KAYÊÊ
JURNAL PENDIDIKAN DAN ILMU SOSIAL

eISSN 0000-0000 & pISSN 0000-000
Vol. 1, No. 1, Tahun 2025
doi.org/10.63822/kayee.vxix.xx
Hal. 01-06

Homepage https://ejournal.rumohjurnal.org/index.php/kayee

Tanggung Jawab Hukum Warga Negara dalam Mengatasi Kejahatan Cyber dan Mendorong Stabilitas Sosial

Amalia Zahra
Program Studi S1 Sains Data, Fakultas Informatika, Telkom University, Bandung, Indonesia

*Email Korespodensi: amaliazahra@student.telkomuniversity.ac.id

ABSTRACT

Cyber crimes are crimes that are based on the internet and digital devices. Data theft, hacking, and widespread online fraud are a few examples of these crimes. To overcome this, the legal responsibility of the state is very important in overcoming this illegal activity through compliance with regulations and active participation of citizens to report if there are illegal or suspicious activities. In the context of Sustainable Development Goal 16, which emphasizes peace and justice for all, cooperation between governments, law enforcement and communities is needed to create peace in the social and also digital spheres.

Keywords: Cybercrime, Regulation, SDGs 16.

ABSTRAK

Kejahatan cyber adalah kejahatan yang berbasis melalui jaringan internet serta perangkat digital. Contoh kejahatan ini adalah seperti pencurian data, perentasan serta penipuan online yang sudah marak terjadi. Dalam mengatasi hal ini tanggung jawab hukum negara sangat penting dalam mengatasi kegiatan ilegal ini melalui kepatuhan terhadap regulasi dan partisipasi aktif warga negara untuk melaporkan jika terdapat kegiatan ilegal atau mencurigakan. Dalam konteks Tujuan Pembangunan Berkelanjutan dalam SDGs 16, yang menekankan mengenai perdamaian dan keadilan untuk semua orang lalu kerjasama antar pemerintah, para penegak hukum serta masyarakat sangat diperlukan untuk menciptakan kedamaian dalam lingkup sosial maupun digital.

Katakunci: Kejahatan cyber, Regulasi, SDGs 16

PENDAHULUAN

Teknologi telah mengalami perkembangan pesat dalam beberapa dekade terakhir, terutama dengan adanya kemajuan di bidang digital dan internet. Kemunculan teknologi informasi dan komunikasi (TIK) telah mengubah cara hidup manusia secara signifikan, mulai dari komunikasi hingga transaksi ekonomi. Kehadiran internet sebagai pusat informasi global memungkinkan akses cepat terhadap data dan pengetahuan, yang mendorong perubahan besar di berbagai sektor seperti pendidikan, kesehatan, dan bisnis. Kemudahan yang ditawarkan teknologi membuatnya menjadi bagian integral dari kehidupan sehari-hari. Selain itu, teknologi telah menghadirkan inovasi-inovasi yang berdampak pada transformasi sosial dan ekonomi. Perkembangan teknologi mobile, misalnya, telah memungkinkan masyarakat untuk tetap terhubung dan melakukan aktivitas sehari-hari melalui perangkat genggam. Platform media sosial, aplikasi e-commerce, serta layanan berbasis cloud menjadi contoh bagaimana teknologi telah mengubah cara berinteraksi dan menjalankan bisnis. Transformasi ini membuka peluang baru bagi peningkatan efisiensi, produktivitas, dan inklusi digital (Hafid *et al*,. 2023).

Namun, perkembangan teknologi juga menimbulkan tantangan baru yang perlu diatasi. Kemajuan di dunia digital membawa dampak besar terhadap isu-isu keamanan, privasi, dan kejahatan digital. Kebutuhan akan regulasi yang adaptif dan kesadaran hukum yang kuat menjadi hal penting untuk memastikan perkembangan teknologi tidak mengancam stabilitas sosial. Oleh karena itu, warga negara memiliki peran penting dalam memastikan penggunaan teknologi yang aman dan bertanggung jawab (Aji, 2023). Perkembangan teknologi, meskipun memberikan banyak manfaat, juga memunculkan berbagai risiko, salah satunya adalah kejahatan cyber. Kejahatan cyber meliputi berbagai tindakan ilegal yang dilakukan melalui media digital, seperti pencurian data, peretasan, penyebaran malware, hingga penipuan online. Meningkatnya penggunaan teknologi dan akses internet memberikan peluang bagi pelaku kejahatan untuk melakukan tindakan yang merugikan individu, perusahaan, maupun negara. Kejahatan ini kerap terjadi karena celah keamanan pada sistem digital yang dieksploitasi oleh pihak tidak bertanggung jawab. Dampaknya bisa sangat serius, termasuk kerugian finansial, pelanggaran privasi, serta gangguan terhadap stabilitas sosial (Putri *et al*,. 2023).

Kejahatan cyber adalah bentuk kejahatan yang dilakukan dengan memanfaatkan teknologi informasi dan komunikasi, terutama melalui jaringan internet. Kejahatan ini dapat mencakup aktivitas yang merusak, mencuri, atau memanipulasi data, serta berbagai tindakan ilegal lainnya yang terjadi di dunia maya. Tujuan dari kejahatan cyber bisa beragam, mulai dari keuntungan finansial hingga sabotase informasi. Seiring dengan semakin berkembangnya teknologi, kejahatan cyber menjadi salah satu tantangan terbesar yang dihadapi oleh masyarakat modern karena dampaknya yang luas dan sulit untuk ditangani secara konvensional. Warga negara memiliki tanggung jawab hukum yang signifikan dalam mengatasi kejahatan siber dan menjaga stabilitas sosial. Tanggung jawab ini mencakup kepatuhan terhadap regulasi yang mengatur keamanan digital, serta partisipasi aktif dalam melaporkan dan mencegah aktivitas mencurigakan di dunia maya. Dengan meningkatkan literasi digital, masyarakat dapat lebih waspada terhadap ancaman cyber dan mendukung upaya pemerintah serta penegak hukum dalam menegakkan keamanan. Selain itu, keterlibatan warga negara dalam kampanye kesadaran keamanan digital dan kerja sama dengan lembaga terkait juga merupakan langkah penting untuk menciptakan linhkungan digital yang aman dan stabil.

Pemilihan judul “Tanggung Jawab Hukum Warga Negara dalam Mengatasi Kejahatan Siber dan Mendorong Stabilitas Sosial" didasari oleh pentingnya peran individu dalam menjaga keamanan dunia

maya di tengah perkembangan teknologi yang pesat. Kejahatan siber semakin menjadi ancaman besar di era digital, dan oleh karena itu, setiap warga negara memiliki tanggung jawab hukum untuk memastikan bahwa mereka tidak hanya menjadi korban, tetapi juga berperan aktif dalam mencegah dan melaporkan aktivitas kriminal di dunia maya. Judul ini menyoroti kesadaran hukum dan peran aktif warga negara dalam menciptakan lingkungan digital yang aman, yang pada gilirannya dapat mendukung terciptanya stabilitas sosial secara keseluruhan. Dengan meningkatkan partisipasi masyarakat dalam upaya penanggulangan kejahatan siber, diharapkan dapat tercapai keadilan yang lebih besar serta memperkuat sistem hukum di tingkat global.

METODE PENELITIAN

Metode pengambilan data dalam penelitian ini menggunakan pendekatan kualitatif dengan studi literatur. Data dikumpulkan melalui analisis berbagai sumber tertulis, seperti jurnal ilmiah, buku, artikel, laporan pemerintah, dan dokumen terkait lainnya yang membahas tentang kejahatan cyber, regulasi yang ada, serta peran lembaga dalam menangani masalah ini. Pendekatan studi literatur memungkinkan peneliti untuk mengidentifikasi pola, tren, dan kesenjangan dalam pengetahuan yang ada mengenai kejahatan cyber serta peran institusi yang relevan, dengan mengandalkan informasi yang telah dipublikasikan sebelumnya. Hasil dari analisis literatur ini diharapkan dapat memberikan pemahaman yang lebih komprehensif mengenai topik yang diteliti dan mendukung pengembangan kebijakan atau strategi yang lebih efektif dalam mengatasi kejahatan cyber.

HASIL DAN PEMBAHASAN

Kejahatan cyber, atau dikenal juga sebagai kejahatan dunia maya, adalah segala bentuk aktivitas ilegal yang dilakukan melalui jaringan internet atau perangkat digital. Jenis kejahatan ini mencakup berbagai tindakan yang bertujuan untuk merusak, mencuri, memanipulasi, atau menyalahgunakan data serta sistem digital. Kejahatan cyber sering kali melibatkan penggunaan komputer, smartphone, atau perangkat digital lainnya sebagai alat utama dalam melakukan tindakan yang melanggar hukum. Bentuk-bentuk kejahatan ini berkembang seiring dengan kemajuan teknologi informasi, yang menyebabkan semakin banyaknya data pribadi dan informasi penting yang tersimpan secara digital. Kejahatan cyber dapat dibedakan menjadi beberapa kategori, seperti penipuan online, pencurian identitas, peretasan, penyebaran virus atau malware, dan serangan siber terhadap infrastruktur digital. Penipuan online sering kali melibatkan taktik manipulatif yang mengelabui korban untuk memberikan informasi sensitif atau melakukan transaksi ilegal. Sementara itu, pencurian identitas terjadi ketika data pribadi dicuri dan digunakan tanpa izin, dengan tujuan untuk mengambil keuntungan finansial atau melakukan tindakan merugikan lainnya. Kejahatan cyber ini tidak hanya menyasar individu, tetapi juga perusahaan dan institusi pemerintah (Putri *et al*,. 2023).

Dalam beberapa kasus, kejahatan cyber berdampak serius pada keamanan dan privasi korban. Misalnya, peretasan terhadap sistem perusahaan dapat mengakibatkan hilangnya data penting, yang berdampak pada kerugian finansial dan reputasi perusahaan. Di sisi lain, serangan siber yang menargetkan infrastruktur kritis, seperti jaringan listrik atau sistem perbankan, dapat mengganggu stabilitas sosial dan ekonomi suatu negara. Oleh karena itu, penanganan kejahatan cyber memerlukan upaya yang komprehensif, mulai dari peningkatan keamanan digital hingga penegakan hukum yang efektif. Pencegahan

dan penanggulangan kejahatan cyber tidak hanya menjadi tanggung jawab pemerintah dan lembaga keamanan, tetapi juga melibatkan kesadaran dan partisipasi aktif masyarakat. Setiap warga negara perlu memahami ancaman yang ada di dunia maya dan mengambil langkah-langkah pencegahan, seperti mengamankan perangkat digital, menggunakan kata sandi yang kuat, serta menghindari berbagi informasi pribadi secara sembarangan. Kesadaran akan pentingnya keamanan digital dan upaya kolektif dalam memerangi kejahatan cyber menjadi kunci untuk menciptakan lingkungan digital yang lebih aman dan terpercaya.

Salah satu contoh fenomena *cyber crime* adalah *phishing* di mana penjahat siber mencoba mencuri data pribadi atau informasi sensitif pengguna melalui teknik penipuan. Phishing biasanya dilakukan dengan mengirim email atau pesan yang tampak berasal dari sumber tepercaya, seperti bank atau platform media sosial, yang meminta pengguna untuk memasukkan informasi pribadi, seperti nomor kartu kredit, kata sandi, atau nomor identitas. Pesan ini sering kali mengarahkan korban ke situs web palsu yang menyerupai halaman asli, sehingga korban tidak menyadari bahwa mereka sedang ditipu. Phishing merupakan salah satu bentuk kejahatan siber yang paling umum dan berbahaya karena memanfaatkan ketidakwaspadaan pengguna internet untuk mendapatkan data penting yang dapat digunakan untuk pencurian identitas atau penipuan keuangan.

Kasus phishing di Indonesia mengalami peningkatan signifikan, menempatkan negara ini di posisi ke-8 dalam daftar negara dengan kebocoran data tertinggi secara global. Pada kuartal II/2022, tercatat sekitar 820 ribu kasus pembobolan, dan serangan phishing melonjak lebih dari 40 persen pada 2023, dengan 709.590.011 upaya serangan. Lonjakan ini terutama terlihat pada Mei dan Juni 2023, yang diduga terkait dengan musim liburan. Industri e-commerce menjadi sasaran utama, dengan platform seperti Tokopedia, Shopee, dan Bukalapak menjadi target serangan. Phishing adalah tindakan pengelabuan untuk mencuri data pribadi, akun, atau informasi finansial. Untuk melindungi diri, pengguna disarankan untuk mengganti kata sandi secara berkala, mengaktifkan verifikasi dua faktor, memantau aktivitas akun, dan melaporkan kejadian ke layanan resmi. Phishing adalah tindakan kriminal yang dapat dihukum penjara hingga 8 tahun atau denda sebesar Rp800.000.000,00 sesuai hukum yang berlaku di Indonesia (Puspitasari dan Sutabri, 2023).

Tujuan Pembangunan Berkelanjutan (SDGs) 16 menekankan pada pentingnya menciptakan perdamaian, keadilan, dan institusi yang kuat untuk memastikan pembangunan yang berkelanjutan dan inklusif. Dalam konteks kejahatan cyber, SDGs 16 sangat relevan karena keamanan digital dan keadilan di dunia maya menjadi faktor kunci dalam mewujudkan masyarakat yang damai dan stabil. Kejahatan cyber, yang mencakup penipuan, pencurian data, peretasan, serta serangan terhadap infrastruktur digital, dapat mengancam stabilitas sosial, ekonomi, dan keamanan suatu negara. Oleh karena itu, upaya untuk mengatasi kejahatan cyber sejalan dengan tujuan SDGs 16 dalam membangun institusi yang mampu menegakkan hukum secara efektif di era digital (Hafid, 2023). Menghadapi kejahatan cyber membutuhkan peraturan yang kuat dan penegakan hukum yang adil untuk melindungi hak-hak warga negara dan menjaga kepercayaan publik terhadap sistem digital. Ini juga mencakup peningkatan literasi digital dan kesadaran masyarakat tentang pentingnya keamanan di dunia maya. Selain itu, penguatan kapasitas lembaga keamanan dan penegak hukum untuk menangani kasus kejahatan cyber secara efisien merupakan bagian dari pencapaian SDGs 16. Dengan adanya regulasi yang jelas dan kerjasama internasional, diharapkan kejahatan cyber dapat dikendalikan, sehingga tercipta masyarakat yang lebih aman dan damai di era digital yang semakin kompleks (Paulina *et al*,. 2024).

Implementasi SDGs 16 dalam menghadapi kejahatan cyber juga berarti memastikan akses yang setara terhadap keadilan bagi semua, termasuk korban kejahatan digital. Hal ini mencakup perlindungan hukum yang memadai bagi individu yang terkena dampak serta penanganan kasus yang transparan dan akuntabel (Paulina *et al*,. 2024). Dalam lingkup yang lebih luas, upaya untuk menanggulangi kejahatan cyber mendukung terciptanya sistem hukum yang responsif terhadap perkembangan teknologi, sehingga hak dan privasi warga negara tetap terjamin. Keberhasilan dalam menangani kejahatan cyber akan memperkuat institusi hukum dan mendorong terciptanya lingkungan yang aman bagi pertumbuhan ekonomi digital. Oleh karena itu, upaya melawan kejahatan cyber merupakan bagian integral dari mencapai tujuan SDGs 16, di mana keamanan digital yang kuat akan mendukung terciptanya masyarakat yang adil dan berkelanjutan. Dengan kerjasama antara warga negara, pemerintah, dan sektor swasta, diharapkan dapat terbentuk ekosistem digital yang aman, di mana hukum ditegakkan secara adil dan transparan, serta perlindungan terhadap data dan privasi individu dapat terjamin dengan baik.

Dalam konteks SDGs 16, yang berfokus pada perdamaian, keadilan, dan institusi yang kuat, lembaga-lembaga memiliki peran penting dalam mengatasi kejahatan cyber untuk menciptakan lingkungan digital yang aman dan stabil. Lembaga penegak hukum, seperti kepolisian dan badan hukum, bertugas untuk mengidentifikasi, menyelidiki, dan menuntut pelaku kejahatan cyber, sehingga memastikan hukum ditegakkan secara adil dan pelanggaran di dunia maya tidak dibiarkan begitu saja. Selain itu, lembaga pemerintah dan non-pemerintah berperan dalam melindungi masyarakat dari ancaman cyber melalui program edukasi dan peningkatan literasi digital. Program-program ini bertujuan untuk meningkatkan kesadaran masyarakat tentang risiko dunia maya dan cara melindungi diri secara efektif. Di sisi lain, pemerintah melalui berbagai lembaga bertanggung jawab untuk merumuskan regulasi dan kebijakan yang mengatur keamanan digital dan perlindungan data. Kebijakan yang kuat dan jelas menjadi fondasi penting dalam menanggulangi kejahatan cyber, memastikan bahwa sistem hukum mampu mengatasi tantangan teknologi, dan mendukung penciptaan masyarakat yang aman dan stabil sesuai dengan tujuan SDGs 16.

KESIMPULAN

Kejahatan cyber merupakan ancaman serius yang berkembang seiring pesatnya kemajuan teknologi digital. Kejahatan ini mencakup berbagai tindakan ilegal seperti peretasan, pencurian identitas, dan penipuan online, yang dapat merusak individu, perusahaan, serta stabilitas sosial. SDGs 16, yang menekankan pada perdamaian, keadilan, dan institusi yang kuat, sangat relevan dalam menghadapi tantangan ini. Lembaga-lembaga, baik pemerintah maupun non-pemerintah, memegang peran penting dalam penegakan hukum, peningkatan literasi digital, serta pembentukan kebijakan yang dapat melindungi masyarakat dari ancaman cyber. Dengan adanya kesadaran hukum dan kerjasama antara berbagai pihak, diharapkan dapat tercipta ekosistem digital yang lebih aman dan teratur.

DAFTAR PUSTAKA

Hafid, M., Firjatullah, F. Z., & Pamungkaz, B. W. (2023). Tantangan Menghadapi Kejahatan Cyber dalam Kehidupan Bermasyarakat dan Bernegara. *Jurnal Pendidikan Tambusai, 7*(2), 9548-9556.

Aji, B. (2023). Tindakan Kejahatan Cyber Crime Dalam Bentuk Deface Website. *Cyber Security dan Forensik Digital, 6*(1), 25-29.

Putri, C. W., Ibrahim, A. L., & Syahuri, T. (2023). Pemberantasan Tindak Pidana Cyber di Provinsi Jawa Barat: Peran Hukum dan Tantangan dalam Penegakan Hukum Terhadap Kejahatan Digital. *Darmabakti: Jurnal Pengabdian dan Pemberdayaan Masyarakat, 4*(1), 113-121.

Mokobombang, M., Darwis, Z., & Mokodenseho, S. (2023). Instrumental Norm Approach pada Pemilih Pemula sebagai Penegakan Demokrasi di Ruang Siber Menjelang Pemilu 2024 di Depok. *Jurnal Hukum dan HAM Wara Sains, 2*(06), 517-525.

Paulina, G., Maulidiyah, S., & Rachman, I. F. (2024). Transformasi Pendidikan Digital Etika: Tantangan dan Strategi Menuju SDGs 2030. *Jurnal Ilmiah Research Student, 1*(5), 256-267.

Puspitasari, D., & Sutabri, T. (2023). Analisis Kejahatan Phising pada Sektor E-commerce di Marketplace Shopee. *Jurnal Digital Teknologi Informasi*, 6(2), 76-81. E-ISSN 2714-9706, P-ISSN 2686-4185.