



DOI: <https://doi.org/10.31933/unesrev.v6i4>

Received: 25 Juli 2024, Revised: 4 Agustus 2024, Publish: 8 Agustus 2024

<https://creativecommons.org/licenses/by/4.0/>

Pencegahan dan Penindakan Tindak Pidana Siber oleh Kepolisian Resort Teluk Bintuni

Duarif¹, Moh. Saleh²

¹ Magister Hukum, Universitas Narotama Surabaya, Indonesia

Email: arifduarif@gmail.com

² Magister Hukum, Universitas Narotama Surabaya, Indonesia

Email: saleh.nwa@gmail.com

Corresponding Author: arifduarif@gmail.com

Abstract: *Prevention and enforcement of cyber crimes by the Bintuni Bay Resort police. The problem in this study is how the form of prevention of cybercrime that has been done by the Bintuni Bay Resort police and how the form of action on cybercrime that has been done by the Bintuni Bay Resort police. The results of this research are: Prevention of cyber crime by the Bintuni Bay police state that in some actions in the Prevention of cyber crime is to do: a. Cyber patrol, b. Cyber education, c. Direct reprimand through social media, d. Direct action in the form of take down social media and e. Law enforcement. Action against cyber crime in Indonesia has established regulations regarding cyber crime in Law Number 19 of 2016 concerning amendments to Law Number 11 of 2008 concerning information and Electronic Transactions (hereinafter referred to as the ITE Law). The formulation of criminal acts in the ITE Law is regulated in Chapter VII: prohibited acts, which includes articles 27 to 37, while the threat of punishment is determined in Chapter XI: criminal provisions, which includes articles 45 to 52.*

Keyword: *Prevention, Action, Cyber Crime.*

Abstrak: Pencegahan dan penindakan tindak pidana siber oleh Kepolisian Resort Teluk Bintuni. Permasalahan dalam penelitian ini adalah bagaimana bentuk pencegahan atas tindak pidana siber yang telah dilakukan oleh Kepolisian Resor Teluk Bintuni dan bagaimana Apa bentuk penindakan atas tindak pidana siber yang telah dilakukan oleh Kepolisian Resor Teluk Bintuni. Hasil penelitian ini adalah: Pencegahan *cyber crime* oleh Polres Teluk Bintuni menyebutkan bahwa Pada beberapa tindakan yang di dalam melakukan pencegahan *cyber crime* adalah dengan melakukan: a. Patroli siber, b. Edukasi siber, c. Teguran langsung melalui medsos, d. Penindakan langsung berupa *take down medsos* dan e. Penegakan hukum. Penindakan terhadap tindak pidana siber di Indonesia telah membentuk peraturan mengenai kejahatan dalam dunia cyber pada Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (selanjutnya disebut UU ITE). Rumusan tindak pidana dalam UU ITE diatur dalam Bab VII: Perbuatan Yang Dilarang, yang mencakup Pasal 27 sampai Pasal 37,

sedangkan ancaman pidananya ditentukan dalam Bab XI: Ketentuan Pidana, yang mencakup Pasal 45 sampai dengan Pasal 52.

Kata Kunci: Pencegahan, Penindakan, Tindak Pidana Siber.

PENDAHULUAN

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 (UUD NRI 1945), Pasal 1 ayat (3) mengamanatkan bahwa negara Indonesia sebagai negara hukum. Menurut Kaelan, ciri dari negara hukum yaitu adanya pengakuan dan perlindungan hak-hak asasi, peradilan yang bebas dan bersih dari pengaruh lain, serta adanya kepastian hukum. Oleh karenanya, segala persoalan warga negara dan pemerintahannya harus didasarkan pada hukum yang berlaku agar terciptanya ketertiban dalam masyarakat. Penegakan hukum yaitu proses yang dilakukan agar tegak dan berfungsinya norma-norma hukum dalam kenyataan sebagai pedoman perilaku dalam lalu lintas atau hubungan hukum dalam kehidupan bermasyarakat dan bernegara. Hukum harus ditegakkan karena nilai-nilai keadilan yang terkandung di dalamnya sangat penting bagi kesejahteraan masyarakat.

Di era digital dewasa ini, masyarakat banyak diberikan berbagai informasi yang beraneka macam melalui teknologi yang semakin canggih. Contohnya dalam kemajuan teknologi informasi terutama pada bidang komputer dan internet. Teknologi informasi ini melibatkan beraneka macam jenis komputer dengan tipologi jaringan yang belum pernah diduga sebelumnya dalam perkembangan sejarah internet. Namun disisi lain ternyata dengan kemajuan Iptek ternyata membawa dampak negatif karena lewat perkembangan internet kejahatan-kejahatan versi baru pun banyak bermunculan salah satunya adalah cyber crime (teknologi informasi). Kemajuan teknologi informasi ini bagaikan dua sisi mata uang yang satu sisi memberikan manfaat untuk kemaslahatan umat dan sisi lainnya menghancurkan umat termasuk munculnya cyber crime prostitution (prostitusi online) dan lain sebagainya.

Kehidupan manusia dari masa ke masa mengalami perkembangan yang sangat pesat. Seiring dengan perkembangan kebutuhan masyarakat di dunia, teknologi informasi (*information technology*) memegang peran penting, baik di masa kini maupun di masa datang. Teknologi Informasi dapat memicu dan memacu perubahan tatanan kebutuhan kebutuhan hidup masyarakat di bidang sosial dan ekonomi, sebelumnya menuju transaksi ataupun sosialisasi secara elektronik. Di samping itu, perkembangan teknologi informasi telah menyebabkan dunia menjadi tanpa batas (*borderless*) dan menyebabkan perubahan sosial yang secara signifikan berlangsung demikian cepat. Teknologi informasi saat ini menjadi pedang bermata dua, karena selain memberikan kontribusi bagi peningkatan kesejahteraan, kemajuan dan peradaban manusia, sekaligus menjadi arena efektif perbuatan melawan hukum. Perkembangan jaringan internet memunculkan dampak negatif, sebagaimana dikemukakan oleh Roy Suryo, seorang pakar teknologi informasi, dalam penelitiannya menyatakan:

“Kejahatan *cyber (cyber crime)* kini marak di lima kota besar di Indonesia dan dalam taraf yang cukup memperhatikan serta yang dilakukan oleh para hacker yang rata-rata anak muda yang keliatannya kreatif, tetapi sesungguhnya mereka mencuri nomor kartu kredit melalui internet”. *Cyber crime* dibagi menjadi 2 kategori, yakni *cyber crime* dalam pengertian sempit dan dalam pengertian luas. *Cyber crime* dalam pengertian sempit adalah kejahatan terhadap sistem komputer, sedangkan *cyber crime* dalam arti luas mencakup kejahatan terhadap sistem atau jaringan komputer dan kejahatan yang menggunakan sarana komputer.

Kejahatan baru ini sangat berdampak pada berbagai aspek bidang kehidupan. Banyak yang menganggap bahwa keberadaan KUHP tidak mampu menjangkau kejahatan baru tersebut sehingga pemerintah menginisiasi lahirnya aturan tentang *cyber crime*. Pemerintah mengeluarkan atau menerbitkan Undang-Undang Tentang Informasi dan Transaksi

Elektronik (UU ITE), yaitu Undang-Undang Nomor 19 Tahun 2016 atas perubahan atas Undang-undang Nomor 11 Tahun 2008. Kesesuaian antara karakteristik pelaku *cyber crime* dengan paradigma pidana dalam pidana kerja sosial atau pidana pengawasan sehingga tujuan pidana akan dapat tercapai. Sejalan dengan pandangan Widodo, dalam mengantisipasi *cyber crime*, Rancangan Undang-Undang Kitab Hukum Pidana mencoba memperluas cakupan untuk dapat menjangkit kejahatan *cyber crime*. Sifat kejahatan *cyber crime* dapat diklasifikasikan sebagai berikut:

1. *Cyber crime* sebagai tindakan criminal

Cyber crime seperti yang dimaksud ialah sebuah tindak kejahatan yang dilakukan dengan konsep kriminalitas yang menggunakan internet sebagai wahana kejahatan. Misalnya carding: mencuri kode PIN ATM milik orang lain buat digunakan dalam transaksi online di internet, dan pemanfaatan media internet (*webserver, mailing list*) untuk mengedarkan alat-alat pembajakan. Pengirim *e-mail anonim* yang bermuatan iklan (*spamming*) juga dapat dicantumkan dalam contoh kejahatan yang memanfaatkan internet sebagai medianya dan dapat dituntut dengan tuduhan pelanggaran privasi.

2. *Cyber crime* sebagai kejahatan “abu-abu”

Kejahatan semacam itu di Internet termasuk dalam area “abu-abu”. Oleh karena itu, karena motif aktivitasnya terkadang bukan kejahatan, maka sulit untuk menentukan apakah perilaku tersebut merupakan kejahatan. Salah satu contohnya adalah *probing* atau *portscanning*. Ini adalah istilah yang digunakan untuk memantau sistem orang lain, dan disalahgunakan dengan mengumpulkan informasi sebanyak mungkin dari sistem.

Dibandingkan dengan kejahatan konvensional, *cyber crime* memiliki karakteristik yang unik yaitu : 1. Perbuatan yang dilakukan secara ilegal, tanpa hak atau tidak etis tersebut terjadi di ruang atau dunia maya, sehingga tidak mungkin untuk menentukan yurisdiksi hukum negara mana yang berlaku untuk tindakan tersebut. 2. Perbuatan tersebut dilakukan dengan menggunakan (perangkat) apapun yang dapat tersambung ke internet. 3. Kerugian material maupun non-material yang disebabkan oleh tindakan-tindakan ini seringkali lebih besar daripada kejahatan tradisional. 4. Pelakunya ialah orang yang dapat menguasai penggunaan internet dan aplikasinya. 5. Perbuatan tersebut acapkali dilakukan secara transnasional

Dari uraian maka diperlukan peran Kepolisian dalam mencegah tindak pidana siber dan menindak para pelaku tindak pidana siber, sesuai tugas dan fungsi Kepolisian dalam Undang-Undang No 2 Tahun 2002 Tentang Kepolisian, maka penulis tertarik untuk melakukan penelitian dengan judul “Pencegahan dan Penindakan Tindak Pidana Siber oleh Kepolisian Resor Teluk Bintuni”.

METODE

Metode pendekatan yang digunakan dalam penelitian ini adalah yuridis Normatif. Menurut Soerjono Soekanto pendekatan yuridis normatif yaitu penelitian hukum yang dilakukan dengan cara meneliti bahan pustaka atau data sekunder sebagai bahan dasar untuk diteliti dengan cara mengadakan penelusuran terhadap peraturan-peraturan dan literatur-literatur yang berkaitan dengan permasalahan yang diteliti.

Spesifikasi yang digunakan dalam penelitian ini adalah deskriptif analitis, yaitu menggambarkan yang jelas, rinci dan sistematis tentang objek yang diteliti. Analitis artinya data yang diperoleh akan dianalisis untuk pemecahan terhadap permasalahan sesuai dengan ketentuan hukum yang berlaku.

Metode pengumpulan data yang digunakan adalah studi kepustakaan (*library research*). Studi kepustakaan yaitu cara memperoleh data secara tidak langsung dari objek penelitian, yaitu dalam bentuk mempelajari literatur, peraturan perundang-undangan, bahan-bahan hukum lain yang ada hubungannya dengan masalah. Analisis data yang peneliti gunakan adalah deskriptif *kualitatif*. Analisis secara *kualitatif* dalam hal ini adalah upaya yang

dilakukan dengan jalan bekerja dengan data, mengorganisasikan data, memilah-milahnya menjadi satuan yang dapat dikelola, mensintesiskannya, mencari dan menemukan pola, menemukan apa yang penting dan apa yang dipelajari, dan memutuskan apa yang dapat diceritakan kepada orang lain.

HASIL DAN PEMBAHASAN

Pencegahan atas tindak pidana siber yang telah dilakukan oleh Kepolisian Resor Teluk Bintuni

Perkembangan teknologi yang begitu pesat akan menimbulkan pengaruh yang begitu besar terhadap aktivitas sehari-hari manusia. Tujuan utama adanya suatu kemajuan pada bidang teknologi dan industri adalah dapat dimanfaatkan oleh manusia, tetapi pada faktanya, terdapat dampak-dampak negative yang terjadi dengan adanya kemajuan teknologi. Dampak negatif yang ditimbulkan oleh adanya kemajuan teknologi tersebut adalah adanya kejahatan yang memanfaatkan kemampuan internet dan teknologi atau yang dikenal dengan kejahatan siber (*cyber crime*).

Cyber crime merupakan suatu tindak kejahatan yang menjadikan internet sebagai ruang atau tempat dalam melakukan kejahatan tersebut. Kejahatan-kejahatan tersebut mencakup kejahatan yang dilakukan melalui internet, kejahatan digital, dan kejahatan yang melibatkan jaringan telekomunikasi. Kejahatan yang termasuk ke dalam *cyber crime* masuk ke dalam ranah hukum pidana. Dalam Kitab Undang-Undang Hukum Pidana (selanjutnya disebut KUHP) berisikan ketentuan-ketentuan hukum yang berfungsi sebagai pelindung untuk masyarakat di berbagai kepentingan, salah satunya dalam ancaman kemajuan teknologi yaitu pada kejahatan siber atau *cyber crime*, seperti kasus-kasus pencurian data pribadi atau pembobolan saldo rekening korban. Terdapat beberapa faktor pemicu adanya kejahatan siber, yaitu sebagai berikut:

1. Kemajuan teknologi

Pelaku kejahatan siber mendapatkan begitu banyak kesempatan dalam melakukan aksi kejahatannya dikarenakan adanya kemajuan teknologi, dengan memanfaatkan eksistensi dari perangkat-perangkat yang terhubung ke internet, serta pelaku memiliki begitu banyak cara untuk mencuri data, merusak sistem, atau lainnya dengan adanya pemanfaatan teknologi informasi yang begitu banyak.

2. Keuntungan finansial

Terdapat dorongan finansial yang begitu besar bagi pelaku kejahatan siber dalam melakukan aksinya. Kegiatan seperti phishing akan membuahkan suatu keuntungan finansial dengan jumlah yang besar bagi pelaku.

3. Anonimitas

Terdapat satu alasan mengapa pelaku melakukan kejahatan siber yaitu dikarenakan adanya kemampuan dari pelaku untuk melakukan aksi kejahatannya secara anonim dengan menggunakan jaringan privat virtual atau yang biasa dikenal dengan VPN, atau dengan cara lainnya untuk menyembunyikan jejak mereka.

4. Kurangnya keamanan sistem

Masih kurang memadainya keamanan suatu sistem yang menyebabkan suatu kerentanan pada perangkat lunak atau pembaruan pada sistem sehingga dapat menjadi celah bagi para pelaku untuk melakukan perubahan dalam bentuk “pengrusakkan” pada sistem yang ia serang.

5. Faktor dari manusia itu sendiri

Pelaku kejahatan siber memanfaatkan rendahnya pengetahuan pengguna dalam memanfaatkan teknologi untuk dapat melakukan aksi kejahatannya seperti phishing.

Beberapa faktor penyebab terjadinya kejahatan siber, seperti adanya keterikatan (*commitment*), keterlibatan (*attachmeint*), keyakinan (*belief*), dan keterampilan (*invovement*), dengan penjelasan sebagai berikut:

1. Keterikatan (*commitment*)

Seseorang yang memiliki keterikatan pada sub sistem yang umum seperti yang terdapat di dalam organisasi, pekerjaan, sekolah, dan lainnya yang memiliki output dalam bentuk manfaat bagi banyak orang, seperti berupa benda, harta, reputasi, masa depan, dan lain sebagainya. Dengan adanya hasil dari keterikatan tersebut, seseorang akan terdorong untuk taat pada aturan yang berlaku.

2. Keterlibatan (*attachment*)

Keterlibatan adalah cara dari manusia untuk melibatkan dirinya sendiri terhadap orang lain, atau yang biasa kita lihat dalam kegiatan bersosialisasi atau tolong menolong antar manusia dalam pelaksanaannya, manusia melibatkan pikiran, perasaan, dan kehendak orang lain, sehingga dirinya menjadi lebih peka. Hubungan antara penyimpangan dengan “keterlibatan” yaitu sejauh apa seseorang tersebut dapat peka terhadap pikiran, perasaan, dan kehendak orang lain.

3. Keyakinan (*belief*)

Keyakinan dalam hal ini merupakan keyakinan atau seseorang terhadap nilai-nilai moral yang berlaku di lingkungannya yang akan menimbulkan ketaatan terhadap suatu norma.

4. Ketrampilan (*invovement*)

Jika seseorang aktif pada kegiatan-kegiatan positif di dalam suatu organisasi maka kecil kemungkinannya seseorang tersebut untuk melakukan penyimpangan atau deviasi.

Dari keempat elemen yang terdapat pada teori kontrol sosial tersebut, jika keempatnya tidak terpenuhi pada diri seseorang, maka dapat menjadi faktor seseorang melakukan tindak kejahatan siber karena seseorang tersebut tidak memiliki kepekaan terhadap pikiran, perasaan, dan kehendak orang lain, tidak memiliki keyakinan terhadap nilai moral sehingga dirinya tidak memiliki kepatuhan terhadap norma yang berlaku, dan orang tersebut tidak memiliki kegiatan positif yang membuat dirinya berpikir untuk mendapatkan keuntungan dari melakukan suatu kejahatan yang merugikan banyak orang.

Indonesia telah mengesahkan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, yang keduanya dikenal dengan UU ITE yang berperan sebagai payung hukum yang mengatur terkait ketentuan-ketentuan pemanfaatan teknologi di Indonesia. Kemudian kejahatan siber tersebut mencuri informasi pribadi korban, maka kasus tersebut juga dapat ditinjau melalui Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP).

Dalam rangka penanggulangan kejahatan termasuk penanggulangan kejahatan siber dapat dilakukan melalui 2 (dua) upaya yaitu upaya preventif dan upaya represif. Penanggulangan kejahatan merupakan tujuan dari sistem peradilan pidana. Tujuan sistem peradilan pidana merupakan sistem peradilan pidana (*criminal justice system*) merupakan suatu sistem yang terdiri dari Kepolisian, Kejaksaan, Pengadilan, dan Lembaga Pemasyarakatan yang bertujuan untuk melindungi dan menjaga ketertiban masyarakat, mengendalikan kejahatan, melakukan penangkapan, dan penahanan terhadap pelaku kejahatan, memberikan batasan bersalah atau tidaknya seseorang, memidana pelaku yang bersalah.

Upaya penanggulangan kejahatan melalui upaya pencegahan merupakan pilihan atau alternatif terbaik, upaya mencegah akan lebih baik dari pada penanggulangan melalui upaya *represif*. Kebijakan penal yang bersifat *represif*, namun sebenarnya juga mengandung unsur *preventif*, karena dengan adanya ancaman dan penjatuhan pidana terhadap delik diharapkan ada efek pencegahan/penangkalnya. Di samping itu, kebijakan penal tetap diperlukan dalam penanggulangan kejahatan, karena hukum pidana merupakan salah satu

sarana kebijakan sosial untuk menyalurkan ketidaksukaan masyarakat atau pencelaan/kebencian sosial.

Penanggulangan kejahatan melalui pendekatan penal akan memiliki fungsi sebagai upaya pencegahan apabila pengaturan pidana tersebut dapat mencegah sejauh mungkin terjadinya tindak pidana tersebut dalam hal ini adalah tindak pidana siber. Jadi, kriteria efektifitas dilihat dari seberapa jauh frekuensi kejahatan dapat ditekan. Dengan kata lain, kriterianya terletak pada seberapa jauh efek pencegahan umum dari pidana penjara dalam mencegah masyarakat pada umumnya untuk tidak melakukan kejahatan.

Bentuk pencegahan kejahatan yang dilakukan melalui sarana non penal. Pencegahan kejahatan melalui upaya non penal ini memiliki dimensi luas yang berusaha mencegah masuknya saran penal dalam penanggulangan pidana tersebut. Kebijakan saran non penal dalam penanggulangan tindak pidana ini merupakan upaya penanggulangan dengan menggunakan sarana di luar hukum pidana. Dengan demikian maka upaya penanggulangan kejahatan melalui sarana non penal ini merupakan tindakan pencegahan terhadap suatu tindak pidana yang memiliki sasaran utama adalah meneliti dan melihat berbagai kondisi sebelum tindak pidana itu terjadi. Faktor-faktor kondusif ini dalam hal kejahatan siber bertitik tolak dari kondisikondisi sosial masyarakat dan perkembangan teknologi dalam masyarakat yang secara langsung maupun tidak langsung berhubungan dan bahkan sebagai faktor utama berkembangnya kejahatan siber ini dalam masyarakat. Upaya-upaya non penal melalui faktor-faktor kondusif penyebab tindak pidana siber ini menduduki posisi strategis dalam penanggulangan kejahatan siber.

Adapun hal yang dilakukan aparat penegak hukum sebagaimana yang dijelaskan oleh anggota Reskrim Polres Teluk Bintuni menyebutkan bahwa ada beberapa tindakan yang dilakukan dalam pencegahan *cyber crime* oleh Polres Teluk Bintuni menyebutkan bahwa ada beberapa tindakan yang di dalam melakukan pencegahan *cyber crime* adalah dengan melakukan:

1. Patroli siber

Patroli siber adalah patroli yang dilakukan di dalam kepolisian dalam pelaksanaannya patroli siber bertujuan untuk mengawasi segala macam bentuk pelanggaran terhadap hukum di dalam internet terkhusus aplikasi media sosial, patroli siber sendiri biasanya dilakukan pada aplikasi seperti instagram, whatsapp, twitter. Patroli siber dilakukan untuk menciptakan ruang internet yang aman serta melindungi masyarakat dari kejahatan. Patroli siber dilakukan di kantor dengan menggunakan sarana dan prasarana berupa laptop atau PC (Personal Computer) dan pada waktu-waktu tertentu saat personil sedang di lapangan tetap melakukan patroli siber dengan menggunakan smartphone. Patroli siber selalu dilaksanakan setiap hari selama proses patroli selain memberikan himbuan proses patroli juga melakukan teguran terhadap perilaku buruk di media sosial bahkan sampai dibuatkan laporan ke Kemenkominfo.

2. Edukasi siber

Edukasi siber sendiri pada dasarnya adalah sebuah pengenalan akan *cyber crime* dan bahayanya. Edukasi siber lebih lagi ditujukan untuk memberikan manfaat informasi tentang *cyber crime* keseluruhan baik, bahayanya, jenis-jenisnya, modusnya serta hukuman akan kejahatan tersebut.

3. Teguran langsung melalui medsos

Teguran langsung merupakan bentuk lanjutan dari patroli siber teguran langsung diharapkan untuk membuat peringatan akan pelanggaran yang dilakukan oleh masyarakat pada media sosial ataupun internet. Teguran langsung yang Polres Teluk Bintuni sendiri bekerja sama dengan Kemenkominfo untuk melakukan tindakan pencegahan hal-hal yang mendapat teguran berupa konten yang bersifat provokasi, sara, ataupun pornografi.

4. Penindakan langsung berupa *take down medsos*

Take down merupakan salah satu strategi dari lima bentuk pencegahan yang dilakukan oleh Polres Teluk Bintuni dalam mencegah *cyber crime*, *take down* sendiri jika dijelaskan adalah suatu tindakan untuk menghentikan ataupun menghapus ketersediaan sesuatu yang berada dalam ruang internet seperti video, website, berita ataupun aplikasi yang kurang baik, seperti melanggar etika, moral dan kesopanan serta hukum.

5. Penegakan hukum.

Penegakan hukum merupakan salah satu bentuk pencegahan, tindakan represif sendiri diperlukan untuk memberi efek jera. Penegakan hukum dilakukan Polres Teluk Bintuni sebagai upaya terakhir dalam tindakan pencegahan pidana yang dilakukan oleh Polres Teluk Bintuni. Tindakan represif merupakan upaya penanggulangan dengan menggunakan sarana penal, yang dilakukan melalui proses hukum sebagaimana yang diatur dalam ketentuan peraturan perundang-undangan terkait seperti UU ITE, KUHP, UU Pornografi dan sebagainya. Sebagaimana diuraikan pada bagian terdahulu kejahatan siber sampai saat ini yang terbanyak merupakan tindak pidana siber yang berkenaan dengan perbuatan-perbuatan lama yang telah diatur dalam peraturan lainnya tetapi dalam pelaksanaan perbuatannya menggunakan sarana komputer, internet maupun teknologi informasi lainnya. Sehingga dalam upaya penanggulangan represif ini selalin menggunakan sarana hukum pidana UU ITE tetapi juga tidak terlepas dari penggunaan peraturan perundang-undangan lainnya.

Bentuk penindakan atas tindak pidana siber yang telah dilakukan oleh Kepolisian Resor Teluk Bintuni

Sanksi pidana, seperti hukuman penjara, denda, atau tindakan hukum lainnya, tidak hanya berfungsi sebagai bentuk hukuman terhadap individu atau kelompok yang terlibat dalam kejahatan siber, tetapi juga sebagai alat pencegahan. Ancaman sanksi pidana yang serius dapat menjadi faktor penghalang bagi para pelaku kejahatan, memberikan pesan bahwa kegiatan kejahatan siber tidak akan dibiarkan tanpa konsekuensi hukum. Oleh karena itu, dalam konteks keamanan siber, penerapan sanksi pidana tidak hanya merupakan respons terhadap kejahatan yang telah terjadi, tetapi juga menjadi strategi proaktif dalam upaya mencegah dan mengurangi potensi kejahatan di masa depan.

Penerapan sanksi pidana yang efektif, diharapkan dapat diciptakan lingkungan hukum yang memadai untuk melindungi informasi sensitif, menjaga stabilitas infrastruktur digital, dan memitigasi dampak yang merugikan akibat kejahatan siber. Dengan kata lain, sanksi pidana bukan hanya merupakan instrumen penegakan hukum, tetapi juga elemen kunci dalam strategi holistik untuk melindungi masyarakat dari ancaman yang semakin rumit dan canggih di dunia maya.

Faktor penghambat penanggulangan tindak pidana siber dibagimenjadi dua, yaitu:

1. Faktor Internal; Penegak hukum antara lain mencakup hakim, polisi, jaksa, pembela, petugas masyarakatan, dan seterusnya. Apabila peraturan perundang-undangan sudah baik, akan tetapi jika mental penegak hukum kurang baik, maka akan terjadi pada sistem penegakan hukum.
2. Faktor eksternal
 - a. Faktor masyarakat

Faktor masyarakat sampai saat ini, kesadaran hukum masyarakat untuk melakukan pengamanan dan merespon aktivitas *cyber crime* masih dirasakan kurang. Hal ini disebabkan antara lain oleh kurangnya pemahaman dan pengetahuan (*lack of information*) masyarakat terhadap jenis kejahatan *cyber crime*. *Lack of information* ini menyebabkan upaya penanggulangan *cyber crime* mengalami kendala, dalam hal ini kendala yang berkenaan dengan penataan hukum dan proses pengawasan (*controlling*) masyarakat terhadap setiap aktivitas yang diduga berkaitan dengan *cyber crime*

b. Faktor budaya

Berkaitan dengan budaya hukum sebagai faktor dalam penegakan hukum dalam hal ini mengenai efektifitas penegakan hukum terhadap pengguna media sosial, maka ada beberapa hal yang ditemukan, antara lain: 1) Mengetahui setelah peraturan perundang-undangan disahkan, maka sejak saat itulah masyarakat dianggap mengetahui adanya suatu aturan hukum, akan tetapi pada kenyataannya masyarakat masih banyak yang belum mengetahui Undang-Undang Informasi dan Transaksi Elektronik. 2) Memahami masyarakat tidak cukup hanya mengetahui aturan, akan tetapi juga harus memahami isi dari aturan tersebut, seperti tujuan dan manfaat dikeluarkannya peraturan tersebut. 3) Menaati setelah mengetahui dan memahami, masyarakat diharapkan mampu mewujudkan pemahaman tersebut melalui perilaku berupa ketaatan dalam berperilaku dalam penggunaan media elektronik.

c. Faktor sarana dan fasilitas

Faktor sarana dan fasilitas yang mendukung kalau peraturan perundang-undangan sudah baik dan juga mentalitas penegaknya baik, akan tetapi fasilitas kurang memadai, maka penegakan hukum tidak akan berjalan dengan semestinya

Terkait dengan solusi atau upaya kepolisian dalam mencegah tindak pidana siber, antara lain: 1. Melakukan langkah-langkah untuk membuat peka warga masyarakat, aparat penegak hukum, dan pengadilan, terhadap pentingnya pencegahan kejahatan yang berhubungan dengan computer dan khususnya internet maupun *cyber crime*. 2. Melakukan upaya-upaya pelatihan bagi para penegak hukum khususnya kepolisian, mengenai kejahatan dibidang ekonomi dan *cyber crime*. 3. Mengambil langkah-langkah yang tepat untuk menjamin bahwa personil penegak hukum yang terlatih dan dilengkapi cukup jumlahnya untuk menjalankan tugas memerangi tindak pidana siber. 4. Mengembangkan dan menggunakan standar forensik yang cocok guna mendapatkan dan membuktikan keaslian data elektronik yang digunakan untuk penyidikan dan penuntutan khususnya tindak pidana siber.

Cyber crime merupakan salah satu kejahatan serius meskipun kelihatan tidak tampak tetapi kerugian materil maupun moril sangat bisa dirasakan oleh para korban. Ini merupakan salah satu kejahatan yang memungkinkan dilakukan oleh orang yang berada di luar yudiksi hukum atau bisa dilakukan lintas negara. Kejahatan dalam dunia maya atau *cyber crime* terjadi begitu banyak belakangan ini disertai dengan berbagai dinamika persoalan yang terjadi dan juga sulit untuk diatasi ataupun diselesaikan secara tindak pidana.

Tindakan *preventif* dalam kejahatan merupakan tindakan yang mengharapakan sesuatu itu dapat ditanggulangi dan dicegah sebelum kejahatan itu terjadi dalam hal yang lain mengharapakan terjadinya penurunan dari kejahatan tersebut atau kejahatan tersebut dapat dihilangkan. Tujuan dari tindakan *prevetif* seperti pencegahan ini tidak lain tidak bukan seperti yang tertulis dalam Tugas dan wewenang Polri tertulis di dalam Undang-Undang Nomor 2 Tahun 2002 tentang Kepolisian Republik Indonesia.

Upaya Polres Teluk Bintuni dalam penindakan tindak pidana Cyber Di Wilayah Hukum Polres Teluk Bintuni yaitu: 1. Prosedur penanganan tindak pidana Cyber. 2. Beberapa tindak pidana cyber, dalam hal pelaporan bersifat delik aduan. untuk melakukan pelaporan bisa dilakukan melalui offline yaitu datang langsung ke Kantor Polres Teluk Bintuni dan bisa juga melalui online dengan membuka website Polres Teluk Bintuni.

Masyarakat umum bisa mengakses alamat website Polres Teluk Bintuni, dan ada beberapa langkah yaitu: a. Masuk ke beranda kemudian pilih layanan dan masuk aduan tindak pidana. b. Dalam aduan tindak pidana, pelapor diwajibkan mengisi laman formulir pengadu seperti data diri dari Nama, NIK, Jenis Kelamin, Tempat Lahir, Tanggal Lahir, Agama, pekerjaan, alamat, Kabupaten, Kecamatan, No Telp dan alamat email serta pengadu/pelapor mempersiapkan scan KTP yang nantinya juga diperlukan untuk diupload

kelengkapan data. c. Klik Next kemudian masuk ke Perkara yang diadakan; d. Dilanjutkan Konfirmasi Pengaduan.

Sebelum diberlakukan Undang-Undang ITE, aparat hukum menggunakan KUHP dalam menangani kasus-kasus kejahatan dunia cyber. Dalam ketentuan-ketentuanyang terdapat di KUHP tentang cyber crime masih bersifat global. Beberapa hal secara khusus diatur dalam KUHP dan disusun berdasarkan tingkat intensitas terjadinya kasus tersebut yaitu: 1. Ketentuan yang berkaitan dengan delik pencurian pada Pasal 362 KUHP; 2. Ketentuan yang berkaitan dengan perusakan/penghancuran barang terdapatdalam Pasal 406 KUHP; 3. Delik tentang pornografi terdapat dalam Pasal 282 KUHP; 4. Delik tentang penipuan terdapat dalam Pasal 378 KUHP; 5. Kejahatan terhadap ketertiban umum terdapat dalam Pasal 154 KUHP; 6. Delik tentang penghinaan terdapat dalam Pasal 311 KUHP; 7. Delik tentang pemalsuan surat terdapat dalam Pasal 263 KUHP; 8. Ketentuan tentang pembocoran rahasia terdapat dalam Pasal 112 KUHP, pasal113 KUHP, & pasal 114 KUHP; 9. Delik tentang perjudian terdapat dalam Pasal 303 KUHP.

Indonesia telah membentuk peraturan mengenai kejahatan dalam dunia cyber pada Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (selanjutnya disebut UU ITE). Rumusan tindak pidana dalam UU ITE diatur dalam Bab VII: Perbuatan Yang Dilarang, yang mencakup Pasal 27 sampai Pasal 37, sedangkan ancaman pidananya ditentukan dalam Bab XI: Ketentuan Pidana, yang mencakup Pasal 45 sampai dengan Pasal 52. Selain itu perbuatan-perbuatan yang merupakan cyber crime, sebagaimana dikemukakan sebelumnya, amat beranekaragam dan cukup rumit berkenaan dengan pembuktian menurut hukum acara pidana, sehingga memerlukan keterampilan dari Penyidik berkenaan dengan masalah-masalah komputer dan internet. Berdasarkan Undang-Undang Republik Indonesia Nomor 2 tahun 2002 tentang Kepolisian Negara Republik Indonesia pada pasal 13 yaitu fungsi kepolisian adalah salah satu fungsi pemerintahan negara di bidang pemeliharaan keamanan dan ketertiban masyarakat, penegakan hukum, pelindung, pengayom, dan pelayanan kepada masyarakat. Sehingga setiap bentuk kegiatan yang mengganggu keamanan dan ketertiban masyarakat menjadi tanggung jawab Polisi.

KESIMPULAN

Pencegahan *cyber crime* oleh Polres Teluk Bintuni menyebutkan bahwa Pada beberapa tindakan yang di dalam melakukan pencegahan *cyber crime* adalah dengan melakukan: a. Patroli siber, b. Edukasi siber, c. Teguran langsung melalui medsos, d. Penindakan lansung berupa *take down medsos* dan e. Penegakan hukum. Penindakan terhadap tindak pidana siber di Indonesia telah membentuk peraturan mengenai kejahatan dalam dunia cyber pada Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (selanjutnya disebut UU ITE). Rumusan tindak pidana dalam UU ITE diatur dalam Bab VII: Perbuatan Yang Dilarang, yang mencakup Pasal 27 sampai Pasal 37, sedangkan ancaman pidananya ditentukan dalam Bab XI: Ketentuan Pidana, yang mencakup Pasal 45 sampai dengan Pasal 52.

REFERENSI

- Abdul Wahid dan Mohammad Labib, *Kejahatan Mayantara (Cyber Crime)*, Refika Aditama, Jakarta, 2005
- Adami Chazawi. *Pelajaran Hukum Pidana 1*. PT Raja Grafindo Persada. Jakarta, 2005
- Asshiddiqie Jimly, Ali Safa'at M, *Teori Hans Kelsen Tentang Hukum*, Konpres, Jakarta, 2012
- Bambang Sunggono, *Metodologi Penelitian Hukum* (Jakarta: Raja Grafindo Persada, 2016)
- Barda Nawawi Arief, *Kebijakan Hukum Pidana*, PT. Citra Aditya Bakti, Bandung, 2002

- Budi Suhariyanto, *Tindak Pidana Teknologi Informasi (CyberCrime)*, Jakarta, PT. RajaGrafindo Persada, 2012
- Chainur Arrasjid, S.H., *Dasar-Dasar Ilmu Hukum*, Sinar Grafika, Jakarta, 2000
- Gibitiah. *Kejahatan Tindak Pidana Pembegalan (Analisis Perbandingan Kitab Undang-Undang Hukum Pidana Dan Hukum Jinayah)*, (Palembang: NoerFikri Offset berkerja sama dengan Fakultas Syariah dan Hukum UIN Raden Fatah, 2016)
- Henny April Yanti Bu'ulolo, Anggreini Atmei Lubis & Wenggedes French, *Studi Kebijakan Penanggulangan Kejahatan Cyber Crime dan Pencemaran Nama Baik di Ruang Siber (Kasus Direktorat Kriminal Khusus Subdit V Cyber Crime Polda Sumatera Utara)*, Journal of Education, Humaniora and Social Sciences (JEHSS) ISSN [2622-3740](https://doi.org/10.34007/jehss.v6i1.1832)(Online) Vol 6, No. 1, Agustus 2023: 532-542, DOI: 10.34007/jehss.v6i1.1832
- Iham fikriansyah - detikEdu *Pengertian Hukum Menurut Para Ahli Serta Bentuk dan Tujuannya"* selengkapnya, Minggu, 30 Apr 2023 12:32 WIB <https://www.detik.com/edu/detikpedia/d-6696943/pengertian-hukum-menurut-para-ahli-serta-bentuk-dan-tujuannya>.
- Lexi J. Moleong, *Metode Penelitian Kualitatif*, Remaja Rosdakarya, Bandung, 2007,
- Lilis Eka Lestari, *Penegakan dan perlindungan hak asasi manusia di Indonesia dalam konteks Implementasi Sila Kemanusiaan Yang Adil dan Beradab*, Lestari Faculty of Law, Universitas Negeri Semarang (UNNES), (Cetak) Vol. 5 No. 2, Agustus 2019
- Maskun, *Kejahatan Siber (Cyber Crime)*, Kencana, Jakarta, 2013
- Miftakhur Rokhman Habibi-Isnatul Liviani, *Kejahatan Teknologi Informasi (Cyber Crime) dan Penanggulangannya dalam Sistem Hukum Indonesia*, Al-Qānūn : Jurnal Pemikiran dan Pembaharuan Hukum Islam Vol. 23, No. 2, Desember 2020
- Moeljatno, *Asas-Asas Hukum Pidana*, PT Rineka Cipta, Jakarta, 2008
- Muhammad Anthony Aldriano, Mas Agus Priyambodo, *Cyber Crime Dalam Sudut Pandang Hukum Pidana*, Sekolah Tinggi Ilmu Hukum IBLAM, Jakarta Pusat, DKI Jakarta, Indonesia, Jurnal Kewarganegaraan Vol. 6 No. 1 Juni 2022
- Muhammad Anthony Aldriano, Mas Agus Priyambodo, *Cyber Crime Dalam Sudut Pandang Hukum Pidana*, Sekolah Tinggi Ilmu Hukum IBLAM, Jakarta Pusat, DKI Jakarta, Indonesia, Jurnal Kewarganegaraan Vol. 6 No. 1 Juni 2022
- Peter Mahmud Marzuki, *Penelitian Hukum*, Kencana, Jakarta, 2006
- pengertian hukum*, <https://fh.unikama.ac.id/id/2017/05/24/pengertian-hukum/>
- Pengertian Hukum: Tujuan, Fungsi, Unsur dan Macam* [Materi A-Z][https:// deepublishstore.com/blog/ materi/ pengertian-hukum/](https://deepublishstore.com/blog/materi/pengertian-hukum/)
- Sahat Maruli Tua Situmeang, Musa Darwin Pane, dan Wahyudi, *Optimalisasi Peran Penegak Hukum Dalam Menerapkan Pidana Kerja Sosial Dan Ganti Rugi Guna Mewujudkan Tujuan Pemidanaan Yang Berkeadilan*, Jurnal Hukum IUS QUIA IUSTUM NO. 3 VOL. 27 SEPTEMBER 2020: 501 - 525 Received: 1 Mei 2020; Accepted: 20 Oktober 2020 ; Published: 15 Desember 2020 [https:// doi.org/10.20885/iustum.vol27.iss3.art4](https://doi.org/10.20885/iustum.vol27.iss3.art4)
- Soerjono Soekanto & Sri Mamudji, *Penelitian Hukum Normatif (Suatu Tinjauan Singkat)*, Rajawali Pers, Jakarta, 2001
- Teguh Prastyo, *Hukum Pidana*, PT. Raja Grafindo Persada, jakarta, 2012
- Tri Andrisman, *Hukum Pidana*, Universitas Lampung, Bandar Lampung, 2011
- Undang-Undang No 2 Tahun 2002 Tentang Kepolisian
- Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik
- Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP).
- Wawan Muhwan Hairri, *Pengantar Ilmu Hukum*, Pustaka Setia, Bandung, 2012
- Zainal Asikin, *Pengantar Ilmu Hukum*, Rajawali Pers, Jakarta, 2011.