitif yang berpotensi membahayakan keamanan nasional. Begitu pula dalam sektor kesehatan, serangan terhadap rumah sakit atau penyedia layanan kesehatan dapat mengancam keselamatan pasien, mencuri rekam medis yang sangat pribadi, atau merusak sistem manajemen yang krusial dalam merawat pasien, bahkan berpotensi menyebabkan kematian jika peralatan medis terganggu. Ancaman-ancaman ini menunjukkan betapa rentannya infrastruktur kritis terhadap serangan siber yang dapat mengakibatkan gangguan sistem yang luas dan merugikan masyarakat secara keseluruhan.

Lebih jauh lagi, kejahatan siber memiliki dampak yang signifikan terhadap data pribadi dan privasi individu. Dalam era digital saat ini, data pribadi seperti nomor identitas, riwayat medis, informasi keuangan, dan data pribadi lainnya menjadi komoditas yang sangat berharga dan sering kali menjadi target utama bagi para hacker.[8] Ketika data pribadi dicuri atau disalahgunakan, individu yang menjadi korban tidak hanya menghadapi kerugian finansial akibat pencurian identitas, tetapi juga berisiko kehilangan privasi mereka.[9] Informasi yang terekspos bisa digunakan untuk melakukan penipuan, penyalahgunaan data, atau bahkan ancaman terhadap keselamatan fisik korban. Kejahatan siber yang menargetkan data pribadi dapat menyebabkan ketakutan dan kecemasan yang mendalam di kalangan masyarakat, karena mereka merasa bahwa privasi mereka tidak lagi terjamin. Di sisi lain, serangan yang melibatkan kebocoran data pribadi dapat memperburuk persepsi publik terhadap kemampuan organisasi untuk melindungi data sensitif, yang berdampak pada hilangnya kepercayaan terhadap perusahaan atau institusi yang terlibat. Dengan demikian, kejahatan siber memiliki dampak yang sangat luas dan beragam terhadap keamanan digital, mencakup kerugian finansial yang signifikan, dampak reputasi yang menghancurkan, ancaman terhadap infrastruktur kritis yang dapat merusak masyarakat, serta pengaruhnya terhadap privasi dan data pribadi individu. Oleh karena itu, penting bagi organisasi, pemerintah, dan individu untuk menginvestasikan sumber daya dalam meningkatkan sistem keamanan digital dan kesadaran akan ancaman siber, serta memperkuat peraturan dan kebijakan terkait perlindungan data untuk menghadapi tantangan yang terus berkembang dalam dunia digital ini.

Faktor-Faktor yang Mendorong Hacker dalam Melakukan Kejahatan Siber

Faktor-faktor yang mendorong hacker untuk melakukan kejahatan siber sangat bervariasi, melibatkan aspek finansial, ideologis, teknis, serta sosial dan psikologis, yang masing-masing dapat memberikan alasan kuat bagi individu untuk terlibat dalam aktivitas ilegal ini. Salah satu motivasi utama yang paling sering ditemui adalah motivasi finansial. Kejahatan siber, seperti pencurian data dan pemerasan, dapat memberikan hacker kesempatan untuk memperoleh keuntungan besar secara cepat.[10] Data pribadi yang dicuri, seperti informasi kartu kredit, nomor identitas, atau rekam medis, dapat dijual di pasar gelap dengan harga tinggi. Selain itu, serangan ransomware, di mana hacker mengenkripsi data korban dan meminta uang tebusan untuk mengembalikannya, juga merupakan bentuk pemerasan yang

[8] Anggraini, Yuli. 2024. "Kekuatan hukum alat bukti elektronik dan kredibilitasnya dalam pembuktian hukum pidana." *Causa: Jurnal Hukum dan Kewarganegaraan* 6.8. hlm. 3.
[9] Idriansyah, Alfi Salsabilah, dan Nur Afifah. 2024. "Perlindungan Hukum Terhadap Korban Cyber Crime di Indonesia dalam Aliran Hukum Pada Kasus Pencurian Data Pribadi." *Media Hukum Indonesia (MHI)* 2.4: 465.
[10] Santhi, Ni Nyoman Putri Purnama, and I. Nengah Nuarta. 2023. "Penguatan Penegakan Hukum Polri dalam Rangka Optimalisasi Penanggulangan Cybercrime di Indonesia." *SCIENTIA: Journal of Multi Disciplinary Science*.

menguntungkan secara finansial. Bagi beberapa hacker, kejahatan siber bukan hanya tentang kerusakan yang ditimbulkan, tetapi juga tentang keuntungan materi yang bisa diperoleh dari aktivitas ini. Dalam beberapa kasus, hacker bahkan bekerja dalam kelompok atau jaringan yang terorganisir, yang memungkinkan mereka untuk mencuri data dalam jumlah besar dan meraup keuntungan yang lebih besar lagi.

Di sisi lain, ada pula hacker yang termotivasi oleh alasan ideologis, terutama dalam kasus yang dikenal sebagai "hacktivism." Hacktivism adalah bentuk aktivisme yang menggunakan peretasan sebagai sarana untuk menyuarakan pandangan politik atau sosial tertentu.[11] Hacker yang terlibat dalam hacktivism sering kali melancarkan serangan untuk memprotes kebijakan pemerintah, perusahaan, atau organisasi tertentu yang mereka anggap tidak adil atau bertentangan dengan nilai-nilai mereka. Misalnya, kelompok hacker seperti Anonymous telah mengadakan serangkaian serangan siber terhadap institusi yang dianggap bertanggung jawab atas pelanggaran hak asasi manusia atau ketidakadilan sosial. Motivasi ideologis ini tidak selalu melibatkan keuntungan finansial, tetapi lebih kepada keinginan untuk mengubah atau memperjuangkan perubahan sosial atau politik melalui saluran yang tidak konvensional, dengan menggunakan kemampuan teknis mereka untuk menembus sistem dan menyebarkan pesan mereka. Selain motivasi eksternal, faktor teknis juga memainkan peran penting dalam mendorong hacker untuk melakukan kejahatan siber. Bagi sebagian hacker, peretasan bukan sekadar cara untuk menghasilkan uang atau menyampaikan pesan, tetapi merupakan tantangan intelektual dan peluang untuk menguji kemampuan teknis mereka.[12] Keahlian dalam meretas sistem, mengatasi enkripsi, atau mengeksploitasi kerentanannya dalam perangkat lunak adalah pencapaian yang sangat dihargai dalam dunia hacker.[13] Bagi beberapa hacker, kemampuan untuk membobol sistem yang sangat aman atau mengatasi masalah teknis yang rumit memberikan rasa pencapaian pribadi yang besar, bahkan meskipun mereka tahu bahwa mereka melanggar hukum. Dengan berkembangnya teknologi dan semakin kompleksnya sistem keamanan, semakin banyak hacker yang tertarik untuk menguji batas kemampuan mereka dan menantang diri mereka untuk mengeksploitasi kelemahan-kelemahan yang ada, sering kali tanpa mempertimbangkan dampak negatif dari tindakan mereka terhadap individu atau organisasi yang menjadi korban.

Selain itu, faktor sosial dan psikologis juga menjadi pendorong utama bagi beberapa hacker untuk terlibat dalam kejahatan siber. Bagi sebagian individu, peretasan menjadi cara untuk membuktikan kemampuan mereka di dunia maya, mendapatkan pengakuan, atau bahkan mencari pengakuan dari kelompok atau komunitas hacker lainnya.[14] Keinginan untuk diakui sebagai "ahli" dalam dunia peretasan atau untuk membuktikan diri sebagai bagian dari kelompok hacker yang prestisius sering kali menjadi motivasi yang sangat kuat. Faktor psikologis seperti rasa ingin tahu, tantangan, atau bahkan perasaan terpinggirkan juga dapat memengaruhi keputusan individu untuk terlibat dalam kegiatan ilegal ini. Beberapa hacker mungkin berasal dari latar belakang yang merasa kurang dihargai atau memiliki motivasi untuk mendapatkan perhatian dan pengakuan dari teman sebaya atau komunitas tertentu. Dalam beberapa kasus, hacker dapat merasa bahwa mereka melakukan sesuatu yang "menghibur" atau memberi mereka rasa kekuasaan atas sistem yang mereka retas, yang dapat meningkatkan

[11] Usman, Noval, and Satria Unggul Wicaksana Prakasa. 2024. "Perlindungan Hukum Data Pribadi dan Pertanggungjawaban Otoritas Terhadap Keamanan Siber Menurut Tinjauan UU PDP." *Doktrina: Journal Of Law* 7.2. hlm. 182.
[12] Djarawula, Markus, Novita Alfiani, and Hanita Mayasari. 2023. "Tinjauan Yuridis Tindak Pidana Kejahatan Teknologi Informasi (Cybercrime) Di Indonesia Ditinjau Dari Perspektif Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik." *Jurnal Cakrawala Ilmiah* 2.10. hlm. 3802.
[13] Bambang Hartono, I Ketut Seregig, and Budi Wibowo. 2021. "Strategies in Countering Hoax and Hate Speech in Indonesia." *Sociological Jurisprudence Journal* 4.2. hlm. 140.
[14] Wiranata, Ganda Arisandi, Yoyok Ucuk, and Dudik Djaja Sidarta. 2024. "Pertanggungjawaban Pidana Terhadap Pelaku Tindak Pidana Phishing." *Court Review: Jurnal Penelitian Hukum* 4.02. hlm 15.

rasa percaya diri atau status mereka di dunia maya. Secara keseluruhan, motivasi hacker dalam melakukan kejahatan siber sangat kompleks dan beragam. Faktor finansial, ideologis, teknis, serta sosial dan psikologis semuanya berperan penting dalam membentuk keputusan mereka untuk terlibat dalam tindakan ilegal tersebut. Setiap hacker memiliki alasan dan tujuan yang berbeda, yang sering kali dipengaruhi oleh latar belakang pribadi, nilai-nilai, serta kesempatan yang ada di dunia digital. Oleh karena itu, pemahaman terhadap motivasi-motivasi ini menjadi penting dalam upaya untuk mencegah kejahatan siber, serta dalam merancang kebijakan dan strategi untuk melindungi sistem digital dan data pribadi dari ancaman yang terus berkembang.

Aspek Yuridis Kejahatan Siber

Upaya pencegahan dan penguatan keamanan digital menjadi hal yang sangat penting dalam menghadapi ancaman siber yang semakin kompleks. Di tingkat individu, langkah pertama yang dapat dilakukan adalah penggunaan kata sandi yang kuat dan unik.[15] Kata sandi yang kuat dapat mengurangi kemungkinan akun individu dibobol oleh pihak yang tidak bertanggung jawab. Pengguna juga perlu menerapkan enkripsi data pribadi mereka, baik saat disimpan di perangkat maupun saat dikirim melalui jaringan internet.[16] Enkripsi dapat memastikan bahwa data yang dikirimkan atau disimpan tidak dapat dibaca oleh pihak yang tidak berwenang, meskipun data tersebut berhasil dicuri. Selain itu, individu harus selalu berhati-hati dalam mengakses jaringan publik, seperti Wi-Fi gratis, yang rentan terhadap serangan. Menggunakan VPN atau Virtual Private Network adalah salah satu cara untuk melindungi data pribadi dari potensi ancaman saat menggunakan jaringan publik. Dengan langkah-langkah ini, individu dapat menjaga keamanan data pribadi mereka dan meminimalkan risiko terjadinya kejahatan siber. Di sisi lain, organisasi dan perusahaan juga memiliki tanggung jawab besar dalam memperkuat sistem keamanan digital mereka untuk melindungi data dan informasi penting.[17] Salah satu langkah utama yang dapat diambil adalah dengan mengimplementasikan sistem keamanan siber yang lebih kuat, seperti firewall yang dapat memblokir akses yang tidak sah, serta perangkat lunak antivirus yang dapat mendeteksi dan menghapus virus atau malware yang masuk ke dalam sistem. Selain itu, proses patching atau pembaruan perangkat lunak secara berkala juga sangat penting untuk menutup celah keamanan yang mungkin dieksploitasi oleh hacker. Sistem keamanan yang terintegrasi dan diperbarui secara teratur akan membantu organisasi mengurangi risiko serangan siber. Tidak kalah pentingnya, perusahaan harus melibatkan pihak ketiga yang ahli dalam keamanan siber untuk melakukan audit dan uji penetrasi, guna memastikan bahwa sistem yang mereka gunakan telah cukup tangguh untuk menghadapi ancaman yang ada.

Peran pemerintah dalam membangun kebijakan dan regulasi yang melindungi data pribadi dan keamanan digital juga sangat krusial. Di Indonesia, salah satu landasan hukum yang mengatur kejahatan siber adalah Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), yang mengatur penggunaan teknologi informasi dan transaksi elektronik, termasuk sanksi terhadap kejahatan siber seperti pencemaran nama baik, penyebaran hoaks, dan peretasan.[18] Selain itu, regulasi yang lebih baru, seperti Peraturan Pemerintah tentang Perlindungan Data Pribadi, juga memberikan perlindungan lebih lanjut terhadap data pribadi individu. Di tingkat internasional, kebijakan seperti General Data Protection Regulation (GDPR) di Uni Eropa

[15] Simorangkir, Amos Saito Hamonangan. 2024. "Peran Pemerintah Dalam Penanganan Kejahatan Siber Di Era Digital Dalam Konteks Hukum Acara Pidana." *Causa: Jurnal Hukum dan Kewarganegaraan* 7.3. hlm. 34.
[16] Fadhilah, Muhammad Gerda. 2024. "Implementasi Pasal 362 KUHP dan Pasal 30 Undang-Undang Informasi dan Transaksi Elektronik Terkait Pertanggung Jawaban Pelaku Pembobolan Rekening Nasabah." *Das Sollen: Jurnal Kajian Kontemporer Hukum Dan Masyarakat* 2.02.
[17] Hartono, Bambang, and Recca Ayu Hapsari. 2019. "Mutual Legal Assistance Pada Pemberantasan Cyber Crime Lintas Yurisdiksi di Indonesia." *Sasi* 25.1: hlm. 67.
[18] Adnan, Alinda Julietha, Dewi Putriyani, Hycal Asmara Wibowo, and Suta Ramadan. 2024. "Perlindungan Hukum terhadap Anak Sebagai Korban Tindak Pidana Cyberbullying." *Indonesian Journal of Criminal Law and Criminology (IJCLC)* 5.1.

memberikan standar yang tinggi mengenai perlindungan data pribadi. Pemerintah Indonesia perlu terus meningkatkan regulasi dan kebijakan yang melindungi data pribadi masyarakat dan mendorong sektor swasta untuk mematuhi standar keamanan siber yang tinggi. Selain itu, pemerintah juga harus bekerja sama dengan negara lain dalam upaya penanggulangan kejahatan siber yang bersifat lintas negara. Pentingnya edukasi dan kesadaran masyarakat mengenai ancaman siber juga tidak bisa diabaikan. Kampanye keamanan digital yang bertujuan untuk meningkatkan pemahaman masyarakat tentang potensi bahaya dan bagaimana cara menghindarinya harus dilakukan secara masif. Edukasi ini mencakup pemahaman tentang ancaman-ancaman siber yang umum, seperti phishing, malware, dan ransomware, serta langkah-langkah yang bisa diambil untuk melindungi diri, seperti menggunakan perangkat lunak antivirus, memperbarui perangkat secara berkala, serta selalu waspada terhadap email atau pesan mencurigakan. Selain itu, pemerintah, organisasi, dan lembaga pendidikan dapat berperan dalam menyediakan pelatihan keamanan digital untuk berbagai kalangan, termasuk anak-anak dan lansia, yang rentan menjadi korban serangan siber. Semakin tinggi tingkat kesadaran dan pengetahuan masyarakat, semakin kecil kemungkinan mereka terjerumus dalam kejahatan siber.

Dalam konteks yuridis, upaya penanggulangan kejahatan siber juga memerlukan perhatian terhadap peraturan perundang-undangan yang berlaku. Di Indonesia, selain UU ITE, ada beberapa peraturan lain yang mengatur tentang perlindungan data pribadi dan tindak pidana yang berhubungan dengan dunia digital, seperti Undang-Undang Perlindungan Data Pribadi yang mengatur kewajiban perusahaan dalam menjaga kerahasiaan dan keamanan data pelanggan. Peraturan ini harus diimplementasikan secara tegas untuk memastikan bahwa individu dan organisasi yang melanggar hukum dapat diberikan sanksi yang sesuai. Di tingkat internasional, penerapan regulasi yang melibatkan perlindungan data pribadi, seperti GDPR, memberikan standar yang lebih ketat yang dapat diadopsi oleh negara lain untuk melindungi warga negaranya dari kejahatan siber. Penerapan hukum terhadap hacker dan kejahatan siber, baik di tingkat nasional maupun internasional, juga sangat penting. Proses hukum terhadap hacker dapat berlangsung melalui penyidikan dan penuntutan yang melibatkan bukti digital, yang seringkali menjadi tantangan besar dalam dunia peradilan.[19] Pembuktian dalam kasus kejahatan siber memerlukan keahlian teknis untuk menganalisis bukti digital, seperti jejak digital yang ditinggalkan oleh hacker di server atau perangkat korban. Selain itu, kerjasama internasional menjadi kunci dalam mengatasi kejahatan siber yang melibatkan pelaku lintas negara. Tantangan utama dalam penegakan hukum kejahatan siber adalah terbatasnya yurisdiksi yang dapat diterapkan pada kasus yang melibatkan pelaku dari negara yang berbeda. Oleh karena itu, kerjasama antara negara dan organisasi internasional sangat penting untuk memastikan bahwa pelaku kejahatan siber dapat dituntut dan diadili sesuai hukum yang berlaku.

KESIMPULAN

Kesimpulan dari pembahasan mengenai kejahatan siber dan upaya pencegahannya menunjukkan bahwa ancaman ini memiliki dampak yang sangat besar terhadap individu, organisasi, dan masyarakat secara keseluruhan. Hacker, dengan berbagai latar belakang dan motivasi, baik itu finansial, ideologis, teknis, maupun sosial-psikologis, memainkan peran sentral dalam serangan siber yang dapat merusak sistem keamanan digital. Oleh karena itu, langkah pencegahan yang dilakukan oleh individu, organisasi, serta pemerintah sangat penting untuk memitigasi risiko tersebut. Individu harus menjaga keamanan data pribadi mereka dengan menggunakan kata sandi yang kuat, enkripsi data, serta berhati-hati dalam mengakses

[19] Hartono, Bambang. 2014. "Hacker Dalam Perspektif Hukum Indonesia." *Masalah-Masalah Hukum* 43.1. hlm. 25.

jaringan publik. Sementara itu, organisasi perlu mengimplementasikan sistem keamanan siber yang lebih kuat, seperti firewall, antivirus, serta melakukan pembaruan sistem secara rutin untuk melindungi informasi mereka dari serangan. Pemerintah juga memiliki peran kunci dalam mengembangkan regulasi yang melindungi data pribadi dan mengatur kejahatan siber secara efektif, seperti UU ITE di Indonesia dan regulasi internasional seperti GDPR di Eropa. Selain itu, edukasi masyarakat juga merupakan bagian yang sangat penting dalam membangun kesadaran tentang potensi bahaya siber dan cara-cara untuk menghindarinya. Kampanye keamanan digital yang menyasar berbagai lapisan masyarakat dapat memperkuat ketahanan terhadap ancaman siber yang terus berkembang. Dalam aspek yuridis, penegakan hukum terhadap kejahatan siber menghadapi tantangan besar, seperti kesulitan pembuktian dan kebutuhan akan kerjasama internasional. Oleh karena itu, penerapan hukum yang tegas dan adanya regulasi yang lebih jelas dan komprehensif dapat meningkatkan efektivitas penanggulangan kejahatan siber. Kejahatan siber tidak hanya menjadi ancaman bagi sektor teknologi, tetapi juga berpengaruh pada aspek sosial, ekonomi, dan politik, yang memerlukan perhatian serius dari semua pihak. Saran yang dapat diberikan adalah perlunya penguatan kolaborasi antara sektor publik dan swasta dalam meningkatkan ketahanan digital, terutama melalui pelatihan intensif, peningkatan kesadaran keamanan siber, dan penerapan kebijakan yang lebih adaptif terhadap perkembangan teknologi.

DAFTAR PUSTAKA

Adnan, Alinda Julietha, Dewi Putriyani, Hycal Asmara Wibowo, and Suta Ramadan. 2024. "Perlindungan Hukum terhadap Anak Sebagai Korban Tindak Pidana Cyberbullying." *Indonesian Journal of Criminal Law and Criminology (IJCLC)* 5.1.

Anggraini, Yuli. 2024. "Kekuatan hukum alat bukti elektronik dan kredibilitasnya dalam pembuktian hukum pidana." *Causa: Jurnal Hukum dan Kewarganegaraan* 6.8.

Budiyanto, S. H. 2025. *Pengantar Cybercrime dalam Sistem Hukum Pidana di Indonesia.* Sada Kurnia Pustaka.

Djarawula, Markus, Novita Alfiani, and Hanita Mayasari. 2023. "Tinjauan Yuridis Tindak Pidana Kejahatan Teknologi Informasi (Cybercrime) Di Indonesia Ditinjau Dari Perspektif Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik." *Jurnal Cakrawala Ilmiah* 2.

Fadhilah, Muhammad Gerda. 2024. "Implementasi Pasal 362 KUHP dan Pasal 30 Undang-Undang Informasi dan Transaksi Elektronik Terkait Pertanggung Jawaban Pelaku Pembobolan Rekening Nasabah." *Das Sollen: Jurnal Kajian Kontemporer Hukum Dan Masyarakat* 2.02.

Hartono, Bambang, and Recca Ayu Hapsari. 2019. "Mutual Legal Assistance Pada Pemberantasan Cyber Crime Lintas Yurisdiksi di Indonesia." *Sasi* 25.1.

Hartono, Bambang, I Ketut Seregig, and Budi Wibowo. 2021. "Strategies in Countering Hoax and Hate Speech in Indonesia." *Sociological Jurisprudence Journal* 4.2.

Hartono, Bambang. 2014. "Hacker Dalam Perspektif Hukum Indonesia." *Masalah-Masalah Hukum* 43.1.

Idriansyah, Alfi Salsabilah, and Nur Afifah. 2024. "Perlindungan Hukum Terhadap Korban Cyber Crime di Indonesia dalam Aliran Hukum Pada Kasus Pencurian Data Pribadi." *Media Hukum Indonesia (MHI)* 2.4.

Kapoyos, Jeremiah Marvin, et al. 2023. "Pentingnya Cybersecurity di Era Society 5.0." *Nusantara Journal of Multidisciplinary Science* 1.5.

Mardiansyach, Dewo. 2023. *Implikasi Delik Pidana Khusus Cybercrime Praktik Perjudian Online.* Diss. Universitas Islam Sultan Agung Semarang.

Retno Wulansari, I Ketut Seregig, Suta Ramadan. 2022. *Pertimbangan Hakim Terhadap Pelaku Tindak Pidana Pembakaran Polsek Candipuro Lampung Selatan (Studi Putusan Nomor: 285/Pid. Sus/2021/PN. KLA)*. Yustisia Tirtayasa, Vol. 2, No. 2.

Santhi, Ni Nyoman Putri Purnama, and I. Nengah Nuarta. 2023. "Penguatan Penegakan Hukum Polri dalam Rangka Optimalisasi Penanggulangan Cybercrime di Indonesia." *SCIENTIA: Journal of Multi Disciplinary Science.*

Simorangkir, Amos Saito Hamonangan. 2024. "Peran Pemerintah Dalam Penanganan Kejahatan Siber Di Era Digital Dalam Konteks Hukum Acara Pidana." *Causa: Jurnal Hukum Dan Kewarganegaraan* 7.3.

Sriwulan, Sriwulan. 2023. *Tinjauan Yuridis Tindak Pidana Cyber Crime Di Indonesia.* Diss. Institut Agama Islam Negeri Palopo.

Suta Ramadan, I Ketut Seregig, Deta Merly Oktavianti. 2022. *Analisis Pertimbangan Hakim dalam Menjatuhkan Sanksi Pidana Terhadap Pelaku Tindak Pidana Penggelapan dalam Jabatan*. PAMPAS: Journal of Criminal Law, Vol. 3, No. 1.

Tamhidah, Mas Atsilah Rahmah. 2023. "Pengaruh Media Sosial Terhadap Penyebaran Informasi Palsu dan Kejahatan Siber." *Innovative: Journal Of Social Science Research* 3.6.

Usman, Noval, and Satria Unggul Wicaksana Prakasa. 2024. "Perlindungan Hukum Data Pribadi dan Pertanggungjawaban Otoritas Terhadap Keamanan Siber Menurut Tinjauan UU PDP." *Doktrina: Journal Of Law* 7.2.

Wiranata, Ganda Arisandi, Yoyok Ucuk, and Dudik Djaja Sidarta. 2024. "Pertanggungjawaban Pidana Terhadap Pelaku Tindak Pidana Phishing." *Court Review: Jurnal Penelitian Hukum* 4.02.