Jurnal Kompilasi Hukum Volume 10, No. 1, Juni 2025
E-ISSN 2598-6414, P-ISSN 2502-5333
open access at : http://jkh.unram.ac.id
Publisher Magister of Law, Faculty of Law Mataram University
This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License

PERBANDINGAN HUKUM PIDANA CYBER CRIME DAN PENGARUHNYA DALAM PENEGAKAN HUKUM ANTARA INDONESIA DAN AMERIKA

COMPARISON OF CYBER CRIME CRIMINAL LAW AND ITS IMPACT ON LAW ENFORCEMENT BETWEEN INDONESIA AND AMERICA

Prigel Aditama
Universitas Bengkulu
E-mail: pratamasyaputra01@gmail.com

Elisabeth Aprilia Sinaga
Universitas Bengkulu
E-mail: elisabetbengkulu177@gmail.com

Citra Anjelika Putri
Universitas Bengkulu
E-mail: citraanjelikaputriii@gmail.com

Abstrak

Semakin berkembangnya zaman, teknologi juga ikut berkembang sejalan dengan kemajuan zaman yang semakin canggih. Dan salah satu teknologi yang berkembang pesat itu ialah teknologi informasi yang mana dengan adanya kemajuan ini dapat menimbulkan jenis kejahatan baru yang sering di sebut *Cyber Crime* atau kejahatan dunia maya. Di era digital saat ini, perlindungan hukum terhadap korban pencurian data pribadi adalah masalah penting. Artikel ini mengkaji perlindungan hukum yang diberikan kepada korban pencurian data pribadi di internet dari sudut pandang hukum Indonesia. Penelitian ini dibuat untuk menganalisis bagaimana perbandingan hukum pidana Cyber Crime antara Indonesia dan Amerika serta mengkaji efektivitas penegakan hukum dalam mengatasi tindak kejahatan dunia maya di kedua negara. Studi ini menggunakan pendekatan yuridis normatif dengan metode analisis komparatif terhadap peraturan perundang-undangan, dan kebijakan penegakan hukum yang relevan. Hasil penelitian ini menunjukkan adanya upaya serius kedua negara dalam menangani kasus Cyber Crime, namun terdapat perbedaan antara dua negara dalam pendekatan hukum dan strategi penegakannya. Dengan demikian penelitian ini akan menunjukkan bagaimana kebijakan keduan negara dalam menangani tindak pidana Cyber Crime.

Kata kunci: *Cyber Crime****; Kejahatan Baru; Penegakan Hukum***

Abstract

As time progresses, technology also develops in line with the increasingly sophisticated progress of the times. And one of the rapidly developing technologies is information technology, which with this progress can give rise to new types of crimes often called cyber crime. This study was conducted to analyze how the comparison of Cyber Crime criminal law between Indonesia and America and to examine the effectiveness of law enforcement in overcoming cybercrime in both countries. This study uses a normative approach with a comparative analysis method of laws and regulations, and relevant law enforcement policies. The results of this study indicate that there are serious efforts by

https://doi.org/10.29303/jkh.v10i1.202

both countries in handling Cyber Crime cases, but there are differences between the two countries in their legal approaches and enforcement strategies. Thus, this study will show how the policies of both countries in handling Cyber Crime.

Keywords: Cyber Crime; New Crime; Law Enforcement

PENDAHULUAN

Istilah perbandingan hukum atau *comparative law* dalam bahasa Inggris, dikenal pula dengan Vergleichende Rechtslehre (bahasa Jerman) dan *Droit Comparé* (bahasa Prancis), merupakan cabang ilmu hukum yang mempelajari sistem hukum dari berbagai negara dengan menggunakan pendekatan perbandingan. Menurut Kamus Besar Bahasa Indonesia, perbandingan hukum adalah cabang ilmu hukum yang menggunakan metode perbandingan terhadap satu atau lebih aspek dari sistem hukum tata negara di dua negara atau lebih. Sementara itu, Black's Law Dictionary menjelaskan bahwa comparative jurisprudence merupakan studi tentang prinsip-prinsip hukum dengan membandingkan berbagai sistem hukum di dunia. Studi perbandingan ini bertujuan untuk memahami kelebihan dan kelemahan masing-masing sistem hukum, serta memberikan wawasan terhadap pengembangan sistem hukum nasional yang lebih adaptif dan responsif terhadap tantangan global.

Di era modern yang ditandai dengan kemajuan pesat teknologi informasi dan komunikasi, batas-batas geografis serta hambatan waktu antarnegara menjadi semakin kabur. Teknologi digital telah mempercepat aliran informasi, meningkatkan konektivitas global, dan mempermudah aktivitas sosial maupun ekonomi lintas negara. Namun, perkembangan ini juga membawa dampak negatif dalam bentuk meningkatnya ancaman kejahatan siber (cyber crime). Fenomena kejahatan siber mencakup berbagai bentuk pelanggaran seperti pencurian data pribadi, peretasan sistem, penyebaran malware, hingga manipulasi data untuk kepentingan tertentu yang berpotensi menyebabkan kerugian ekonomi maupun psikologis yang serius bagi korbannya. Kondisi ini menuntut negara-negara di dunia untuk menyusun regulasi yang kuat dan sistem penegakan hukum yang adaptif terhadap ancaman digital yang terus berkembang.

Indonesia dan Amerika Serikat merupakan dua negara dengan karakteristik sistem hukum dan budaya yang berbeda, tetapi sama-sama menghadapi tantangan serius dalam menangani kejahatan siber. Indonesia telah memiliki sejumlah peraturan perundang-undangan yang mengatur tentang kejahatan siber, namun masih menghadapi kendala dalam pelaksanaan, koordinasi antarinstansi, dan kapasitas penegakan hukum. Di sisi lain, Amerika Serikat mengatur kejahatan siber melalui berbagai undang-undang federal dan negara bagian, seperti Computer Fraud and Abuse Act (CFAA) dan Digital Millennium Copyright Act (DMCA), serta memiliki institusi penegakan hukum yang relatif kuat dan terkoordinasi. Perbedaan inilah yang membuka peluang untuk melakukan studi perbandingan yang mendalam terhadap sistem hukum pidana kedua negara dalam menangani kejahatan siber.

Penelitian ini bertujuan untuk mengkaji dan membandingkan pendekatan hukum pidana dalam penanganan kejahatan siber di Indonesia dan Amerika Serikat. Melalui analisis komparatif terhadap regulasi, mekanisme penegakan hukum, dan efektivitas sistem yang berlaku, diharapkan dapat ditemukan praktik-praktik terbaik yang dapat diadaptasi oleh Indonesia. Penelitian ini juga mempertimbangkan faktor sosial dan budaya yang mempengaruhi persepsi dan respons masyarakat terhadap kejahatan siber. Dengan pendekatan yuridis-normatif, penelitian ini tidak hanya menyajikan analisis

hukum secara tekstual, tetapi juga bertujuan memberikan kontribusi konkret dalam perumusan kebijakan nasional yang lebih efektif, adaptif, dan melindungi kepentingan publik dalam era digital yang terus berubah

Di dalam bukunya yang berjudul "Penelitian Hukum" Prof. Dr. Peter Mahmud Marzuki, S.h., M.S., LL.M. mengatakan bahwa saat ia mengikuti Sandwich Program di Belanda tahun 1989-1990 metode penelitian yang paling dianjurkan oleh mereka ialah metode perbandingan hukum. Hal ini sejalan dengan penelitian penulis dan oleh karena itu pula dalam penelitian ini, kami para penulis menggunakan metode penelitian yuridis normatif dengan menggunakan pendekatan perbandingan atau komparatif terhadap peraturan perundang-undangan, dan kebijakan penegakan hukum yang relevan antara Indonesia dan Amerika. Jenis data yang kami digunakan dalam penelitian ini adalah data sekunder, premier, dan tersier.

Data-data tersebut kami peroleh dengan cara menulusuri bahan-bahan yang berkaitan dengan masalah tindak pidana cyber crime. Untuk teknik pengumpulan data penelitiannya kami menggunakan metode penelitian studi kepustakan (library research) yaitu dengan membaca dan mempelajari berbagai literatur yang ada yang berkaitan menggunakan metode deskriptif dengan pendekatan kualitatif yakni penelitian yang mempelajari berbagai norma-norma hukum. Bahan yang didapat di analisis dari Presfektif Hukum yang ada di Indonesia dan Amerika. Bahan-bahan yang diperoleh dari literatur dianalisis melalui metode perbandingan hukum (komparasi) yaitu dengan mencari fakta yang konkrit kemudian ditarik kesimpulan secara general yang bersifat umum[1].

ANALISIS PEMBAHASAN

Bentuk pengaturan tindak pindana cyber crime di Indonesia dan Amerika Serikat

Dengan berkembang pesatnya teknologi saat ini yang mana salah satunya yaitu teknologi informasi maka timbulah pula kejahatan baru yang memanfaatkan perkembangan teknologi tersebut yang sering disebut sebagai *cyber crime*.[2] Tidak dapat dipungkiri bahwa hampir semua orang saat ini sangat bergantung dengan teknologi informasi. Hal inilah yang menjadi celah untuk timbulnya kejahatan baru yang memanfaatkan dunia internet sebagai alatnya. Ini dapat terjadi karena semua orang di zaman sekarang hampir selalu memanfaatkan teknologi informasi dalam menjalankan berbagai hal dalam keseharian mereka, misalya saja transaksi jual beli, berkomunikasi satu sama lain, bekerja, pengelolaan keuangan, penyimpanan data baik itu milik pribadi atau bahkan data penting milik negara, dan hal-hal lainnya yang bersifat sensitiv (Shaikh et al., 2024).

Oleh karena itu, negara-negara di berbagai dunia perlu menegakkan aturan yang dapat melindungi orang-orang yang aktivitasnya memanfaatkan teknologi informasi dari kejatan yang memanfaatkan perkembangan teknologi informasi ini (Kshetri, n.d.). Salah satu negara yang telah menerapkan aturan tentang teknologi informasi ini ialah Indonesia yang mana diatur dalam Undang-undang Nomor 1 Tahun 2024 tentang

1 Peter Mahmud Marzuki, "Penelitian Hukum, Cetakan Ke-11," *Jurnal Pembangunan Hukum Indonesia* 4, no. 2 (2022).

2 Curtis, Joanna dan Oxburgh, Gavin, Understanding cybercrime in 'real world' policing and law enforcement, Vol. 96(4), The Police Journal: Theory, Practice and Principles, 2022, hal. 573-575

Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Semasa berlakunya Undang-Undang Nomor 11 Tahun 2008 belumlah optimal dan ideal untuk menangani tindak pidana cybercrime. Pada periode berlakunya Undang-Undang Nomor 11 Tahun 2008, segala kritik tentang hak asasi manusia dalam hal kebebasan berpendapat masih rentan dikriminalisasi serta Menkominfo selaku eksekutif di bidang ITE masih mengabaikan infrastruktur pendukung akses internet bagi masyarakat, yang mana hal tersebut juga menggambarkan sekilas arah politik kebijakan (legal policy) pemerintah saat itu yang tidak memprioritaskan isu ITE sebagai prioritas utama.[3] Namun, dengan semakin maraknya tindak pidana *cyber crime* yang terjadi maka aturan tentang tindak pidana *cyber crime* juga harus di perbaharui. Hingga akhirnya keluarlah Undang-Undang Nomor 1 Tahun 2024 dimana dalam Undang-Undang ini mendapatkan penguatan ekstra, yang salah satunya berupa penambahan kewenangan bagi penyidik pejabat pegawai negeri sipil (penyidik PPNS) di bidang ITE untuk dapat melakukan pemutusan akses ITE secara sementara terhadap akun media sosial, rekening bank, uang elektronik, dan/atau aset digital yang dimiliki pelanggar hukum.

Di dalam Undang-Undang tersebut diatur bentuk-bentuk tindak pidana *cyber crime* yang terdapat pada pasal 27 sampai pasal 35 Undang-undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, yang diantaranya yaitu: 1) *Cybercrime* yang menggunakan informasi elektronik sebagai alat kejahtan, yakni Pornografi Online (*Cyber-Porno*), Perjudian Online, Pencemaran nama baik melalui media sosial, penipuan melalui informasi elektronik, pemalsuan melalui informasi elektronik, pemerasan dan pengancaman melalui informasi elektronik, penyebaran berita bohong melalui informasi elektronik, pelanggaran terhadap hak cipta, *cyber terrorism*. 2) *Cybercrime* yang berkaitan dengan informasi elektronik, jaringan sebagai sasaran untuk melakukan kejahatan, yakni akses tidak sah (*illegal acces*), menggangu sistem informasi elektronik dan data informasi elektronik, penyadapan atau intersepsi tidak sah, pencurian data, dan menyalahgunakan peralatan informasi elektronik (Sosial et al., 2023).

Beberapa Pasal di dalam UU ITE yang mengatur tentang tindak pidana cybercrime terdapat pada Pasal 27 sampai dengan Pasal 35 dan beberapa Pasal yang mengatur ancaman pidanya terdapat pada Pasal 45 sampai Pasal 52.[4] Salaha satu bunyi Pasal tersebut berupa: Pasal 29 "Setiap Orang dengan sengaja dan tanpa hak mengirimkan Informasi Elektronik dan/atau Dokumen Elektronik secara langsung kepada korban yang berisi ancaman kekerasan dan/atau menakut-nakuti" dan ancaman pidananya berupa Pasal 45B "Setiap Orang yang dengan sengaja dan tanpa hak mengirimkan informasi Elektronik dan/atau Dokumen Elektronik secara langsung kepada korban yang berisi ancaman kekerasan dan/atau menakut-nakuti sebagaimana dimaksud dalam pasal 29 dipidana dengan pidana penjara paling lama 4 (empat) tahun dan/atau denda paling banyak Rp750.000.000,00 (tujuh ratus lima puluh juta rupiah".

Selain Indonesia, negara lain yang menegakkan aturan tentang cybercrime adalah Amerika Serikat. Dimana aturan tersebut diatur di dalam Computer Fraud and Abuse Act (CFAA). Adapun bentuk-bentuk tindak pidana cyber crime yang terdapat dalam peraturan tersebut ialah berupa Memperoleh Informasi Keamanan Nasional (a)(1),

3 Awawangi, Reydi Vridell, *PENCEMARAN NAMA BAIK DALAM KUHP DAN MENURUT UU NO. 11 TAHUN 2008 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK*, Vol. 3(4), Lex Crimen, 2014, hal. 114-122

4 Pasal 27-35 dan Pasal 45-52 Undang-undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

Mengakses Komputer dan Memperoleh Informasi (a)(2), Pelanggaran di Komputer Pemerintah (a)(3), Mengakses Komputer untuk Menipu dan Memperoleh Nilai (a)(4), Sengaja Merusak dengan Mengetahui Penularannya (a)(5)(A), Merusak Secara Ceroboh dengan Akses yang Disengaja (a)(5)(B), Menyebabkan Kerusakan dan Kerugian Secara Lalai melalui Akses yang Disengaja (a)(5)(C), Perdagangan Kata Sandi (a)(6), Pemerasan yang Melibatkan Komputer (a)(7) (Newman, n.d.).

Di Amerika aturan yang mengatur tindak pidana *cyber crime* juga terdapat di dalam U.S. Code yaitu kitab undang-undang hukum pidana Amerika Serikat yang mengatur keseluruhan dari hukum yang ada. Terdapat 19 pasal yang mengatur tentang *cyber crime*. Contoh beberapa Pasal tersebut berupa:

a. 18 U.S.C § 1028 – *Fraud and related activity in connection with identification documents, authentication features, and information.*
b. Dalam pasal ini, diuraikan tentang tinda pidana penipuan dan tindak pidana lainnya yang berhubungan dengan pemalsuan dan penipuan dokumen-dokumen identifikasi, fitur otentikasi dan informasi. Seperti dalam KUHP Indonesia, terdapat perbuatan-perbuatan yang dilarang, yaitu memiliki, membuat, memiliki alat untuk membuat, menyimpan, memiliki dengan niat yang tidak baik, mengirimkan, menggunakan, atau menukarkan dengan sengaja dan tanpa hak. Hukuman untuk tindak pidana yang ada di pasal ini adalah hukuman penjara dari waktu 5 tahun sampai dengan 30 tahun penjara. Percobaan perbuatan pidana dihukum dengan hukuman yang sama dengan perbuatan yang telah dilakukan.
c. 18 U.S.C. § 1028a – *Aggravated identity theft*. Siapapun dilarang untuk menggunakan, mengirimkan, memiliki, tanpa hak yang sah, identifikasi atau dokumen palsu. Bagi yang melanggar akan dihukum penjara 2 sampai dengan 5 tahun. Dalam poin (b), pengadilan tidak diperbolehkan memberikan masa percobaan kepada orang yang melakukan pelanggaran pasal ini.
d. 18 U.S.C. § 1029 – *Fraud and related activity in connection with access devices* Pasal ini menguraikantentangperbuatanpembajakankomputer,baikkomputermilikpemerintah Amerika Serikat mau pun komputer milik warga. Hukuman yang diberikan adalah hukuman penjara mulai dari 5 sampai dengan 20 tahun. Percobaan tindak pidana dihukum dengan hukuman penjara dari 5 sampai 10 tahun.
e. 18 U.S.C. § 1030 – *Fraud and related activity in connection with computers*. Pasal ini menguraikan tentang perbuatan pembajakan komputer, baik komputer milik Amerika Serikat mau pun komputer milik warga. Hukuman yang diberikan adalah hukuman penjara mulai dari 5 sampai dengan 20 tahun. Percobaan tindak pidana dihukum dengan hukuman penjara dari 5 sampai dengan 10 tahun.
f. 18 U.S.C. § 1037 – *Fraud and related activity in connection with electronic mail* Secara umum, pasal ini menguraikan tentang ilegalnya pengiriman email dari komputer yang telah dibajak, perbuatan memalsukan kop surat elektronik, menggunakan informasi palsu saat mengakses surat elektronik. Pelanggaran akan pasal ini dihukum dengan hukuman penjara tidak lebih dari 3 sampai 5 tahun.
g. 18 U.S.C. § 1043 – *Fraud by wire, radio, or television.* Barangsiapa yang menggunakan televisi, radio, dan kabel dengan mengirimkan tulisan, tanda, sinyal, gambar atau suara dengan tujuan menguntungkan diri sendiri dengan cara menipu, dihukum penjara tidak lebih dari 20 tahun. Jika pelanggaran pasal ini menyebabkan kerugian pada institusi keuangan, maka pelakunya akan dikenai denda sebesar $1.000.000 dan/atau hukuman penjara tidak lebih dari 30 tahun.

h. 18 U.S.C. § 1466A, 2251, dan 2252, *child pornography*. 3 pasal ini secara umum mengatur tentang perbatan pornografi seksual terhadap anak. Pasal 1466A mengatur tentang dilarangnya pendistribusian, kepemilikan penerimaan segala bentuk gambar, kartun, patung yang berbentuk atau melibatkan tubuh anak. Pasal 2251 melarang tentang pornografi seksual terhadap anak. Dalam pasal 2251 diuraikan pula pelanggaran maupun percobaan pelanggaran terhadap pasal tersebut dan beberapa pasal yang sesuai dengan pasal ini, dihukum paling sedikit 30 tahun sampai dengan 35 tahun, atau hukuman seumur hidup. Pasal 2252 mengatur tentang perbuatan pornografi seksual anak yang terdapat dalam video, gambar, buku, majalah, film, atau materi lain yang mengandung gambar bergerak. Percobaan pelanggaran dan pelanggaran perbuatan ini dihukum paling sedikit 5 tahun dan paling lama 40 tahun.

Dari pemaparan di atas, terlihat adanya perbedaan mendasar antara sistem pemidanaan cybercrime di Indonesia dan Amerika Serikat. Dari segi kerangka hukum, Indonesia mengandalkan UU ITE sebagai regulasi utama, dengan tambahan aturan dalam KUHP dan KUHAP, sedangkan Amerika Serikat memiliki berbagai undang-undang khusus, seperti CFAA, ECPA, dan CISA, yang secara rinci mengatur berbagai bentuk cybercrime. Dari segi efektivitas penegakan hukum, Indonesia masih menghadapi berbagai kendala dalam pembuktian kejahatan siber, keterbatasan alat bukti elektronik, dan koordinasi antar lembaga, sementara Amerika Serikat memiliki sistem yang lebih kuat dengan dukungan dari FBI, Department of Justice (DOJ), dan Cybersecurity and Infrastructure Security Agency (CISA), yang secara khusus menangani kejahatan siber.

Dan dari segi sistem sanksi, sanksi di Indonesia cenderung lebih ringan dibandingkan Amerika Serikat.[5] Hukuman maksimal dalam UU ITE umumnya berkisar antara empat hingga sepuluh tahun penjara dengan denda hingga Rp5 miliar, sementara di Amerika Serikat, hukuman bagi pelaku cybercrime bisa mencapai puluhan tahun penjara dan denda jutaan dolar, terutama dalam kasus yang merugikan banyak pihak. Dari segi mekanisme fleksibilitas hukum, sistem di Indonesia masih bergantung pada hukum pidana klasik, tanpa adanya mekanisme seperti plea bargaining, sementara Amerika Serikat menerapkan plea bargaining, yang memungkinkan pengurangan hukuman bagi pelaku yang bekerja sama dengan aparat penegak hukum.

Berdasarkan peraturan peraturan yang diterapkan kedua negara dapat dilihat bagaimana perbandingan antara kedua negara tersebut dalam menangani tindak pidana cybercrime. Dalam hal ini Amerika memiliki peraturan yang lebih matang dibandingkan Indonesia dalam menghadapi tindak pidana cybercrime yang terlihat dari peraturannya dimana Amerika memiliki beberapa Undang-Udang yang aturannya jelas dalam mengatur tindak pidana cybercriem. Sedangkan di Indonesia aturan yang mengatur tindak pidana cybercriem belumlah ideal karena masih banyak Pasal yang malah dapat disalah gunakan (Pasal Karet).[6]

Pengaruh Dari Penegakan Kebijakan Hukum Tindak Pidana *Cyber Crime* Di Indonesia dan Amerika

Meskipun sudah ada beberapa pasal yang bisa menjerat pelaku *cyber cime* ke penjara masih dijumpai adanya hambatan-hambatan dalam pelaksanaan di lapangan yang antara lain sebagai berikut (Aprilianti, 2025):

5 IrfanSantoso dkk, *Kebijakan Hukum Pidana Terhadap Perbuatan Melawan Hukum Dalam UU ITE Pasca Berlakunya Pedoman Implementasi Pasal-Pasal Tertentu UU ITE*, Vol. 3(4), LocusJournal of Academic Literature Review, 2024, hal. 333-334

6 Shinta Ressmy Cakra Ningrat, *Pasal Karet UU ITE dan Peyelesaian Konflik Digital di Indonesia*, Vol. 4(2), Indonesian Journal of Social and Political Sciences, 2023, hal. 43-49

a. Perangkat Hukum Yang Belum Memadai

Para penyidik (khususnya Polri) melakukan analogi atau perumpamaan dan persamaan terhadap pasal-pasal yang ada dalam KUHP sependapat bahwa perlu dibuat undang-undang yang khusus mengatur *cyber crime*.

b. Kemampuan Penyidik

kemampuan penyidik Polri dalam penguasaan operasional komputer dan pemahaman terhadap hacking komputer serta kemampuan melakukan penyidikan terhadap kasus-kasus masih sangat minim. Beberapa faktor yang mempengaruhi adalah:

1) Kurangnya pengetahuan tentang komputer.
2) Pengetahuan teknis dan pengalaman para penyidik dalam menangani kasus-kasus Cybercrime masih terbatas.
3) Sistem Pembuktian dalam Hukum Acara Pidana yang menyulitkan para penyidik (M. Yustia A., 2010).

c. Alat Bukti

Saat ini telah ada alat bukti baru yang dikenal dengan alat bukti elektronik yang berupa informasi elektronik dan dokumen elektronik sebagai bentuk perkembangan dan perluasaan alat bukti yang telah ada. Dalam Pasal 44 UU ITE disebutkan selain yang telah ada di KUHAP juga dikenal dengan alat bukti yang berupa informasi elektronik dan/atau dokumen elektronik sebagaimana dimaksud dalam Pasal 1 angka (1) dan angka (4) serta Pasal 5 ayat (1), ayat (2), dan ayat (3) UU ITE.

Berdasarkan Pasal 1 angka (1) UU ITE yang termasuk ke dalam informasi elektronik adalah satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, electronic data interchange (EDI), surat elektronik (electronic mail), telegram, teleks, telecopy atau sejenisnya, huruf, tanda, angka, kode akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya.

Sementara itu menurut Pasal 1 angka (4) disebutkan yang dimaksud dengan dokumen elektronik adalah setiap informasi elektronik yang dibuat, diteruskan, dikirimkan, diterima, atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal, atau sejenisnya, yang dapat dilihat, ditampilkan, dan/atau didengar melalui komputer atau sistem elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto atau sejenisnya, huruf, tanda, angka, kode akses, simbol atau perforasi yang memiliki makan atau arti atau dapat dipahami oleh orang yang mampu memahaminya.

Persoalan alat bukti yang dihadapi di dalam penyidikan terhadap *cyber crime* antara lain berkaitan dengan karakteristik kejahatan *cyber crime* itu sendiri, yaitu ; sasaran atau media *cyber crime* adalah data dan/atau sistem komputer atau sistem internet yang sifatnya mudah diubah, dihapus, atau disembunyikan oleh pelakunya, *cyber crime* seringkali dilakukan hampir tanpa saksi, di sisi lain, saksi korban seringkali berada jauh di luar negeri sehingga menyulitkan penyidik melakukan pemeriksaan saksi dan pemberkasan hasil penyidikan.

d. Yurisdiksi

Suatu negara yang diakui hukum internasional dalam pengertian konvensional, didasarkan pada batas-batas geografis, sedangkan untuk komunikasi multimedia itu

bersifat internasional, multi yurisdiksi, dan tanpa batas, sehingga sampai saat ini belum dapat dipastikan bagaimana yurisdiksi suatu negara dapat diberlakukan terhadap komunikasi multimedia sebagai salah satu pemanfaatan teknologi informasi. Dengan demikian terkait kewenangan hukum (yurisdiksi) dalam penindakannya juga dapat menimbulkan permasalahan yang serius, hal ini dikarena internet yang tidak mengenal batas wilayah. Sehingga bisa saja terjadi tarik menarik kewenangan antara beberapa negara yang merasa dirugikan oleh tindak pidana siber dalam penegakan hukumnya.

e. Permasalahan Mengenai Locus Delicti (Tempat Kejadian Tindak Pidana)

`Dalam tindak pidana siber penyidik dapat menemukan kesulitan dalam menentukan lokasi atau tempat yang akurat terjadinya tindak pidana. Karena pelaku dapat merubah atau menghapus "jejak digital" perangkat yang dipergunakannya untuk melakukan tidak pidana siber maupun mensetting lokasi yang berbeda dengan lokasi yang sebenarnya.

f. Permasalahan Mengenai Tempus Delicti (Waktu Kejadian Tindak Pidana)

Penyidik tidak bisa menentukan kapan terjadinya tindak pidana secara tepat, karena para pelaku tindak pidana siber biasanya juga memiliki kemampuan untuk dapat mengacaukan waktu dan tanggal perbuatannya dilakukan.

Contoh Kasus Cyber Crime di Indonesia dan Penegakkan Hukumnya

a. Kasus Hacker Bjorka Terhadap Pembocoran Data:

Hacker dengan nama samaran Bjorka merupakan salah satu dari anggota Breacbed forum. Breached Forums adalah situs web dengan layanan utama berupa forum diskusi online. Sebagai sebuah situs web, Breached Forums beralamatkan di "breached.to" yang bisa diakses secara bebas oleh siapa pun.[7] bjorka dalam komunitas tersebut mendapatkan predikat sebagai God atau Dewa dan Bjorka telah menjual milyaran data pribadi dari hasil pembobolan yang dilakukannya. Bjorka pertama kali beraksi dengan mElakukan pembobolan data pribadi pengguna aplikasi Tokopedia pada Tahun 2020. Diamana data-data yang dijual berupa IDE pengguna, nomor telepon, kata sandi dan email. Akibat hal tersebut Tokopedia menanggung kerugian secara besar-besaran dikarenakan data kebocoran tersebut yang dijual olehnya di dark web memiliki nilai sebesar Rp74 juta. Lalu membobol 270 juta data pengguna Wattpad pada Juni tahun 2020. Ketiga meretas data 1,3 Miliar kartu SIM, yang mana hal ini membuat masyarakat Indonesia khawatir terhadap data yang pribadi mereka, tidak sampai itu saja situs KPU (komisi Pemilihan Umum) juga di retas olehnya. Dengan meretas situs tersebut bjorka mendapatkan NIK dan KK juga nama lengkap, setalah aksi-aksi yang telah ia lakukan tersebut, ia terus berlanjut membocorkan isi surat rahasia BIN kepada Presiden, hingga berlanjut pada aksi berikutnya dengan mengungkap data pribadi milik Jhony G. Plate setelah itu membongkar identitas pembunuh Munir, seorang aktivis Indonesia dan terakhir mengungkapkan motif sesungguhnya mengapa Bjorka melakukan aksi-aksinya.

Namun dengan sering terjadinya peretasan yang dilakukan oleh bjorka, warga internet dan media sosial di Indonesia mulai curiga kepada pemerintah karena tidak dapat melindungi informasi pribadi masyarakat Indonesia. Kebijakan yang dilakukan oleh pemerintah sangat tidak efektif, sehingga terjadi peretasan dan yang dilakukan

7 Kompas, *Apa Itu Breached Forums yang Terlibat 4 Kasus Kebocoran Data di Indonesia Sebulan Terakhir?*, https://tekno.kompas.com/read/2022/09/07/16150067/apa-itu-breached-forums-yang-terlibat-4-kasus-kebocoran-data-di-indonesia diakses pada tanggal 19 Februari 2025.

oleh Bjorka. Berdasarkan ketentuan Pasal 30 Undang-Undang Informasi dan Transaksi Elektronik Nomor 11 Tahun 2008 (UU ITE) yang mengatur tentang penolakan akses terhadap komputer dan/atau sistem elektronik dengan cara membobol atau melanggar sistem keamanan, maka Bjorka saat ini menghadapi ancaman berupa delapan tahun penjara dan denda sebesar Rp 800 juta (Dwi Putra et al., n.d.).

UU ITE hanya mengancam sanksi terhadap peretas dan membiarkan kelalaian instansidanlembagayangbertanggungjawab.(AdityaPutra,2021)PemerintahIndonesia berusaha mengatasi kejadian peretasan ini dengan membentuk payung hukum yang menutupi kejadian tersebut, termasuk UU No. 36/1999 tentang Telekomunikasi, UU No. UU Hak Cipta No. 19 Tahun 2002 15/2003 tentang Pemberantasan Terorisme, dan UU No. 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Undang-undang ini mengkriminalisasi bentuk-bentuk kejahatan dunia maya, yang dimana pelanggarnya akan menghadapi hukuman pidana.

Dalam menghadapi kemajuan teknologi yang semakin pesat juga terdapat bentuk-bentuk kejahatan baru yang harus menjadi perhatian serius dikarenakan penyelesaiannya yang rumit, maka kepolisian Indonesia melakukan beberapa upaya tindakan agar dapat mencegah kasus serupa dapat terjadi seperti Personel yaitu Polri mengirimkan anggotanya untuk ikut serta berbagai kursus di negara-negara yang maju agar dapat diterapkan di Indonesia, seperti kursus CETS di negara Kanada, *Computer Forensic* di Jepang dan *Virtual Undercover* di negara Washington; memperbarui dan mengikuti teknologi baik dalam sarana maupun prasarana; melakukan kerja sama serta koordinasi, hal itu dilakukan Polri karena dalam melakukan penyidikan kasus *cyber crime* tidak mengenal adanya batas wilayah, sehingga diperlukan kerja sama dan koordinasi dengan penegak hukum negara lain. Dan terakhir Polri memberikan sosialisasi serta pelatihan kepada Polda dan jaksa serta hakim mengenai *cyber crime* agar memiliki persepsi yang sama dalam menangani kasus *cyber crime* ini terutama dalam hal pembuktian dan alat bukti yang digunakan oleh pelaku (Saleh, 2024).

Pengaruh Kebijakan hukum dalam mengatasi kejahatan cyber crime di Indonesia dapat dilihat dari penerapan Pasal-pasal dalam Undang-Undang ITE yang mengatur tindakan yang dilarang dan memberikan dasar hukum bagi penegakan hukum terkait dengan cyber crime. Pendekatan punitif dan pendekatan budaya digunakan dalam menangani kasus-kasus tersebut, dengan upaya untuk memberi pengaruh pada peningkatan kesadaran masyarakat dan aparat penegak hukum serta mengembangkan kode etik penggunaan teknologi internet yang baik. Pendekatan Ini diharapkan dapat mengurangi pelanggaran teknologi sebagai langkah pencegahan

Penegakan Hukum mengenai tindak pidana cyber crime menjadi pengaruh penting dalam menghadapi dinamika kejahatan digital di kawasan suatu negara, terutama Indonesia, berdasarkan beberapa kajian normatif yang dilakukan melalui Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) yang disahkan pada tahun 2008 melalui undang undang nomor 11 tahun 2008 dan mengalami perubahan pada tahun 2016 dengan undang undang Nomor 19 tahun 2016, kemudian dilakukan pembaharuan kembali pada UU tersebut menjadi UU No. 1 tahun 2024 tentang perubahan kedua

atas UU Nomor 11 Tahun 2008 tentang informasi dan Transaksi Elektronik, yang memiliki beberapa kekuatan yang signifikan, kerangka hukum yang komprehensif, mencakup berbagai aspek dunia siber, mulai dari pengakuan dokumen elektronik sebagai alat bukti yang sah hingga pengaturan transaksi elektronik. Hal inilah yang memberikan landasan hukum untuk berbagai aktivitas digital, termasuk e-commerce, komunikasielektronik,danperlindungankonsumen,PengakuanAlatBuktiElektronik. Hal ini memperkuat penegakan hukum dalam kasus yang melibatkan transaksi digital atau kejahatan siber, seperti penipuan daring atau pelanggaran privasi, penekanan pada perlindungan konsumen, melindungi konsumen dari potensi penyalahgunaan teknologi, seperti pencurian identitas dan penipuan daring. Sejak disahkannya UU ITE sebagai hukum siber pertama di Indonesia, undang-undang ini telah digunakan untuk menjerat berbagai pelaku tindak pidana kejahatan siber. Menurut laporan South East Asia Freedom of Expression Network (SAFEnet), tercatat sebanyak 285 kasus telah diproses berdasarkan UU ITE sejak tahun 2008 hingga 2019.[8] Hal ini memberikan jaminan hukum bagi masyarakat dalam berinteraksi di dunia digital. Pengaruh yang cukupbesardirasakanmasyarakatterhadapUUITEinibertujuanmemberikankepastian hukum dalam penggunaan teknologi informasi, melindungi hak masyarakat di dunia maya serta mencegah dan menindak kejahatan cyber. Namun, Undang-undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik masih memiliki Beberapa tantangan dalam penegakkannya termasuk hasil pengujian materi di Mahkamah Konstitusi yang mengubah interpretasi hukum, kesulitan dalam penyidikan kejahatan teknologi informasi, dan sifat virtual ruang siber yang memungkinkan penyebaran konten ilegal dengan mudah.(Santoso et al., 2024)

Sedangkan untuk pengaruh peraturan di Amerika dapat dilihat dimana Undang-Undangnya mengatur berbagai hal dalam ranah teknologi informasi. Berbagai Undang-Undang yang mengatur tentang hal ini yaitu:

1) The National Institute of Standards and Technology (NIST) Cybersecurity Framework.NationalInstituteofStandardsandTechnology(NIST)mengembangkan Cybersecurity Framework untuk menyediakan pedoman dan praktik terbaik bagi organisasi dalam mengelola dan meningkatkan manajemen risiko keamanan siber mereka. Kerangka kerja ini mencakup standar, pedoman, dan praktik untuk meningkatkan keamanan siber. Organisasi di Amerika Serikat didorong untuk menggunakan Kerangka Kerja Keamanan Siber NIST untuk menilai dan meningkatkan postur keamanan siber mereka, yang sejalan dengan kebutuhan manajemen risiko dan tujuan bisnis mereka. Kemampuan adaptasi kerangka kerja ini memungkinkannya untuk diterapkan di berbagai sektor, yang berkontribusi pada dunia maya yang lebih tangguh dan aman.
2) Health Insurance Portability and Accountability Act (HIPAA).

HIPAA menetapkan standar untuk perlindungan informasi kesehatan pasien yang sensitif. Entitas yang tercakup, termasuk penyedia layanan kesehatan dan perusahaan asuransi kesehatan, harus mematuhi peraturan HIPAA untuk

8 Kominfo, Mengungkap Kegaduhan Publik Soal UU ITE, Menkominfo: Implementasinya untuk Pemanfaatan Ruang Digital, https://aptika.kominfo.go.id/2021/02/mengungkap-kegaduhan-publik-soal-uu-ite-menkominfo-implementasinya-untuk-pemanfaatan-ruang-digital/ diakses pada tanggal 19 Februari 2025.

memastikan kerahasiaan, integritas, dan ketersediaan informasi kesehatan. Peraturan Keamanan HIPAA menguraikan kerangka kerja komprehensif untuk mengamankan PHI elektronik (ePHI). Peraturan ini mengamanatkan bahwa entitas yang tercakup, seperti penyedia layanan kesehatan, rencana kesehatan, dan lembaga kliring layanan kesehatan, menerapkan perlindungan administratif, fisik, dan teknis untuk memastikan kerahasiaan, integritas, dan ketersediaan ePHI. Kerangka kerja tersebut mencakup langkah-langkah seperti kontrol akses, enkripsi, kontrol audit, dan penilaian risiko. Entitas yang tercakup diharuskan untuk melakukan penilaian risiko secara berkala untuk mengidentifikasi dan mengurangi potensi kerentanan dalam sistem informasi mereka dan mengadopsi kebijakan dan prosedur untuk melindungi ePHI dari akses atau pengungkapan yang tidak sah. Kerangka kerja yang disediakan oleh HIPAA sangat penting untuk mempengaruhi tingkat kepercayaan pada sistem layanan kesehatan dan melindungi informasi kesehatan sensitif individu dalam lingkungan layanan kesehatan yang semakin digital dan saling terhubung.

3) Gramm-Leach-Bliley Act (GLBA)

GLBA mengharuskan lembaga keuangan untuk menjaga kerahasiaan informasi keuangan pribadi nasabah. GLBA mencakup ketentuan mengenai keamanan dan kerahasiaan informasi pribadi nonpublik dan mengamanatkan pengembangan dan penerapan program keamanan informasi. Berdasarkan GLBA, dapat mempengaruhi lembaga keuangan dimana lembaga keuangan diharuskan untuk mengembangkan, menerapkan, dan memelihara program keamanan informasi yang komprehensif. Program-program ini harus mencakup perlindungan administratif, teknis, dan fisik untuk melindungi keamanan, kerahasiaan, dan integritas informasi nasabah. Undang-Undang tersebut juga mengamanatkan bahwa lembaga keuangan memberikan pemberitahuan privasi yang jelas dan ringkas kepada konsumen, yang merinci praktik berbagi informasi lembaga tersebut dan memberikan nasabah pilihan untuk memilih tidak membagikan informasi mereka dengan pihak ketiga yang tidak terafiliasi.

4) Federal Information Security Modernization Act (FISMA)

Undang-Undang Modernisasi Keamanan Informasi Federal (FISMA), yang disahkan pada tahun 2002, merupakan undang-undang keamanan siber utama di Amerika Serikat. Undang-undang ini mengamanatkan lembaga federal untuk menerapkan kontrol keamanan guna melindungi sistem informasi dan data mereka. Tujuan utamanya adalah untuk memastikan kerahasiaan, integritas, dan ketersediaan informasi yang dikumpulkan, disimpan, dan digunakan oleh lembaga federal. Denagn adanya FISMA, mempengaruhi lembaga untuk membuat program keamanan informasi yang komprehensif, yang mencakup penilaian risiko rutin, pengujian keamanan, perencanaan respons insiden, dan pemantauan berkelanjutan terhadap kontrol keamanan. Selain itu, lembaga diharuskan melaporkan kepatuhan mereka terhadap hukum kepada Office of Management and Budget (OMB)/ Kantor Manajemen dan Anggaran dan Department of Homeland Security (DHS)/ Departemen Keamanan Dalam Negeri. FISMA menunjuk National Institute of Standards and Technology (NIST)/Institut Standar dan Teknologi Nasional sebagai badan utama yang bertugas membuat standar dan pedoman keamanan bagi lembaga federal. "Publikasi Khusus NIST 800-53" menyediakan kerangka kerja komprehensif yang merinci kontrol keamanan yang harus diadopsi lembaga federal untuk memenuhi persyaratan FISMA.

5) Cybersecurity Information Sharing Act (CISA)

Undang-Undang Pembagian Informasi Keamanan Siber (CISA), yang disahkan pada tahun 2015 oleh Kongres AS, mendorong perusahaan swasta untuk berbagi informasi tentang ancaman siber dengan pemerintah dan memberikan perlindungan tanggung jawab atas pembagian tersebut. Dalam hal ini CISA memiliki pengaruh untuk meningkatkan pertukaran informasi ancaman siber antara pemerintah dan sektor swasta, yang bertujuan untuk melindungi infrastruktur penting dan keamanan nasional dari serangan siber. CISA mengizinkan perusahaan swasta untuk berbagi data ancaman siber dengan lembaga federal, termasuk epartment of Homeland Security (DHS)/Departemen Keamanan Dalam Negeri, dan memungkinkan pembagian informasi secara timbal balik dari pemerintah ke entitas swasta(Oluomachi et al., 2024).

Peraturan-peraturan dan kebijakan keamanan siber di atas memiliki pengaruh penting dalam menjaga lanskap digital Amerika Serikat. Dalam beberapa tahun terakhir, meningkatnya frekuensi dan kecanggihan ancaman siber telah mendorong pemerintah untuk menetapkan kerangka kerja yang komprehensif guna melindungi infrastruktur penting, data sensitif, dan keamanan nasional. Efektivitas peraturan dan kebijakan ini menjadi subjek pengawasan dan evaluasi yang berkelanjutan. Salah satu inisiatif penting dalam bidang keamanan siber adalah the Cybersecurity Enhancement Act tahun 2014, yang memperkuat upaya penelitian dan pengembangan, menetapkan praktik terbaik, dan meningkatkan koordinasi antara pemerintah dan sektor swasta. Undang-undang tersebut menekankan pentingnya berbagi informasi dan kolaborasi untuk mengurangi ancaman siber secara efektif(Ajayi, 2016).

Pembentukan CISA pada tahun 2018 menandai tonggak sejarah dalam konsolidasi upaya keamanan siber dalam pemerintahan Amerika (Chairul et al., 2019). CISA memainkan peran utama dalam mengokordinasikan inisiatif keamanan siber, memberikan dukungan kepada entitas infrastruktur penting, dan menyebarluaskan intelijen ancaman. Upaya lembaga ini ditujukan untuk memperkuat ketahanan negara terhadap ancaman siber. Selain itu, regulasi di sektor khusus, seperti HIPAA untuk sektor perawatan kesehatan dan PCI DSS untuk industri keuangan, berkontribusi pada pendekatan yang lebih khusus dalam menangani kerentanan sektor khusus. Peraturan ini mengamanatkan tindakan dan praktik keamanan siber tertentu, yang mendorong sikap proaktif terhadap ancaman siber dalam industri yang menangani informasi sensitif(Chairul et al., 2019).

b. Contoh Kasus Cyber Crime Di Amerika Dan Penegakan Hukumnya

Pada tahun 2016, Donal Trump resmis terpilih menjadi Presiden Amerika Serikat ke-45, setelah resmi memenangkan pemilihan umum melawan kandidat Hillary Clinton. Trump berhasil meraih kemenangan di negara-negara bagian seperti Florida dan Ohio, bahkan Pennsylvania yang sering kali dikuasai oleh calon dari Partai Demokrat. Dia juga berhasil menang di Wisconsin, yang sebelumnya diprediksi bakal dimenangkan oleh Hillary Clinton. Dengan kampanye yang menarik banyak perhatian, kemenangan Trump menjadi sebuah hasil yang tidak terduga (Indah et al., 2022).

Pada tahun 2018, sejumlah media berita utama di Inggris menerbitkan hasil penyelidikan bersama yang menunjukkan bahwa Cambridge Analytica (CA), sebuah firma konsultan politik dan analisis data, berhasil mengumpulkan lebih kurang 87 juta informasi pribadi dari pengguna Facebook yang kemudian dimanfaatkan tanpa seizin pemilik informasi tersebut. Studi ini bertujuan untuk memahami dan menganalisis

pelanggaran hak data yang melibatkan Cambridge Analytica dan Facebook selama pemilihan presiden di Amerika Serikat tahun 2016.

CA diketahui berkolaborasi dengan kampanye Donald Trump melalui pengumpulan informasi pengguna dari pemilih di AS, serta memanfaatkan informasi tersebut untuk mengembangkan perangkat lunak yang mampu memprediksi dan mempengaruhi keputusan di tempat pemungutan suara. CA mengklaim memiliki 5.000 poin data untuk setiap pemilih di AS. Dengan menerapkan analisis psikografi pada kumpulan data yang mereka miliki, CA mengklaim dapat mengidentifikasi tipe kepribadian masing-masing individu dan selanjutnya mengirimkan pesan atau iklan untuk memengaruhi tindakan mereka. Dalam dokumen resmi perusahaan, CA menyatakan bahwa mereka telah menyediakan keahlian dan wawasan yang mendukung kampanye Trump.

Aksesibilitas informasi serta pengaruh politik yang dimiliki oleh perusahaan-perusahaan teknologi menghadapi protes dan kritik dari pengguna berkenaan dengan pelanggaran privasi serta perlindungan data, dan juga keterlibatan dalam pemilu serta aktivitas politik lain. Perdebatan mengenai CA berpusat pada efeknya terhadap perlindungan privasi dan informasi pribadi. Setelah terungkapnya skandal data CA dan keterlibatannya dalam pemilihan presiden di AS, masyarakat global mendesak tindakan terkait hak atas data. Selain itu, terdapat tekanan pada perusahaan teknologi, khususnya Facebook, untuk mengatur penggunaan informasi pribadi pengguna.

CA diduga melakukan pemodelan data, menargetkan dan menayangkan iklan digital, serta menyusun daftar dan polling untuk proyek kampanye seperti Make America Number One dan Defeat Crooked Hillary saat pemilihan presiden 2016. Fokus utama dari operasi CA adalah untuk menciptakan Principal Audience (PA), yaitu segmen pemilih yang dianggap paling mungkin dapat dipengaruhi. Setelah PA diidentifikasi, tahap berikutnya adalah menentukan jenis pesan atau iklan yang akan disampaikan. Pada bulan Maret 2018, The Guardian, The New York Times, dan Channel 4 News secara bersamaan menerbitkan hasil penyelidikan untuk mengungkap fakta tentang apa yang terjadi di dalam CA dan Facebook. Kemudian pada bulan Juni 2018, Christopher Wylie memberikan kesaksian di depan Kongres AS mengenai CA sebagai direktur penelitian di perusahaan itu. Wylie menghadirkan bukti terkait data Facebook yang telah dimanfaatkan oleh perusahaan tersebut. Mereka memanfaatkan Facebook untuk meraih akses ke lebih dari 87 juta akun individu dan menggunakan informasi tersebut untuk mempengaruhi pemilih Afrika-Amerika. Kumpulan data itu mencakup rincian lengkap dari puluhan ribu pengguna seperti nama, jenis kelamin, usia, lokasi, pembaruan status, suka, teman, bahkan pesan pribadi.

Dari hasil yang diperoleh, CA mampu mengenali individu yang memiliki tingkat neurotisisme tinggi dan yang cenderung mengalami kemarahan impulsif atau mengikuti teori konspirasi. Mereka kemudian memberikan perhatian terhadap kelompok ini, menyebarluaskan cerita melalui grup Facebook, iklan, atau tulisan yang telah terbukti dalam uji internal perusahaan dapat memicu kemarahan dan meningkatkan partisipasi. CA dapat melakukannya berkat fitur tertentu dalam algoritma Facebook, yang mulai merekomendasikan cerita dan halaman serupa demi meningkatkan keterlibatan pengguna. Selanjutnya, CA menciptakan halaman palsu di Facebook dan

platform lain yang menyerupai forum nyata. Mereka melakukannya dengan menjangkau komunitas lokal melalui pembuatan halaman alt-right dengan nama tiruan seperti Smith Country Patriots atau I love My Country. Dengan menciptakan halaman ini, algoritma rekomendasi Facebook memastikan bahwa halaman-halaman tersebut muncul di beranda pengguna yang menyukai konten serupa. Setelah individu bergabung dengan grup palsu tersebut, CA akan membagikan video dan artikel yang dapat menstimulasi emosi serta kemarahan. Selain penggunaan grup palsu dan iklan digital, mereka juga memanfaatkan trolling dan perundungan siber sebagai metode efektif untuk mengendalikan kelompok alt-right. Bannon mengubah CA menjadi alat untuk intimidasi otomatis dan kekerasan psikologis dalam skala besar, salah satunya dengan menyebarkan konten mengenai persaingan rasial di Amerika Serikat. Gambar di bawah menunjukkan bagaimana perpaduan antara psikologi perilaku, data besar, dan keterlibatan yang terarah dapat mengubah perilaku sasaran.

Kampanye iklan digital yang bernama Defeat Crooked Hillary diklaim sangat berhasil dalam mencapai dan meyakinkan pemilih yang masih merasa ragu. Secara keseluruhan, iklan tersebut mendapatkan tayangan sebanyak 21.718.189 kali dan lebih dari 1.433.331 orang mengunjungi defatcrookedhillary.com serta 2016truths.com. Iklan itu menunjukkan performa terbaik di platform Facebook dan Google Search. Video dengan judul 'Can't Run Her House' juga dikatakan sangat berhasil dalam mempengaruhi wanita di kelompok pemilih yang ragu untuk tidak memilih Hillary Clinton. Setelah melakukan survei tentang Ad Recall and Impact, CA menemukan bahwa iklan ini menunjukkan efektivitas khususnya di negara bagian Florida, dengan meningkatnya minat untuk memilih Donald Trump sebesar lebih dari 8 persen. Video ini ditampilkan kepada sekelompok pemilih yang menganggap keamanan nasional sebagai salah satu dari tiga isu paling penting bagi mereka. Selain menyebarluaskan iklan di media sosial, CA juga merancang dan mengelola tiga situs web yaitu Defeat Crooked Hillary, 2016 Truths, dan Save the Supreme Court.

Platform media sosial memiliki kemampuan untuk mengawasi dan mengatur apa yang dapat dilihat atau dialami oleh pengguna di dunia maya, dengan niat mempertahankan kehadiran pengguna di situs mereka selama mungkin. Dengan cara menarik perhatian, mengumpulkan informasi pribadi, dan menjual akses data pengguna, perusahaan dapat menargetkan pengguna dengan iklan yang mengundang klik serta konten yang menjadi viral, yang kadang-kadang menghasilkan efek samping yang tidak diinginkan. Efek samping ini termasuk memperdaya pengguna dengan individu yang menyebarkan informasi yang salah serta menciptakan lingkungan daring yang memicu kemarahan, seperti yang dilakukan oleh CA. Hal ini akan diuraikan lebih lanjut di sub-bab berikut yang membahas tentang data yang berfungsi sebagai kekuatan dalam modifikasi perilaku, terutama dalam konteks perilaku pemilih.

Privasi data merupakan suatu hak yang dijamin dalam Piagam Internasional Hak Asasi Manusia PBB, seperti yang dinyatakan dalam Kovenan Internasional tentang Hak Sipil dan Politik (ICCPR). Dalam Pasal 17 GC No. 16-10 ICCPR, terdapat pernyataan bahwa "pengumpulan dan penyimpanan informasi pribadi pada komputer, bank data, dan perangkat lain, baik oleh otoritas publik maupun individu atau badan swasta,

harus diatur oleh hukum" (Komite Hak Asasi Manusia PBB, 1988). Melalui ICCPR, komisi hak asasi manusia PBB menyatakan bahwa untuk menghargai hak privasi, pemerintah perlu mengatur cara perusahaan swasta menangani data pribadi (Human Rights Watch, 2021). Walaupun perjanjian terkait hak asasi manusia seperti ICCPR hanya mengikat negara, terdapat Prinsip Panduan tentang Bisnis dan Hak Asasi Manusia yang menekankan bahwa pelaku bisnis wajib menghormati hak asasi manusia. UNHCHR juga secara khusus mengingatkan perusahaan yang beroperasi secara daring untuk memperhatikan hak asasi manusia dalam kegiatan bisnis mereka.

Sebagai akibat dari keterlibatan dalam masalah data CA, Facebook dikenakan sanksi sebesar 5 miliar dolar AS. Berdasarkan informasi dari laman resmi Komisi Negara Bagian Federal AS, jumlah denda tersebut merupakan sanksi terbesar yang pernah diberikan kepada sebuah perusahaan karena pelanggaran privasi pengguna dan hampir dua puluh kali lipat lebih tinggi dibandingkan sanksi privasi ataupun keamanan data yang diberlakukan di seluruh dunia. Mengenai denda ini, Prof Carroll memiliki perspektif yang berbeda dibandingkan Eduard Blasi. Sanksi tersebut mungkin efektif untuk mencegah tindakan perusahaan, tetapi dianggap kurang memadai sebagai sebuah hukuman. Menurut Prof Carroll, "denda akibat penyalahgunaan data hanyalah biaya dalam menjalankan bisnis." Oleh karena itu, penjelasan tentang algoritma seharusnya menjadi alat utama dalam regulasi perlindungan data. Selain itu, perusahaan dari semua ukuran, baik kecil, menengah, besar, maupun yang bersifat monopoli, harus menghadapi konsekuensi, misalnya, data dan algoritma berharga mereka dapat dirampas dan dihancurkan jika terbukti melakukan penyalahgunaan data secara besar-besaran atau mengeksploitasi data dengan cara yang melawan hak asasi manusia (Khadam et al., 2023).

KESIMPULAN

Perkembangan teknologi yang kian pesat mulai memunculkan bentuk kejahatan baru yaitu dalam bentuk kejahatan siber. Hampir semua detail kehidupan modern bergantung pada teknologi informasi, yang memberikan kesempatan bagi penjahat untuk memanfaatkan kelemahan yang ada dalam sistem digital. Oleh karena itu, sejumlah negara, termasuk Indonesia dan Amerika Serikat, telah menciptakan peraturan untuk mengatasi dan mencegah tindakan kriminal siber. Di Indonesia, kejahatan siber diatur melalui Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), yang terus diperbaharui, yang kemudian sekarang diatur dalam Undang-Undang No. 1 Tahun 2024. Peraturan ini memperluas kewenangan bagi aparat penegak hukum dalam menangani isu kejahatan siber, walaupun masih terdapat sejumlah tantangan dalam pelaksanaan dan ruang hukum yang bisa dieksploitasi. Sementara itu, di Amerika Serikat, terdapat regulasi yang lebih maju, seperti Computer Fraud and Abuse Act (CFAA) dan berbagai undang-undang lainnya yang mengatur secara spesifik beragam bentuk kejahatan siber. Sistem hukum di AS juga lebih ketat, dengan sanksi yang jauh lebih berat dibandingkan di Indonesia, serta memiliki institusi khusus seperti FBI dan CISA yang fokus pada keamanan siber.

Kekuatan utama Undang-Undang ITE terletak pada cakupan regulasinya yang mencakup aspek perlindungan informasi elektronik, transaksi digital, dan penanganan tindak pidana cyber. Namun kelemahan mendasar muncul dalam penegakan hukum

yang sering dianggap belum mencapai kata efektif dan konsisten, rendahnya kapasitas penegak hukum serta minimnya harmonisasi antara peraturan perundang-undangan yang berkaitan dengan hukum cyber menjadi kendala signifikan. Meskipun Hukum cyber crime di Indonesia telah memiliki fondasi yang baik, terdapat berbagai kebutuhan lain untuk mendorong efisiensi dan relevansi nya, dengan mengambil pelajaran dari negara Amerika serikat, Indonesia dapat memposisikan diri sebagai pengembangan hukum cyber yang responsif dan adaptif terhadap tantangan digital. Secara keseluruhan, perbandingan antara kebijakan hukum kejahatan siber di Indonesia dan Amerika Serikat menunjukkan bahwa Amerika memiliki sistem yang lebih holistik dan efisien dalam menghadapi ancaman siber. Indonesia masih berhadapan dengan berbagai kendala terkait penegakan hukum, pembuktian kasus kejahatan siber, dan perlindungan atas hak digital masyarakat.

1. Rekomendasi untuk Penelitian Selanjutnya:
   a. Studi Lapangan Mendalam Penelitian kualitatif yang lebih mendalam mengenai pengalaman korban dari kedua pendekatan (restorative justice dan sanksi disipliner) dapat memberikan wawasan lebih tentang dampak jangka panjang dari masing-masing model. Penelitian ini bisa mencakup wawancara dengan korban, pelaku, serta pihak terkait lainnya untuk mengukur efektivitas program rehabilitasi. Misalnya, studi kasus yang relevan seperti kasus di Bekasi pada tahun 2023 dan Kim Garam pada 2018 bisa dianalisis untuk mendapatkan perspektif yang lebih holistik.
   b. Pendekatan Interdisipliner Untuk memperkaya analisis, penelitian mendatang bisa mengintegrasikan perspektif psikologi untuk menilai dampak psikologis dari kedua pendekatan tersebut, terutama efek trauma pada korban. Sosiologi juga bisa digunakan untuk menganalisis dampak sosial dari praktik penyelesaian kasus di kedua negara. Sebagai contoh, bisa dilakukan pengukuran tingkat depresi pada korban yang mengikuti mediasi di Indonesia dibandingkan dengan korban yang mengalami sanksi disipliner di Korea Selatan.
   c. Partisipasi Stakeholder Melibatkan berbagai stakeholder yang terlibat dalam implementasi kebijakan seperti guru, orang tua, serta komunitas lokal sangat penting dalam desain penelitian berikutnya. Hal ini dapat membantu peneliti memahami lebih mendalam tantangan yang dihadapi pada tingkat lokal dalam implementasi kebijakan. Fokus Group Discussion (FGD) dengan Komite Kekerasan Sekolah di Korea Selatan dan Komite Perlindungan Anak di Indonesia akan memberikan wawasan langsung tentang isu-isu yang dihadapi dalam praktiknyaPerbandingan Global Penelitian selanjutnya dapat memperluas cakupan dengan membandingkan model penanganan kasus bullying dari negara-negara lain yang memiliki pendekatan berbeda, seperti negara-negara Skandinavia yang lebih menekankan pada pencegahan (preventif) atau Amerika Serikat yang menerapkan kebijakan zero tolerance. Perbandingan ini bisa mengidentifikasi best practices yang dapat diadopsi oleh Indonesia dan Korea Selatan dalam meningkatkan penanganan bullying.
   d. Kebijakan Berbasis Bukti Penelitian lebih lanjut dapat mendorong kebijakan berbasis bukti yang mendalam, termasuk analisis dampak dari Rancangan Undang-Undang Perlindungan Anak di Indonesia atau amendemen pada Juvenile Act di Korea Selatan. Data empiris mengenai tingkat rekidivisme pelaku dapat menjadi dasar untuk reformasi kebijakan yang lebih efektif, serta mengukur keberhasilan kebijakan yang sudah diterapkan.
   e. Implikasi Praktis

- Indonesia: Perlu dilakukan standarisasi mekanisme rehabilitasi bagi korban dan pelaku, serta penguatan regulasi terkait dengan cyberbullying. Masyarakat harus diberikankesadaranyanglebihtentangperlindungandatapribadidancaramelindungi diri dari dampak bullying di dunia maya.
- Korea Selatan: Mengintegrasikan pendekatan restoratif dalam sistem yang sudah ada, untuk mengurangi stigmatisasi pada pelaku. Meskipun sistem disipliner sangat penting, upaya restorasi bisa memberikan peluang lebih besar untuk rehabilitasi pelaku tanpa mengabaikan sistem disiplin yang sudah ada.

2. Metodologi yang Dapat Ditingkatkan

   Untuk penelitian lebih lanjut, ada beberapa aspek metodologi yang bisa diperbaiki guna menghasilkan hasil yang lebih mendalam dan valid:

   - Penggunaan Alat Analisis yang Lebih Canggih: Penggunaan teknik analisis yang lebih maju, seperti analisis regresi atau model statistik yang lebih kompleks, dapat membantu mengukur hubungan antara kebijakan dan hasil yang diinginkan, serta memberikan gambaran yang lebih jelas mengenai faktor-faktor yang mempengaruhi efektivitas kebijakan.
   - Sampel yang Lebih Besar dan Diversifikasi: Penelitian dapat menggunakan sampel yang lebih besar dan beragam untuk memastikan hasil yang lebih representatif, terutama jika ingin menggali lebih dalam perbedaan efektivitas antara kedua negara atau bahkan dalam konteks internasional.
   - Pendekatan Multi-Disiplin: Mengintegrasikan pendekatan multi-disiplin seperti psikologi, sosiologi, dan hukum akan memberikan gambaran yang lebih komprehensif dan realistis mengenai pengaruh kebijakan terhadap para korban dan pelaku bullying, serta masyarakat secara keseluruhan.

3. Kontribusi terhadap Kebijakan

   Hasil dari penelitian ini dapat memberikan kontribusi yang signifikan bagi kebijakan atau praktik administratif terkait dengan penanganan kejahatan siber dan bullying anak, baik di Indonesia maupun Korea Selatan

   - Indonesia: Penelitian ini dapat membantu merumuskan kebijakan yang lebih efektif dalam mengatur tindak pidana cyber crime dan pelanggaran data pribadi. Pemerintah dapat memperbaiki sistem hukum terkait dengan perlindungan anak di dunia maya, serta memastikan mekanisme penegakan hukum lebih efisien.
   - Korea Selatan: Penelitian ini juga dapat memberikan wawasan bagi Korea Selatan dalam mengintegrasikan pendekatan restoratif dalam penegakan hukumnya. Hal ini akan mendukung terciptanya sistem yang tidak hanya menghukum, tetapi juga memberikan kesempatan bagi rehabilitasi pelaku untuk kembali ke masyarakat dengan lebih baik.
   - Penelitian ini diharapkan dapat memberikan kontribusi pada perbaikan kebijakan yang lebih baik, baik secara normatif maupun praktis, dan menyediakan dasar yang kuat untuk kebijakan yang lebih inklusif dan berbasis bukti.

DAFTAR PUSTAKA

Artikel Jurnal

Ajayi, E. F. G. (2016). Challenges to enforcement of cyber-crimes laws and policy. Journal of Internet and Information Systems, 6(1), 1–12. https://doi.org/10.5897/jiis2015.0089

Aprilianti, A. (2025). Efektivitas dan Implementasi Undang-Undang Informasi dan Transaksi Elektronik sebagai Hukum Siber di Indonesia: Tantangan dan Solusi. Begawan Abioso, 15(1), 41–50. https://doi.org/10.37893/abioso.v15i1.1002

Chairul, M., Umanailo, B., Nwankwo, W., Fachruddin, I., Mayasari, D., Kurniawan, R., Agustin, N., Ganefwati, R., Daulay, P., Meifilina, A., Alamin, T., Fitriana, R., Sutomo, S., Sulton, A., Noor, I. L., Rozuli, A. I., George, T., & Hallatu, R. (2019). Cybercrime Case As Impact Development Of Communication Technology That Troubling Society. INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH, 8(09). www.ijstr.org

Khadam, N., Anjum, N., Alam, A., Ali Mirza, Q., Assam, M., Ismail, E. A. A., & Abonazel, M. R. (2023). How to punish cyber criminals: A study to investigate the target and consequence based punishments for malware attacks in UK, USA, China, Ethiopia & Pakistan. Heliyon, 9(12). https://doi.org/10.1016/j.heliyon.2023.e22823

Oluomachi, E., Ahmed, A., Ahmed, W., & Samson, E. (2024). ASSESSING THE EFFECTIVENESS OF CURRENT CYBERSECURITY REGULATIONS AND POLICIES IN THE US. International Journal of Scientific and Research Publications, 14(2), 78. https://doi.org/10.29322/IJSRP.14.02.2024.p14610

Santoso, I., Syahrin, A., Mulyadi, M., & Agusmidah, A. (2024). Kebijakan Hukum Pidana Terhadap Perbuatan Melawan Hukum Dalam UU ITE Pasca Berlakunya Pedoman Implementasi Pasal - Pasal Tertentu UU ITE. Locus Journal of Academic Literature Review, 3(4), 329–335. https://doi.org/10.56128/ljoalr.v3i4.312

Buku dan Buku Teks

Marzuki, P. M. (2021). Penelitian Hukum (Suwito, Ed.; Revisi, Vol. 15). K E N C A N A.

Laporan dan Studi Kasus

Aditya Putra, F. (2021). Tata Kelola Ekosistem Berbagi Informasi Keamanan Siber pada Information Sharing and Analysis Center (ISAC) Sektor Pemerintah Daerah di Indonesia.

Agus Fajar Syaefudin, M., Fajar Ari Sudewo, S., Kus Rizkianto, M., & Hukum Siber, M. (n.d.). HUKUM SIBER (Perbandingan Indonesia dan Malaysia).

Dwi Putra, R., Ul Hosnah, A., & Zaki Rizaldi, M. (n.d.). Analisis Kasus Cybercrime Dengan Studi Kasus Hacker Bjorka Terhadap Pembocoran Data. http://jurnal.um-tapsel.ac.id/index.php/justitia

Indah, M., Arfin, B., Wawan, S., & Darmawan, B. (2022). Data Rights di Era Surveillance Capitalism: Skandal Data Cambridge Analytica & Facebook dalam Pemilihan Presiden Amerika Serikat 2016. Hasanuddin Journal of International Affairs (Vol. 2, Issue 2). Online.

Sosial, J. I., Humaniora, D., Ramadoni, S. R., Pramasta Gegana, R., & Sanata, K. (2023). LANGGONG: Sejarah Undang-Undang ITE: Periodisasi Regulasi Peran Negara dalam Ruang Digital (Vol. 3, Issue 2). https://jurnal.fkip.unmul.ac.id/index.php/langgong

Artikel Berita dan Online

Kshetri, N. (n.d.). Pattern of Global Cyber War and Crime: A Conceptual Framework.

Artikel dan Review Teoritis

Shaikh, S. H., Pandurang Datir, A., & Satish Birajdar, A. (2024). Cyber Security in the Age of Digital Transformation.

M. Yustia A. (2010). Pembuktian dalam Hukum Pidana Indonesia terhadap Cyber Crime. PRANATA HUKUM.

Newman, B. R. (n.d.). Pleading with Particularity: Decoding When Computer Fraud and Pleading with Particularity: Decoding When Computer Fraud and Abuse Act Claims Must Comply with Rule 9(b). Pepperdine Law Review (Vol. 52). https://digitalcommons.pepperdine.edu/plr/vol52/iss1/4