Jurnal Ilmu Hukum "THE JURIS" Vol. VII, No. 2, Desember 2023
ISSN 2580-0299, e-ISSN 2580-8370
http://ejournal.stih-awanglong.ac.id/index.php/juris

KEBIJAKAN PENEGAKAN HUKUM DALAM UPAYA MENANGANI CYBER CRIME YANG DILAKUKAN OLEH POLRI VIRTUAL DI INDONESIA

Mohamad Suarno Nur[1], Fenty Puluhuwa[2], Fence M. Wantu[3]
[1,2,3]Pascasarjana Prodi Magister Hukum, Universitas Negeri Gorontalo, Indonesia
mohammadnoer2@gmail.com, fence.wantu@yahoo.co.id, fentypuluhulawa@ung.ac.id

Naskah diterima: 5 November 2023; revisi: 3 Desember 2023; disetujui: 30 Desember 2023

Abstract

This research aims to understand and analyze the legal regulatory policies regarding information technology crimes in addressing cybercrime committed by virtual police in Indonesia. In the midst of technological advancements and their negative impacts, especially cybercrimes, handling cybercrime becomes a complex challenge. This study involves normative legal analysis focusing on doctrines and legal principles found in legislation and court decisions.The results indicate that the criminal legal regulations related to cybercrime in Indonesia are not yet fully adequate. Although Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions has regulated some aspects, further harmonization and adjustment are still needed in line with the development of cybercrimes. In dealing with cybercrime, the roles of virtual police and cyber police in Indonesia need to be clearly understood. Virtual police emphasize preventive efforts, while cyber police follow up on cases through law enforcement. The existence of this difference needs to be socialized so that the public understands their roles in combating cybercrime.

Keywords: *Cyber Crime, Criminal Law Regulation, Enforcement of Virtual Police Law*

✉Alamat korespondensi:
Universitas Negeri Gorontalo
Email: mohammadnoer2@gmail.com

I. PENDAHULUAN

Dunia saat ini dicirikan oleh kemajuan dalam teknologi informasi dan komunikasi yang mempengaruhi berbagai aspek kehidupan manusia. Adanya internet, sejenis media baru, dan kemajuan dalam teknologi informasi dan komunikasi telah membawa perubahan besar dalam kehidupan sosial, ekonomi, dan budaya dunia. Di era modern, kehidupan manusia sangat bergantung pada teknologi.Di satu sisi, adanya e-mail, e-commerce, cyber bank, bisnis online, internet banking, dan sebagainya adalah beberapa contoh bagaimana teknologi dapat memberikan banyak manfaat. Di sisi lain, juga berdampak negatif dengan munculnya kejahatan internet.

Kemajuan teknologi informasi dan komunikasi dalam masyarakat saat ini tidak hanya membawa manfaat, tetapi juga menyebabkan ketidaksesuaian dalam penggunaannya, yang mengarah pada kejahatan siber (Arief, 2012).

Mengenai karakteristik kejahatan di dunia maya, Mamoun Alazab, Roderic Broadhurst, Peter Grabosky, dan Steve Chon mengatakan: "Cyber criminals may operate as loose networks, but evidence suggests that members are still located in close geographic proximity even when their attacks are cross-national." laundering, high tech white collar crime, dan sebagainya dapat menunjukkan peningkatan cyber crime. Bahkan dalam dokumen Perserikatan Bangsa-Bangsa, istilah baru digunakan untuk kejahatan cyber, seperti Dogpiling, Dixing, Doxware, Kejahatan terkait identitas, Pelecehan seksual berbasis gambar, impersonasi online, Roasting, Pharming, Sextortion, dan Zero day. Kanada, India, Inggris, Brazil, Jerman, Australia, Spanyol, Mexico, dan beberapa negara lainnya adalah 20 negara tertinggi yang menjadi korban kejahatan cyber, menurut Laporan Cybercrime FBI 2017.

Meskipun Indonesia tidak berada di antara dua puluh negara tertinggi yang melaporkan korban cybercrime, negara ini termasuk dalam daftar negara-negara yang merupakan pusat cybercrime. Pada tahun 1990-an, kasus cybercrime pertama kali terjadi di Indonesia. Kasus pemakaian domain www.mustikaratu.com diadili di pengadilan Negeri Jakarta Selatan. Tjandra Sugiono, terdakwa dalam kasus ini, menghadapi dakwaan berdasarkan 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. Hakim Pengadilan Negeri Jakarta Selatan memutuskan bahwa terdakwa dibebaskan dari semua tuduhan karena tindakan yang didakwakan tidak terbukti. Data statistik laporan cyber crime di Indonesia pada tahun 2019 mencapai 4.586 laporan dalam satu tahun, tetapi pada tahun 2020 hanya 2.259 laporan. Kasus penyebaran konten provokatif menduduki -daftar kasus tertinggi, diikuti oleh penipuan online, pornografi, akses ilegal, dan kasus lainnya.

Penanganan kejahatan maya bukanlah hal yang mudah untuk diatasi. Selain sifat kejahatan maya itu sendiri, undang-undang yang ada di Indonesia belum dapat menangani perkembangan kejahatan maya. Hanya Undang-undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang mengatur perlindungan data pribadi di Indonesia.

Perlindungan hak pribadi, prinsip perdagangan elektronik, masalah yurisdiksi, prinsip persaingan usaha tidak sehat dan perlindungan konsumen, hak atas kekayaan intelektual, dan hukum internasional adalah komponen dari Undang-Undang Informasi dan Transaksi Elektronik (ITE).Pada dasarnya, penanggulangan kejahatan dengan hukum pidana merupakan bagian dari usaha penegakan hukum, dan politik hukum pidana merupakan bagian dari kebijakan penegakan hukum. Upaya hukum termasuk hukum pidana digunakan sebagai salah satu upaya mengatasi masalah sosial, termasuk dalam bidang kebijaksanaan penegakan hukum. Kebijaksanaan penegakan hukum ini juga bertujuan untuk mencapai kesejahteraan masyarakat pada umumnya.

Kejahatan baru ini memiliki dampak yang signifikan pada berbagai aspek kehidupan. Pemerintah memberlakukan undang-undang cybercrime karena banyak orang percaya bahwa KUHP tidak dapat menangani kejahatan baru tersebut. Undang-undang tentang Informasi dan Transaksi Elektronik (UU ITE), atau Undang-undang Nomor 19 Tahun 2016, yang diubah dari Undang-undang Nomor 11 Tahun 2008, adalah sumber informasi saat ini (Hermawan, 2019). Widodo berpendapat bahwa penjatuhan pidana kepada pelaku cybercrime adalah tindakan yang tidak bijak dan tidak tepat. Ini karena karakteristik pelaku tindak pidana tidak sesuai dengan sistem pembinaan narapidana di Lembaga Permasyarakatan. Akibatnya, tujuan pemidanaan yang diatur dalam Undang-undang Permasyarakatan tidak akan tercapai. Menurutnya, pidana kerja sosial atau pidana pengawasan dapat digunakan sebagai pengganti pemidanaan tersebut (Widodo, 2013). Namun, menurut Barda Nawawi Arief, upaya penanggulangan cyber crime, khususnya di Indonesia, dapat dilihat dari berbagai sudut

pandang dari sudut pandang hukum pidana, yaitu aspek pertanggungjawaban pidana atau pemidanaan (termasuk aspek alat bukti/pembuktian), aspek kriminalisasi (formulasi tindak pidana), dan aspek yurisdiksi. Barda Nawawi Arief mengatakan kebijakan kriminalisasi merupakan suatu kebijakan dalam menetapkan suatu perbuatan yang semula bukan tindak pidana (tindakan yang tidak dapat dipidana) menjadi tindak pidana. Oleh karena itu, kebijakan untuk mengkriminalisasi tindak pidana teknologi informasi merupakan bagian dari kebijakan kriminal dengan menggunakan sarana hukum pidana. Oleh karena itu, itu termasuk dalam "kebijakan hukum pidana", khususnya kebijakan yang dibuat tentangnya. Menurut Arief, kebijakan kriminalisasi mencakup masalah lebih dari hanya menetapkan, merumuskan, dan memformulasikan tindakan yang dapat dipidana (termasuk sanksi pidananya).Sistem hukum pidana, atau kebijakan legislatif, disusun secara harmonis. Konferensi Industri Informasi Internasional (IIIC) menyatakan, "The IIIC recognizes that government action and international traties to harmonizes laws and coordinate legal procedurs are key in the fight against cybercrime, but warns that these should not be relied upon as the onlu instuments." Teknologi memungkinkan cybercrime dan membutuhkan kepercayaan yang kuat pada teknologi untuk solusi. dipidana, termasuk sanksi pidananya, tetapi juga mencakup masalah.

Cyber police dan virtual police berbeda dalam menangani dan menyelidiki cyber crime. Peran virtual police adalah mendidik masyarakat tentang Undang-undang Informasi dan Transaksi Elektronik (ITE), sedangkan cyber police menindaklanjuti kasus jika tindakan yang dilakukan oleh masyarakat tidak dapat ditegur oleh cyber police. Dengan kata lain, cyber police muncul sebelum penyelidikan lebteknologi untuk solusi Ots dipidana, termasuk sanksi pidananya, tetapi juga mencakup masalah. Selanjutnya, jika akun mengunggah gambar bertuliskan yang berpotensi melanggar hukum, gambar tersebut akan disimpan untuk didiskusikan dengan tim ahli yang terdiri dari ahli pidana, ahli bahasa, dan ahli informasi dan transaki elektronik. Diajukan ke direktur siber atau pejabat yang ditunjuk siber untuk pengesahan jika ahli menunjukkan bahwa konten tersebut mengandung pelanggaran pidana. Selanjutnya, peringatan polisi virtual dikirim secara pribadi ke akun yang bersangkutan secara resmi. Karena peringatan dari polisi virtual tidak ingin diketahui oleh orang lain, peringatan akan dikirim melalui pesan langsung.

Kehadiran virtual police ini cenderungmasih baru di kalangan masyarakat, padahal diketahui pihak kepolisian sudah memiliki tim siber yang fungsinya tidak jauh berbeda dengan polisi virtual. Masih banyak masyarakat yang belum mengetahui perbedaan antara polisi virtual dan polisi siber, salah satu alasannya yaitu kurangkan pengedukasian kepada masyarakat dengan cakupan yang lebih luas. Sejalan dengan hal ini, Koordinator Wilayah Peradi Jawa Tengah, Badrus Zaman menjelaskan perbedaan dari keduanya yaitu jika polisi virtual lebih mengedepankan upaya preventif, sedangkan polisi siber sudah pasti melakukan penegakan hukum sesuai regulasi yang ada karena polisi siber sudah dapat mendeteksi melanggar rambu-rambu UU ITE.

Beberapa penelitian sebelumnya ada yang membahas peran kepolisian dalam menangani kasus cyber crime seperti dalam artikel yang ditulis oleh Abdul Agis yang berjudul "Peran Kepolisian dalam Penyidikan Penyalahgunaan Informasi dan Transaksi Elektronik". Selain itu, penelitian lainnya yang menganalisa tentang kesiapan dari aparatur yang ditulis oleh Rudi Hermawan yang berjudul "Kesiapan Aparatur Pemerintah dalam Menghadapi Cyber Crime di Indonesia". Terdapat juga penelitian yang mengusut tentang apa saja fungsi kepolisian dalam artikel yang ditulis oleh Sukinta yang berjudul "Peran Kepolisian Dalam Melakukan Penyidikan Tindak Pidana Penyebaran Berita Bohong di Indonesia". Selain dari sisi kepolisian, juga terdapat dari sudut pandang hukum yang dibahas pada artikel "Tinjauan Yuridis Efektivitas UU Nomor 19 Tahun 2016 Tentang Perubahan Atas UU No 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik" yang ditulis oleh Refland, Hero Soepono, dan Grace.

II. METODE PENELITIAN

Tulisan ini menggunakan metode penelitian hukum normatif karena fokus kajian berdasarkan pada doktrin melalui analisis kaidah hukum yang ditemukan dalam 4 Aloysius Wisnubroto, Kebijakan Hukum Pidana Dalam Penanggulangan Penyalahgunaan Komputer, Universitas peraturan perundang-undangan atau dalam berbagai putusan pengadilan dengan menggunakan tiga pendekatan, yaitu pendekatan undang-undang, pendekatan konseptual, dan pendekatan kasus.Sementara teknik pengumpulan data melalui data sekunder, yaitu dilakukan dengan cara studi dokumen dengan bahan penelitian yang bersifat primer, sekunder, dan tersier. Hasil penelitian dianalisis dan diuraikan secara deskriptif kualitatif, artinya data yang dikumpulkan dengan membandingkan antara teori yang berlaku dengan fakta-fakta yang terdapat di lapangan.

III. HASIL DAN PEMBAHASAN

Kebijakan Hukum Pidana Terhadap Tindak Pidana Teknologi Informasi Berdasarkan Hukum Positif Saat Ini Dalam bahasa Inggris, "pilcy" atau "politiek" berarti dasar umum yang berfungsi untuk mengarahkan pemerintah. Dalam arti luas, ini juga mencakup unsur-unsur aparat penegak hukum dalam hal mengelola, mengatur, atau menyelesaikan kepentingan umum, masalah atau masalah masyarakat, penyusunan peraturan perundang-undangan, dan pengaplikasian hukum atau peraturan dengan cara yang sesuai. (Atmajaya Yogyakarta, Yogyakatya, 1999, Halaman 10) Digunakan hukum pidana di Indonesia sebagai suatu sarana untuk menanggulangi suatu bentuk kejahatan sepertinya tidak menjadi permasalahan yang mendasar, hal ini dapat dilihat dari adanya praktik perundang-undangan yang selama ini menunjukkan bahwa penggunaan hukum pidana merupakan bentuk bagian yang tak terpisahkan dari kebijakan atau politik hukum yang digunakan oleh Indonesia. Penggunaan hukum pidana selama ini dianggap sebagai hal yang normal, artinya dengan kondisi tersebut eksistensinya sudah tak lagi dipermasalahkan Dalam Kitab Undang-Undang Hukum Pidana Kitab Undang–Undang Hukum Pidana yang biasa disingkat menjadi KUHP merupakan sistem utama bagi peraturan-peraturan hukum pidana di Indonesia. Perumusan tindak pidana yang tercantum dalam KUHP mayoritas masih bersifat konvensional dan belum secara langsung dikaitkan dengan perkembangan dari cyber crime itu sendiri. Beberapa peraturan perundang- undangan yang berhubungan dengan tindak pidana teknologi informasi diluar dari pengaturan KUHP yaitu:

1. Undang-Undang Nomor 36 Tahun 1999 Tentang Telekomunikasi
2. Undang-Undang Nomor 19 Tahun 2002 TentangHak Cipta
3. Undang-Undang Nomor 25 Tahun 2003 Tentang Perubahan atas Undang- Undang Nomor 15 Tahun 2002 Tentang Tindak Pidana Pencucian Uang
4. Undang-Undang Nomor 15 Tahun 2003 Tentang Pemberantasan Tindak Pidana Terorisme

Dalam Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik

Seiring dengan perkembangan zaman, dan dalam mengatur cyber space dan cyber crime telah terbit peraturan yang khusus mengatur tentang tindak pidana teknologi informasi yang tercantum dalam UU Nomor 19 Tahun 2016 Tentang Perubahan Atas UU Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. UU ITE ini diharapkan dapat menjadi kekuatan pengendali dan penegak ketertiban bagi kegiatan pemanfaatan teknologi informasi.

Selain memenuhi syarat sosiologis, UU ITE juga telah memenuhi syarat secara filosofis. Secara filosofis, lahirnya UU ITE ini didasarkan pada amanat yang terkandung dalam Pasal 28F Undang- Undang Dasar Negara Republik Indonesia Tahun 1945 yang menyatakan " Setiap orang berhak untuk mencari, memperoleh, memiliki, meyimpan, mengolah, dan menyampaikan informasi dengan menggunakan segala jenis saluran yang tersedia". Dalam Undang-undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, tindakan cybercrime meliputi hal-hal berikut: 1) Tindakan yang melanggar kesusilaan: Pasal 27 ayat (1) UU Nomor 11 Tahun 2008 menyatakan bahwa "Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan atau mentransmisikan dan/ atau membuat dapat diaksesnya Informasi Elektronik dan/ atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan", tetapi dalam pasal tersebut tidak dijelaskan mengenai perbuatan yang (Mudadi & Barda Nawawi, Teori-teori dan Kebijakan Pidana, PT. Alumni Bandung, 2010, Hal. 157). memiliki muatan yang melanggar kesusilaan.

Sementara dalam konteks perbuatan yang melanggar kesusilaan melalui media elektronik, terdapat beberapa tindakan yang tergolong dalam Pasal 27 ayat (1) UU Nomor 11 Tahun 2008, yaitu cyber pornografi dan prostitusi online. Tindak pidana ini akan semakin berat hukumannya apabila dilakukan terhadap anak di bawah umur. Salah satu permasalahan yang ditimbulkan dari kemajuan teknologi informasi melalui jaringan internet adalah beragamnya situs yang menampilkan adegan pornografi. Seolah-oleh sekarang ini, sulit sekali memproteksi jaringan internet dari serbuan pebisnis hiburan yang menjual pornografi. Penghinaan/Pencemaran nama baik Penghinaan/Pencemaran nama baik di cyber space diatur dalam Pasal 27 ayat (3) UU Nomor 11 Tahun 2008 yang menyatakan "Setiap orang dengan sengaja dam tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diakseskan Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan penghinaan dan/atau pencemaran nama baik". Dalam UU ITE ini, pembuat undang-undang menyetarakan antara penghinaan

dengan pencemaran, pada penghinaan sendiri merupakan suatu kelompok perbuatan, sedangkan salah satu bentuk penghinaan ialah pencemaran.

Dokumen Elektronik yang memiliki muatan perjudian "Penguntitan (Cyberstalking) Penguntitan tercantum dalam Pasl 29 UU Nomor 11 Tahun 2008 yang menyatakan "Setiap orang dengan sengaja dan tanpa hak mengirimkan Informasi Elektronik dan/atau Dokumen Elektronik yang berisi ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi" Pengaturan tentang penguntitan yang diatur dalam UU ITE sekilas mirip dengan pengaturan cyberstalking di beberapa negara, seperti Amerika Serikat, Kanada,dan Inggris yangdalam ketentuannya diatur mengenai tindakan pelecehan, ancaman, atau tindakan lain yang dilakukan untuk menimbulkan rasa takut, baik dengan kata- kata maupun tindakan tertentu. Perbuatan tersebut dilakukan dengan menggunakan atau melalui teknologi informasi dan komunikasi, misalnya dengan mail bombs, unsolicited mail, dan obsence or threatenig email.

Penyebaran berita bohong (hoax)

Penyebaran berita bohong diatur dalam Pasal 28 ayat (1) UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang menyatakan "Setiap orang dengan sengaja dan tanpa(Sigid Suseno, Yurisdiksi Tindak Pidana Siber, Refika Aditama, Bandung, 2012, Hal. 177-178) hak menyebarkan berita bohing dan menyesarkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik". Dokumen Elektronik yang sedang ditansmisikan. Ketentuan sebagaimana dimaksud pada ayat (1) dan ayat (2) tidak berlaku terhadap intersepsi atau penyadapan yang dilakukan dalam rangka penegakan hukum atas permintaan kepolisian, kejaksaan, atau institusi lainnya yang kewenangannya ditetapkan berdasarkan undang-undang.

Ketentuan lebih lanjut mengenai tata cara intersepsi sebagaimana dimaksud pada ayat (3) diatur dengan undang- undang. Penjelasan yang dimuat dalam Pasal 31 ayat (1) yang dimaksud dengan intersepsi atau penyadapan adalah kegiatan untuk mendengarkan, merekam, membelokkan, mengubah, menghambat, dan/atau memcatat transmisi Informasi Elektronik dan/atau Dokumen Elektronik yang tidak bersifat publik, baik menggunakan jaringan kabel komunikasi maupun jaringan nirkabel, seperti pancaran elektromagnetis atau radio frekuensi.

1) Akses ilegal Akses ilegal dilarang dalam Pasal 30 UU Nomor 11 Tahun 2008 yang diatur dalam ayat :
2) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik orang lain dengan cara apapun.
3) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apapun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik.
4) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum menagakses Komputer dan/atau Sistem Elektronik dengan cara apapun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan. \
5) Dalam Undang-undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, tindakan cybercrime meliputi hal-hal berikut: 1) Tindakan yang melanggar kesusilaan: Pasal 27 ayat (1) UU Nomor 11 Tahun 2008 menyatakan bahwa "Setiap orang dengan sengaja dan tanpa hak mendistribusikan.
6) Kejahatan terhadap Informasi Elektronik/Dokumen Elektronik/ Data interference Kejahatan ini menjadikan Informasi Elektronik dan/atau Dokumen Elektronik sebagai sasaran dalam melakukan kejahatan yang diatur dalam Pasal 32 UU Nomor 11 Tahun 2008 dinyatakan sebagai berikut:
    1. Setiap orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun mengubah, menambah, mengurangi, melakukan tranmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik orang lain atau publik.
    2. Setiap orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun memindahkan atau mentransfer Informasi Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik orang lain yang tidak berhak.
    3. Terhadap perbuatan sebagaimana dimaksud pada ayat (1) yang mengakibatkan terbukanya suatu Informasi Elektronik dan/atau Dokumen Elektronik yang bersifat rahasia menjadi

dapat diakses oleh publik dengan keutuhan data yang tidak sebagaimana mestinya.

Gangguan terhadap sistem elektronik Gangguan terhadap sistem elektronik adalah kejahatan yang dilakukan dengan menyerang sistem sebagaimana yang diatur dalam Pasal 33 UU Nomor 11 Tahun 2008 menyatakan "Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan tindakan apa pun yang berakibat terganggunya Sistem Elektronik dan/atau mengakibatkan Sistem Elektronik menjadi tidak bekerja sebagaimana mestinya."

Tinjauan Umum Tentang Cyber Crime Istilah cyber crime saat ini merujuk pada suatu tindakan kejahatan yang berhubungan denga cyber space atau dunia maya dan tindakan kejahatan tersebut menggunakan komputer. Beberapa ahli yang menyakan antara tindak kejatan cyber dengan tindak kejahatan komputer, dan terdapat juga yang membedakan diantara keduanya. Dalam beberaoa literatur, cyber crime sering di identikkan sebagai computer crime. Andi Hamzah dalam bukunya "Aspek-aspek Pidana di Bidang Komputer" mengartikan cyber crime sebagai kejahatan di bidang computer. secara umum dapat diartikan sebagai penggunaan komputer secara ilegal. Menurut freddy haris, cyber crime merupakan suatu tindak pidana dengan karakteristik-karakteristik sebagai berikut:

Kualifikasi kejahatan dunia maya (cyber crime) sebagaimana dalam buku Barda Nawawi Arief, adalah kualifikasi (cyber crime) menurut Convention on cybercrime 2001 di Budapest Hongaria, yaitu :

1) Illegal Interception Sengaja dan tanpa hak mendengar atau menangkap secara diam- diam pengiriman dan pemancaran data komputer yang tidak bersifat publik ke, dari atau di dalam sistem komputer dengan menggunakan alat bantu.
2) Data Interference Sengaja dan tanpa hak melakukan perusakan, penghapusan, perubahan atau penghapusan data komputer. *System Interference* Sengaja melakukan gangguan atau rintangan serius tanpa hak terhadap berfungsinya sistem komputer. *Misuse of Devive* Penyalahgunaan perlengkapan komputer, termasuk program komputer, password komputer, kode masuk (*access code*). *Computer Related Forgery* Pemalsuan (dengan sengaja dan tanpa hak memasukkan mengubah, menghapus data autentik menjadi tidak autentik dengan maksud digunakan sebagai data autentik) *Computer Related Fraud* Penipuan (dengan sengaja dan tanpa hak menyebabkan hilangnya barang/kekayaan oranglain dengan cara memasukkan, mengubah, menghapus data komputer atau dengan mengganggu berfungsinya komputer/sistem komputer, dengan tujuan untuk memperoleh keuntungan ekonomi bagi dirinya sendiri atau orang lain).

IV. KESIMPULAN

Pertama dan terpenting, sistem penegakan hukum Indonesia dalam hal penanggulangan kejahatan cyber masih kurang efektif. Faktor hukum, faktor penegak hukum, faktor sarana dan fasilitas penegakan hukum, dan faktor masyarakat adalah empat faktor yang dapat mempengaruhi penegakan hukum terhadap cyber crimes. Dari keempat faktor tersebut, faktor hukum (substansi hukum), yang banyak mengandung kelemahan dan faktor penegak hukum, adalah yang paling berpengaruh pada kelemahan penegakan hukum saat ini terhadap penanggulangan cyber crimes dalam anatomi kejahatan transnasional.

Kedua, kebijakan kriminalisasi terhadap perbuatan dalam dunia maya harus terus diharmonisasikan seiring maraknya kejahatan di dunia cyber yang semakin canggih. Hal ini disebabkan tindak pidana teknologi informasi yang tidak mengenal batas-batas teritorial dan beroperasi secara maya. Oleh karena itu, menuntut pemerintah harus selalu berupaya mengantisipasi aktivitas- aktivitas baru yang diatur oleh hukum yang berlaku. Ketiga, walaupun di Indonesia sudah terdapat aturan hukum yang mengatur tentang tindak pidana teknologi informasi secara jelas, haruslah aturan tersebut diperbarui seiring dengan perkembangan zaman yang semakin maju dan semakin banyaknya juga jenis cyber crime yang berbeda bentuknya yang mungkin akan terjadi di masa yang akan datang.

Keempat, pentingnya masyarakat dapat memahami dan dapat membedakan antara virtual police dan cyber police sebagai aparat yang ikut menanggulangi cyber crime. Kesadaran masyarakat akan hukum juga merupakan salah aspek penting untuk melaraskan tujuan agar tercapainya pemberantasan cyber crime yang marak terjadi.

REFERENSI

Abdul Wahid dan Mohammad Labib, *Kejahatan Mayantara (Cybercrime)*, Cetakan kedua (Bandung: Refika Aditama, 2010).

Arikunto Suharsimi, Prosedur Penelitian: Suatu Pendekatan Praktik (Jakarta: Rineka Cipta, 2006).

Chairul Huda*, Dari Tindak Pidana Tanpa Kesalahan Menuju Kepada Tiada Pertanggung jawab Pidana Tanpa Kesalahan*, Cetakan ke-2, Jakarta, Kencana, 2006

Dewa Gede Atmadja, *Asas-asas Hukum dalam Sistem Hukum,* jurnaa Kertha Wicaksana, Vol.12, No. 2.

Edmon Makarim, *Tanggung Jawab Hukum Penyelenggara Sistem Elektronik,* (Jakarta: Raja Grafindo Persada, 2010)

Fence M. Wantu, Idee Des Recht (*Kepastian Hukum, Keadilan Dan Kemanfaatan) Implementasi Dalam Proses Peradilan Perdata* Begawan Hukum Universitas Gajah Mada Yogyakarta, 2011)

Fence M Wantu, Jurnal Dinamika Hukum (*Kepastian Hukum, Keadilan Dan Kemanfaatan) Implementasi Dalam Proses Peradilan Perdata, UGM, Vol 12 No 3, 2012*

Fenty U Paluhulawa, etal. Legal Weak Protoction of Personal Data in the 4,0 Industrial Revolution Era, Jambura Law Review: (Volume 2 issue 02: 182-200, 2020).

Frans Maramis, *Hukum PIdana Umum dan Tertulis di Indonesia*, Jakarta, Raja Grafindo Persada, 2012

Hanafi, Mahrus*, Sisitem Pertanggung Jawaban Pidana*, Cetakan pertama, Jakarta, Rajawali Pers, 2015

I Made Agus Windara, Jurnal Hukum Kendala Dalam Penanggulangan Cybercrime Sebagai Suatu Tindak Pidana Khusus, Universitas Udayana, 2018

Irwansyah , Peneltian Hukum Pilhan Metode & Praktik Penulisan Artikel, Edisi Revisi, (Yogyakarta, Mitra Buana Media , 2021).

J. Remmelink, *Pengantar Hukum Pidana Material; Prolegomena dan Uraian Tentang Teori - Ajaran Dasar,* T ristam P. Moeliono (penerjemah), (Yogyakarta: Maharsa, 2014)

Johnny Ibrahim, Teori dan Metodologi Penelitian Hukum Normatif, (Malang Bayumedia)

Leden Marpaung, *Asas - Teori-Praktik Hukum Pidana,* cetakan ketujuh, (Jakarta: Sinar Grafika 2012)

Marchelino Cristian N, *Penerapan Asas Kekhususan Sistematis sebagai Limitasi antara Hukum Pidana dan Hukum Pidana Administrasi,* Jurnal Hukum Unsrat edisi No.10, Vol. 23 desember 2018.

Muhammad Prima , Jurnal Permasalahan Hukum dalam Menanggulangi Cyber Crime di Indonesia, UGM, 2017

Romli Atmasasmita. Beberapa Kelemahan UU Nomar 27/2022 tentang Perlindungan Data Pribadi. Diakses melalui: https://nasional.sindon.ws.com/read/923975/18/beberspa-kelsmahan-ma:nomor-272022-tentang-perlindungen-data-pribadi-1666815001

Rosalinda Elsina Latumahina, *Aspek Hukum Perlindungan Data Pribadi di Dunia Maya*, Jurnal Gema Aktualita, Edisi No. 2, Vol. 3, Desember 2014

Sekaring Ayumeida Kusnadi , Jurnal Hukum ,Perlindungan Hukum Data Pribadi Sebagai Hak Privasi, Universitas Wijaya Putra, 2021

Tim APJII, "Penetrasi dan Profil Perilaku Pengguna Internet Indoensia", *Buletin Asosiasi Penyelenggara Jasa internet Indonesia (APJII),* Edisi 40 Mei 2020.