

ANALISIS YURIDIS PENGARUH ESKALASI PENGGUNAAN MEDIA SOSIAL TERHADAP PENINGKATAN KEJAHATAN SIBER DI INDONESIA BERDASARKAN UU NO 1 TAHUN 2024

Jaozi¹, Appe Hutaauruk², Hotman Sinambela³

¹²³Fakultas Hukum Universitas Mpu Tantular

Email: jaozirpl@gmail.com, maju_08ok@yahoo.co.id

Abstrak - Perkembangan teknologi informasi dan komunikasi telah mendorong peningkatan penggunaan media sosial di Indonesia secara signifikan. Media sosial memberikan berbagai manfaat bagi masyarakat, seperti kemudahan komunikasi, pertukaran informasi, serta pengembangan aktivitas ekonomi digital. Namun di sisi lain, eskalasi penggunaan media sosial juga memunculkan berbagai bentuk kejahatan siber yang semakin kompleks. Penelitian ini bertujuan untuk menganalisis secara yuridis pengaruh peningkatan penggunaan media sosial terhadap meningkatnya kejahatan siber di Indonesia serta mengevaluasi efektivitas pengaturan hukum dalam Undang-Undang Nomor 1 Tahun 2024 tentang perubahan kedua atas Undang-Undang Informasi dan Transaksi Elektronik. Penelitian ini menggunakan metode penelitian hukum normatif dengan pendekatan perundang-undangan dan pendekatan konseptual. Data yang digunakan berupa bahan hukum primer, sekunder, dan tersier yang diperoleh melalui studi kepustakaan. Hasil penelitian menunjukkan bahwa penggunaan media sosial yang masif membuka peluang bagi pelaku kejahatan untuk melakukan berbagai bentuk cybercrime seperti penipuan daring, pencurian identitas, penyebaran hoaks, dan peretasan sistem informasi. Meskipun Undang-Undang Nomor 1 Tahun 2024 telah memperbarui beberapa ketentuan penting dalam regulasi kejahatan siber, implementasinya masih menghadapi berbagai kendala seperti anonimitas pelaku, kompleksitas bukti digital, serta keterbatasan yurisdiksi lintas negara. Oleh karena itu, penanggulangan kejahatan siber tidak hanya memerlukan penguatan regulasi, tetapi juga peningkatan literasi digital masyarakat serta penguatan kapasitas aparat penegak hukum dalam menghadapi tantangan kejahatan digital di era teknologi informasi. Kata kunci: cybercrime, media sosial, hukum siber, UU ITE, perlindungan hukum.

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi dalam beberapa dekade terakhir telah membawa perubahan signifikan dalam kehidupan masyarakat. Internet sebagai salah satu produk utama perkembangan teknologi informasi telah mengubah cara manusia berinteraksi, berkomunikasi, serta melakukan berbagai aktivitas ekonomi dan sosial. Melalui internet, berbagai bentuk komunikasi dapat dilakukan secara cepat tanpa dibatasi oleh ruang dan waktu.

Salah satu manifestasi perkembangan internet adalah munculnya berbagai platform media sosial yang memungkinkan individu untuk berbagi informasi, membangun jaringan sosial, serta berinteraksi secara virtual. Media sosial seperti Facebook, Instagram, WhatsApp, dan Twitter telah menjadi bagian penting dalam kehidupan masyarakat modern. Kehadiran media sosial tidak hanya memfasilitasi komunikasi antarindividu tetapi juga menjadi sarana pertukaran informasi, hiburan, hingga aktivitas ekonomi digital.

Namun demikian, perkembangan teknologi informasi juga membawa konsekuensi berupa munculnya berbagai bentuk kejahatan baru yang dikenal sebagai kejahatan siber atau cybercrime. Kejahatan siber merupakan bentuk kejahatan yang memanfaatkan teknologi informasi dan jaringan komputer sebagai sarana utama untuk melakukan tindak pidana. Cybercrime mencakup berbagai aktivitas ilegal seperti penipuan daring, pencurian identitas, peretasan sistem komputer, penyebaran malware, hingga penyebaran informasi palsu atau hoaks melalui media digital.

Peningkatan penggunaan media sosial di Indonesia telah memberikan peluang yang semakin besar bagi pelaku kejahatan siber untuk menjalankan aksinya. Dengan jumlah pengguna internet yang terus meningkat setiap tahun, media sosial menjadi salah satu platform utama yang dimanfaatkan oleh pelaku kejahatan siber untuk melakukan berbagai tindak kriminal. Kejahatan siber yang terjadi melalui media sosial dapat menimbulkan kerugian yang tidak hanya bersifat ekonomi tetapi juga psikologis dan sosial bagi korban.

Dalam rangka menghadapi tantangan tersebut, pemerintah Indonesia telah mengeluarkan berbagai regulasi yang bertujuan untuk mengatur aktivitas di ruang digital, salah satunya melalui Undang-Undang Informasi dan Transaksi Elektronik. Regulasi ini kemudian mengalami beberapa perubahan guna menyesuaikan dengan perkembangan teknologi informasi yang semakin pesat, termasuk melalui Undang-Undang Nomor 1 Tahun 2024 sebagai perubahan terbaru terhadap Undang-Undang ITE.

Meskipun demikian, perkembangan kejahatan siber yang semakin kompleks menimbulkan pertanyaan mengenai efektivitas regulasi yang ada dalam memberikan perlindungan hukum kepada masyarakat. Oleh karena itu, diperlukan kajian hukum yang komprehensif untuk memahami hubungan antara penggunaan media sosial dengan peningkatan kejahatan siber serta bagaimana regulasi yang ada mampu mengatasi fenomena tersebut.

Berdasarkan latar belakang tersebut, penelitian ini bertujuan untuk menganalisis pengaruh penggunaan media sosial terhadap peningkatan kejahatan siber di Indonesia serta mengkaji efektivitas pengaturan hukum dalam Undang-Undang Nomor 1 Tahun 2024 dalam menangani fenomena kejahatan siber di era digital.

TINJAUAN PUSTAKA

Konsep Tindak Pidana dalam Hukum Pidana

Dalam sistem hukum pidana Indonesia, istilah tindak pidana merupakan konsep fundamental yang menjadi dasar dalam menentukan adanya suatu perbuatan yang dapat dikenakan sanksi pidana. Meskipun demikian, peraturan perundang-undangan di Indonesia tidak secara eksplisit memberikan definisi tunggal mengenai istilah tindak pidana. Dalam praktiknya, berbagai istilah digunakan untuk merujuk pada konsep tersebut, seperti perbuatan pidana, peristiwa pidana, delik, maupun tindak pidana itu sendiri. Keberagaman terminologi ini tidak terlepas dari sejarah perkembangan hukum pidana Indonesia yang banyak dipengaruhi oleh sistem hukum Belanda melalui asas konkordansi, sehingga istilah yang digunakan berasal dari istilah Belanda *strafbaar feit*, yang secara umum diartikan sebagai perbuatan yang dapat dipidana (Wahyuni, 2017).

Para ahli hukum pidana memberikan definisi yang berbeda mengenai tindak pidana. Moeljatno memandang bahwa perbuatan pidana adalah perbuatan yang dilarang oleh suatu aturan hukum yang disertai ancaman pidana bagi siapa pun yang melanggarnya. Dalam definisi ini, tindak pidana mencakup tiga unsur utama, yaitu subjek hukum yang dituju oleh norma hukum (norm addressaat), perbuatan yang dilarang (strafbaar), dan ancaman pidana yang dikenakan apabila norma tersebut dilanggar (Hakim, 2020).

Sementara itu, Van Hammel mendefinisikan tindak pidana sebagai perilaku manusia yang dirumuskan dalam undang-undang, bersifat melawan hukum, patut dipidana, dan dilakukan dengan kesalahan. Definisi ini menegaskan bahwa suatu perbuatan tidak dapat dianggap sebagai tindak pidana apabila tidak memenuhi unsur melawan hukum dan unsur kesalahan dari pelakunya. Dengan demikian, tidak setiap perbuatan yang menimbulkan kerugian dapat secara otomatis dikategorikan sebagai tindak pidana apabila tidak terdapat unsur kesalahan atau pertanggungjawaban pidana.

Pandangan lain dikemukakan oleh Van Hattum yang menekankan bahwa suatu tindakan tidak dapat dipisahkan dari pelakunya. Menurutnya, istilah strafbaar mengandung makna bahwa suatu perbuatan layak untuk dijatuhi hukuman karena tindakan tersebut menimbulkan konsekuensi hukum yang dapat dipertanggungjawabkan oleh pelakunya. Oleh karena itu, tindak pidana tidak hanya dilihat dari aspek perbuatan, tetapi juga dari keterkaitan antara perbuatan tersebut dengan pelaku yang melakukannya (Lamintang & Lamintang, 2019).

Dengan demikian, dapat disimpulkan bahwa tindak pidana merupakan suatu perbuatan manusia yang dilarang oleh undang-undang, bersifat melawan hukum, dilakukan dengan kesalahan, serta diancam dengan sanksi pidana. Keberadaan unsur-unsur tersebut menjadi dasar penting dalam menentukan apakah suatu perbuatan dapat dikualifikasikan sebagai tindak pidana atau tidak.

Unsur-unsur Tindak Pidana

Dalam kajian hukum pidana, pembahasan mengenai tindak pidana tidak dapat dilepaskan dari analisis terhadap unsur-unsurnya. Unsur tindak pidana merupakan elemen yang harus terpenuhi agar suatu perbuatan dapat dikategorikan sebagai perbuatan pidana. Secara umum, unsur tindak pidana berkaitan dengan tindakan manusia yang dapat berupa tindakan aktif (een doen) maupun tindakan pasif berupa kelalaian (een nalaten) yang melanggar kewajiban hukum tertentu (Lamintang & Lamintang, 2019).

Dalam doktrin hukum pidana dikenal dua aliran utama yang menjelaskan struktur unsur tindak pidana, yaitu aliran monisme dan aliran dualisme.

Aliran monisme memandang bahwa unsur perbuatan pidana dan pertanggungjawaban pidana merupakan satu kesatuan yang tidak dapat dipisahkan. Tokoh utama aliran ini adalah Simons yang menyatakan bahwa suatu peristiwa pidana hanya dapat terjadi apabila seluruh unsur delik terpenuhi secara bersamaan. Unsur-unsur tersebut meliputi: perbuatan yang sesuai dengan rumusan delik, sifat melawan hukum, serta adanya kesalahan pada pelaku. Dengan kata lain, seseorang tidak dapat dipidana apabila salah satu unsur tersebut tidak terpenuhi (Mangkepriyanto, 2019).

Sebaliknya, aliran dualisme memisahkan antara unsur perbuatan pidana dengan unsur pertanggungjawaban pidana. Dalam pandangan ini, unsur objektif dan unsur subjektif dipandang sebagai dua komponen yang berbeda. Unsur objektif berkaitan dengan perbuatan

yang dilakukan oleh pelaku, sedangkan unsur subjektif berkaitan dengan keadaan batin atau kesalahan pelaku. Andi Zainal Abidin Farid membagi unsur tindak pidana ke dalam dua kategori utama, yaitu *actus reus* yang merujuk pada perbuatan pidana dan *mens rea* yang berkaitan dengan kesalahan atau niat pelaku (Sofyan & Azisa, 2016).

Berdasarkan kedua pendekatan tersebut, dapat disimpulkan bahwa suatu tindak pidana pada prinsipnya harus memenuhi beberapa unsur penting, yaitu adanya perbuatan yang dilarang oleh undang-undang, adanya sifat melawan hukum, adanya kesalahan pelaku, serta adanya subjek hukum yang dapat dimintai pertanggungjawaban pidana. Apabila salah satu unsur tersebut tidak terpenuhi, maka perbuatan tersebut tidak dapat dikualifikasikan sebagai tindak pidana.

Konsep Ruang Siber (*Cyberspace*)

Perkembangan teknologi informasi dan komunikasi telah melahirkan suatu ruang interaksi baru yang dikenal sebagai *cyberspace* atau ruang siber. *Cyberspace* merupakan lingkungan virtual yang terbentuk dari integrasi jaringan komputer dan teknologi komunikasi digital yang memungkinkan individu untuk berinteraksi tanpa dibatasi oleh ruang dan waktu.

Istilah *cyberspace* pertama kali diperkenalkan oleh William Gibson dalam karya fiksi ilmiahnya pada awal tahun 1980-an. Seiring perkembangan teknologi internet, konsep *cyberspace* tidak lagi hanya menjadi istilah dalam dunia fiksi, tetapi berkembang menjadi ruang sosial baru yang memfasilitasi berbagai aktivitas manusia secara digital.

Menurut Piliang (2012), *cyberspace* dapat dipahami sebagai ruang imajiner yang memungkinkan manusia melakukan berbagai aktivitas sosial yang sebelumnya hanya terjadi dalam dunia nyata. Dalam ruang ini, interaksi sosial berlangsung melalui perantara teknologi informasi sehingga menciptakan realitas baru yang bersifat virtual.

Dalam konteks hukum di Indonesia, konsep *cyberspace* berkaitan erat dengan istilah informasi elektronik dan transaksi elektronik sebagaimana diatur dalam Undang-Undang Informasi dan Transaksi Elektronik. Informasi elektronik didefinisikan sebagai sekumpulan data elektronik yang memiliki arti dan dapat dipahami oleh pihak yang berkepentingan, sedangkan transaksi elektronik merupakan perbuatan hukum yang dilakukan melalui sistem elektronik atau jaringan komputer.

Dengan demikian, *cyberspace* dapat dipahami sebagai ruang digital yang memungkinkan berlangsungnya berbagai aktivitas manusia, termasuk aktivitas ekonomi, komunikasi, maupun interaksi sosial, yang semuanya dilakukan melalui sistem elektronik berbasis jaringan komputer.

Konsep dan Jenis Kejahatan Siber (*Cybercrime*)

Seiring dengan berkembangnya *cyberspace*, muncul pula berbagai bentuk kejahatan baru yang dikenal sebagai kejahatan siber atau *cybercrime*. *Cybercrime* merupakan bentuk kejahatan yang memanfaatkan teknologi informasi, komputer, dan jaringan internet sebagai sarana maupun sasaran kejahatan.

Departemen Kehakiman Amerika Serikat mendefinisikan kejahatan komputer sebagai setiap tindakan ilegal yang memerlukan pengetahuan tentang teknologi komputer untuk melakukan, menyelidiki, atau menuntut suatu kejahatan. Sementara itu, Organisation for Economic Cooperation and Development (OECD) menggunakan istilah *computer related*

crime untuk menggambarkan segala bentuk perilaku ilegal atau tidak sah yang melibatkan pemrosesan data secara otomatis atau transmisi data digital.

Maskun (2013) menjelaskan bahwa cybercrime merupakan kejahatan yang berkaitan dengan pemanfaatan teknologi informasi tanpa batas geografis. Kejahatan ini memiliki karakteristik yang sangat bergantung pada keamanan sistem informasi dan kredibilitas data digital yang digunakan oleh pengguna internet.

Dalam praktiknya, cybercrime dapat terjadi dalam berbagai bentuk, antara lain akses ilegal terhadap sistem komputer (unauthorized access), penyebaran konten ilegal (illegal contents), penyebaran virus komputer, pemalsuan data digital (data forgery), kegiatan spionase siber (cyber espionage), hingga pencurian data pribadi dan penipuan kartu kredit (carding). Selain itu, terdapat pula kejahatan seperti cyberstalking, yaitu tindakan mengganggu atau melecehkan seseorang melalui media digital secara berulang.

Berbagai bentuk cybercrime tersebut menunjukkan bahwa perkembangan teknologi digital tidak hanya memberikan manfaat bagi masyarakat, tetapi juga membuka peluang baru bagi terjadinya kejahatan yang semakin kompleks.

Definisi dan Karakteristik Kejahatan Siber

Perkembangan teknologi informasi telah mendorong transformasi kejahatan konvensional menjadi bentuk kejahatan digital yang dikenal sebagai kejahatan siber. Interpol mendefinisikan cybercrime sebagai tindak kriminal yang dilakukan melalui jaringan komputer, perangkat digital, atau sistem informasi dengan tujuan mencuri, merusak, atau memanipulasi data digital.

Dalam perspektif hukum internasional, Konvensi Budapest tentang Kejahatan Siber mengelompokkan cybercrime ke dalam beberapa kategori utama, yaitu kejahatan terhadap kerahasiaan dan integritas data komputer, kejahatan yang berkaitan dengan konten ilegal, serta kejahatan yang berkaitan dengan penipuan dan pelanggaran hak kekayaan intelektual.

Kejahatan siber memiliki karakteristik yang berbeda dengan kejahatan konvensional. Menurut Wall (2007), cybercrime memiliki beberapa karakteristik utama, yaitu bersifat non-fisik, lintas batas negara (borderless crime), sulit dideteksi, serta memerlukan keahlian teknis khusus dalam proses investigasi.

Selain itu, bukti dalam kejahatan siber umumnya berbentuk bukti digital yang mudah dimodifikasi atau dihapus. Oleh karena itu, proses pembuktian dalam kasus cybercrime memerlukan teknik forensik digital yang memadai agar bukti tersebut dapat digunakan secara sah dalam proses peradilan (Casey, 2011).

Media Sosial sebagai Ekosistem Siber

Media sosial merupakan salah satu platform utama dalam ekosistem cyberspace yang memungkinkan pengguna untuk berinteraksi, berbagi informasi, serta membangun jaringan sosial secara virtual. Media sosial berkembang pesat seiring dengan kemajuan teknologi internet dan munculnya konsep Web 2.0 yang memungkinkan pengguna tidak hanya menjadi konsumen informasi tetapi juga produsen konten.

Menurut Nasrullah (2017), media sosial merupakan medium di internet yang memungkinkan penggunanya untuk mempresentasikan dirinya, berinteraksi, bekerja sama, berbagi informasi, serta membangun hubungan sosial secara virtual. Media sosial juga

memungkinkan terciptanya konten yang dihasilkan oleh pengguna (user generated content) yang menjadi ciri utama dari platform digital modern.

Van Dijk (2013) menyatakan bahwa media sosial merupakan platform komunikasi yang berfokus pada keberadaan pengguna dan memungkinkan mereka untuk melakukan berbagai aktivitas sosial secara online. Media sosial tidak hanya menjadi sarana komunikasi, tetapi juga menjadi ruang sosial baru yang membentuk komunitas digital.

Karakteristik utama media sosial antara lain jaringan antar pengguna (network), pertukaran informasi (information), penyimpanan data digital (archive), interaksi sosial (interactivity), simulasi sosial (simulation of society), serta produksi konten oleh pengguna (user generated content). Karakteristik tersebut menjadikan media sosial sebagai salah satu ruang interaksi digital yang paling dinamis dalam masyarakat modern.

Teori Kriminologi dalam Analisis kejahatan Siber

Untuk memahami fenomena cybercrime secara lebih komprehensif, berbagai teori kriminologi dapat digunakan sebagai kerangka analisis. Salah satu teori yang relevan adalah teori anomie yang menjelaskan bahwa kejahatan dapat muncul ketika norma sosial mengalami disintegrasi atau ketika struktur sosial tidak mampu menyediakan sarana yang sah bagi individu untuk mencapai tujuan sosial tertentu.

Teori lain yang relevan adalah teori asosiasi diferensial yang menyatakan bahwa perilaku kriminal dipelajari melalui interaksi sosial dengan kelompok yang mendukung perilaku tersebut. Dalam konteks cybercrime, individu dapat mempelajari teknik peretasan atau penipuan digital melalui komunitas online yang memiliki pengetahuan teknis mengenai sistem komputer.

Selain itu, teori kontrol sosial menjelaskan bahwa lemahnya ikatan sosial dan kontrol dari institusi sosial dapat meningkatkan kemungkinan seseorang melakukan tindakan kriminal. Dalam dunia digital, anonimitas internet sering kali melemahkan kontrol sosial sehingga membuka peluang terjadinya kejahatan siber.

Salah satu teori yang paling sering digunakan dalam analisis cybercrime adalah Routine Activity Theory yang dikemukakan oleh Cohen dan Felson. Teori ini menjelaskan bahwa kejahatan terjadi ketika tiga unsur utama bertemu dalam suatu situasi tertentu, yaitu adanya pelaku yang termotivasi, adanya target yang rentan, dan tidak adanya pengawasan yang memadai. Dalam konteks dunia digital, ketiga unsur tersebut dapat terjadi secara bersamaan karena luasnya ruang siber dan terbatasnya mekanisme pengawasan.

Dengan demikian, pendekatan kriminologi memberikan perspektif penting dalam memahami penyebab dan dinamika kejahatan siber, sehingga dapat membantu merumuskan strategi pencegahan dan penanggulangan yang lebih efektif.

METODE PENELITIAN

Penelitian ini menggunakan metode penelitian hukum 31ormative yang berfokus pada kajian terhadap norma-norma hukum yang mengatur kejahatan siber di Indonesia. Pendekatan yang digunakan dalam penelitian ini adalah pendekatan perundang-undangan (statute approach) dan pendekatan konseptual (conceptual approach).

Bahan hukum yang digunakan dalam penelitian ini terdiri atas bahan hukum primer berupa peraturan perundang-undangan yang berkaitan dengan kejahatan siber, termasuk Undang-Undang Nomor 1 Tahun 2024 tentang perubahan Undang-Undang Informasi dan Transaksi Elektronik. Selain itu digunakan pula bahan hukum sekunder berupa buku, jurnal ilmiah, serta literatur hukum yang relevan dengan topik penelitian.

Pengumpulan data dilakukan melalui studi kepustakaan (library research). Selanjutnya data yang diperoleh dianalisis secara kualitatif dengan metode deskriptif-analitis untuk mengkaji hubungan antara penggunaan media sosial dan peningkatan kejahatan siber serta efektivitas regulasi hukum dalam menanggulangi kejahatan tersebut.

HASIL PENELITIAN DAN PEMBAHASAN

Strategi Pencegahan Kejahatan Siber melalui Penguatan Literasi Digital dan Etika Siber

Perkembangan teknologi informasi dan komunikasi telah membawa perubahan signifikan dalam berbagai aspek kehidupan masyarakat, termasuk dalam cara manusia berinteraksi, memperoleh informasi, serta melakukan aktivitas ekonomi dan sosial. Digitalisasi memberikan berbagai manfaat berupa efisiensi, kemudahan akses informasi, serta inovasi dalam berbagai sektor. Namun di sisi lain, perkembangan ini juga membuka peluang munculnya berbagai bentuk kejahatan siber (cybercrime) yang semakin kompleks dan sulit dideteksi.

Kejahatan siber dapat dilakukan oleh berbagai kelompok usia, mulai dari anak-anak hingga orang dewasa. Rendahnya hambatan teknis serta kemudahan akses internet memungkinkan berbagai tindakan ilegal dilakukan dengan relatif mudah, seperti phishing, hacking, penyebaran malware, hingga penyebaran informasi palsu (fake news). Kondisi tersebut menunjukkan bahwa pencegahan kejahatan siber tidak hanya dapat dilakukan melalui pendekatan hukum dan penegakan hukum semata, tetapi juga memerlukan pendekatan edukatif melalui penguatan literasi digital masyarakat.

Literasi digital merupakan kemampuan individu untuk memahami, menggunakan, mengevaluasi, dan menciptakan informasi melalui teknologi digital secara kritis dan bertanggung jawab. Gilster mendefinisikan literasi digital sebagai kemampuan untuk memahami dan menggunakan informasi dalam berbagai bentuk yang tersedia melalui media elektronik. Dalam konteks ini, literasi digital tidak hanya mencakup kemampuan teknis menggunakan perangkat teknologi, tetapi juga mencakup kemampuan berpikir kritis, kesadaran etika digital, serta kemampuan menjaga keamanan data pribadi.

Literasi digital memiliki beberapa dimensi penting. Pertama, literasi informasi yang berkaitan dengan kemampuan mengidentifikasi, menemukan, serta mengevaluasi informasi secara kritis. Kemampuan ini sangat penting untuk mencegah penyebaran misinformasi dan hoaks yang banyak beredar di internet. Kedua, literasi media yang memungkinkan individu memahami pesan media secara kritis serta menyadari potensi bias dalam konten digital. Ketiga, literasi teknologi yang berkaitan dengan kemampuan menggunakan perangkat digital secara efektif dan aman.

Selain itu, literasi komunikasi digital juga menjadi aspek penting dalam membangun interaksi yang sehat di ruang digital. Pengguna media sosial perlu memahami etika komunikasi daring, menghindari ujaran kebencian (hate speech), serta tidak melakukan tindakan yang dapat

merugikan orang lain seperti cyberbullying. Dalam konteks keamanan digital, literasi digital juga mencakup kesadaran mengenai pentingnya perlindungan data pribadi, penggunaan kata sandi yang kuat, serta kewaspadaan terhadap upaya penipuan daring.

Generasi muda merupakan kelompok yang paling rentan terhadap berbagai risiko di ruang digital karena mereka merupakan pengguna internet yang paling aktif. Tanpa kemampuan literasi digital yang memadai, generasi muda berpotensi terlibat dalam kejahatan siber baik sebagai korban maupun sebagai pelaku. Oleh karena itu, penguatan literasi digital menjadi langkah strategis untuk meningkatkan kesadaran hukum dan etika dalam penggunaan teknologi informasi.

Upaya peningkatan literasi digital tidak dapat dilakukan secara individual, tetapi memerlukan keterlibatan berbagai pihak, termasuk keluarga, lembaga pendidikan, serta pemerintah. Integrasi pendidikan literasi digital dalam kurikulum pendidikan formal, penyelenggaraan pelatihan digital, serta kampanye kesadaran keamanan siber merupakan langkah-langkah yang dapat dilakukan untuk membangun masyarakat digital yang lebih aman dan bertanggung jawab.

Peran Penyelenggara Sistem Elektronik dalam Mitigasi Risiko Siber

Selain literasi digital masyarakat, upaya pencegahan kejahatan siber juga memerlukan peran aktif dari penyelenggara sistem elektronik (PSE). Dalam ekosistem digital modern, PSE memiliki tanggung jawab penting dalam memastikan keamanan, keandalan, serta integritas sistem elektronik yang mereka kelola.

Penyelenggara sistem elektronik merupakan pihak yang menyediakan, mengelola, dan mengoperasikan sistem elektronik untuk kepentingan publik maupun privat. Dalam menjalankan perannya, PSE memiliki kewajiban untuk memastikan bahwa sistem elektronik yang mereka operasikan terlindungi dari berbagai ancaman siber, termasuk peretasan, pencurian data, maupun serangan malware.

Upaya mitigasi risiko siber oleh PSE dapat dilakukan melalui berbagai strategi. Salah satu strategi utama adalah implementasi sistem keamanan siber yang kuat, seperti penggunaan firewall, enkripsi data, serta sistem deteksi intrusi (intrusion detection system). Teknologi keamanan ini berfungsi untuk melindungi sistem elektronik dari akses tidak sah serta menjaga kerahasiaan data pengguna.

Selain itu, PSE juga perlu melakukan pemantauan sistem secara berkelanjutan guna mendeteksi potensi ancaman siber secara dini. Pemantauan sistem memungkinkan organisasi untuk segera merespons insiden keamanan sebelum menimbulkan dampak yang lebih luas. Pengembangan dan pemeliharaan sistem secara berkala juga menjadi langkah penting untuk memastikan bahwa sistem tetap aman dari kerentanan teknologi.

Kepatuhan terhadap regulasi keamanan siber juga menjadi bagian penting dari tanggung jawab PSE. Di Indonesia, berbagai regulasi telah mengatur kewajiban keamanan sistem elektronik, termasuk dalam Undang-Undang Informasi dan Transaksi Elektronik serta berbagai regulasi teknis terkait keamanan sistem elektronik. Kepatuhan terhadap regulasi tersebut menjadi dasar bagi terciptanya ekosistem digital yang aman serta dapat dipercaya oleh masyarakat.

Sinergi Penegakan Hukum dan Pendekatan Keadilan Restoratif

Penanggulangan kejahatan siber tidak hanya bergantung pada upaya pencegahan, tetapi juga memerlukan mekanisme penegakan hukum yang efektif. Dalam sistem hukum pidana modern, penegakan hukum tidak lagi hanya berorientasi pada pemberian sanksi kepada pelaku kejahatan, tetapi juga mempertimbangkan aspek pemulihan bagi korban serta masyarakat.

Pendekatan keadilan restoratif (restorative justice) menjadi salah satu alternatif dalam penanganan kasus kejahatan tertentu, termasuk dalam beberapa kasus kejahatan siber yang tidak menimbulkan dampak besar. Keadilan restoratif menekankan pada upaya pemulihan hubungan antara pelaku, korban, serta masyarakat yang terdampak oleh suatu tindak pidana.

Dalam pendekatan ini, penyelesaian perkara dapat dilakukan melalui mekanisme dialog atau mediasi antara pelaku dan korban dengan tujuan mencapai kesepakatan mengenai bentuk pemulihan yang adil. Pendekatan ini tidak hanya berfokus pada penghukuman pelaku, tetapi juga memberikan kesempatan bagi pelaku untuk bertanggung jawab atas perbuatannya serta memperbaiki kerugian yang ditimbulkan.

Sinergi antara penegakan hukum formal dan pendekatan keadilan restoratif dapat memberikan solusi yang lebih komprehensif dalam menangani kejahatan siber. Pendekatan ini memungkinkan tercapainya keseimbangan antara aspek keadilan, pemulihan korban, serta pencegahan kejahatan di masa depan.

Dampak Eskalasi Media Sosial terhadap Peningkatan Kejahatan Siber

Perkembangan media sosial dalam beberapa tahun terakhir telah mengubah pola interaksi sosial masyarakat secara signifikan. Media sosial memungkinkan komunikasi berlangsung secara cepat dan luas tanpa batas geografis. Namun demikian, eskalasi penggunaan media sosial juga membawa konsekuensi berupa meningkatnya berbagai bentuk kejahatan siber.

Media sosial sering kali dimanfaatkan oleh pelaku kejahatan sebagai sarana untuk melakukan berbagai tindakan kriminal. Salah satu bentuk kejahatan yang sering terjadi adalah phishing, yaitu penipuan yang dilakukan dengan cara memperoleh informasi pribadi korban melalui manipulasi psikologis. Selain itu, media sosial juga sering digunakan untuk melakukan cyberbullying yang dapat menimbulkan dampak psikologis serius bagi korban.

Selain peningkatan kuantitas kejahatan siber, perkembangan teknologi juga menyebabkan peningkatan kualitas metode kejahatan siber. Pelaku kejahatan kini menggunakan teknik yang semakin canggih, seperti social engineering, yaitu manipulasi psikologis untuk memperoleh informasi rahasia dari korban. Serangan yang bersifat terarah (targeted attack) juga semakin sering terjadi, di mana pelaku terlebih dahulu mengumpulkan informasi mengenai target sebelum melakukan serangan.

Selain itu, terdapat pula bentuk serangan siber yang lebih kompleks seperti Advanced Persistent Threat (APT), yaitu serangan siber yang dilakukan secara terorganisir dan berkelanjutan dengan tujuan memperoleh akses jangka panjang terhadap sistem tertentu. Serangan semacam ini sering kali menargetkan organisasi besar, lembaga pemerintah, maupun infrastruktur kritis.

Beberapa faktor utama yang mendorong peningkatan kejahatan siber antara lain keterbukaan media sosial yang memungkinkan pelaku memperoleh informasi secara mudah, rendahnya kesadaran keamanan digital di kalangan pengguna, serta perkembangan teknologi

yang semakin canggih. Kombinasi faktor-faktor tersebut menciptakan lingkungan digital yang rentan terhadap berbagai bentuk kejahatan siber.

Oleh karena itu, upaya penanggulangan kejahatan siber perlu dilakukan secara komprehensif melalui peningkatan literasi digital masyarakat, penguatan sistem keamanan teknologi, serta penegakan hukum yang efektif. Pendekatan yang terintegrasi ini diharapkan dapat menciptakan ekosistem digital yang lebih aman dan berkelanjutan bagi masyarakat.

KESIMPULAN

Berdasarkan hasil penelitian dan pembahasan mengenai eskalasi penggunaan media sosial dan kaitannya dengan peningkatan kejahatan siber di Indonesia, dapat ditarik beberapa kesimpulan sebagai berikut.

Pertama, strategi pencegahan kejahatan siber pada era digital yang ditandai dengan eskalasi penggunaan media sosial memerlukan pendekatan yang bersifat komprehensif dan multisektoral. Upaya preventif tidak hanya bergantung pada penegakan hukum, tetapi juga harus didukung oleh penguatan literasi digital masyarakat. Literasi digital berperan penting dalam meningkatkan kesadaran pengguna terhadap risiko siber, seperti phishing, cyberbullying, serta penyalahgunaan data pribadi. Melalui literasi digital, masyarakat diharapkan mampu menggunakan media sosial secara bijak, menjaga keamanan data pribadi, serta mematuhi norma dan etika komunikasi di ruang digital. Selain itu, strategi pencegahan juga diperkuat melalui kewajiban bagi Penyelenggara Sistem Elektronik (PSE) untuk memastikan keamanan dan keandalan sistem elektronik yang mereka kelola. Ketentuan dalam Undang-Undang Nomor 1 Tahun 2024 menegaskan tanggung jawab tersebut, termasuk kewajiban perlindungan terhadap kelompok rentan, khususnya anak di ruang siber. Dalam konteks penegakan hukum, penerapan pendekatan restorative justice juga memberikan alternatif penyelesaian perkara yang lebih edukatif dan berorientasi pada pemulihan.

Kedua, eskalasi penggunaan media sosial memberikan dampak signifikan terhadap peningkatan kuantitas dan kompleksitas kejahatan siber di Indonesia. Media sosial telah menjadi sarana yang efektif bagi pelaku kejahatan untuk melakukan berbagai bentuk tindakan kriminal berbasis digital, seperti penyebaran konten ilegal, penipuan daring, pencurian data pribadi, serta manipulasi informasi melalui teknik social engineering. Karakteristik media sosial yang terbuka, anonim, dan lintas batas negara menyebabkan kejahatan siber semakin sulit dideteksi serta memperumit proses penegakan hukum. Selain itu, keberadaan jejak digital yang bersifat permanen sering kali memperbesar dampak kerugian bagi korban. Dalam konteks ini, Undang-Undang Nomor 1 Tahun 2024 berperan sebagai instrumen hukum yang memberikan kerangka pengaturan yang lebih jelas terhadap berbagai bentuk pelanggaran di ruang digital, termasuk melalui pengaturan delik terkait penyalahgunaan media elektronik serta perlindungan terhadap kelompok rentan. Dengan demikian, penanganan dampak negatif dari eskalasi media sosial tidak dapat hanya mengandalkan pendekatan represif melalui sanksi pidana, tetapi juga harus diimbangi dengan penguatan literasi digital, peningkatan keamanan sistem elektronik, serta tanggung jawab penyelenggara sistem elektronik dalam menjaga keamanan ruang siber.

Saran

Berdasarkan kesimpulan penelitian, beberapa rekomendasi yang dapat diajukan adalah sebagai berikut.

Pertama, pemerintah perlu memperkuat program literasi digital secara berkelanjutan melalui integrasi dalam sistem pendidikan formal maupun program edukasi masyarakat. Upaya ini penting untuk meningkatkan kesadaran masyarakat terhadap risiko kejahatan siber serta membangun budaya penggunaan teknologi yang aman, kritis, dan bertanggung jawab.

Kedua, Penyelenggara Sistem Elektronik (PSE) perlu meningkatkan standar keamanan sistem elektronik melalui penerapan teknologi keamanan siber yang lebih komprehensif, termasuk perlindungan data pengguna dan mekanisme deteksi dini terhadap potensi serangan siber. Hal ini penting untuk meminimalkan risiko kebocoran data dan penyalahgunaan informasi digital.

Ketiga, aparat penegak hukum perlu memperkuat kapasitas penegakan hukum di bidang kejahatan siber melalui peningkatan kemampuan investigasi digital serta kerja sama lintas lembaga dan lintas negara. Dengan demikian, penanganan kejahatan siber dapat dilakukan secara lebih efektif dalam menghadapi karakteristik kejahatan yang bersifat lintas batas dan berbasis teknologi.

DAFTAR REFERENSI

- Alexy, R. (2021). *Gustav Radbruch's concept of law: In law's ideal dimension*. Oxford University Press.
- Asshiddiqie, J. (2009). *Teori Hans Kelsen tentang hukum*. Konstitusi Press.
- Cahyani, D. D. (2021). *Interaksi sosial dalam perspektif sosiologi*. Rajawali Pers.
- Casey, E. (2011). *Digital evidence and computer crime* (3rd ed.). Academic Press.
- Cohen, L. E., & Felson, M. (2010). Social change and crime rate trends: A routine activity approach. In E. E. Flynn (Ed.), *Classics in criminology*. Butterworth-Heinemann.
- Diantha, I. M. P. (2017). *Metodologi penelitian hukum normatif dalam justifikasi teori hukum*. Kencana.
- Djumhana, M. (1993). *Hukum perbankan di Indonesia*. Citra Aditya Bakti.
- Efendi, J., & Ibrahim, J. (2018). *Metode penelitian hukum normatif dan empiris*. Prenadamedia Group.
- Fuller, L. (1964). *The morality of law*. Yale University Press.
- Fuady, M. (2014). *Hukum perbankan modern*. Citra Aditya Bakti.
- Garner, B. A. (2004). *Black's law dictionary* (8th ed.). West Publishing.
- Gilster, P. (1997). *Digital literacy*. Wiley.
- Hadjon, P. M. (1987). *Perlindungan hukum bagi rakyat di Indonesia*. Bina Ilmu.
- Hermansyah. (2013). *Hukum perbankan nasional Indonesia*. Kencana.
- Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2015). *Cybercrime and digital forensics: An introduction*. Routledge.
- Howard, P. N., & Parks, M. R. (2012). Social media and political change. *Journal of Communication*, 62(2), 359–362.
- Huda, N. (2005). *Negara hukum, demokrasi, dan judicial review*. UII Press.
- Kansil, C. S. T. (2009). *Kamus istilah hukum*. Gramedia Pustaka Utama.

- Kaplan, A. M., & Haenlein, M. (2010). Users of the world, unite! The challenges and opportunities of social media. *Business Horizons*, 53(1), 59–68.
- Kasmir. (2014). *Manajemen perbankan*. RajaGrafindo Persada.
- Ketaren, E. (2016). Cybercrime, cyber space, dan cyber law. *Jurnal Komunikasi dan Bisnis*, 4(1), 1–10.
- Kelsen, H. (2010). *Teori umum tentang hukum dan negara* (R. Muttakin, Trans.). Nusa Media.
- Leawoods, H. (2000). Gustav Radbruch: An extraordinary legal philosopher. *Washington University Journal of Law & Policy*, 2.
- Mandiberg, M. (2012). *The social media reader*. New York University Press.
- Makarim, E. (2020). Tanggung jawab hukum pengendali data dalam sistem elektronik. *Jurnal Hukum IUS QUIA IUSTUM*, 27(2).
- Marzuki, P. M. (2015). *Penelitian hukum*. Prenadamedia Group.
- Mertokusumo, S. (2009). *Penemuan hukum: Sebuah pengantar*. Liberty.
- Nasrullah, R. (2017). *Media sosial: Perspektif komunikasi, budaya, dan sosioteknologi*. Simbiosis Rekatama Media.
- Nazir, M. (2009). *Metode penelitian*. Ghalia Indonesia.
- Pramono, N. (2006). *Bunga rampai hukum bisnis aktual*. Citra Aditya Bakti.
- Radbruch, G. (1950). *Legal philosophy* (K. Wilk, Trans.). Harvard University Press.
- Rahardjo, S. (2009). *Ilmu hukum progresif*. Kompas.
- Rismana. (2016). Intensitas penggunaan media sosial dan perilaku menyimpang. *Kencana*.
- Sinaga, G. G., et al. (2023). Analisis peran OJK terhadap perlindungan data nasabah bank. *Jurnal Pendidikan Tambusai*, 7(3), 28374–28383.
- Siregar, A. N., & Putra, M. A. P. (2025). Penegakan perlindungan data pribadi nasabah bank. *Jurnal Media Akademik*, 3(7).
- Sugiyono. (2005). *Komunikasi antarpribadi*. UNNES Press.
- Usanti, T. P., & Somad, A. (2017). *Hukum perbankan*. Prenadamedia Group.
- Usman, R. (2003). *Aspek-aspek hukum perbankan di Indonesia*. Gramedia Pustaka Utama.
- Van Dijk, J. (2013). *The culture of connectivity: A critical history of social media*. Oxford University Press.
- Walgito, B. (2003). *Pengantar psikologi umum*. Andi Offset.
- Wahyudi Djafar. (2019). Hukum perlindungan data pribadi di Indonesia. *Jurnal Hukum dan Pembangunan*, 49(2).
- Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan atas Undang-Undang Informasi dan Transaksi Elektronik.
- Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.
- Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan.
- Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen.