PENERAPAN SANKSI PIDANA TERHADAP PELAKU KEJAHATAN PENIPUAN *ONLINE CYBER CRIME* DI ERA DIGITALISASI

Jeremia Londok
Fakultas Hukum, Universitas Sam Ratulangi
Email: londok.jere@gmail.com

Abstrak

Pada era digitalisasi yang semakin berkembang pesat, kemajuan teknologi informasi dan komunikasi telah membawa perubahan besar dalam berbagai aspek kehidupan masyarakat. Namun, di balik kemudahan dan kecepatan akses informasi, muncul pula tantangan baru dalam bentuk kejahatan siber atau *Cyber Crime*. Kejahatan ini semakin kompleks dengan modus yang terus berkembang, sehingga menuntut adanya sistem hukum yang kuat dan penerapan sanksi pidana yang efektif untuk memberikan perlindungan kepada masyarakat. *Cyber Crime* mencakup berbagai bentuk kejahatan yang dilakukan melalui perangkat teknologi, seperti penipuan online, peretasan data pribadi, penyebaran hoaks, dan pencurian identitas. Dalam konteks hukum Indonesia, kejahatan siber diatur dalam beberapa peraturan perundang-undangan, antara lain Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) yang kemudian direvisi dengan Undang-Undang Nomor 19 Tahun 2016. Selain itu, Kitab Undang-Undang Hukum Pidana (KUHP) juga memiliki beberapa pasal yang dapat diterapkan dalam menjerat pelaku kejahatan siber. Meskipun regulasi terkait *Cyber Crime* telah diatur dalam perundang-undangan, realitas di lapangan menunjukkan bahwa penerapan sanksi pidana terhadap pelaku kejahatan siber masih menghadapi berbagai kendala. Beberapa di antaranya adalah kurangnya pemahaman aparat penegak hukum terhadap aspek teknis kejahatan siber, kelemahan dalam penegakan hukum, serta tantangan dalam mengidentifikasi dan menangkap pelaku yang sering kali beroperasi lintas negara. Salah satu tantangan terbesar dalam penegakan hukum terhadap *cyber crime* adalah kesenjangan antara regulasi yang ada dengan implementasi di lapangan. Kasus-kasus mengenai kejahatan siber di Indonesia menunjukkan bahwa sering kali hukum tidak dapat diterapkan secara optimal, baik karena keterbatasan bukti digital maupun karena kurangnya koordinasi antara lembaga penegak hukum dan instansi terkait.

Kata Kunci: Penerapan sanksi pidana terhadap pelaku kejahatan, Penipuan *online cyber crime* di era digitalisasi.

1. Pendahuluan

Tindak pidana atau delik merupakan suatu perbuatan yang dilarang oleh hukum pidana dan diancam dengan sanksi bagi pelakunya. Dalam Kitab Undang-Undang Hukum Pidana (KUHP), konsep tindak pidana tidak didefinisikan secara eksplisit, namun secara umum dapat dipahami sebagai perbuatan yang memenuhi unsur-unsur yang ditetapkan dalam peraturan perundang-undangan pidana. Menurut van Hamel, tindak pidana adalah perbuatan yang oleh peraturan hukum pidana dinyatakan sebagai perbuatan yang dapat dihukum dan bertentangan dengan hukum yang berlaku. Sementara itu, Simons berpendapat

bahwa tindak pidana adalah suatu pelanggaran terhadap norma hukum yang bersifat objektif, yang menimbulkan gangguan terhadap ketertiban umum dan oleh karena itu dikenakan hukuman bagi pelakunya. Didalam sistem hukum pidana Indonesia, tindak pidana terdiri dari dua unsur utama, yaitu unsur subjektif dan unsur objektif. Unsur subjektif berkaitan dengan aspek kesalahan pelaku, termasuk niat (*mens rea*) dan motif, sedangkan unsur objektif mencakup perbuatan yang dilakukan (*actus reus*) serta akibat hukum yang ditimbulkan. Dengan kata lain, suatu perbuatan dapat dikategorikan sebagai tindak pidana apabila memenuhi unsur kesalahan pelaku serta adanya tindakan yang secara nyata melanggar ketentuan hukum pidana. Pemahaman ini penting untuk membedakan tindak pidana dari sekadar perbuatan yang tidak etis atau melanggar norma sosial, tetapi tidak memiliki konsekuensi hukum pidana. Perbedaan mendasar antara tindak pidana dan perbuatan melawan hukum lainnya terletak pada konsekuensi hukum dan sistem pemidanaannya. Perbuatan melawan hukum dalam konteks hukum perdata, misalnya, lebih berorientasi pada kerugian yang dialami oleh individu atau pihak tertentu, yang dapat diselesaikan melalui mekanisme ganti rugi atau perbuatan hukum lainnya. Sebaliknya, tindak pidana berkaitan dengan kepentingan umum, di mana negara bertindak sebagai pihak yang berwenang dalam menegakkan hukum dan menjatuhkan sanksi kepada pelaku. Menurut Sudarto, hukum pidana memiliki sifat represif yang bertujuan untuk menjaga ketertiban dan mencegah pelanggaran lebih lanjut, sementara hukum perdata lebih bersifat restitutif atau pemulihan. Perkembangan teknologi informasi dan komunikasi telah membawa dampak besar dalam berbagai aspek kehidupan, termasuk dalam dunia kejahatan. Salah satu bentuk kejahatan yang muncul akibat kemajuan teknologi adalah *cyber crime* atau kejahatan siber. Secara umum, *cyber crime* dapat didefinisikan sebagai tindak pidana yang dilakukan dengan menggunakan teknologi komputer dan internet sebagai alat utama atau sebagai sasaran. Menurut Bambang Wahyudi, *cyber crime* adalah segala bentuk kejahatan yang dilakukan di dunia maya dengan memanfaatkan jaringan komputer sebagai sarana utama untuk melakukan tindakan yang melanggar hukum. Definisi serupa juga dijelaskan dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), yang menyebutkan bahwa kejahatan siber meliputi akses ilegal, peretasan, pencurian data, penyebaran informasi palsu, serta berbagai bentuk penyalahgunaan teknologi informasi untuk kepentingan tertentu. Didalam menghadapi kejahatan siber yang semakin berkembang, Indonesia telah menerapkan berbagai regulasi untuk mengatur dan menindak pelaku *cyber crime*. Salah satu peraturan utama yang menjadi landasan hukum dalam menangani kejahatan siber adalah Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), yang kemudian direvisi melalui Undang-Undang Nomor 19 Tahun 2016. Selain UU ITE, regulasi lainnya seperti Kitab Undang-Undang Hukum Pidana (KUHP**)** serta peraturan terkait lainnya juga memiliki peran dalam mengatur aspek hukum *cyber crime* di Indonesia. UU ITE merupakan peraturan pertama di Indonesia yang secara khusus mengatur mengenai kejahatan siber. Undang-undang ini mencakup berbagai aspek terkait aktivitas digital, termasuk transaksi elektronik, informasi dan dokumen elektronik, serta berbagai bentuk pelanggaran yang dilakukan di dunia maya. Beberapa pasal dalam UU ITE mengatur tindak pidana seperti akses ilegal ke sistem elektronik, manipulasi data, pencurian informasi digital, pencemaran nama

baik melalui media elektronik, serta penyebaran berita bohong yang merugikan masyarakat. Seiring dengan perkembangan teknologi dan maraknya penyalahgunaan internet, UU ITE mengalami revisi melalui Undang-undang Nomor 19 Tahun 2016, yang bertujuan untuk memperjelas beberapa ketentuan dan mengurangi potensi penyalahgunaan hukum dalam penerapannya. Selain UU ITE, KUHP juga memiliki peran dalam mengatur tindak pidana siber, meskipun tidak secara spesifik menyebutkan istilah *cyber crime*. Beberapa pasal dalam KUHP yang dapat diterapkan dalam kasus kejahatan siber antara lain pasal-pasal mengenai penipuan (Pasal 378 KUHP), pemalsuan dokumen (Pasal 263 KUHP), serta penghinaan dan pencemaran nama baik (Pasal 310 dan 311 KUHP). Dalam banyak kasus, KUHP sering digunakan secara bersamaan dengan UU ITE untuk menjerat pelaku kejahatan siber, terutama dalam kasus yang berkaitan dengan manipulasi data dan penipuan daring.

Rumusan Masalah:

1. Bagaimanakah bentuk penerapan sanksi pidana terhadap pelaku kejahatan *Cyber Crime* di era digitalisasi?
2. Bagaimanakah bentuk perlindungan hukum bagi korban tindak pidana kejahatan *Cyber Crime* di era digitalisasi?

2. Metode Penelitian

Penelitian hukum normatif merupakan penelitian yang menitikberatkan kajian pada hukum sebagai kumpulan peraturan yang berlaku dan berperan sebagai pedoman bagi perilaku individu dalam masyarakat. Sementara itu, penelitian hukum normatif-empiris, yang juga dikenal sebagai penelitian hukum normatif-terapan *(applied law research)*, bertujuan untuk menganalisis penerapan norma hukum positif, seperti Peraturan Perundang-Undangan dan kontrak, dalam berbagai peristiwa hukum di masyarakat guna memperoleh hasil yang telah ditentukan. Penelitian hukum empiris (*empirical law research*), yang dikenal juga sebagai penelitian hukum sosiologis, merupakan metode penelitian yang menelaah hukum sebagai perilaku nyata (*actual behavior*), yakni sebagai fenomena sosial yang tidak tertulis dan dialami langsung oleh individu dalam kehidupan bermasyarakat. Penelitian ini berfokus pada bagaimana hukum diterapkan dalam kehidupan sehari-hari, serta bagaimana masyarakat memahami dan merespons keberlakuan hukum tersebut dalam praktiknya.

3. Hasil dan Pembahasan

3.1 Penerapan Sanksi Pidana Terhadap Pelaku Kejahatan *Cyber Crime* di Era Digitalisasi

Didalam era digitalisasi yang terus berkembang, kejahatan siber atau *cyber-crime* telah menjadi salah satu tantangan utama dalam sistem hukum pidana modern. Kemajuan teknologi informasi yang semestinya membawa kemudahan dan efisiensi justru dimanfaatkan oleh sebagian oknum untuk melakukan tindak kejahatan melalui dunia maya. Berbeda dengan kejahatan konvensional, kejahatan siber memiliki sifat unik yang menuntut pendekatan hukum yang berbeda, baik dari segi pembuktian, penelusuran pelaku, hingga penerapan sanksi pidana. Oleh karena itu, dalam rangka memahami bagaimana sanksi pidana dapat diterapkan secara efektif terhadap pelaku kejahatan siber, perlu terlebih dahulu

diuraikan karakteristik dasar dari kejahatan *cyber-crime* di era digital ini. Perkembangan teknologi informasi telah mendorong transformasi signifikan dalam berbagai aspek kehidupan manusia, termasuk dalam bidang kriminalitas. Kejahatan tidak lagi terbatas pada ruang fisik, melainkan telah beralih ke dunia maya yang tidak mengenal batas wilayah geografis. Kejahatan yang dilakukan dengan menggunakan atau menyasar sistem komputer dan jaringan internet ini dikenal sebagai *cyber-crime*. Karakter utama dari *cyber-crime* adalah kemampuannya menembus yurisdiksi negara karena dilakukan secara daring (*online*), sehingga pelaku dapat berada di negara yang berbeda dengan korban atau sistem yang diserangnya. Kejahatan ini memanfaatkan ruang digital sebagai alat, objek, maupun lokasi terjadinya tindak pidana. Sifat lintas batas negara (Transnasional) dari *cyber-crime* membuatnya sulit ditangani oleh hukum pidana konvensional yang pada umumnya masih berorientasi pada asas teritorial. Dalam banyak kasus, pelaku kejahatan siber beroperasi dari luar negeri menggunakan jaringan komputer pribadi atau publik, sehingga memperumit pelacakan identitas dan lokasi mereka. Hal ini menimbulkan kebutuhan mendesak akan kerja sama internasional dalam upaya penegakan hukum atas kejahatan siber, termasuk melalui mekanisme *mutual legal assistance* atau ekstradisi antarnegara. Selain itu, pendekatan hukum nasional pun dituntut untuk beradaptasi terhadap tantangan globalisasi kejahatan digital tersebut. Karakteristik lain dari *cyber-crime* adalah tingkat anonimitas pelaku yang sangat tinggi. Teknologi memungkinkan seseorang menyembunyikan identitas aslinya melalui *proxy*, *Virtual Private Network* (VPN), atau akun palsu di media sosial. Bahkan, pelaku dapat menyusup ke sistem orang lain dan menggunakannya sebagai alat untuk melakukan kejahatan, sehingga sulit bagi penyidik untuk menentukan siapa pelaku sesungguhnya. Anonimitas ini menjadikan pelaku *cyber-crime* lebih berani dan agresif karena merasa terlindungi oleh kerahasiaan identitas digital mereka. Pada sisi lain, pembuktian dalam perkara *cyber-crime* juga mengalami tantangan tersendiri. Bukti-bukti digital seperti log aktivitas, data transaksi elektronik, dan komunikasi daring bersifat tidak kasat mata dan mudah dihapus atau dimodifikasi. Hal ini menuntut aparat penegak hukum untuk menguasai teknik digital forensik agar mampu mengidentifikasi, mengumpulkan, dan menjaga integritas barang bukti elektronik yang sah menurut hukum acara pidana. Kurangnya pemahaman teknis aparat sering kali menyebabkan bukti tidak dapat digunakan di pengadilan atau bahkan kasus dihentikan sebelum diproses lebih lanjut. Bentuk-bentuk *cyber-crime* di Indonesia yang umum terjadi antara lain adalah *phishing*, yaitu praktik menipu korban agar memberikan data pribadi seperti username, password, atau nomor kartu kredit dengan menyamar sebagai lembaga resmi. Selain itu, terdapat pula *online fraud* atau penipuan daring melalui toko palsu di e-commerce, *hacking* terhadap situs pemerintah atau lembaga keuangan, penyebaran hoaks dan ujaran kebencian di media sosial, serta pencurian data pribadi (*data breach*) yang kian marak. Kejahatan-kejahatan tersebut tidak hanya merugikan secara ekonomi, tetapi juga berpotensi mengganggu stabilitas sosial dan politik. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), yang telah diubah melalui Undang-Undang Nomor 19 Tahun 2016, menjadi instrumen hukum utama dalam menangani tindak pidana siber di Indonesia. UU ini memuat ketentuan pidana terhadap berbagai pelanggaran yang dilakukan melalui sistem elektronik, seperti akses ilegal, penyadapan, manipulasi data, penipuan daring, hingga

penyebaran informasi bohong atau ujaran kebencian. Sanksi pidana dalam UU ITE terdiri dari pidana penjara dan/atau denda yang besarannya bervariasi tergantung jenis pelanggarannya. Pasal 30 ayat (1) UU ITE menyebutkan bahwa setiap orang yang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer atau sistem elektronik milik orang lain dapat dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp600.000.000,00. Selain itu, Pasal 27 ayat (3) mengatur mengenai pencemaran nama baik melalui media elektronik yang dapat dikenakan sanksi pidana penjara paling lama 4 (empat) tahun dan/atau denda paling banyak Rp750.000.000,00. Ketentuan ini memperlihatkan bahwa UU ITE tidak hanya menindak kejahatan teknologi tinggi, tetapi juga kejahatan yang bersifat sosial dalam dunia maya seperti penghinaan dan fitnah secara daring. Sanksi pidana dalam UU ITE juga memiliki karakteristik khusus, seperti keberadaan pidana tambahan berupa pemblokiran konten atau sistem, serta pemberlakuan pidana kumulatif antara pidana penjara dan denda. Hal ini menunjukkan pendekatan yang lebih tegas dan modern dalam menghadapi kejahatan digital, di mana konsekuensi hukum tidak hanya bertujuan untuk menghukum pelaku, tetapi juga melindungi ruang digital dari konten atau aktivitas yang merugikan publik. KUHP tidak secara eksplisit menyebut istilah *cyber-crime*, beberapa pasal di dalamnya tetap dapat digunakan untuk menjerat pelaku kejahatan siber, terutama jika tindakan mereka memenuhi unsur tindak pidana umum. Pasal-pasal dalam KUHP yang sering digunakan antara lain Pasal 378 tentang penipuan, Pasal 362 tentang pencurian, Pasal 263 tentang pemalsuan surat, serta Pasal 310 dan 311 tentang penghinaan atau pencemaran nama baik. Penggunaan pasal-pasal ini menjadi pelengkap bagi ketentuan dalam UU ITE, khususnya dalam konteks penuntutan dan penjatuhan pidana di pengadilan.

3.2 Perlindungan Hukum Bagi Korban Tindak Pidana Kejahatan *Cyber Crime* di Era Digitalisasi

Pada era digitalisasi yang semakin maju, kejahatan siber tidak hanya berdampak pada tatanan hukum dan keamanan negara, tetapi juga memberikan kerugian nyata bagi individu, kelompok, maupun institusi sebagai korban. Tidak seperti kejahatan konvensional yang sering kali terlihat dan langsung disadari, korban *Cyber Crime* kerap tidak menyadari bahwa dirinya telah dirugikan, bahkan setelah kerugian terjadi. Kejahatan ini bisa merampas data pribadi, mencuri dana, hingga merusak reputasi korban melalui penyebaran informasi palsu. Oleh karena itu, penting untuk memahami siapa saja yang berpotensi menjadi korban serta bagaimana bentuk kerentanan yang mereka alami, sebagai langkah awal dalam membangun sistem perlindungan hukum yang lebih efektif dan responsif terhadap kebutuhan korban di era digital. Perkembangan teknologi informasi dan komunikasi telah membawa dampak besar terhadap siapa saja yang dapat menjadi korban kejahatan siber. Di Indonesia, korban tidak hanya berasal dari kalangan masyarakat umum yang kurang memahami teknologi, tetapi juga dari kalangan profesional, pelaku usaha mikro, kecil, dan menengah (UMKM), serta institusi pemerintahan dan pendidikan. Kejahatan siber bersifat tidak pandang bulu dan dapat menyerang siapa saja yang terhubung dengan internet, baik melalui perangkat komputer, ponsel pintar, maupun sistem digital lainnya. Sebagai contoh, UMKM sering menjadi target serangan phising atau malware karena sistem keamanan digital mereka yang lemah. Di sisi

lain, individu pengguna media sosial juga kerap menjadi korban penipuan, pencurian identitas, maupun penyebaran konten palsu. Bahkan lembaga pendidikan pun tidak luput dari ancaman serangan *ransomware* yang mengenkripsi data penting dan meminta tebusan dalam mata uang kripto. Karakteristik umum dari korban kejahatan siber di Indonesia adalah minimnya pemahaman tentang ancaman digital dan rendahnya perlindungan terhadap data pribadi. Banyak di antara mereka tidak menyadari bahwa informasi pribadi seperti nomor KTP, foto, atau akses akun dapat dimanfaatkan untuk tindak pidana. Hal ini menyebabkan tingginya tingkat kerentanan yang sering kali tidak diantisipasi oleh masyarakat, terutama di wilayah dengan literasi digital yang masih rendah. Jenis kerugian yang dialami oleh korban kejahatan siber sangat beragam, mulai dari kerugian finansial, pelanggaran privasi, hingga dampak psikologis yang mendalam. Pada kasus penipuan daring, korban dapat kehilangan uang dalam jumlah besar karena ditipu melalui skema jual beli palsu, undian fiktif, hingga investasi bodong yang tersebar di media sosial. Di sisi lain, pelaku kejahatan dapat mengakses rekening atau dompet digital korban secara ilegal dan menguras isinya dalam waktu singkat. Secara normatif, beberapa regulasi telah mengatur tentang perlindungan korban kejahatan siber di Indonesia. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE), yang telah beberapa kali direvisi, memberikan dasar hukum bagi korban untuk menuntut pelaku atas kerugian akibat informasi palsu, akses ilegal, peretasan, pencemaran nama baik, dan sebagainya. Selain itu, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) juga memberi ruang hukum bagi korban yang mengalami kebocoran, penyalahgunaan, atau pencurian data pribadi. Pada konteks kelembagaan, perlindungan terhadap korban kejahatan siber melibatkan sejumlah institusi negara. Kementerian Komunikasi dan Informatika (Kominfo) memiliki peran penting dalam menyosialisasikan keamanan digital dan menindak konten ilegal melalui patroli siber. Kominfo juga membuka kanal pengaduan masyarakat terkait penyalahgunaan data, konten berbahaya, dan ancaman digital lainnya. Sedangkan Otoritas Jasa Keuangan (OJK) melindungi nasabah dari kejahatan siber dalam sektor keuangan digital, seperti penipuan perbankan dan fintech ilegal. Polri, khususnya melalui Direktorat Tindak Pidana Siber (Dittipidsiber), bertugas menerima laporan, melakukan penyelidikan dan penyidikan terhadap pelaku kejahatan siber. Dalam praktiknya, Polri sering bekerja sama dengan instansi lain seperti BI, OJK, maupun platform digital. Namun, dalam hal pendampingan korban, peran Lembaga Perlindungan Saksi dan Korban (LPSK) menjadi sangat relevan.

4. Kesimpulan dan Saran

Kesimpulan:

1. Penerapan sanksi pidana terhadap pelaku kejahatan *Cyber Crime* di era digitalisasi masih menghadapi tantangan serius dari aspek yuridis, teknis, dan sosial. Sifat kejahatan yang lintas negara, tingginya anonimitas pelaku, serta sulitnya pembuktian barang bukti elektronik memperumit proses penegakan hukum.
2. Perlindungan hukum bagi korban tindak pidana kejahatan *Cyber Crime* di era digitalisasi masih menghadapi berbagai tantangan serius, mulai dari belum optimalnya implementasi regulasi, belum tersedianya mekanisme pemulihan yang terpadu, hingga adanya

ketimpangan posisi antara korban, pelaku, dan penyedia platform digital.

Saran:

1. Untuk meningkatkan efektivitas penerapan sanksi pidana terhadap kejahatan *Cyber Crime*, diperlukan langkah strategis yang mencakup penguatan kapasitas aparat penegak hukum melalui pelatihan forensik digital dan penyediaan infrastruktur investigasi yang memadai, pembaruan regulasi yang responsif terhadap perkembangan teknologi digital, serta peningkatan literasi digital masyarakat.
2. Untuk memperkuat perlindungan hukum bagi korban kejahatan siber, dibutuhkan pembentukan lembaga atau sistem pendampingan korban yang terintegrasi dan mudah diakses, serta penguatan peran lembaga-lembaga yang telah ada seperti LPSK, Kominfo, dan Polri agar berorientasi pada pemulihan korban.