



PENEGAKAN HUKUM PIDANA DI INDONESIA TERHADAP PENGARUH NEGATIF PERKEMBANGAN CYBER CRIME

Susiana Kifli

Fakultas Hukum, Universitas Muhammadiyah Palembang, Palembang, Indonesia
susiana_kifli@um-palembang.ac.id



Diterima: 31 Mei 2025 – Diperbaiki: 20 Juni 2025 – Diterima: 30 Juni 2025

Abstract

The rapid development of information and communication technology is also accompanied by the widespread misuse of information and communication technology, so that it becomes a very disturbing problem, namely the occurrence of crimes committed in cyberspace or what is commonly known as "cybercrime". Various crimes have occurred in cyberspace, these cases are certainly detrimental and have negative impacts. Apart from the digital divide, cybercrime in Indonesia is still rampant. The type of research used in this writing is normative legal research. In the discussion of the development of criminal law in the future, in addition to using the law enforcement theory of Soerjono Soekanto, the resolution and prevention of cybercrime must be balanced with the regulation and development of the entire criminal law system, which includes the development of the structure, culture, and substance of criminal law. In such conditions, criminal law policy occupies a strategic position in the development of modern criminal law. Criminal law policy intends to achieve peace and prosperity for all people.

Keywords: *Cybercrime, Criminal Law, Law Enforcement*

✉ Alamat korespondensi:

Fakultas Hukum, Universitas Muhammadiyah Palembang, Palembang, Indonesia
susiana_kifli@um-palembang.ac.id

I. PENDAHULUAN

Perkembangan teknologi saat ini sangat begitu pesat menjadikan dunia bagaikan sebuah labirin kaca dan semua kalangan mulai dari anak kecil, dewasa sampai ke lansia dapat mengaksesnya. Saat ini banyak sekali platform-platform yang menawarkan media komunikasi dengan sangat mudah dipakai oleh masyarakat di Indonesia. Dengan kecanggihan yang diberikan oleh media komunikasi tersebut banyak orang-orang yang mendapat dampak positif dari menggunakan platform tersebut, akan tetapi dibalik kecanggihan teknologi komunikasi tersebut terdapat beberapa oknum yang menyalahgunakan platform tersebut.

Platform media komunikasi sampai saat semakin banyak variasi yang bisa menjadi pilihan untuk digunakan. Semua pengguna dapat dengan mudah berinteraksi dengan pengguna lainnya. Teknologi saat ini berkembang pesat dan menjadi pusat informasi bagi banyak orang. Selain mempunyai dampak positif, perkembangan teknologi yang semakin pesat juga terdapat pula dampak negatif yang ditimbulkan. Yaitu juga dapat digunakan untuk melakukan kejahatan. Dalam bentuk tindakan kriminal termasuk dalam tindakan pidana.

Hukum Pidana adalah hukum yang mengatur tentang pelanggaran dan kejahatan terhadap kepentingan umum. Pelanggaran dan kejahatan tersebut diancam dengan hukuman yang merupakan penderitaan atau siksaan bagi yang bersangkutan (Masriani, 2006). Mezger mengatakan bahwa Hukum Pidana dapat didefinisikan sebagai aturan hukum, yang mengikatkan kepada suatu perbuatan yang memenuhi syarat-syarat tertentu suatu akibat yang berupa pidana (Sudarto, 1990). Perkembangan dan isu aktual dalam hukum pidana mencakup berbagai aspek yang berkaitan dengan penegakan hukum, perubahan norma, serta tantangan baru yang dihadapi oleh sistem hukum pidana. Dalam hal ini, beberapa poin utama yang perlu dicermati melibatkan reformasi hukum, perkembangan teknologi, dan isu-isu hak asasi manusia (Saputri & Marpaung, 2021).

Perkembangan ilmu pengetahuan dan teknologi jelas telah mempengaruhi perkembangan hukum, termasuk hukum pidana, khususnya dalam hal perilaku (kejahatan). yang dalam dunia modern saat ini tidak dapat dibedakan dan bahkan sering bergantung pada perkembangan teknologi maju ("hitech" atau "lanjutan"). teknologi khususnya di bidang informasi dan elektronika melalui jaringan internasional (Internet). Kemajuan ilmu pengetahuan dan teknologi selalu membawa dampak, baik langsung maupun tidak langsung. Salah satu aspek penting dalam perkembangan hukum pidana adalah adanya upaya reformasi hukum. Reformasi ini bisa mencakup perubahan dalam ketentuan-ketentuan pidana, proses peradilan, dan sanksi pidana. Negara-negara mungkin merespon perubahan sosial, ekonomi, atau politik dengan merevisi peraturan-peraturan hukum pidana mereka agar tetap relevan dan efektif. Reformasi juga dapat terkait dengan peningkatan akses keadilan, transparansi, dan akuntabilitas sistem peradilan pidana.

Peraturan Indonesia mengenai kejahatan siber atau elektronik diatur secara ketat oleh Undang-Undang Republik Indonesia No. 19 Tahun 2016 tentang perubahan atas Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Kemudian, mengenai tindak pidana maksiat melalui sarana elektronik, ketentuan tersebut dapat kita temukan pada klausul pelanggaran Pasal 45 ayat (1) juncto Pasal 27 ayat (1) Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, kemudian diubah menjadi UU No. 1 Tahun 2024 yang merupakan perubahan kedua atas UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Istifarrah, 2020). Dalam perkembangannya, hukum pidana terus beradaptasi dengan dinamika masyarakat dan perubahan teknologi. Isu faktual hukum pidana melibatkan masalah aktual yang mempengaruhi sistem hukum pidana, seperti kejahatan cyber, terorisme, dan perubahan dalam paradigma keadilan pidana.

II. METODE PENELITIAN

Penelitian ini dilakukan dengan jenis penelitian hukum normatif berupa penelitian kepustakaan dengan menggunakan tiga sumber hukum yaitu dokumen hukum primer, dokumen hukum sekunder, dan dokumen hukum tersier (Efendi, 2016). Kajian hukum ini menitik beratkan pada kajian kepustakaan yang artinya akan menelaah dan mengkaji lebih jauh peraturan-peraturan hukum yang ada dan berlaku saat ini. Penelitian ini memerlukan dokumen hukum karena akan melengkapi dan mendukung dokumen hukum dalam penelitian kepustakaan (Muhammad, 2004).

III. HASIL DAN PEMBAHASAN

Dalam perkembangannya *cyber crime* (tindak pidana mayantara) sering dibahas di berbagai forum internasional, yaitu pada Konres PBB mengenai "*The Prevention of Crime and the Treatment of Offenders*" yang telah membahas masalah ini sampai tiga kali, yaitu pada Kongres VIII/1990 di Havana, Kongres X /2000 di Wina, dan terakhir pada Kongres XI /2005 di Bangkok (tanggal 18-25 April). Di samping itu telah ada pula Konvensi *cyber crime* Dewan Eropa (*Council of Europe Cyber Crime Convention*) yang ditanda tangani di Budapest pada tanggal 23 November 2001 oleh berbagai negara, termasuk Kanada, Jepang, Amerika, dan Afrika Selatan (Mira, 2017).

Kongres dan Konvensi Internasional tersebut, didahului atau diikuti dengan berbagai pertemuan dan kajian ilmiah lainnya di berbagai negara yang sulit untuk dihitung, dari berbagai kajian itu ada yang meresahkan perkembangan *cyber crime* terutama dibidang kesusilaan dan eksploitasi seksual, antara lain dengan diadakannya *The First World Congress Against Commercial Sexual Exploitation of Children di Stockholm*, 27-31 Agustus 1996, dan *International Conference on "Combatting Child Pornography on the Internet"*, Vienna, Hofburg, 29 September - 1 Oktober 1999. Perhatian terhadap masalah *cyber crime* ini juga berkembang di Indonesia terutama dengan diadakan berbagai seminar nasional, sebagaimana yang ditulis oleh Barda Nawawi Arief dalam Buku Tindak Pidana Mayantara yang merupakan himpunan dari makalah yang disampaikan pada delapan seminar nasional yang diadakan sejak tahun 2001 sampai tahun 2005 (Riska, 2019).

Secara luas, tindak pidana siber ialah semua tindak pidana yang menggunakan sarana atau dengan bantuan Sistem Elektronik. Itu artinya semua tindak pidana konvensional dalam Kitab Undang-Undang Hukum Pidana sepanjang dengan menggunakan bantuan atau sarana Sistem Elektronik seperti pembunuhan, perdagangan orang, dapat termasuk dalam kategori tindak pidana siber dalam arti luas. Akan tetapi, dalam pengertian yang lebih sempit, pengaturan tindak pidana siber diatur dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana yang telah diubah oleh Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Undang-Undang ITE terbaru adalah UU No. 1 Tahun 2024 yang merupakan perubahan kedua atas UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. UU ini mulai berlaku sejak tanggal 2 Januari 2024. UU ini mengatur tentang berbagai hal terkait informasi dan transaksi elektronik, termasuk tanda tangan elektronik, segel elektronik, dan identitas digital.

Salah satu unsur dari *cyber crime* adalah penggunaan teknologi informasi dalam modus operandinya. Sifat inilah yang membuat *cyber crime* berbeda dengan tindak pidana lainnya. Namun demikian, kejahatan yang terjadi sebenarnya adalah kejahatan biasa (konvensional) dan masih memungkinkan diselesaikan dengan menggunakan KUHP. Sedangkan menurut Harkristuti Harkrisnowo, dalam masalah *cyber crime* ada beberapa rumusan pidana tradisional yang dapat digunakan, yaitu:

- a. Pencurian
- b. Penggelapan
- c. Pembukaan Rahasia
- d. Pemalsuan
- e. Pengancaman
- f. Pornografi
- g. Penghasutan
- h. Pelecehan Seksual
- i. Penghinaan
- j. Penyebaran kabar bohong

Dalam suatu perbuatan penyebarluasan pornografi yang dilakukan oleh seseorang atau kelompok yang sangat ditentang oleh negara melalui peraturan hukum yang ada. Penggunaan media sosial internet adalah suatu kejahatan yang memiliki klasifikasi yang berbeda dengan kejahatan yang lainnya. Seperti muatan yang telah diatur dalam Undang-Undang ITE terkait dengan *Cyberphornography* yaitu mengenai seperti tindak pidana cyber. 19 Dalam muatan peraturan Undang-Undang ITE hal ini dimuat pada Pasal 27 sampai dengan pasal 36, dan dalam pasal 42 Undang-Undang ITE diatur mengenai ketentuan suatu penyidik untuk membuktikan bahwa sistem pembuktian yang diyakini adalah sistem pembuktian dalam Undang-Undang ITE yang berdasarkan sistem yang

telah diyakini oleh KUHAP. Berdasarkan Ketentuan Umum dalam Bab I Pasal 1 Angka 1 Undang-Undang No. 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik telah dijelaskan bahwa Informasi Elektronik yaitu suatu kumpulan data elektronik yang termasuk data seperti tulisan, suara gambar, rancangan, *electronic data interchange* (EDI), surat elektronik (email), telegram, ataupun sejenisnya, yang terdapat huruf, tanda, angka, kode akses, symbol, atau data yang telah diolah dan yang memiliki arti yang dapat dijelaskan oleh orang-orang yang dapat mengetahui. Peraturan hukum yang telah mengatur tentang kejahatan kesusilaan melalui media sosial di media elektronik telah diatur secara khusus dalam Pasal 27 sampai dengan Pasal 42 dalam tindak pidana Undang-Undang ITE (Sumarwani, 2014). Penjelasan di atas hal tersebut terdapat pasal pasal terkait dengan penyebarluasan konten pornografi pada media sosial. Hadirnya Undang-Undang ITE akan membuat masyarakat Indonesia yang memiliki pemahaman mengenai hukum akan berhati-hati dan akan lebih bijak menggunakan internet terutama media sosial. Kejahatan tindak pidana pornografi (*cyberporn*) dapat dilakukan secara individual, seperti dengan sengaja menyebarkan video porno seseorang ke media sosial sehingga menjadi konsumsi para pengguna media sosial lain. Tentunya dimassa yang tergantung dengan media sosial memunculkan keresahan pada masyarakat karena dengan mudahnya oknum melakukan kejahatan pornografi. Dalam hal ini menunjukkan dampak negatif pada sisi pornografi yang sangat mengkhawatirkan, termasuk perilaku seks bebas, perilaku seksual, eksploitasi seksual dan seks menyimpang (Salami & Bintoro, 2013).

Kejahatan dunia maya merupakan salah satu risiko paling signifikan yang dihadapi bisnis pada tahun 2025, dan pelaku kejahatan dunia maya tidak pilih-pilih saat menargetkan bisnis. Meski demikian, dalam banyak kasus, semakin besar atau sukses bisnis Anda, semakin besar pula risiko Anda menerima ancaman dunia maya. Misalnya, hanya 40% perusahaan rintisan tahap awal dan pra-awal yang yakin akan menghadapi ancaman dunia maya, tetapi 72% perusahaan rintisan Seri C memperkirakan akan terjadi serangan. Salah satu kasus *cyber crime* di Indonesia tahun 2024 yang menunjukkan *insider threat* sama berbahayanya dengan serangan eksternal. Kasusnya terkait kebocoran data 380 ribu data pelanggan Biznet Networks, yang disusul 150 ribu lebih data milik jaringan Biznet lainnya. Berdasarkan klaim awal, pelaku mengaku sebagai karyawan Biznet. Akan tetapi, setelah investigasi mendalam, Biznet memastikan kebocoran data dilakukan oleh pihak eksternal. Perusahaan lalu menggandeng kepolisian untuk mengusut kasus tersebut secara menyeluruh (Salami & Bintoro, 2013).

Serangan siber yang menargetkan Indonesia telah membawa dampak besar baik bagi sektor publik maupun swasta. Beberapa kasus serangan siber terbesar yang terjadi di Indonesia tidak hanya merusak reputasi banyak institusi, tetapi juga menyebabkan kerugian finansial yang sangat besar. Fenomena kasus *cyber crime* di Indonesia kini menjadi ancaman serius bagi keamanan digital warga. Dari penipuan online, peretasan data sensitif, hingga serangan malware, bentuk kejahatan siber semakin beragam dan canggih. Pemerintah dan pelaku industri digital dituntut untuk terus meningkatkan kewaspadaan menghadapi lonjakan kasus kejahatan siber di Indonesia yang kian mengkhawatirkan. Memahami modus operandi dan cara melindungi diri dari serangan siber menjadi keterampilan vital di era digital ini. Tanpa kesadaran dan kesiapan menghadapi ancaman online, siapapun bisa menjadi korban berikutnya.

Menurut Soejono Soekanto, secara konseptual, maka inti dari penegakan hukum terletak pada kegiatan menyerasikan hubungan nilai-nilai yang dijabarkan di dalam kaidah-kaidah yang baik untuk menciptakan, memelihara, dan mempertahankan kedamaian pergaulan hidup. Penegakan hukum memiliki proses atau upaya untuk melakukan tegaknya suatu aturan yang berfungsi untuk norma-norma yang berlaku secara nyata sebagai pedoman dalam kehidupan bermasyarakat dan bernegara. Teori penegakan hukum menurut Joseph Goldstein, adalah suatu penegakan hukum yang membedakan menjadi tiga, yaitu:

- a. Konsep penegakan hukum bersifat total (*Total Enforcement*) merupakan ruang lingkup pada hukum pidana yang sebagaimana telah dirumuskan pada hukum pidana substantif. Namun total *enforcement* tidak dilakukan sepenuhnya karena adanya suatu aturan yang membatasi penegak hukum merupakan aturan yang ketat ada pada hukum acara pidana, merupakan adanya aturan-aturan penangkapan, penahanan, penyitaan, dan sebagainya. Dimana ruang lingkup penegakan hukum acara pidana substantif yang disebut sebagai *area of no enforcement*. Setelah total *enforcement* dikurangi dengan *area of no enforcement*.

- b. Konsep penegakan hukum bersifat aktual (*Full enforcement*) yaitu para penegak hukum yang menegakan hukumnya secara maksimal dan terus dianggap harapannya tidak realistis karena adanya keterbatasan pada bentuk waktu, personil, financial dalam penyidikan dan sebagainya.
- c. Konsep penegakan hukum bersifat aktual (*Actual Enforcement*) merupakan ada pada penegakan hukum, di mana penegakan hukum harus diliat secara realistis, sehingga pada penegakan hukum yang akan dijalankan harus secara aktual dan tidak dapat dihindari karena keterbatasan-keterbatasan tertentu, sekalipun untuk pemantauan secara terpadu dan dapat memberikan arahan yang positif.

Pengertian penegakan hukum dapat pula ditinjau dari sudut objeknya, yaitu dari segi hukumnya. Pengertian yang mencakup makna luas dan sempit. Dalam arti luas, penegakan hukum mencakup nilai-nilai keadilan yang tertera di dalamnya yaitu aturan formal maupun nilai-nilai keadilan yang hidup dalam masyarakat. Sedangkan dalam arti sempit, penegakan hukum hanya menyangkut penegakan formal dan tertulis saja. Oleh karena itu, yang dimaksud dengan penegakan hukum merupakan upaya yang dilakukan untuk dijadikan hukum, baik dalam arti sempit maupun arti yang luas. Sebagai pedoman dalam perilaku setiap perbuatan hukum, oleh para pelaku yang bersangkutan maupun aparaturnya untuk menjamin fungsi dan norma-norma hukum yang berlaku dalam kehidupan bermasyarakat dan bernegara. Penegakan hukum terhadap *cyber crime* mutlak memerlukan alat sebab karakteristik dari kejahatan ini adalah dilakukan dengan alat baik yang berwujud maupun yang tidak berwujud. Penentuan waktu dan tempat terjadinya *cyber crime* ditentukan saat kapan alat itu bekerja efektif, oleh sebab itu analisis telematika sangat diperlukan.

Pengaruh perkembangan *cyber crime* terhadap penegakan hukum pidana, sebagaimana mengutip pendapat Soerjono Soekanto tentang faktor yang mempengaruhi penegakan hukum pidana, yang terdiri dari:

1. Faktor hukum (undang-undang);
2. Faktor penegak hukum;
3. Faktor sarana dan fasilitas;
4. Faktor masyarakat;
5. Faktor kebudayaan

Adapun penjelasan dari faktor-faktor diatas, sebagai berikut:

1. Faktor yang mempengaruhi penegakan hukum yang pertama, yakni undang-undang menjadi faktor utama dalam menunjang lahirnya penegakan hukum. Menurut Purwacaraka dan Soerjono Soekanto, yang diartikan dengan undang-undang dalam arti materiil adalah peraturan tertulis yang berlaku umum dan dibuat oleh penguasa pusat atau penguasa daerah yang sah. Maka undang-undang tersebut mencakup peraturan pusat yang berlaku untuk semua warga negara atau golongan tertentu saja maupun yang berlaku umum di sebagian wilayah negara dan peraturan setempat yang hanya berlaku di suatu tempat atau daerah saja (Soekanto, 2008). Dalam hal ini, undang-undang tersebut adalah Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Yang mana dalam kepengaturan undang-undang tersebut jelas mengatur mengenai larangan tindak pidana perjudian melalui media elektronik. Aturan yang ada dianggap sudah memberikan efek jera bagi pelakunya, dapat dilihat pada pasal 27 ayat (2) jo pasal 45 Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.
2. Faktor Penegak Hukum, yakni penegak hukum yang dimaksud adalah mereka yang berkecimpung dibidang penegakan hukum yang mencakup mereka yang bertugas di Kehakiman, Kejaksaan, Kepolisian, Pengacara, dan Pemasyarakatan. Menurut Soerjono Soekanto, seorang penegak hukum sebagaimana halnya dengan warga-warga masyarakat lainnya, lazimnya mempunyai beberapa kedudukan dan peranan. Dengan demikian tidaklah mustahil, bahwa antara berbagai kedudukan dan peranan timbul konflik (*status conflict* dan *conflict of roles*). Apabila di dalam kenyataan terjadi suatu kesenjangan antara peranan yang seharusnya dengan peranan yang sebenarnya dilakukan atau peranan aktual, maka terjadi suatu kesenjangan peran (*role-distance*).
3. Faktor sarana dan fasilitas Sarana dan fasilitas yang kurang mendukung, baik dari kuantitas maupun kualitas dari sarana maupun fasilitas yang dimiliki oleh masing-masing petugas

penegak hukum belum sesuai dengan beban tugas yang mereka jalankan. Karena untuk menangkap atau membuktikan pelaku kejahatan sarannya harus lebih canggih dari sarana atau alat yang digunakan oleh penjahat. Tentunya untuk peningkatan kualitas dan kuantitas dari sarana ini akan menambah anggaran bagi negara untuk menyiapkannya.

4. Faktor masyarakat Partisipasi masyarakat sangat diperlukan terhadap pelaksanaan penegakan hukum, karena bagian yang terpenting dalam penegakan hukum adalah kesadaran hukum masyarakat. Semakin tinggi kesadaran hukum masyarakat maka akan semakin memungkinkan penegakan hukum yang baik dan semakin rendah tingkat kesadaran hukum masyarakat, maka akan semakin sukar untuk melaksanakan penegakan hukum yang baik. Demikian juga halnya dengan tindak pidana mayantara (*cyber crime*). Tetapi yang menjadi hambatan di kalangan masyarakat adanya rasa takut untuk dijadikan saksi walaupun sudah ada ketentuan mengenai perlindungan saksi dan korban. Termasuk juga karena kurangnya pengetahuan hukum dari masyarakat.
5. Faktor kebudayaan yaitu hukum ataupun aturan yang dibuat oleh manusia atau suatu daerah sangat dipengaruhi oleh kebiasaan setempat, norma, dan nilai-nilai yang hidup pada masyarakat itu sendiri. Keberadaan hukum dalam masyarakat diantaranya adalah untuk mengatur kepentingan-kepentingan tersebut bisa bertentangan satu sama lainnya. Untuk itu, hukum mengatur sedemikian rupa sehingga dalam suatu lalu lintas kepentingan tidak saling bertentangan. Sumber daya masyarakat yang kurang sadar hukum terhadap Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik sehingga perlu adanya upaya hukum preventif untuk meningkatkan kesadaran masyarakat. Masyarakat kurang paham terhadap teknologi yang telah berkembang sehingga membuat suatu kejahatan baru yaitu *cyber crime* (Ketaren, 2016).

Pemerintah Indonesia juga sedang meningkatkan upaya penegakan hukum untuk mengatasi kasus hacking. UU ITE adalah landasan utama dalam mengatur dan menindak kejahatan siber. Undang-undang ini memberikan kerangka hukum yang kuat untuk menangani berbagai bentuk kasus peretasan di Indonesia. Kepolisian Indonesia telah membentuk unit khusus *cybercrime* untuk menangani kasus-kasus peretasan. Unit ini bekerja sama dengan lembaga internasional untuk memerangi kejahatan siber lintas batas. Kolaborasi ini penting mengingat sifat global dari kasus *hacking* di Indonesia. Beberapa kasus peretasan besar telah berhasil diungkap oleh penegak hukum Indonesia. Namun, tantangan masih ada dalam proses penyelidikan dan penuntutan. Keterbatasan sumber daya dan keahlian teknis sering menjadi hambatan dalam menangani kasus hacking yang semakin canggih. Pemerintah juga fokus pada edukasi masyarakat tentang keamanan siber. Langkah ini penting untuk mencegah terjadinya kasus peretasan di Indonesia. Dengan upaya komprehensif ini, diharapkan ancaman *cybercrime* di Indonesia dapat diminimalisir dan ditangani secara efektif.

IV. KESIMPULAN

Penegakan hukum dalam penanggulangan *cyber crime* di Indonesia belum dilaksanakan secara optimal. Faktor-faktor yang akan mempengaruhi penegakan hukum terhadap *cyber crime* meliputi faktor hukum, faktor penegak hukum, faktor sarana dan fasilitas dalam penegakan hukum dan faktor masyarakat. Dari keempat faktor tersebut maka faktor yang paling berpengaruh pada lemahnya penegakan hukum yang ada terhadap penanggulangan *cyber crime* 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.

REFERENSI

- Barda NA. (2007). *Tindak Pidana Mayantara Perkembangan Kajian Cyber Crime di Indonesia*. PT. RajaGrafindo Persada. Jakarta.
- Efendi, Jonaedi. (2016). *Metode Penelitian Hukum*. Prenadamedia Group. Jakarta.
- Istifarrah, Ayya Sofia. (2020). Pertanggungjawaban Pidana Pelaku Pendistribusian Konten Yang Bermuatan Asusila Melalui Media Elektronik. *Jurist-Diction*, 3(4).
- Ketaren, Eliasta. (2016). Cybercrime, Cybeer Space, dan Cyber Law. *Jurnal TIMES*, V(2), 35-42.

- Masriani, Yulies Tiena. (2006). *Pengantar Hukum Indonesia*. Jakarta: Sinar Grafika.
- Muhammad, Abdulkadir. (2004). *Hukum dan Penelitian Hukum*. Citra Aditya Bakti. Bandung.
- Purwandani, Riska. (2019). Peran Media Sosial Instagram Dalam Interaksi Sosial. *Jurnal Ilmu Komunikasi*, 7(7).
- Salami, Rochani Urip, & Bintoro, Rahadi Wasi. (2013). Alternatif Penyelesaian Sengketa Dalam Sengketa Transaksi Elektronik (E-Commerce). *Jurnal Dinamika Hukum*, 13(1).
- Saputri, Agil, Marpaung, Lintje Anna, & Melisa. (2021). Analisis Terhadap Pelaku Tindak Pidana Kesusilaan Melalui Media Elektronik. *Jurnal Indonesia Sosial Sains*, 2(2).
- Soekanto, Soejono. (2008). *Faktor-Faktor Yang Mempengaruhi Penegakan Hukum*. Rajawali Pers. Jakarta.
- Sofia Istifarrah, Ayya. (2020). Pertanggungjawaban Pidana Pelaku Pendistribusian Konten Yang Bermuatan Asusila Melalui Media Elektronik. *Jurist-Diction*, 3(4).
- Sudarto. (1990). *Hukum Pidana*. Purwokerto: Fakultas Hukum Universitas Jenderal Soedirman Purwokerto Tahun Akademik 1990-1991.
- Sumarwani, Sri. (2014). Tinjauan Yuridis Pidanaan Cyber Crime Dalam Perspektif Hukum Pidana Positif. *Jurnal Pembaharuan Hukum*, 1(3).
- Ziveria, Mira. (2017). Pemanfaatan Media Sosial Facebook sebagai Sarana Efektif Pendukung Kegiatan Perkuliahan di Program Studi Sistem Informasi. *Jurnal Sains dan Teknologi*, 4(2).