Jurnal Bevinding Vol 02 No 01 Tahun 2024
Fakultas Hukum Universitas Islam Batik Surakarta
E-ISSN 3024-9805

Dampak Cyber Crime Terhadap Keamanan Nasional dan Strategi Penanggulangannya: Ditinjau Dari Penegakan Hukum

Dwi Shinta Wati[1], Siti Nurhaliza[2], Mulia Wulan Sari[3], Rizka Amallia[4]
dwishintawati2@gmail.com, sitinurhaliza22@gmail.com, muliawulan71@gmail.com, rizkaamallia18@gmai.com
Program Studi Hukum, Fakultas Hukum, Universitas Bandar Lampung

ABSTRAK

Cyber crime merupakan ancaman nyata dalam keamanan dan pertahanan nasional. Cyber crime telah menjadi ancaman yang serius terhadap keamanan nasional karena dampaknya yang semakin meluas seiring berjalannya kompleksitas teknologi informasi. Kejahatan siber ini bisa mengganggu keadaan stabilitas ekonomi, politik, dan sosial di suatu negara bahkan sampai ke tahap membahayakan infrastruktur kritis negara. Upaya penanggulangan, pencegahan, dan kerja sama yang efektif sangat dibutuhkan untuk melindungi negara dari dampak negatif dari cyber crime, yaitu meliputi penguatan infrastruktur keamanan, mengedukasi kesadaran masyarakat akan resiko dari cyber crime, serta penguatan penegakan hukum terhadap pemberian sanksi yang tegas kepada pelaku cyber crime. Dengan begitu, kerja sama antara pemerintah, sektor swasta, dan masyarakat menjadi kunci dalam menghadapi ancaman cyber crime terhadap keamanan nasional.
Kata kunci: Cyber crime, Keamanan, Negara, dan Kerja sama.

ABSTRACT

Cyber crime is a real threat to national security and defense. Cyber crime has become a serious threat to national security because its impact is increasingly widespread along with the complexity of information technology. This cybercrime can disrupt the economic, political and social stability of a country, even to the point of endangering the country's critical infrastructure. Effective mitigation, prevention and cooperation efforts are urgently needed to protect the country from the negative impacts of cyber crime, which include strengthening security infrastructure, educating public awareness of the risks of cyber crime, as well as strengthening law enforcement to provide strict sanctions to perpetrators of cyber crime. In this way, cooperation between the government, private sector and society is key in facing the threat of cyber crime to national security.
Keywords: Cyber crime, Security, State, and Cooperation.

A. PENDAHULUAN

Perkembangan teknologi di era globalisasi sekarang ini begitu pesat terutama pada sektor teknologi informasi yang membuat masyarakat dengan mudah dapat menerima dan memberikan informasi kepada masyarakat luas. Manfaat dari teknologi informasi selain memberikan dampak positif juga memberikan dampak negatif yakni

memberi peluang untuk dijadikan saranaa melakukan cyber crime.[1]Dalam perkembangan zaman yang selalu berkembang, keamanan nasional pada negara semakin rentan mengalami serangan cyber crime yang semakin pesat dan mengganggu. Serangan ini bukan hanya membuat ancaman pada infrastruktur kritis, akan tetapi dapat merusak kestabilan politik, mengambil data sensitif milik individu, perusahaan, bahkan negara dan mencuri privasi serta keamanan individu. Kerugian yang ditimbulkan dari cyber crime pada keamanan nasional sudah mengambil perhatian utama bagi pemerintah, organisasi internasional, dan sektor swasta di seluruh dunia khususnya Indonesia. Pentingnya mengetahui dan mengatasi kejahatan cyber crime terhadap keamanan nasional mendorong perlunya penelitian yang mendalam tentang fenomena ini. Dalam pembahasan ini, jurnal ini berfungsi untuk menganalisis dampak cyber crime terhadap keamanan nasional serta memberikan strategi penanggulangan yang tepat. Melalui pemanfaatan pemahaman yang lebih luas tentang sifat, pola, dan motivasi di balik serangan cyber crime, penulis mengharapkan dapat dikembangkan strategi yang lebih proaktif dan adaptif untuk menjaga kepentingan negara dan masyarakat.

Kemajuan teknologi informasi membawa implikasi yang mendalam terhadap tatanan sosial dan hukum. Fenomena jejak digital, yang kini menyertai setiap transaksi online, memberikan dinamika baru bagi penegakan hukum[2]. Berkembangnya cyber crime dapat terlihat dari munculnya berbagai istilah seperti online business crime, cyber money laundering, high tech white collar crime, dan sebagainya. Bahkan, dalam dokumen PBB, cyber crime memiliki istilah baru yaitu, Dogpiling, Dixing, Doxware, Kejahatan terkait identitas, Pelecehan seksual berbasis gambar, online impersonation, Roasting, Pharming, Sextortion, dan Zero day. Dalam FBI Cybercrime Report 2017, Kepolisian Amerika Serikat merilis 20 negara tertinggi yang menjadi korban dari tindak kejahatan cyber crime selain Amerika Serikat diantaranya Kanada, India, Inggris, Brazil, Jerman, Australia, Spanyol, Mexico, dan beberapa negara lainnya. Indonesia tidak termasuk dalam 20 negara tertinggi yang menjadi korban cyber crime, tetapi termasuk dalam negara yang menjadi asal dimana cyber crime dilakukan. Kasus cyber crime pertama kali di Indonesia terjadi pada tahun 1990-an dengan munculnya kasus pemakaian nama domain www.mustikaratu.com yang disidangkan di pengadilan Negeri Jakarta Selatan. Kasus ini menyeret seorang terdakwa yang bernama Tjandra Sugiono dengan dakwaan Pasal 382 bis KUHP dan Pasal 48 ayat (1) jo Pasal 19 huruf b UU Nomor 5 Tahun 1999 tentang Larangan Praktik Monopoli dan Persaingan Usaha Tidak Sehat. Dalam pemeriksaan perkara tersebut majelis hakim Pengadilan Negeri Jakarta Selatan memutuskan bahwa perbuatan yang didakwakan tidak terbukti sehingga terdakwa dibebaskan dari segala dakwaan.

[1] Hasan, Z., Apriano, I. D., Simatupang, Y. S., & Muntari, A. (2023). Penegakan Hukum Terhadap Pelaku Tindak Pidana Perjudian Online. *Jurnal Multidisiplin Dehasen (MUDE)*, *2*(3), 375-380.

[2] Iqbal, M., Ardie, H. J., & Hasan, Z. ANALISIS HUKUM DALAM MELACAK JEJAK DIGITAL DAN MEMAHAMI TINDAK PIDANA PENCUCIAN UANG DALAM ERA TEKNOLOGI. *Iqtishaduna: Jurnal Ilmiah Mahasiswa Hukum Ekonomi Syari'ah*, 286-298.

Topik ini penting untuk dibahas karena saat ini Indonesia sedang mengalami transisi dari ekonomi tradisional ke ekonomi digital. Masa ekonomi tradisional ialah keadaan sebelum hadirnya teknologi informasi yang mempunyai daya tarik massal. Pada masa perekonomian tradisional, perdagangan barang dan jasa, serta transaksi lainnya antar masyarakat umum, dilakukan secara tenang karena tidak melibatkan alat teknologi. Transaksi tersebut mewajibkan para pihak yang akan melakukan transaksi harus bertemu secara fisik pada waktu dan lokasi yang telah disepakati bersama. Sedangkan ekonomi digital ialah kegiatan yang telah dijelaskan sebelumnya tetapi dapat dilakukan melalui pemanfaatan teknologi informasi dan komunikasi, sehingga mengantarkan era baru yang dikenal sebagai "ekonomi digital" sehingga membuka peluang kejahatan oleh orang yang tidak bertanggung jawab. Eksploitasi data dan kebocoran data dari media elektronik dalam ekonomi digital semakin sering terjadi. Oleh karena itu, untuk mencegah terulangnya situasi seperti ini, perlu adanya pertimbangan yang matang dalam menyusun peraturan mengenai perlindungan informasi pribadi yang dimiliki oleh setiap individu serta cara menggunakan nasihat hukum atau non-hukum sebagai "penjaga" untuk memastikan ekonomi digital terus tumbuh. Namun kebocoran data pribadi di Indonesia terkandung dalam instrumen hukum yang sangat baru dan tidak dapat diandalkan.

Salah satu contoh kasus cyber crime yang dialami oleh individu ialah permasalahan penggunaan data pribadi menggunakan metode penipuan yang terjadi di Indonesia pada tahun 2019[3]. Kasus ini berupa permintaan untuk mengikuti simulasi *computer assisted test* (CAT) yang dikirimkan oleh akun @cpnsindonesia.id di akun sosial media Instagram, walaupun permintaan tersebut tidak menghasilkan hasil negatif apa pun karena belum ada korban yang tertarik. Namun tetap saja ajakan untuk mengikuti uji coba simulasi CPNS "CAT" ini terkesan penipuan karena pada saat pendaftaran, setiap peserta wajib memasukkan informasi pribadinya yang bersifat privasi pada URL yang disediakan. Akibatnya, mereka yang mempunyai otoritas yang ilegalitas pasti akan menggunakan data pribadi tersebut ke dalam hal yang tidak sah. Sehubungan dengan kejadian tersebut akhirnya BKN segera memberikan informasi tersebut melalui akun Twitter pribadinya yang berbunyi "BKN tidak pernah menjalin kerja sama dengan institusi mana pun dalam menyelenggarakan simulasi ujian berbasis CAT, meskipun memang benar ada, pasti akan diberitahukan melalui akun sosial media resmi milik BKN".

Penting bagi hukum Indonesia untuk berevolusi seiring dengan perubahan sosial dan teknis. Aturan hukum dapat dibuat lebih efektif dan efisien dengan bantuan teknologi, terutama digitalisasi. Masyarakat mengharapkan proses hukum yang lebih cepat, lebih transparan, dan lebih mudah diakses, dan sistem hukum Indonesia perlu mengadopsi teknologi digital untuk mengikuti perubahan budaya dan substansi.[4]Menurut pendapat yang

[3] Tribun timur.com, "Dituding Akan Salah Gunakan Data Peserta Tryout Tes Cpns 2019, Klarifikasi Akun Cpns Indonesia.Id," Tribun News .Com, last modified 2019, https://makassar.tribunnews.com/2019/06/26/ditudingakan-salah-gunakan-data-peserta-tryout-tes-cpns-2019iniklarifikasi-akun-cpnsindonesiaid

[4] Irawan, H., & Hasan, Z. (2024). Dampak Teknologi Terhadap Strategi Litigasi dan Bantuan Hukum: Tren dan Inovasi di Era Digital. *Innovative: Journal Of Social Science Research, 4*(2), 4600-4613.

dikemukakan oleh Widodo[5], cyber crime diartikan ke dalam istilah "kegiatan dari individu, kelompok, dan badan hukum yang menggunakan komputer sebagai alat melakukan kejahatan kepada korban yang dituju". Beberapa tipikal kejahatan yang terjadi di internet ialah sebagai berikut: 1). *Illegal contents* atau konten yang tidak sah, yaitu memasukkan data palsu, tidak sah, dan melanggar hukum serta mengganggu ketertiban umum dalam internet. 2). *Illegal acces/unauthorized access to computer system and service* atau akses ilegal/akses tidak sah terhadap sistem dan layanan komputer, yaitu bentuk kejahatan yang dilakukan menggunakan cara meretas/menyusup ke dalam suatu sistem jaringan komputer secara tidak sah, atau tanpa sepengetahuan dari pemilik sistem jaringan komputer yang disadapnya. 3). *Cyber espionage* atau spionase dunia maya, yaitu bentuk kejahatan yang menggunakan jaringan internet dengan cara memasuki sistem jaringan komputer pihak yang akan ditargetkan atau korban untuk dijadikan sasaran untuk dimata-matai. 4). *Data forgery* atau pemalsuan data, yaitu tindakan modus kriminal di sosial media yang dilakukan dengan cara memalsukan data dokumen penting yang disimpan sebagai dokumen tanpa kertas melalui internet. Kejahatan sejenis ini biasanya menargetkan dokumen e-commerce, seolah-olah adanya "typo" yang pada akhirnya akan merugikan korban, karena korban akan memasukkan data pribadi dan nomor kartu kredit kepada pelaku. 5). *Cyber sabotage and extortion* atau sabotase dan pemerasan dunia maya, yaitu modus yang dijalankan dengan cara mengganggu, merusak, atau menghancurkan data yang terhubung ke internet, program komputer, atau sistem jaringan komputer. Biasanya kejahatan semacam ini dilakukan dengan cara memasukkan logic bomb, seperti virus komputer atau program tertentu, sehingga data, program komputer atau sistem jaringan komputer tidak bisa dipakai dan tidak dapat berjalan secara normal atau tidak dapat berjalan, tetapi telah dikendalikan oleh pelaku sesuai kebutuhan. 6). *Infringements of privacy*, yaitu suatu kejahatan yang menargetkan informasi pribadi yang disimpan dalam formulir data hak milik personal yang tersimpan secara computerized, apabila orang lain mengetahuinya, maka hal itu dapat menyebabkan kerugian terhadap korban secara materiil maupun immaterial, seperti bocornya nomor PIN ATM, dan lainnya. 7). *Offense against intellectual property* atau (pelanggaran terhadap Hak atas Kekayaan Intelektual), yaitu tindakan kejahatan yang menyasar hak kekayaan intelektual yang dimiliki pihak lain di Internet. Contohnya mempraktikkan tampilan website orang lain secara ilegal.

Dalam penulisan ini, akan dibahas berbagai unsur penting yang berhubungan dengan dampak cyber crime terhadap keamanan nasional, termasuk jenis-jenis serangan yang paling general, kerentanan infrastruktur kritis, konsekuensi politik dan ekonomi, hingga tantangan dalam menanggapi serangan yang semakin kompleks ditinjau dari penegakan hukum. Selain itu, akan dibahas juga berbagai strategi penanggulangan yang telah diusulkan dan diimplementasikan oleh pemerintah, organisasi internasional, dan sektor swasta di berbagai negara. Diharapkan bahwa jurnal ini dapat memberikan kontribusi yang berharga bagi

[5] Yuni Fitriani dan Roida Pakpahan, "Analisa Penyalahgunaan Media Sosial untuk Penyebaran Cybercrime di Dunia Maya atau Cyberspace," Cakrawala: Jurnal Humaniora20, no. 1 (Maret 2020): 22.

pemahaman kita tentang ancaman cyber crime terhadap keamanan nasional serta membantu dalam merancang kebijakan dan praktik terbaik untuk melindungi negara dari serangan cyber di masa depan.

B. METODE PENELITIAN

Metode penelitian yang dipakai oleh penulis ialah Hukum Normatif. Metode hukum normatif merupakan analisis yang melibatkan teori hukum, prinsip-prinsip hukum, dan argumen hukum yang mendasari suatu isu hukum. Penulis akan menganalisis literatur hukum, dokumen-dokumen teoritis, dan pendapat para ahli hukum untuk membangun argumen dan pemahaman hukum yang lebih mendalam dan demi kesempurnaan tulisan ini. Metode hukum normatif berfungsi sebagai alat bantu untuk memahami analisis yang mendasari sistem hukum di suatu negara.[6]

Selain metode penelitian di atas, penulis juga menggunakan dua bahan hukum yaitu bahan hukum sekunder dan bahan hukum primer. Bahan hukum sekunder ialah sekumpulan buku yang berisi prinsip dan metode dasar tentang hukum hingga perkembangan hukum di masa sekarang. Sedangkan bahan hukum primer ialah bahan yang bersifat otoritas yakni memiliki nilai kekuasaan seperti undang-undang, atau peraturan pemerintah. Dalam tulisan ini, bahan yang dipakai ialah Undang-Undang Negara Republik Indonesia tahun 1945, Undang-Undang Negara Republik Indonesia tahun 2016 Nomor 19 mengenai Perubahan Perundang-undangan tahun 2008 Nomor 11 mengenai Informasi dan Transaksi Elektronik.[7]

C. HASIL DAN PEMBAHASAN

1. Dampak Cyber Crime Terhadap Keamanan Nasional

Dampak cyber crime terhadap keamanan nasional tidak bisa diremehkan. Serangan siber dapat menimbulkan kerentanan dalam infrastruktur penting seperti sistem keuangan, kesehatan, serta energi. Hal ini membuat gangguan dalam layanan publik, kebocoran data sensitif, hingga yang paling parah yaitu sabotase terhadap operasi militer dan intelijen. Tidak hanya itu, serangan yang dilakukan oleh negara asing atau kelompok terorganisir menimbulkan ancaman kedaulatan dan posisi negara, serta memicu konflik internasional.

Apabila diuraikan lebih jelasnya, kejahatan cyber crime dapat mengganggu keamanan nasional dalam berbagai unsur, yaitu sebagai berikut:[8]

a). Menargetkan Infrastruktur Kritis

Cyber crime bisa melumpuhkan infrastruktur kritis seperti jaringan listrik, air, dan transportasi, yang dapat menimbulkan kekacauan dan kerusakan yang fatal. Contohnya, yang

---

[6] Harkristuti Harkrisnowo. (2018). Dalam Buku yang Berjudul *"Metode Penelitian Hukum dan Statistik, Sinar Grafika".*

[7] B Djulaeka and Devi Rahayu, Buku Ajar: Metode Penelitian Hukum (surbaya: Scopindo Media Pustaka, 2019), 33.

[8] Siaran Pers No. 83/PIH/KOMINFO/11/2013 Ancaman Cyber Attack Dan Urgensi Keamanan Informasi Nasional. (2013) from https://sdppi.kominfo.go.id/berita-ancaman-cyber-attack-dan-urgensi-keamanan-informasi-nasional-26-2079

terjadi di tahun 2017, munculnya serangan WannaCry ransomware melumpuhkan komputer di rumah sakit, bank, dan perusahaan di seluruh dunia. Gangguan pada infrastruktur kritis tersebut bisa mengganggu keselamatan umum, merusak perekonomian, hingga memicu konflik sosial.

b). Mencuri Data Sensitif

Cyber crima bisa mencuri data sensitif seperti data pemerintah, data keuangan, dan data individu. Data ini dapat dipakai untuk tujuan kriminal seperti penipuan identitas, pemerasan, atau bahkan spionase. Kebocoran data sensitif bisa merusak kepercayaan publik terhadap pemerintah dan institusi, dan menimbulkan berdampak negatif pada reputasi negara di mata internasional.

c). Menyebarkanluaskan Propaganda dan Disinformasi

Cyber crime bisa dimanfaatkan untuk menyebarkanluaskan propaganda dan disinformasi guna adanya kerusuhan sosial, merusak stabilitas politik, dan merusak citra negara. Contohnya seperti yang terjadi di tahun 2016, intervensi siber difitnah dilakukan guna memengaruhi hasil pemilihan presiden Amerika Serikat.

d). Melumpuhkan Layanan Publik

Cyber crime bisa mengurangi layanan publik seperti situs web pemerintah, layanan e-government, dan sistem perbankan. Hal ini bisa mengganggu akses masyarakat kepada layanan penting dan menghambat aktivitas ekonomi. Gangguan layanan publik dapat mengakibatkan frustrasi dan kemarahan dari masyarakat, dan dapat merusak kepercayaan publik terhadap pemerintah.

e). Mengintimidasi dan Membungkam Suara Kritis

Cyber crime dapat dimanfaatkan untuk mengintimidasi dan membungkam suara kritis, seperti jurnalis, aktivis, dan pembela hak asasi manusia. Hal tersebut mengakibatkan penyusutan ruang publik dan demokrasi, dan dapat menghambat kemajuan sosial.

2. Strategi Penanggulangan Melalui Penegakan Hukum Berupa Undang-Undang

a. Undang-Undang Negara Republik Indonesia Tahun 1945

UUD 1945 merupakan landasan hukum fundamental bangsa Indonesia yang mempunyai peran krusial dalam penanggulangan berbagai permasalahan dan mewujudkan cita-cita nasional. Penegakan UUD 1945 yang tepat menjadi peran utama dalam mencapai tujuan tersebut khususnya untuk mencegah kejahatan cyber crime. Dibawah ini merupakan berbagai strategi penanggulangan yang dapat dilakukan melalui penegakan hukum berupa UUD 1945:[9]

a). Melalui Penguatan Lembaga Penegak Hukum

- Memaksimalkan kapasitas dan profesionalisme dari kinerja aparat penegak hukum, seperti Polri, Kejaksaan, dan KPK, untuk menegakkan hukum yang adil, transparan, dan akuntabel.
- Mendirikan sistem peradilan yang independen dan berintegritas tinggi, bebas dari intervensi politik dan kepentingan pribadi.

[9] Peter Mahmud Marzuki. Penelitian Hukum, Edisi Revisi. jakarta: Kencana, 2013.

- Memaksimalkan mekanisme pengawasan terhadap kinerja aparat penegak hukum untuk mencegah terjadinya kejahatan siber baik yang berasal dari individu, kelompok, maupun perusahaan.

b). Peningkatan Kesadaran Hukum Masyarakat

- Memberikan edukasi hukum yang rutin terhadap masyarakat tentang bahaya dan risiko dari kejahatan cyber crime.
- Mengajak masyarakat turut aktif dalam proses penegakan hukum, seperti melalui program-program patroli bersama dan pelaporan apabila terjadi kasus kejahatan siber.
- Menerapkan budaya hukum yang kuat di masyarakat dengan menumbuhkan kesadaran untuk menghormati hukum dan norma-norma sosial sehingga tidak adanya pelaku kejahatan yang muncul.

c). Pembenahan Regulasi dan Perundang-undangan Oleh Aparat Hukum

- Melakukan evaluasi dan revisi terhadap peraturan perundang-undangan yang sudah tidak bisa berlaku, tumpang tindih, atau tidak sesuai dengan tujuan UUD 1945.
- Memastikan kesamaan antara peraturan perundang-undangan di tingkat pusat dan daerah untuk menghindari tumpang tindih dan multitafsir.
- Mendorong partisipasi publik dalam proses legislasi untuk memastikan bahwa peraturan perundang-undangan yang dibuat mencerminkan kebutuhan dan aspirasi masyarakat.

d). Penegakan Hak Asasi Manusia (HAM)

- Memastikan adanya unsur HAM dalam setiap proses penegakan hukum, mulai dari penyelidikan, penyidikan, penuntutan, hingga peradilan.
- Memberikan perlindungan hukum bagi korban kejahatan siber dan memastikan mereka mendapatkan akses terhadap keadilan.
- Mencegah terjadinya pelanggaran HAM seperti cyber crime dengan memperkuat mekanisme pencegahan dan pemulihan hak-hak korban.

e). Penegakan Supremasi Hukum

- Menjamin bahwa hukum ditegakkan secara adil dan tanpa pandang bulu, termasuk terhadap aparat penegak hukum, pejabat publik, dan kelompok-kelompok yang memiliki pengaruh kuat.
- Memberikan akses yang sama terhadap hukum bagi semua orang, tanpa diskriminasi berdasarkan suku, agama, ras, golongan, atau status sosial ekonomi.
- Menindak tegas pelaku cyber crime dengan memberikan sanksi yang tegas dan proporsional.

f). Pemanfaatan Teknologi Informasi dan Komunikasi (TIK)

- Menggunakan teknologi informasi dan komunikasi (TIK) untuk memberi pengetahuan bagaimana cara menjauhi dan menanggulangi cyber crime.
- Membuat sistem pelaporan pelanggaran hukum secara online yang mudah diakses dan direspon dengan cepat.
- Memanfaatkan media sosial untuk menyebarkan informasi tentang hukum dan edukasi kepada masyarakat agar pelaku merasa terancam dan mengurungkan niatnya.

g). Kerjasama Antar Lembaga

- Menjalin kerja sama dan koordinasi antar lembaga penegak hukum, seperti Polri, Kejaksaan, dan KPK, untuk menindaklanjuti kasus-kasus yang kompleks dan lintas wilayah.
- Mengajak lembaga-lembaga terkait lainnya, seperti Kementerian/Lembaga, organisasi masyarakat sipil, dan akademisi, dalam upaya penegakan hukum.
- Menjalin kerja sama internasional untuk memerangi kejahatan lintas negara dan ekstradisi pelaku kejahatan.

Penegakan UUD 1945 secara efektif membutuhkan komitmen dan kerjasama dari semua pihak, baik pemerintah, aparat penegak hukum, maupun masyarakat. Dengan strategi yang tepat dan konsistensi dalam menanggulangi kejahatan cyber crime, diharapkan UUD 1945 dapat menjadi pondasi yang kuat untuk membangun cita-cita nasional dan menciptakan Indonesia yang adil, makmur, dan sejahtera.

b. Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik

Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) memainkan penting terhadap penanggulangan kejahatan cyber. Strategi yang dapat diambil menggunakan Undang-Undang tersebut ialah sebagai berikut:

a). Penguatan Penegakan Hukum

Yaitu memaksimalkan kapasitas penegak hukum dalam menyelidiki dan menindaklanjuti kejahatan siber sesuai yang ada pada UU ITE.

b). Pencegahan

Yaitu membuat kampanye edukasi kepada masyarakat tentang pentingnya kesadaran siber dan bagaimana melakukan penyelamatan diri dari serangan siber.

c). Kerjasama Internasional

Yaitu melibatkan lembaga dan negara lain dalam pertukaran informasi dan penegakan hukum untuk menindak kejahatan siber yang melintasi batas-batas negara.

d). Pengembangan Teknologi Keamanan

Yaitu meningkatkan pengembangan teknologi keamanan informasi yang dapat membantu dalam mendeteksi, mencegah, dan merespons serangan siber.

e). Audit dan Pemantauan

Yaitu melakukan audit secara rutin kepada infrastruktur teknologi informasi dan pemantauan terhadap kegiatan yang berpeluang untuk mendeteksi dini potensi serangan siber.

f). Perlindungan Korban

Yaitu memberikan perlindungan kepada korban kejahatan siber, baik secara hukum dan secara psikologis.

g). Pengawasan Terhadap Konten Digital

Yaitu menjamin bahwa konten digital yang beredar tidak melanggar ketentuan UU ITE guna meminimalisir risiko penyebaran informasi yang merugikan atau palsu.

Undang-Undang Negara Republik Indonesia Nomor 19 Tahun 2016 yakni Perubahan atas Undang-Undang Republik Indonesia Nomor 11 Tahun 2011 tentang Informasi dan

Transaksi Elektronik berisikan norma perlindungan data personal yang terdapat pada pasal 26, artinya penggunaan data individu dan seluruh informasi yang diperoleh dari alat teknologi yang dikendalikan oleh orang yang tidak bertanggung jawab seharusnya harus sudah mendapat persetujuan oleh orang yang bersangkutan berdasarkan hukum positif yang telah berlaku di Indonesia. Ketentuan ini memiliki dua aspek legitimasi pengolahan data personal, yakni:

a). consent atau persetujuan

b). norma hukum positif

Tak hanya tertuang dalam Perjanjian UU, khususnya pada Pasal 26 UU, pemerintah juga memberikan dukungan atau solusi ketika pengguna elektronik gagal melakukan autentikasi atau melakukan pelanggaran terkait data pribadi, sehingga dapat mengakibatkan terungkapnya informasi pribadi kepada pihak-pihak yang terlibat dalam kejadian tersebut. Selain untuk mencegah terjadinya penyalahgunaan data pribadi, pemerintah melalui UU tersebut memberikan arahan kepada pengembang sistem elektronik dalam mengembangkan sistem yang berorientasi pada pemenuhan kebutuhan dan pemenuhan permintaan. mengenai data pribadi yang tampaknya tidak lagi sesuai yang diminta atau tidak sah. Dalam hal ini pemerintah berusaha melakukan penyaringan atas data-data yang masuk ke dalam sistem elektronik.

3. Contoh Kasus Cyber Crime di Indonesia

a). Pada tahun 2019, terjadi serangan siber terhadap Badan Penyelenggara Pemilu (Bawaslu) menjelang Pemilihan Umum Presiden. Serangan ini ditengarai bertujuan untuk mengganggu proses pemilu. Serangan ini merupakan salah satu dari sejumlah kejadian yang terjadi selama proses pemilu tersebut. Pelaku serangan diduga menggunakan metode serangan berupa DDoS (Distributed Denial of Service) yang berfungsi untuk mematikan layanan Bawaslu di internet. Serangan ini di Indonesia pada 17 April 2019, saat pemungutan suara berlangsung.

Penyelidikan awal mengungkapkan bahwa serangan tersebut berasal dari luar negeri, meskipun belum ada kejelasan mengenai identitas pelaku atau negara asal serangan, serangan tersebut telah membuat kekhawatiran terhadap keamanan data dan integritas proses pemilihan umum, menanggapi hal itu, Bawaslu mengatakan bahwa sistem pengawasan mereka tetap berjalan dengan aman meskipun adanya oleh serangan tersebut.

Serangan siber seperti ini menunjukkan betapa pentingnya adanya perlindungan terhadap infrastruktur digital negara, terkhusus dalam konteks pemilu, di mana data yang akurat dan akses yang terjamin menjadi krusial dalam menjaga kepercayaan publik pada berjalannya proses demokratis. Hal ini juga menekankan pentingnya usaha pencegahan dan penegakan hukum terhadap kejahatan siber di Indonesia.

b). Pada tahun 2022, terjadi kebocoran data pribadi sebanyak 100 juta penduduk Indonesia pengguna dari Badan Penyelenggara Jaminan Sosial (BPJS Kesehatan).

Kasus ini menjadi pusat perhatian publik karena melibatkan informasi pribadi dari 100 juta penduduk pengguna BPJS Kesehatan, data tersebut meliputi nomor kepesertaan, nama lengkap, tanggal lahir, dan nomor Kartu Tanda Penduduk (KTP). Kebocoran data ini pertama kali diketahui oleh seorang peneliti keamanan pada bulan Maret 2020. Ia

mengungkap dan menemukan bahwa data pribadi dari sekitar 100 juta peserta BPJS Kesehatan telah tersebar secara online dan bisa diakses bebas oleh siapa pun. Data tersebut dipercaya telah bocor sejak tahun 2013.

Penyelidikan terhadap kebocoran data tersebut menunjukkan bahwa penyebab kebocoran terjadi karena kelemahan dalam sistem keamanan informasi BPJS Kesehatan. Beberapa penyebab yang mungkin membuat kebocoran tersebut antara lain kurangnya perlindungan data, pengelolaan yang belum memadai terhadap informasi sensitif, dan kurang maksimal dalam infrastruktur teknologi informasi.

Kasus kebocoran data BPJS Kesehatan memunculkan keprihatinan serius pada perlindungan data individu masyarakat Indonesia dan membuka pikiran akan pentingnya peningkatan keamanan siber di lembaga pemerintah dan organisasi swasta. Ini juga memicu permintaan untuk reformasi dalam pengelolaan data pribadi dan penegakan hukum terhadap pelanggaran keamanan data di Indonesia.

A. Komputer Sebagai Target

Kejahatan cyber crime ini dilakukan oleh kelompok kriminal yang bisa muncul dari siapa dan kapan saja. Tidak seperti kejahatan yang menggunakan komputer sebagai alat, kejahatan ini memerlukan pengetahuan teknis oleh pelaku. Dengan demikian seiring perkembangan teknologi, maka berkembang pula sifat kejahatannya. Kejahatan ini relatif baru dalam sejarah komputer, yang menjelaskan betapa tidak siapnya masyarakat dan dunia pada umumnya untuk memberantas kejahatan ini. Ada banyak kejahatan dari sifat ini yang dilakukan setiap hari di internet. Kejahatan yang terutama menargetkan jaringan komputer atau perangkat meliputi:

- Virus komputer
- Denial-of-service attacks atau Penolakan serangan layanan
- Malware (malicious code)
- dan sebagainya.

Bila individu merupakan target utama cyber crime, komputer bisa dianggap sebagai alat ketimbang target.[10] Kejahatan ini umumnya kurang melibatkan keahlian teknis. Kelemahan manusia umumnya dieksploitasi. Kerusakan yang ditangani sebagian besar bersifat psikologis dan tidak berwujud, membuat tindakan hukum terhadap varian ini lebih sulit. Inilah kejahatan yang telah ada selama berabadabad di dunia offline. Penipuan, pencurian, dan sejenisnya sudah ada bahkan sebelum pengembangan peralatan berteknologi tinggi. Penjahat yang sama hanya diberi alat yang meningkatkan potensi korbannya dan membuatnya semakin sulit dilacak dan ditangkap. Kejahatan yang menggunakan jaringan komputer lainnya meliputi:

- Penipuan dan pencurian identitas (walaupun hal ini semakin banyak menggunakan malware hacking atau phishing, menjadikannya sebagai contoh kejahatan komputer "sebagai sasaran" dan "komputer sebagai alat")
- Perang informasi

[10] Richet, J.L. (2013) From Young Hackers to Crackers, International Journal of Technology and Human Interaction (IJTHI), 9(3), 53-62.

- Penipuan phishing
- Spam
- Pornografi, termasuk pelecehan dan ancaman. Pengiriman email massal yang tidak diminta untuk tujuan komersial (spam) tidak sah di beberapa wilayah hukum. Phishing sebagian besar disebarkan melalui email. Email phishing mungkin berisi tautan ke situs web lain yang terpengaruh oleh malware. Atau, mungkin berisi tautan ke perbankan online palsu atau situs web lain yang digunakan untuk mencuri informasi akun pribadi.

D. PENUTUP

1. Kesimpulan

Berdasarkan penulisan di atas, penulis menyimpulkan bahwa dampak cyber crime terhadap keamanan nasional dalam konteks penegakan hukum dapat menyebabkan beberapa konsekuensi yang signifikan di Indonesia. Pertama, cyber crime dapat mengganggu infrastruktur kritis seperti sistem energi, transportasi, dan keuangan, mengancam stabilitas nasional. Kedua, pencurian data sensitif oleh pelaku kejahatan siber dapat membahayakan keamanan nasional dengan mengungkapkan informasi rahasia atau merusak kepentingan negara. Selain itu, cyber crime juga dapat digunakan untuk kegiatan spionase dan sabotase yang bertujuan merusak infrastruktur atau proses penting negara. Penegakan hukum harus memperkuat kerjasama internasional dan mengembangkan kapasitas untuk mendeteksi, menyelidiki, dan menuntut pelaku cyber crime secara efektif agar dapat melindungi keamanan nasional dari ancaman ini. Penegakan hukum di Indonesia dapat memainkan peran penting dalam menciptakan strategi penanggulangan terhadap kasus tersebut.

2. Saran

Berdasarkan penulisan di atas, penulis mempunyai saran yang dapat digunakan untuk mengatasi tantangan ini, yaitu sebagai berikut:

1. Penegakan hukum perlu ditingkatkan dengan penguatan kapasitas, baik melalui pelatihan dan pendidikan bagi petugas penegak hukum maupun dengan menyusun undang-undang yang tepat sesuai dengan perkembangan teknologi dan tren cyber crime yang baru.
2. Melakukan kolaborasi antara pemerintah dan sektor swasta juga sangat penting untuk melindungi infrastruktur kritis dan berbagi informasi tentang ancaman yang mungkin muncul.
3. Seharusnya publik mempunyai kesadaran yang tinggi tentang ancaman cyber crime juga perlu diperhatikan melalui kampanye pendidikan dan sosialisasi. Dengan pendekatan holistik dan kolaboratif seperti ini, diharapkan penegakan hukum dapat lebih efektif dalam melindungi keamanan nasional dari ancaman cyber crime yang semakin kompleks.

DAFTAR PUSTAKA

Buku

B Djulaeka and Devi Rahayu. (2019) Buku Ajar: Metode Penelitian Hukum (surbaya: Scopindo Media Pustaka)

Harkristuti Harkrisnowo. (2018). Dalam Buku yang Berjudul *"Metode Penelitian Hukum dan Statistik, Sinar Grafika"*

Jurnal

Hasan, Z., Apriano, I. D., Simatupang, Y. S., & Muntari, A. (2023). Penegakan Hukum Terhadap Pelaku Tindak Pidana Perjudian Online. Jurnal Multidisiplin Dehasen (MUDE), 2(3)

Iqbal, M., Ardie, H. J., & Hasan, Z. ANALISIS HUKUM DALAM MELACAK JEJAK DIGITAL DAN MEMAHAMI TINDAK PIDANA PENCUCIAN UANG DALAM ERA TEKNOLOGI. *Iqtishaduna: Jurnal Ilmiah Mahasiswa Hukum Ekonomi Syari'ah*

Irawan, H., & Hasan, Z. (2024). Dampak Teknologi Terhadap Strategi Litigasi dan Bantuan Hukum: Tren dan Inovasi di Era Digital. *Innovative: Journal Of Social Science Research*, *4*(2)

Peter Mahmud Marzuki. (2013). Penelitian Hukum, Edisi Revisi. jakarta: Kencana.

Richet, J.L. (2013) From Young Hackers to Crackers, International Journal of Technology and Human Interaction (IJTHI), 9(3)

Yuni Fitriani dan Roida Pakpahan. (2022). "Analisa Penyalahgunaan Media Sosial untuk Penyebaran Cybercrime di Dunia Maya atau Cyberspace," Cakrawala: Jurnal Humaniora20, no. 1 Maret: 22.

Website

Siaran Pers No. 83/PIH/KOMINFO/11/2013 Ancaman Cyber Attack Dan Urgensi Keamanan Informasi Nasional. (2013) from https://sdppi.kominfo.go.id/berita-ancaman-cyber-attack-dan-urgensi-keamanan-informasi-nasional-26-2079

Tribun timur.com, "Dituding Akan Salah Gunakan Data Peserta Tryout Tes Cpns 2019, Klarifikasi Akun Cpns Indonesia.Id," Tribun News .Com, last modified 2019, https://makassar.tribunnews.com/2019/06/26/ditudingakan-salah-gunakan-data-peserta-tryout-tes-cpns-2019iniklarifikasi-akun-cpnsindonesiaid.