

PENANGGULANGAN TINDAK PIDANA SIBER BERDASARKAN UNDANG-UNDANG INFORMASI DAN TRANSAKSI ELEKTRONIK

Rudy Gunawan Bastari
Magister Hukum Universitas Islam Batik Surakarta

ABSTRAK

This research aims to explore and understand the law enforcement processes in addressing cybercrime in Indonesia. The research methodology combines juridical and empirical approaches by analyzing the content of the Electronic Information and Transactions Law (UU ITE) and involving the analysis of current data related to cybercrime, public responses, and the effectiveness of law enforcement. The research results provide an overview of the challenges faced in the efforts to enforce the law against cybercrime, including the lack of legal and moral awareness in society. Additionally, this research also aims to design and propose efforts to combat cybercrime in Indonesia in the future. This identification opens the door for regulatory updates and comprehensive legal awareness improvements to strengthen the efforts against cybercrime in the future.

ARTICLE INFO

Article History:

Accepted 03 Juni 2023

Available online 30 Jul 2023

Kata kunci: Cyber, Electronic Transactions, Criminal

I. PENDAHULUAN

Teknologi komputer telah membawa suatu inovasi baru dalam kehidupan saat ini, yakni internet. Keberadaan internet kini menjadi sangat vital bagi manusia di seluruh dunia. Beberapa jenis bisnis bahkan tidak dapat beroperasi tanpa keterlibatan internet. Manusia semakin merasa nyaman menjalani aktivitas sehari-hari, dan mereka yang telah terbiasa dengan internet merasa tidak nyaman jika aksesnya terhambat (Soekamto, 2005)

Fenomena internet dan digitalisasi memberikan dampak yang signifikan terhadap kehidupan manusia, membawa perubahan paradigmatik dalam berbagai sektor, termasuk kegiatan ekonomi, sosial, dan politik. Meskipun teknologi membawa kemudahan dan inovasi, namun kemajuan ini juga diiringi dengan tantangan baru, seperti maraknya kejahatan siber. Kejahatan siber telah menjadi ancaman global yang melintasi batas negara dan merugikan individu, perusahaan, serta pemerintahan.

Dalam pertimbangan Undang-Undang Nomor 11 Tahun 2008, disebutkan bahwa

pesatnya perkembangan Teknologi Informasi telah mengakibatkan perubahan signifikan dalam kehidupan manusia di berbagai bidang, yang secara langsung mempengaruhi munculnya bentuk-bentuk perbuatan hukum baru. Teknologi informasi dan komunikasi telah mengubah perilaku masyarakat serta peradaban manusia secara global. Selain itu, kemajuan teknologi dan informasi telah menghapus batas-batas (borderless) di dunia, menyebabkan perubahan sosial yang terjadi dengan sangat cepat. Teknologi informasi kini menjadi alat dua sisi, memberikan kontribusi positif terhadap kesejahteraan dan kemajuan manusia, tetapi juga menjadi sarana efektif untuk tindakan melawan hukum . (Atmasmita, 2007)

Sementara menciptakan peluang baru dalam kehidupan masyarakat, internet juga membuka peluang baru bagi tindak kejahatan. Di dunia maya, orang melakukan berbagai perbuatan jahat yang tidak dapat dilakukan di dunia nyata. Tindak kejahatan ini dilakukan dengan menggunakan komputer sebagai alat pelaksanaannya. Kejahatan di bidang telematika

ini merupakan dampak negatif dari kemajuan teknologi yang berdampak luas pada berbagai aspek kehidupan modern saat ini.

Indonesia memiliki peraturan utama yang mengatur informasi dan transaksi elektronik, yaitu Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, yang kemudian direvisi menjadi Undang-Undang Nomor 19 Tahun 2016. Undang-Undang ITE ini mengandung ketentuan-ketentuan yang melarang melakukan tindakan tertentu yang dapat dikenakan sanksi pidana. Di dalamnya, terdapat perbuatan-perbuatan yang dianggap sebagai tindak pidana komputer dengan sanksi yang telah ditetapkan.

Menurut Barda Nawawi Arief (2006), upaya pencegahan tindak pidana, khususnya dalam hal tindak pidana siber, menunjukkan fokus kebijakan pada pembaharuan undang-undang. Meskipun pembaharuan undang-undang merupakan langkah yang penting, kompleksitas masalah tindak pidana siber menuntut pendekatan integral. Selain reformasi hukum, pendekatan ini juga melibatkan reformasi sosial, ekonomi, politik, budaya, moral, dan administratif

Pemberantasan tindak pidana sering kali menggunakan sanksi pidana sebagai cara yang umum. Hingga saat ini, penerapan sanksi pidana terhadap tindak pidana siber dianggap sebagai metode yang diharapkan dapat memberantasnya. Dalam Rancangan KUHP tahun 2015, terdapat perubahan dalam ketentuan mengenai sistem pidana, termasuk jenis dan ukuran pidana. Sistem double track diterapkan untuk pidana dan tindakan, sementara ukuran pidana mencakup minimum dan maksimum.

Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) menjadi landasan hukum utama dalam menangani kejahatan siber di Indonesia. Namun, implementasi dan efektivitas UU ITE dalam penegakan hukum masih menghadapi berbagai kendala. Perubahan cepat dalam metode kejahatan siber, kurangnya kesadaran masyarakat terhadap ancaman digital, serta tuntutan regulasi yang terus berkembang menjadi faktor-faktor yang mempengaruhi

penegakan hukum. Oleh karena itu, penelitian ini dilakukan untuk mengidentifikasi kendala-kendala tersebut dan merumuskan upaya penanggulangan kejahatan siber yang lebih efektif di masa depan. (Nitibaskara, 2001)

Oleh karena itu, pola pemidanaan dalam Undang-Undang ITE perlu disesuaikan dengan pola pemidanaan yang diusulkan dalam konsep Rancangan KUHP terbaru ini. Efek dari sanksi pidana merupakan masalah empiris, karena persepsi manusia terhadap sanksi tersebut dapat bervariasi. Beberapa pihak berpendapat bahwa peningkatan kriminalitas disebabkan oleh sanksi atau hukuman yang terlalu ringan, sementara yang lain berpendapat bahwa sanksi yang terlalu ringan tidak akan memberikan efek jera yang cukup

Selain itu, penelitian ini diinisiasi oleh kebutuhan untuk memahami dinamika kompleks antara perkembangan teknologi dan penegakan hukum dalam konteks kejahatan siber di Indonesia. Pemahaman ini menjadi krusial dalam menyusun strategi penanggulangan yang dapat mengimbangi perubahan-perubahan teknologi dan metode kejahatan. Dengan merinci latar belakang tersebut, penelitian ini berharap dapat memberikan kontribusi dalam merancang kebijakan yang lebih responsif dan efektif dalam menanggulangi kejahatan siber di Indonesia.

II. METODE PENELITIAN

Penelitian ini mengadopsi metode penelitian yuridis empiris yang memadukan dua pendekatan utama, yaitu pendekatan hukum (yuridis) dan pendekatan pengamatan serta analisis data empiris. (Soekamto, 2005). Pendekatan yuridis digunakan untuk mengkaji kerangka hukum yang mengatur kejahatan siber, terutama Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan peraturan-peraturan terkait. Analisis yuridis ini memungkinkan peneliti untuk memahami landasan hukum serta kerangka regulasi yang menjadi dasar dalam menanggulangi kejahatan siber di Indonesia. Selain itu, metode yuridis juga melibatkan peninjauan putusan pengadilan terkait dengan

kasus kejahatan siber untuk mendapatkan pemahaman mendalam tentang bagaimana hukum diterapkan dalam praktiknya

III. HASIL PENELITIAN DAN PEMBAHASAN

1. Penegakan Hukum dalam Menanggulangi Kejahatan Siber (Cyber Crime) di Indonesia

Dalam era globalisasi yang terus berkembang, kemajuan teknologi informasi, beserta pembentukan hukum teknologi informasi, memerlukan langkah-langkah antisipatif dari aparat penegak hukum. Langkah ini diperlukan agar tercapai keseimbangan dan tata pergaulan di tengah-tengah kehidupan kelompok, golongan, ras, dan suku, serta masyarakat di dalam negeri maupun dalam konteks hubungan regional dan internasional. Hal ini diharapkan dapat menciptakan perlindungan yang optimal dan kesejahteraan bagi masyarakat Indonesia, sesuai dengan tujuan nasional yang tercantum dalam alinea keempat UUD 1945, sekaligus sebagai elemen dasar penyelenggaraan negara hukum di Indonesia. (Golose, 2006).

Dalam konteks perkembangan terkini, UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, yang kemudian diubah oleh UU Nomor 19 Tahun 2016, dianggap sebagai payung hukum yang mengatur ruang siber dan kejahatan siber (cyber crimes). UU ITE ini diharapkan menjadi kekuatan pengendali dan penegak ketertiban untuk segala bentuk pemanfaatan teknologi informasi, tidak hanya terbatas pada aktivitas internet, melainkan mencakup seluruh kegiatan yang melibatkan perangkat komputer dan instrumen elektronik lainnya.

Undang-undang ini dianggap telah memenuhi persyaratan keberlakuan hukum, baik secara yuridis, sosiologis, maupun filosofis. Dari segi filosofis, pembentukan UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, yang diubah oleh UU Nomor 19 Tahun 2016, didasarkan pada amanat Pasal 28F Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, yang menegaskan hak setiap orang untuk berkomunikasi, memperoleh informasi, dan mengembangkan diri secara

baik dalam lingkungan sosialnya. Secara yuridis, undang-undang ini mencakup regulasi terkait dengan semua aspek kegiatan internet, perangkat komputer, dan instrumen elektronik lainnya, serta dibentuk oleh lembaga yang berwenang, yaitu Dewan Perwakilan Rakyat sebagai lembaga legislatif.

Dari perspektif sosiologis, masyarakat membutuhkan Undang-undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, yang telah mengalami perubahan melalui Undang-Undang Nomor 19 Tahun 2016, untuk mengatur berbagai aktivitas yang terjadi selama interaksi di ruang siber. Perkembangan globalisasi informasi memerlukan suatu peraturan yang melindungi kepentingan para pengguna internet dalam mengakses berbagai informasi. Regulasi dalam undang-undang ini sejalan dengan nilai-nilai agama, moral, dan kaidah yang diterima secara universal, membuat keberadaan hukum siber (termasuk instrumen hukum internasional yang mengaturnya) diakui, diterima, dan diterapkan oleh masyarakat informasi.

Dalam konteks penegakan hukum terhadap kejahatan transnasional, termasuk kejahatan siber, faktor hukum yang utama yang sering kali menjadi hambatan adalah masalah yurisdiksi. Keraguan dalam menentukan yurisdiksi di ruang siber diakui oleh para pakar hukum. Tien S. Saefullah menyatakan bahwa yurisdiksi suatu negara, yang diakui dalam konteks konvensional, didasarkan pada batasan geografis dan waktu, sementara ruang siber bersifat internasional, multi-yurisdiksi, dan tanpa batasan geografis, sehingga masih belum jelas bagaimana yurisdiksi suatu negara dapat diterapkan terhadap komunikasi multimedia dalam era pemanfaatan teknologi informasi saat ini. (Raharjo, 2009)

Penetapan yurisdiksi menjadi isu sentral dalam penegakan hukum siber, terutama dalam konteks penegakan hukum terhadap kejahatan transnasional. Masalah ini diatur dalam Pasal 2 Undang-undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik yang telah diubah oleh

Undang-Undang Nomor 19 Tahun 2016. Pasal ini menyatakan bahwa undang-undang ini berlaku untuk setiap individu yang melakukan perbuatan hukum sesuai yang diatur dalam undang-undang ini, baik berada di wilayah hukum Indonesia maupun di luar wilayah hukum Indonesia, asalkan perbuatannya memiliki konsekuensi hukum di wilayah hukum Indonesia dan/atau di luar wilayah hukum Indonesia serta merugikan kepentingan Indonesia. Pasal 1 angka 21 mengklarifikasi bahwa "orang" merujuk pada individu, termasuk warga negara Indonesia, warga negara asing, atau badan hukum.

Dalam penjelasan Pasal 2, dijelaskan bahwa undang-undang ini memiliki yurisdiksi tidak hanya untuk perbuatan hukum yang terjadi di Indonesia atau dilakukan oleh warga negara Indonesia, tetapi juga berlaku untuk perbuatan hukum di luar wilayah hukum Indonesia, baik oleh warga negara Indonesia maupun asing, atau badan hukum Indonesia maupun asing, asalkan memiliki dampak hukum di Indonesia. Hal ini mengingat pemanfaatan Teknologi Informasi untuk Informasi Elektronik dan Transaksi Elektronik dapat melintasi batas wilayah atau bersifat universal. Konsep "merugikan kepentingan Indonesia" mencakup, namun tidak terbatas pada, kerugian terhadap kepentingan ekonomi nasional, perlindungan data strategis, harkat dan martabat bangsa, pertahanan dan keamanan negara, kedaulatan negara, warga negara, serta badan hukum Indonesia. (Ali, 2010)

2. Upaya Penanggulangan Kejahatan Siber di Indonesia di Masa Depan

Ketidakoptimalan dalam penegakan hukum terhadap kejahatan siber disebabkan oleh kurangnya sarana dan fasilitas yang memadai. Penanggulangan kejahatan siber memerlukan alat karena kejahatan ini dapat dilakukan dengan berbagai perangkat, baik berwujud maupun tidak berwujud. Waktu dan tempat terjadinya kejahatan siber ditentukan oleh efektivitas alat yang digunakan, sehingga analisis telematika menjadi penting untuk mengungkap kejahatan tersebut. Onno W. Purbo

menjelaskan bahwa cara untuk menelusuri, mendeteksi, dan menanggulangi kejahatan siber sangat bergantung pada aplikasi dan topologi jaringan yang digunakan. Beberapa aplikasi yang digunakan termasuk gnacktrack dan backtrack. Hal ini menunjukkan bahwa sarana dan fasilitas yang memadai memiliki peran krusial dalam penegakan hukum. Tanpa sarana atau fasilitas tertentu, penegakan hukum akan kesulitan mencapai tujuannya. Sarana dan fasilitas yang dibutuhkan meliputi tenaga manusia yang terdidik dan trampil, organisasi yang efisien, peralatan yang memadai, keuangan yang mencukupi, dan sebagainya. Jika hal-hal tersebut tidak terpenuhi, penegakan hukum tidak dapat berjalan dengan lancar. (Mansur, 2005)

Dalam upaya meningkatkan penanggulangan kejahatan siber yang semakin meningkat, Polri, khususnya Bareskrim Mabes Polri, telah berupaya untuk melakukan sosialisasi mengenai kejahatan siber dan cara penanganannya kepada satuan di kewilayahan (Polda). Sosialisasi dilakukan melalui pelatihan dan peningkatan kemampuan penyidikan anggota Polri dengan mengirimkan personelnya untuk mengikuti berbagai kursus yang berkaitan dengan kejahatan siber. Pengiriman personel Polri tidak hanya terbatas di tingkat nasional, namun juga mencakup kursus di negara-negara maju agar pengetahuan dan keterampilan yang diperoleh dapat diaplikasikan secara efektif di Indonesia. (Saeullah, 2002)

Pelatihan, kursus, dan ceramah kepada aparat penegak hukum, seperti Jaksa dan Hakim, perihal kejahatan siber perlu dilakukan. Hal ini disebabkan oleh kurangnya keberadaan satuan unit khusus yang menangani kejahatan dunia maya di kalangan Jaksa dan Hakim. Oleh karena itu, diperlukan sosialisasi, terutama setelah pengesahan UU ITE, agar tercipta kesamaan persepsi dan pemahaman dalam menangani kejahatan siber. Peran Jaksa dan Hakim yang menguasai aspek cyber sangat penting mengingat meningkatnya jumlah tindak pidana teknologi yang dapat melibatkan

peristiwa di satu daerah, luar daerah, bahkan di luar negeri. Kurangnya sarana dan prasarana dalam penegakan hukum terhadap kejahatan siber dapat signifikan mempengaruhi kinerja aparat penegak hukum dalam menghadapi kejahatan teknologi tinggi.

Pencegahan dan penanggulangan kejahatan siber memerlukan pendekatan baik penal maupun non-penal yang terintegrasi dan saling terkait. Pembicaraan tentang masyarakat menjadi suatu keharusan dalam konteks pembahasan hukum, karena hukum dan masyarakat adalah dua sisi dari satu mata uang. Pembicaraan tentang hukum tanpa mempertimbangkan masyarakat sebelumnya dapat dianggap hampa makna. Kesadaran hukum dari pihak yang menjadi korban untuk melaporkan kejahatan yang mereka alami masih sangat rendah. Berdasarkan laporan Norton Cybercrime Report dari Symantec, hampir setengah (45 persen) dari korban kejahatan siber tidak pernah menyelesaikan secara tuntas kejahatan yang mereka alami. Meskipun sebanyak 86 persen dari pengguna yang disurvei mengakui pernah menjadi korban kejahatan siber, kesadaran untuk melaporkan masih rendah. Terutama pada kasus eksploitasi seksual, korban jarang melaporkan kejadian tersebut karena adanya rasa malu. Kesadaran hukum yang rendah di masyarakat memengaruhi pemahaman dan ketaatan mereka terhadap hukum. Menurut Dikdik M. Arief Mansur dan Elisatris Gultom, beberapa alasan kurangnya kesadaran hukum masyarakat Indonesia antara lain adalah kurangnya pemahaman dan pengetahuan masyarakat terhadap jenis kejahatan siber. Kurangnya informasi menyebabkan kesulitan dalam penanggulangan kejahatan siber, terutama dalam hal kepatuhan hukum dan pengawasan terhadap aktivitas yang diduga terkait dengan kejahatan siber. Oleh karena itu, dapat dikatakan bahwa penegakan hukum yang optimal memerlukan kesadaran hukum dan moral yang tinggi dari masyarakat. (Yoan, 2010)

IV. KESIMPULAN

Berdasarkan hasil pembahasan di atas, dapat ditarik kesimpulan bahwa kemunculan internet sebagai hasil dari perkembangan teknologi komputer telah memberikan dampak signifikan dalam kehidupan sehari-hari. Internet diakui sebagai elemen penting di berbagai sektor bisnis dan aktivitas pribadi. Namun, disebutkan bahwa eksistensi beberapa jenis bisnis bahkan menjadi tidak mungkin tanpa adanya internet. Pada konteks ini, penulis menyoroti pentingnya internet dalam memfasilitasi kehidupan manusia dan bisnis global, namun juga mencermati risiko kejahatan siber yang muncul seiring dengan perkembangan tersebut.

Adanya perubahan drastis dalam kehidupan manusia yang disebabkan oleh perkembangan teknologi informasi, khususnya internet. Penelitian ini mencatat bahwa perkembangan teknologi informasi telah membawa dampak besar terhadap perilaku masyarakat dan peradaban manusia secara global. Fenomena ini, sejalan dengan Undang-Undang Nomor 11 Tahun 2008, memunculkan bentuk-bentuk perbuatan hukum baru yang perlu ditangani dengan efektif. Di samping kontribusi positifnya, teknologi informasi juga membuka peluang baru bagi kejahatan, terutama dalam ranah kejahatan siber.

Penegakan hukum terhadap kejahatan siber di Indonesia. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik merupakan kerangka hukum utama yang mengatur bidang ini. Penelitian ini menekankan perlunya strategi kebijakan yang terfokus pada upaya pembaruan undang-undang untuk menghadapi kompleksitas masalah kejahatan siber. Penelitian juga mencatat upaya pihak berwenang, seperti Bareskrim Mabes Polri, dalam meningkatkan keterampilan aparat penegak hukum, seperti Jaksa dan Hakim, dalam menangani kejahatan siber melalui pelatihan dan sosialisasi. Kesadaran hukum dan moral masyarakat juga dianggap krusial dalam upaya penegakan hukum yang optimal.

DAFTAR PUSTAKAGenerasi”, Genta Publishing.
Yogyakarta. 2010.

- Arief, Barda Nawawi. “Tindak Pidana Mayantara (Perkembangan Kajian Cybercrime Di Indonesia)”. PT. Raja Grafindo Persada. Jakarta. 2006.
- Ali, H. Zainuddin. “Filsafat Hukum”. Sinar Grafika. Jakarta. 2010.
- Atmasasmita, Romli. Teori dan Kapita Selekta Krimonologi”. Refika Aditama. Bandung. 2007.
- Direktorat II Ekonomi dan Khusus Unit V IT & *Cybercrime* Bareskrim Mabes Polri, pada Tahun 2016.
- Golose, Petrus Reinhard. Perkembangan Cybercrime dan Upaya Penanganannya di Indonesia Oleh Polri, Makalah pada Seminar Nasional tentang “Penanganan Masalah Cybercrime di Indonesia dan Pengembangan Kebijakan Nasional yang Menyeluruh Terpadu”, diselenggarakan oleh Deplu. BI, dan DEPKOMINFO, Jakarta. 10 Agustus 2006.
- Moeljatno, “Azas-azas Hukum Pidana. Bina aksara. Jakarta. 1985.
- Mansur, Dikdik M. Arief dan Elisatris Gultom, “Cyber Law: Aspek Hukum Teknologi Informasi”. Refika Aditama. Bandung. 2005.
- Nitibaskara, Tubagus Ronny Rahman. “Ketika Kejahatan Berdaulat: Sebuah Pendekatan Kriminologi, Hukum dan Sosiologi”. Peradaban. Jakarta. 2001.
- Rahardjo, Satjipto. “Hukum dan Perilaku Hidup yang Baik adalah Dasar Hukum yang Baik”. Kompas. Jakarta. 2009.
- Soekanto, Soerjono. “Faktor-Faktor Yang Mempengaruhi Penegakan Hukum”, PT. Raja Grafindo Persada. Jakarta. 2005.
- Saefullah, Tien S. “Jurisdiksi sebagai Upaya Penegakan Hukum dalam Kegiatan Cyberspace, artikel dalam Cyberlaw: Suatu Pengantar”. Pusat Studi *Cyberlaw* Fakultas Hukum UNPAD. ELIPS. 2002.
- Yoan N, Bernard L. Tanya. Simanjuntak dan markus Yage, “Teori Hukum strategi Tertib Manusia Lintas Ruang dan