Locus Journal of Academic Literature Review
Volume 2 Issue 3, March 2023.
P-ISSN: 2829-4262, E-ISSN: 2829-3827

Penegakan Hukum *Cybercrime* di Wilayah Hukum Kepolisian Daerah Sumatera Utara

Ruth Gladys Sembiring[1], Madiasa Ablisar[2], Mahmud Mulyadi[3], Jelly Leviza[4].

[1.] Program Studi Magister Ilmu Hukum, Fakultas Hukum, Universitas Sumatera Utara.
E-mail: ruthgsembiring@gmail.com (CA)
[2.3.4.] Dosen Fakultas Hukum, Universitas Sumatera Utara.

Abstrak: Tujuan penelitian ini untuk menganalisis dan mengetahui tentang undang-undang No. 19 tahun 2016 tentang perubahan atas undang-undang No. 11 tahun 2008 tentang informasi dan transaksi elektronik telah secara akomodatif atau belum mengatur perbuatan-perbuatan pidana yang dikategorikan sebagai *cybercrime*; bentuk-bentuk *cybercrime* yang sering terjadi diwilayah polda sumatera utara; dan penegakan hukum *cybercrime* oleh pihak kepolisian diwilayah polda sumatera utara. Penelitian ini adalah penelitian hukum normatif dan didukung dengan penambahan data atau unsur empiris. Hasil penelitian ini dapat diketahui yaitu undang-undang No.19 Tahun 2016 tentang Informasi dan Transaksi Elektronik tentang perubahan atas Undang-Undang No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik yang cukup relatif akomodatif secara normatif dalam menjawab kebutuhan masyarakat dalam melakukan kegiatan di dunia c*yber*. Bentuk-Bentuk tindak *cybercrime* yang sering terjadi diwilayah Polda Sumatera utara ialah pencemaran nama baik, judi *online* serta konten asusila. Penegakan hukum oleh pihak kepolisian awalnya menerima laporan atau aduan terkait masalah tindak *cyber* selanjutnya melakukan penyidikan dalam menetapan status terlapor sebagai tersangka dalam penegakan hukum tindak *cybercrime* yang dilakukan setelah adanya bukti-bukti yang jelas serta dapat dihubungkan secara langsung dengan terlapor atau penindakan langsung.

Katakunci: *Cybercrime,* Kepolisian Daerah, Penegakan hukum.

Sitasi: Sembiring, R. G., Ablisar, M., Mulyadi, M., & Leviza, J. (2023). Penegakan Hukum Cybercrime di Wilayah Hukum Kepolisian Daerah Sumatera Utara . *Locus Journal of Academic Literature Review*, *2*(3), 292–304. https://doi.org/10.56128/ljoalr.v2i3.145

1. Pendahuluan

Kehadiran undang-undang terkait dengan pengaturan *CyberCrime* ini tentu saja sangat dibutuhkan dalam penegakan hukum pidana, terutama kejahatan-kejahatan yang memang lahir dari kehadiran teknologi tersebut. Pentingnya undang-undang ini didukung dengan kenyataan bahwa kejahatan di dunia maya banyak terjadi di Indonesia. Namun dalam pelaksanaan prakteknya, penegakan hukum pidana dengan UU ITE ini ternyata menimbulkan masalah hukum bagi orang-orang yang menggunakan sarana teknologi informasi untuk menyampaikan kritik terhadap pemerintah berupa jeratan hukum pidana. Hal tersebut di atas terjadi karena UU ITE

tidak saja mengatur masalah *CyberCrime* sebagaimana yang diatur dalam *convention on CyberCrime* , tetapi juga mengatur perbuatan pidana berupa penghinaan yang menggunakan media teknologi informasi. Beberapa contoh dikutip dari beberapa media, kasus *Cyber* crime yang pemah terjadi di Indonesia antara lain:

a. Tokopedia dilaporkan mengalami peretasan, bahkan jumlahnya diperkirakan 91 juta akun dan 7 juta akun merchant, tidak lagi 15 juta seperti diberitakan sebelumnya. Padahal di tahun 2019, Tokopedia mengungkapkan bahwa ada sekitar 91 juta akun aktif di platformnya. Artinya hampir semua akun di Tokopedia berhasil diambil datanya oleh peretas. Pelaku menjual data di darkweb berupa user ID, email, nama lengkap, tanggal lahir, jenis kelamin, nomor handphone dan password yang masih ter-hash atau tersandi. Semua dijual dengan harga US$5.000 atau sekitar Rp74 juta. Bahkan ada 14.999.896 akun Tokopedia yang datanya saat ini bisa didownload.
b. Website DPR Diretas: *Hacker* Ganti Nama Jadi Dewan Penghianat Rakyat. Peretasan situs DPR RI pada Kamis (8/10) ternyata bukan yang pertama di tahun 2020 ini. Aksi peretasan pada Juni 2020 lalu pernah membuat situs web DPR RI sempat tidak bisa diakses. Peretasan situs DPR RI pada Kamis lalu mengubah tampilan laman depan situs web milik lembaga tinggi negara dengan alamat dpr.go.id. Kepanjangan DPR berubah menjadi Dewan Pengkhianat Rakyat dari yang awalnya Dewan Perwakilan Rakyat Republik Indonesia. Saat ini, Jumat (9/10/2020), kepanjangan DPR RI di situsnya telah kembali dan bisa diakses seperti semula. Peretasan situs DPR RI menjadi Dewan Pengkhianat Rakyat mendapat perhatian warganet.
c. Kasus indra kenz, Kasus investasi bodong aplikasi Binomo yang melibatkan influencer atau pemengaruh masih terus dikembangkan kepolisian. Pada 24 Februari 2022, Bareskrim Polri telah mentapkan Indra Kusuma atau Indra Kenz sebagai tersangka. Indra Kenz merupakan influencer yang menjadi afiliator atau pihak ketiga yang mempromosikan aplikasi Binomo. Polisi menjerat Indra Kenz dengan berbagai pasal dari Undang-Undang Informasi dan Transaksi Elektronik (ITE) dan Tindak Pidana Pencucian Uang (TPPU) dengan ancaman 20 tahun hukuman penjara. aparat mengatakan bisa menelusuri lingkaran penipuan dan TPPU ini dengan memaksimalkan keahlian tim *Cyber* crime dan bantuan Pusat Pelaporan dan Analisis Transaksi Keuangan (PPATK).
d. Kasus bobolnya sistem komputer di Mabes Polri pada tahun 1999. Ketika itu, apabila komputer diaktifkan maka yang muncul adalah gambar porno;
e. Data Mabes Polri selama tahun 2002 terdapat 23 kasus *Cyber* crime di Indonesia, terdiri atas 15 kasus *Cyber* crime yang menjadikan teknologi informasi sebagai sarana (misalnya credt cardfiaud, stock exhange fiaud, banking fiaud, child pornography dun drug tarfJking;) dan 8 kasus *Cyber* crime yang menjadikan teknologi informasi sebagai sasaran (misalnya Denial of Sewice Attack, defacing, dun cracking).
f. Kasus Deni Firmansyah, merusak jaringan IT KPU dan berhasil menempus IP tnp.kpu.go.id yang mengubah hasil perolehan suara dengan cara jumlah perolehan suara dikalikan 10 namun tidak berhasil, kasus ini terjadi di warna warnet di jalan Kaliurang, Yogjakarta pada hari Jumat dan Sabtu tanggal 16 dan 17 April 2004,

kemudian tanggal 22 April 2004, Dani Firmasyah berhasil ditangkap oleh Satuan *Cyber* Crime Distreskrimsus Polda Metro.

g. Kasus pembobolan sibs resmi Presiden RI yang terjadi pada hari Minggu, tanggal 17 Maret 2007 pukul 05.30 Wib, situs resmi Presiden Susilo Bambang Yudhoyono (www presidensby.info). dibobol hacker. Halaman utama situs yang dikelola juru bicara Kepresidenan Andi Mallarangeng itu berubah tampilannya menjadi surat tuntutan yang ditujukan kepada SBY. Pengirim surat mengatasnamakan on behalf undergroud community dun beralamat di the word where the devils gather. Komunitas tersebut mengeluarkan tiga tuntutan pertama meminta penurunan harga bandwith, agar masyarakat bisa menikrnati internet, kedua, meminta SBY mendukung dan melaksanakan IGOS (lndonesia Go Open Source) dan yang ketiga, Menuntut pemberantasan korupsi, kolusi, dan nepotisme (KNN), pornografi dan porno ak~i).~ dan masih banyak lagi kasus-kasus lainnya.

Melihat fenomena serta sejumlah pendapat di atas, tidak dapat dipungkiri bahwa *CyberCrime* semakin menuntut perhatian yang lebih luas dari aparat hukum dan pembuat UU, agar peluang kerugian yang ditimbukan oleh adanya pemanfaatan teknologi informasi yang tidak semestinya, dibutuhkan perangkat peraturan dan perundangan yang membatasi sekaligus menghukum penggunaan teknologi informasi untuk kejahatan, karena *CyberCrime* apapun bentuknya tergolong tindakan kejahatan yang harus dihukum. Sebagai salah satu aparat penegak hukum dalam sistem peradilan pidana yang diberi wewenang oleh undang-undang, polisi harus siap menghadapi jenis kejahatan di bidang teknologi informasi. Polisi berwenang melakukan penyelidikan dan penyidikan terhadap peristiwa kejahatan di bidang teknologi informasi. Pasal 42 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik menegaskan bahwa penyidikan terhadap tindak pidana di bidang teknologi informasi dilakukan berdasarkan ketentuan dalam hukum acara pidana (Raharjo, 2002).

Upaya penanggulangan terhadap tindak pidana teknologi informasi tersebut ditangani oleh satu unit khusus di Badan Reserse Kriminal (BARESKRIM) MABES POLRI yaitu Direktorat II Ekonomi dan Khusus Unit V IT dan *Cyber* crime dan juga unit penanggulangan *Cyber* crime di beberapa Kepolisian Daerah (Polda). Beberapa Kepolisian daerah seperti Sumatera Utara, Jawa Timur, Jawa Tengah, Bali, dan DIY telah membentuk suatu unit khusus di bidang teknologi informasi. Pembentukan unit tersebut bertujuan untuk melakukan penanggulangan dan penanganan kejahatan teknologi informasi. Pembentukan unit-unit tersebut diharapkan dapat menanggulangi tindak pidana yang berbasis teknologi informasi di daerah Provinsi.

Direktorat Reserse kriminal khusus Kepolisian Daerah Sumatera Utara sebagai institusi penegak hukum mempunyai peran yang sangat besar dalam penegakan hukum, khususnya penegakan hukum terhadap tindak pidana *CyberCrime* melalui media sosial, yang biasanya ditangani oleh Subdit V/*Cyber* Crime. Data tindak pidana ujaran kebencian (hatespeech) pada Ditreskrimsus Polda Sumut dari tahun 2018 – 2021.

Berdasarkan penjelasan tersebut diatas, penelitian ini penting untuk dilakukan karena pertama, *CyberCrime* adalah kejahatan yang kian meningkat tiap tahunnya dan semakin luas terjadi. Kedua, penegakan hukum terhadap *CyberCrime* perlu dilakukan

agar masyarakat tidak merasa dirugikan karena aktivitas *CyberCrime* yang dapat dikategorikan sebagai tindak pidana. Ketiga, karena kejahatan *CyberCrime* dalam wilayah Polda Sumatera Utara menjadi salah satu tempat dalam penegakan hukum atas kejahatan tindak *Cybercrime*.

2. Metode Penelitian

Penelitian ini adalah penelitian hukum normatif dan didukung dengan penambahan data atau unsur empiris. Sifat penelitian ini deskriptif analitis. Sumber data yang digunakan adalah data primer dan data sekunder. Data primer didapat dengan cara observasi dan wawancara langsung sumber literatur utama yang berkaitan langsung dengan obyek penelitian di Polda Sumatera Utara, sedangkan data sekunder data yang menunjang dan mendukung data primer yang diperoleh dari bahan-bahan pustaka yang terdiri dari bahan hukum primer, bahan hukum sekunder, dan bahan hukum tersier. Data tersebut didapat melalui teknik studi kepustakaan dan studi lapangan. Setelah pengumpulan data dilakukan selanjutnya data tersebut dianalisis secara kualitatif dan pada akhirnya menarik kesimpulan secara deduktif yang kemudian menginterpretasikannya dalam bentuk deskriptif atau dengan kata-kata yang informatif dan argumentatif.

3. Hasil dan Pembahasan

3.1 Pengaturan Cybercrime dalam Undang-Undang No. 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik

Sejak 21 April 2008, bangsa Indonesia memasuki babak baru dalam pengaturan mengenai penggunaan teknologi informasi dan transaksi elektronik yaitu adanya pengesahan Rancangan Undang-Undang Tentang Informasi dan Transaksi Elektronik yang kemudian diundangkan menjadi Undang-Undang Negara Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (LN Republik Indonesia Tahun 2008 Nomor 58; TLN Republik Indonesia Nomor 4843). Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (selanjutnya disingkat UU-ITE) merupakan undang-undang pertama di Indonesia yang secara khusus mengatur tindak pidana siber, undang-undang ini memiliki sejarah tersendiri dalam pembentukan dan pengundangannya. Rancangan UU-ITE mulai dibahas sejak Maret 2003 oleh Kementrian Negara Komunikasi dan Informatika dengan nama Rancangan Undang-Undang Informasi Komunikasi dan Transaksi Elektronik (Sitompul, 2012).

Pada awalnya, RUU ini merupakan penyatuan dua rancangan undang-undang yang disusun oleh dua kementrian yaitu Departemen Perhubungan dengan Departemen Perindustrian dan Perdagangan, bekerja sama dengan Lembaga Kajian Hukum dan Teknologi Universitas Indonesia, Tim dari Fakultas Hukum Universitas Padjajaran, serta Tim Asistensi dari Institut Teknologi Bandung. Kemudian, berdasarkan surat Presiden RI. No. R. /70/Pres/9/2005 tanggal 5 September 2005, naskah UU-ITE secara resmi disampaikan kepada DPR RI. Pada tanggal 21 April 2008, undang-undang ini disahkan; dengan demikian proses pengundangan UU-ITE telah berlangsung sekitar lima tahun.

Oleh karena itu, UU-ITE terdiri dari 13 Bab dan 54 Pasal ini merupakan undang-undang yang relatif baru baik dari segi pengundangannya dan juga segi materi yang diatur. Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik tersebut multak diperlukan bagi negara Indonesia, karena saat ini Indonesia merupakan slah satu negara yang telah menggunakan dan memanfaatkan teknologi informasi secara luas dan efisien, dan secara faktual belum banyak memiliki ketentuan hukum terutama dari aspek hukum pidana (Sitompul, 2012).

Undang-Undang Informasi dan Transaksi Elektronik atau UU ITE merupakan *Cyber*law pertama di Indonesia yang mengatur secara khusus tentang informasi dan transaksi elektronik. Materi UU ITE dapat dikelompokkan menjadi dua bagian besar yaitu pengaturan informasi dan transaksi elektronik dan pengaturan mengenai perbuatan yang dilarang (*CyberCrime*). Ketentuan *CyberCrime* yang merupakan instrumen internasional yang digunakan oleh banyak negara. Dua muatan besar yang diatur dalam UU-ITE ialah mengenai pengaturan transaksi elektronik dan mengenai tindak pidana *Cyber*. Materi UU-ITE tersebut merupakan implementasi dari beberapa prinsip ketentuan internasional, cakupan materi UU-ITE, secara umum antara lain berisi tentang informasi dan dokumen elektronik, pengiriman dan penerimaan surat elektronik, tanda tangan elektronik, sertifikat elektronik, penyelenggaraan sistem elektronik, transaksi elektronik, hak atas kekayaan intelektual dan privasi, serta ketentuan pidana yang berkaitan dengan pemanfaatan informasi dan transaksi elektronik.

Undang-undang Nomor 19 Tahun 2016 tentang Perubahan Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik merupakan bentuk dari perubahan Undang- undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik. Namun terkait dengan bentuk-bentuk dari tindak pidana *CyberCrime* yang diatur tidak ada perubahan, sehingga segala bentuk tindak pidana masih sama halnya dengan yang diatur dalam Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik.

Indonesia tidak memiliki definisi hukum untuk kejahatan *Cyber*. Sebenarnya, Undang-Undang Nomor 11 Tahun 2008 sebagai amandemen dengan Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE) adalah pengertian dari apa yang dimaksud dengan *CyberCrime* tersebut. Dalam UU ITE terdapat kejahatan yang menargetkan internet, komputer, dan teknologi terkait. Di bawah Undang-Undang Informasi dan Transaksi Elektronik, ada tujuh jenis kejahatan yang diklasifikasikan sebagai kejahatan yang menargetkan internet, komputer, dan teknologi terkait. Kejahatan-kejahatan tersebut dianggap sebagai kejahatan kontemporer yang menghasilkan bentuk kejahatan baru (Tobing & Tobing, 2012).

Tabel 1.
Jenis Kejahatan Cyber Yang Menargetkan Internet dan Sejenisnya

Jenis Kejahatan	**Ketentuan dalam UU ITE**
Meretas (*Hacking*)	Pasal 30
Intersepsi ilegal	Pasal 31 Ayat (1) dan Pasal 31 Ayat (2)
Mengotori (*Defacing*)	Pasal 32
Pencurian Elektonik	Pasal 32 ayat (2)
Interference	Pasal 33
Memfasilitasi tindak pidana terlarang	Pasal 34
Pencuri Identitas Identitas	Pasal 35

Sumber: Undang-Undang No. 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.

Selanjutnya dalam UU ITE terdapat konten ilegal dengan menggunakan internet, komputer dan teknologi terkait untuk melakukan kejahatan. Di bawah UU ITE, ada tujuh jenis kejahatan yang diklasifikasikan sebagai kejahatan yang menargetkan internet, komputer, dan teknologi terkait. Kejahatan ini terkait dengan publikasi dan distribusi konten ilegal. Tidak seperti kejatan yang menargetkan internet yang menganggap bentuk kejahatan baru, tindak pidan aini dianggap sebagai kejahatan lama, tetapi perkembangan teknologi telah menciptakan media baru untuk memberikan kebebasan berekspresi. Oleh karena itu, legislator mengatur ulang kejahatan dalam Undang-Undang Informasi dan Transaksi Elektronik. Sebenarnya, semua jenis kejahatan ini sudah diatur dalam tindakan kriminal lainnya namun seiring dengan berkembangnya teknologi maka pemerintah membuat suatu aturan untuk mengatur tindak pidana tersebut.

Tabel 2.
Beberapa Jenis Tindak Pidana Konvensional yang Terjadi Dalam Ranah Digital Bertransformasi Menjadi CyberCrime

Jenis Perbuatan *Cyber*	**Ketentuan dalam UU ITE**	**Ketentuan dalam Undang-Undang Lainnya**
Pornografi	Pasal 27 Ayat (1)	Undang-Undang No. 44 Tahun 2008 tentang Pornografi dan Kitab Undang-Undang Hukum Pidana (KUHP)
Judi	Pasal 27 Ayat (2)	KUHP
Fitnah	Pasal 27 Ayat (3)	KUHP
Pemerasan	Pasal 27 Ayat (4)	KUHP
Tipuan yang membahayakan konsumen	Pasal 28 Ayat ayat (1)	Undang-Undang No. 8 Tahun 1999 tentang Perlindungan Konsumen

Ujaran kebencian	Pasal 28 Ayat (2)	KUHP
Ancaman kekerasan terhadap orang lain	Pasal 29	KUHP

Sumber : Undang-Undang No. 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik

Perspektif yuridis, khususnya dalam ruang lingkup hukum pidana, banyak terobosan yang penting dalam UU-ITE tersebut, antara lain sebagai berikut

a. Penegasan secara cermat beberapa istilah yang berkaitan dengan dunia mayantara, misalnya pengertian komputer, data, transaksi elektronik, dan lain-lain;
b. Tindak pidana yang diatur banyak yang sudah merujuk pada ketentuan yang diatur dalam Conventionon *CyberCrime*, baik tindak pidana yang menjadikan komputer sebagai sasaran maupun menggunakan komputer sebagai alat kejahatan;
c. Beberapa kejahatan tradisional yang menggunakan komputer, misalnya perjudian, pornografi, perbuatan tidak menyenangkan, pencemaran nama baik, penghinaan dan lain-lain yang sudah dijadikan tindak pidana;
d. Ancaman bagi setiap orang yang melakukan tindak pidana berupa jenis pidana (*strafsourt*) menggunakan sistem ancaman kumulatif-alternatif, dan lama pemidanaan atau besarnya ancaman denda (strafmaad) cukup tinggi dibandingkan dengan ancaman dalam hukum pidana konvensional;
e. Tanda tangan elektronik (digital signature) diakui sebgai alat bukti yang memiliki kekuatan hukum yang sama dengan tanda tangan konvensional yang menggunakan tinta basah dan bermaterai. Surat elektronik (e-mail), website, dan perangkat-perangkat virtual lainnya sudah diakui sebagai alat bukti yang sah sehingga dapat digunakan sebgai alat bukti yang sah dalam proses peradilan pidana, selain sebagaimana diatur dalam Pasal 184 KUHAP;
f. Ruang lingkup keberlakuan UU-ITE adalah untuk setiap orang yang melakukan perbuatan hukum di wilayah Indonesia maupun di luar negeri yang memiliki akibat hukum di Indonesia (Sjafitri, n.d)

Revisi Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) resmi berlaku usai melewati 30 hari sejak disahkan menjadi UU pada 27 Oktober 2016. Menurut Indriani (2016), ada beberapa perubahan di UU ITE yang baru yaitu sebagai berikut:

a. Untuk menghindari multitafsir terhadap ketentuan larangan mendistribusikan, mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik bermuatan penghinaan dan/atau pencemaran nama baik pada ketentuan Pasal 27 ayat (3), dilakukan 3 (tiga) perubahan sebagai berikut: Pertama, menambahkan penjelasan atas istilah "mendistribusikan, mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik". Mendistribusikan adalah mengirimkan dan/atau menyebarkan Informasi Elektronik dan/atau Dokumen Eletronik kepada banyak orang atau berbagai pihak melalui Sistem Elektronik. Mentransmisikan adalah mengirimkan Informasi Elektronik dan/atau Dokumen Eletronik yang ditujukan kepada satu pihak lain melalui Sistem Elektronik. Membuat dapat

diakses adalah semua perbuatan lain selain mendistribusikan dan mentransmisikan melalui Sistem Elektronik yang menyebabkan Informasi Elektronik dan/atau Dokumen Elektronik dapat diketahui pihak lain atau publik.

b. Menegaskan bahwa ketentuan tersebut adalah delik aduan bukan delik umum.
c. Menegaskan bahwa unsur pidana pada ketentuan tersebut mengacu pada ketentuan pencemaran nama baik dan fitnah yang diatur dalam KUHP.
d. Menurunkan ancaman pidana pada 2 (dua) ketentuan pada pasal 29 sebagai berikut: Pertama, ancaman pidana penghinaan dan/atau pencemaran nama baik diturunkan dari pidana penjara paling lama 6 (enam) tahun menjadi paling lama 4 (tahun) dan/atau denda dari paling banyak Rp 1 miliar menjadi paling banyak Rp 750 juta. Kedua, ancaman pidana pengiriman informasi elektronik berisi ancaman kekerasan atau menakut-nakuti dari pidana penjara paling lama 12 (dua belas) tahun menjadi paling lama 4 (empat) tahun dan/atau denda dari paling banyak Rp 2 miliar menjadi paling banyak Rp 750 juta. Ketiga, melaksanakan putusan Mahkamah Konstitusi terhadap 2 (dua) ketentuan sebagai berikut:
e. Mengubah ketentuan Pasal 31 ayat (4) yang semula mengamanatkan pengaturan tata cara intersepsi atau penyadapan dalam Peraturan Pemerintah menjadi dalam Undang-Undang.
f. Menambahkan penjelasan pada ketentuan Pasal 5 ayat (1) dan ayat (2) mengenai keberadaan Informasi Elektronik dan/atau Dokumen Elektronik sebagai alat bukti hukum yang sah.
g. Melakukan sinkronisasi ketentuan hukum acara pada Pasal 43 ayat (5) dan ayat (6) dengan ketentuan hukum acara pada KUHAP, yaitu : Pertama, penggeledahan dan/atau penyitaan yang semula harus mendapatkan izin Ketua Pengadilan Negeri setempat, disesuaikan kembali dengan ketentuan KUHAP. Kedua, penangkapan penahanan yang semula harus meminta penetapan Ketua Pengadilan Negeri setempat dalam waktu 1×24 jam, disesuaikan kembali dengan ketentuan KUHAP.
h. Memperkuat peran Penyidik Pegawai Negeri Sipil (PPNS) dalam UU ITE pada ketentuan Pasal 43 ayat (5) terkait kewenangan membatasi atau memutuskan akses terkait dengan tindak pidana teknologi informasi dan kewenangan meminta informasi dari Penyelenggara Sistem Elektronik terkait tindak pidana teknologi informasi.
i. Menambahkan ketentuan mengenai "*righttobeforgotten*" atau "hak untuk dilupakan" pada ketentuan Pasal 26, yaitu setiap Penyelenggara Sistem Elektronik wajib menghapus Informasi Elektronik yang tidak relevan yang berada di bawah kendalinya atas permintaan orang yang bersangkutan berdasarkan penetapan pengadilan dan setiap Penyelenggara Sistem Elektronik wajib menyediakan mekanisme penghapusan Informasi Elektronik yang sudah tidak relevan. (Menambahkan ketentuan atau kewajiban menghapus konten yang tidak relevan bagi penyelenggara sistem elektronik sebagai jaminan pemenuhan atas perlindungan data pribadi. Pelaksanaan ketentuan ini dilakukan atas permintaan orang yang bersangkutan berdasarkan penetapan pengadilan.)
j. Memperkuat peran Pemerintah dalam memberikan perlindungan dari segala jenis gangguan akibat penyalahgunaan informasi dan transaksi elektronik (Memberikan landasan yang kuat bagi pemerintah untuk mencegah penyebarluasan konten

negatif di internet) dengan menyisipkan kewenangan tambahan pada ketentuan Pasal 40 yaitu Pemerintah wajib melakukan pencegahan penyebarluasan Informasi Elektronik yang memiliki muatan yang dilarang dan Pemerintah berwenang melakukan pemutusan akses dan/atau memerintahkan kepada Penyelenggara Sistem Elektronik untuk melakukan pemutusan akses terhadap Informasi Elektronik yang memiliki muatan yang melanggar hukum.

Selanjutnya, secara garis besar jika berbicara mengenai apakah Undang-Undang No. 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik telah relatif Akomodatif mengatur mengenai tindak *CyberCrime*, UU ITE sebenarnya telah relatif akomodatif menjawab kebutuhan orang-orang dalam melakukan kegiatan di dunia *Cyber*. UU ITE telah mengakomodir ketentuan material dan juga prosedural. Dengan demikian UU ITE memberikan dan menjamin kepastian hukum dalam melaksanakan aktivitas melalui Sistem Informasi Elektronik. Namun, sejak terbentuknya UU ITE di Indonesia didalam kenyataan atau realita dunia *Cyber*, kejahatan tersebut tetap sulit untuk dijinakkan karena *Cyberspace* merupakan dunia virtual yang sulit ditemukan secara nyata tetapi dapat dikunjungi oleh berjuta pengguna di seluruh dunia setiap saat. Karakteristik inilah yang mempengaruhi UU ITE itu mempunyai kendala dalam penerapannya, serta masih terdapat masalah yurisdiksi hukum yang belum sempurna. Karena pada kenyataannya tindak pidana *Cyber* sering bersifat lintas negara sehingga menimbulkan pertanyaan mengenai yuridiksi yang berlaku atas perbuatan atau akibat tindak pidana serta atas pelakunya. Hal ini disadari oleh Indonesia bahwa keterbatasan perundang-undangan konvensial yang dimiliki sulit untuk menjawab masalah ini, sehingga memandang perlu untuk menyesuaikan hukumnya untuk tetap menjaga kedaulatan negara serta kepentingan negara dan warganya.

3.2 Penegakan Hukum *Cybercrime* di Wilayah Kepolisian Daerah Sumatera Utara

Berdasarkan hasil penelitian lapangan maka diperoleh data tentang bentuk-bentuk *CyberCrime* di lingkungan Polda Sumut dari tahun 2020 sampai dengan mei 2022 sebagaimana berikut :

Tabel 3.
Rekapitulasi Data Tindak Pidana Cyber diPolda Sumut

No.	Jenis Tindak Pidana *Cyber*	Tahun			Jumlah	Ket
		2020	2021	2022		
1.	Pencemaran Nama Baik	9	23	19	51	1 kasus dilimpahkan ke pengadilan. 7 kasus berstatus Surat Perintah Penghentian Penyidikan. 2 dilimpahkan ke Polres tempat kejadian.
2.	Judi Online	13	5	3	21	1 kasus dilimpahkan ke pengadilan.

						1 kasus Selesai
3.	Konten Asusila/Pornografi	11	9	16	36	11 kasus berstatus Surat Perintah Penghentian Penyidikan. 1 dilimpahkan ke Polres tempat kejadian.
4.	Penipuan Investasi	7	6	2	15	1 kasus dilimpahkan ke pengadilan
Jumlah		40	43	40	123	(Data kasus ini terhitung sampai dengan Mei 2022.)

Sumber: Ditreskrimsus Polda Sumut, 2022.

Berdasarkan tabel diatas, data kasus *Cyber* dari tahun 2020 sampai mei 2022, tindak pidana *Cyber* yang paling banyak terjadi ialah pada tahun 2021. Pada tahun 2020 tindak pidana *Cyber* yang paling sering terjadi ialah judi online selanjutnya diurutan kedua terbanyak ialah tindak pidana konten asusila/pornografi dan diikuti oleh tindak pidana pencemaran nama baik serta kasus dalam penipuan investasi. Pada tahun 2021 tindak pidana *Cyber* berupa judi online mengalami penurunan kasus secara trastis terhitung sejak 2020 diikuti oleh kasus konten asusila/pornografi dan tindak pidana penipuan dalam investasi, sedangan kasus pencemaran nama baik mengalami peningkatan kasus sejak tahun 2020. Pada bulan Mei tahun 2022 terhitung adanya penurunan pada beberapa tindak pidana *Cyber* yaitu pencemaran nama baik dimana pada tahun 2021 tindak pidana ini menjadi salah satu tindak pidana yang mengalami peningkatan secara drastis. Diikuti oleh kasus-kasus judi online dan penipuan investasi yang juga mengalami penurunan kasus tiap tahunnya yang mana situasi ini mengambarkan adanya penegakan hukum yang baik sehingga terjadinya beberapa penurunan kasus di beberapa tindak pidana *Cyber*.

Secara faktual, penyidik sering kali mendapatkan beberapa dalam melakukan Penyidikan terhadap kasus kejahatan dunia maya atau *CyberCrime* dimana dalam mengusut pelaku mengenai identitas pelaku yang kerap menggunakan nama samaran bukan nama yang sebenarnya. Sulitnya menemukan locus atau tempat kejadian tindak pidana *CyberCrime* sering terjadi, karena pelaku bisa saja berpindah-pindah tempat ketika melakukan kejahatan *CyberCrime*. Misalnya dalam kasus ujaran kebencian/pencemaran nama baik berdasarkan wawancara dengan Irayata bahwa "kasus pencemaran nama baik/ujaran kebencian yang di lakukan dimedia sosial, para Penyidik harus terlebih dahulu memanggil ahli bahasa untuk membuat terang suatu kalimat atau ucapan yang tertulis dimedia sosial tersebut apakah terpenuhi unsur ujaran kebenciannya, dan penyidik pun terkadang harus memanggil ahli hukum pidana untuk membuat terang perkara bahwa ucapan atau kalimat ujaran kebencian tersebut merupakan suatu tindak pidana."

Irayata dalam wawancara juga menyatakan bahwa hambatan yang di alamai oleh kepolisian dalam menanggulangi perjudian *online* antara lain:

a. Tindak pidana perjudian on-line dapat di lakukan dimana saja, kapan saja, dan siapa saja tanpa selama masih terhubung dengan jaringan internet dan di dukung perangkat teknologi seperti laptop dan handphone android,
b. Dalam melakukan perjudian on-line, pelaku tidak memerlukan kawan atau lawan main seperti perjudian konvensional, selama terkoneksi dengan jaringan internet maka pelaku perjudian dapat bermain judi dengan pelaku lainnya dalam aplikasi judi yang disediakan.
c. Sistem taruhan yang menggunakan Uang Elektronik atau saldo, menyulitkan kepolisian dalam melacak barang bukti taruhan yang dilakukan oleh pelaku tindak pidana perjudian on-line.
d. Sulitnya mengungkap Bandar judi on-line, dikarenakan kebanyakan pusat server rumah judi on-line berada di luar negeri sehingga menyulitkan aparat dalam menumpas perjudian on-line sampai ke bandar besar.
e. Sulitnya melakukan pemblokiran situs atau website perjudian on-line dikarenakan banyaknya alternatif website yang ditawarkan oleh pihak rumah judi sehingga menyulitkan pihak kepolisian dan pihak kemenkominfo dalam melakukan pemblokiran situs dan website perjudian *online*.

Berdasarkan penelitian yang dilakukan, maka dapat disimpulkan beberapa kendala yang menghambat upaya penanggulangan *cybercrime*, penulis kemudian membaginya ke dalam beberapa aspek berdasarkan hasil wawancara dan penelusuran referensi lainya, yaitu:

a. Aspek Sumber Daya Manusia
   Penyidik kepolisian memiliki peran penting dalam upaya penanggulangan *CyberCrime,* dimana kemampuan/kualitas penyidik dan jumlah personil penyidik di setiap unit *CyberCrime* harus memadai dan diperhatikan karena sangat berpengaruh untuk mengungkap kasus-kasus *CyberCrime* yang dilaporkan oleh masyarakat, adanya unit *CyberCrime* di lingkungan kepolisian membuktikan bahwa dibutuhkannya penyidik khusus yang memiliki kemampuan di bidang informasi dan transaksi elektronik guna menangani kejahatan-kejahatan di dunia maya secara maksimal.

b. Aspek Alat Bukti Pada tindak pidana *CyberCrime*
   Hal alat bukti berbeda dengan alat bukti pada tindak pidana umum dimana sasaran atau media *CyberCrime* merupakan data-data atau sistem elektronik dengan dihubungkan ke internet, dan selain itu karena hampir seluruh masyarakat memilki telefon genggam (HP) dan fasilitas umum lainnya yang menjadi masalah/kendala terhadap penyidik *CyberCrime,* dalam hal ini penulis akan menjelaskan secara rinci mengenai kendala aspek alat bukti sesuai dengan data dan hasil wawancara penulis yang mana mengenai aspek alat bukti dalam penanggulangan kejahatan *CyberCrime* sendiri memiliki kendala yang mana mulai dari alat bukti digital mudah dihilangkan dan atau dihapus jika tidak ditangani dengan cepat dan tepat dalam suatu tindak pidana *cybercrime*, dan pelaku menggunakan fasilitas umum dalam

melakukan tindak pidana *cybercrime*. seperti barang bukti digital mudah dihilangkan jika tidak ditangani dengan tepat waktu. selain itu, pelaku menggunakan fasilitas umum dalam melakukan tindak *cybercrime,* dan keberadaan para saksi tidak di tempat yang sama dengan korban dan pelaku (Sumadi, 2016).

c. Aspek Fasilitas
Pada tindak *CyberCrime* dalam mengungkap kasus-kasus *CyberCrime* dibutuhkan fasilitas yang mampu menunjang kinerja aparat kepolisian/penyidik, fasilitas tersebut berupa laboratorium forensik komputer yang digunakan untuk mengungkap data-data yang bersifat digital serta merekam dan menyimpan bukti-bukti yang berupa softcopy (gambar, program, html, suara, dan lain sebagainya). Komputer forensik dikenal sebagai digital forensik, adapun tujuannya ialah untuk mengamankan dan menganalisis bukti digital, serta memperoleh berbagai fakta yang objektif dari sebuah kejadian atau pelanggaran keamanan dari sistem informasi, berbagai fakta tersebut akan menjadi bukti yang akan digunakan dalam proses hukum. Melalui internet forensik, penyidik dapat mengetahui siapa saja orang yang mengirim email, kapan dan dimana keberadaan alamat pengirim berdasarkan server pengirim, dan dalam contoh lain kita bisa melihat siapa pengunjung website secara lengkap dengan informasi IP Address, alat elektronik yang dipakainya dan keberadaannya serta kegiatan apa yang dilakukan pada website tersebut.

Selanjutnya penyidik di Polda Sumatera Utara mengatakan hal lain yang di lakukan Kepolisian daerah sumatera utara untuk mencegah tindak pidana dunia maya (*CyberCrime*) adalah dengan mengadakan pengawasan terhadap situs-situs yang mengandung konten pornografi dan konten perjudian *online*, dengan bekerja sama dengan Kemenkominfo untuk melakukan bloking terhadap situs-situs yang mengandung unsur tindak pidana. Kerjasama yang di lakukan Polri dengan Kemenkominfo tersebut berupa kesepakatan untuk mencegah meluasnya penyakit masyarakat dan memberikan jaminan keamanan untuk megakses situs-situs internet yang aman bagi masyarakat. Upaya-upaya yang dilakukan oleh Kepolisian Daerah Sumatera Utara didukung dengan sumber daya yang optimal adalah upaya untuk mencegah, menghambat dan menghentikan tindakan pelaku kejahatan yang sedang berupaya atau sedang melakukan tindakan yang bertentangan dengan hukum khususnya tentang tindak *Cybercrime*.

4. Penutup

Berdasarkan pembahasan diatas diperoleh kesimpulan bahwa Undang-Undang No.19 Tahun 2016 tentang Informasi dan Transaksi Elektronik tentang perubahan atas Undang-Undang No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik yang telah cukup relatif akomodatif secara normatif dalam menjawab kebutuhan masyarakat dalam melakukan kegiatan di dunia *Cyber.* Selanjutnya, Bentuk-bentuk tindak *CyberCrime* yang sering terjadi diwilayah Polda Sumatera utara ialah pencemaran nama baik, judi online serta konten asusila. Sampai dengan bulan Mei Tahun 2022 kasus pencemaran nama baik adalah bentuk tindak *CyberCrime* yang paling

sering terjadi dari tahun ke tahun. Disusul oleh kasus konten asusila/pornografi yang mengalami penurunan jumlah kasus tiap tahunnya dan juga kasus judi online yang merupakan tindak pidana *CyberCrime* yang mengalami penurunan jumlah kasus paling drastis sampai Tahun 2022. Peran kepolisian khususnya diwilayah Polda Sumatera Utara dalam penegakan hukum tindak *cybercrime* sampai Tahun 2022 dapat dilihat dari hasil penelitian dimana pihak kepolisian awalnya menerima laporan atau aduan terkait masalah tindak *cyber* selanjutnya melakukan penyidikan dalam menetapan status terlapor sebagai tersangka dalam penegakan hukum tindak *CyberCrime* yang dilakukan setelah adanya bukti-bukti yang jelas serta dapat dihubungkan secara langsung dengan terlapor atau penindakan langsung. Proses pembuktian terlapor sebagai tersangka (pelaku) dilakukan dengan memeriksa alat-alat bukti fisik, keterangan saksi dan korban, keterangan saksi ahli, serta keterangan terlapor.

Referensi

Indriani, F. (2016). Tinjauan Yuridis Tindak Pencemaran Nama Baik Melalui Media Sosial Berdasarkan Pasal 27 Ayat (3) Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik Dikaitkan dengan Kebebasan Berpendapat. *Jurnal Online Mahasiswa (JOM) Bidang Ilmu Hukum*, *3*(1), 1–15.

Raharjo, A. (2002). *Cybercrime: Pemahaman dan upaya pencegahan kejahatan berteknologi*. Citra Aditya Bakti.

Sitompul, J. (2012). *Cyberspace, cybercrimes, cyberlaw: tinjauan aspek hukum pidana*. PT Tatanusa.

Sumadi, H. (2016). Kendala dalam menanggulangi tindak pidana penipuan transaksi elektronik di Indonesia. *Jurnal Wawasan Yuridika*, *33*(2), 175–203.

Tobing, R. L., & Tobing, R. L. (2012). *Penelitian hukum tentang efektivitas Undang-Undang nomor 11 tahun 2008 Tentang Informasi dan Transaksi Elektronik*. Badan Pembinaan Hukum Nasional, Kementerian Hukum dan Hak Asasi Manusia RI.

Wawancara Irayata, Tim Subdit Cyber Crime Ditreskrimsus Polda Sumut, tanggal 15 Agustus 2022.

****