TINJAUAN HUKUM INFORMASI DAN TRANSAKSI ELEKTRONIK DALAM KAITAN DENGAN PERBUATAN KEJAHATAN HACKING [1]

Oleh :
Damaiyela M.C Lahamendu [2]
Cornelis Dj. Massie [3]
Decky J. Paseki [4]

ABSTRAK

Penelitian ini bertujuan untuk mengetahui, memahami, dan mengerti bagaimana pengaturan terhadap perbuatan hacking dan cracking dalam perspektif hukum informasi dan transaksi elektronik dan untuk mengetahui, memahami, dan mengerti akibat hukum yang ditimbulkan dari perbuatan hacking dan cracking dalam perspektif hukum informasi dan transaksi elektronik. Dengan menggunakan metode penelitian normatif, dapat ditarik kesimpulan yaitu : 1. Definisi kejahatan hacking telah diatur dalam Undang-Undang Informasi dan Transaksi Elektronik Pasal 40. Permasalahan kejahatan didunia maya selama ini tidak diatur dalam Kitab Undang- Undang Pidana (KUHP), maka dari itu terbentuklah Undang- undang Nomor 1 Tahun 2024 Tentang Perubahan Kedua Undang- undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik yang menjadi lex specialis dalam mengatur tindakan di bidang telematika. Namun tindakan tersebut merupakan suatu tindakan ilegal dan hal tersebut telah diatur dalam Undang-Undang Informasi dan Transaksi Elektronik terdapat dalam Pasal 30. 2. Akibat yang ditimbulkan dari tindakan hacking dan craking merupakan suatu perbuatan melawan hukum tanpa hak membobol dan juga merusak system jaringan computer milik orang/ badan hukum tanpa izin dari pemilik tersebut. Sanksi yang dikenakan akibat tindakan ini adalah sanksi pidana yang telah diatur dalam Undang-Undang Informasi dan Transaksi Elektronik selanjutnya dijelaskan dalam pasal 45 samapai dengan pasal 51.

Kata Kunci : *hacking, ITE*

PENDAHULUAN

A. Latar Belakang

Teknologi informasi (*Information Technology*) memegang peran yang sangat penting, baik dimasa sekarang maupun dimasa yang akan datang. Teknologi informasi di yakini akan membawa keuntungan yang sangat besar bagi negara-negara di dunia. Ada 2 hal yang membuat teknologi informasi dianggap penting dalam memacu pertumbuhan ekonomi dunia. *Pertama*, teknologi informasi mendorong permintaan atas produk-produk teknologi informasi itu sendiri. Seperti, sarana membangun jaringan internet dan sebagainya. *Kedua*, memudahkan transaksi bisnis terutama bisnis dalam bidang keuangan di samping bisnis-bisnis pada umumnya.[5]

Teknologi informasi secara perlahan membantu merubah perilaku dan peradaban manusia secara global. Perkembangan teknologi informasi ini telah menyebabkan dunia menjadi tanpa batas *(borderless)* dan menyebabkan perubahan sosial secara signifikan berlangsung demikian. Sehingga dapat dikatakan bahwasanya teknologi informasi yang berkembang ini bisa diistilahkan sebagai pedang bermata dua, karena dapat memberikan dampak yang baik dan buruk sekaligus. Tetapi teknologi mutakhir untuk meningkatkan kesejahteraan, kemajuan, dan peradaban manusia, dan bisa menjadi sarana efektif perbuatan melawan hukum.[6]

Seiring perkembangannya zaman kemudian lahirlah suatu rezim baru yang dikenal dengan istilah siber atau hukum telematika. Hukum telematika sendiri merupakan perwujudan dari konvergensi hukum telekomunikasi, hukum media, dan hukum informatika. Maka dari itu yang menjadi permasalahan hukum yang sering dihadapi adalah ketika terkait dengan penyampaian informasi, komunikasi, dan atau transaksi secara elektronik, dalam hal ini khususnya dalam membuktikan suatu perbuatan hukum yang dilakukan melalui sistem elektronik.[7]

Perkembangan teknologi informasi khususnya teknologi media internet tidak hanya memenuhi kebutuhan dan memberikan kenyamanan bagi masyarakat yang menginginkan sesuatu yang praktis tapi juga menyebabkan munculnya jenis-jenis kejahatan baru, yaitu dengan memanfaatkan komputer dan media internet sebagai modus operandi. Melalui media internet beberapa jenis tindak pidana semakin mudah untuk dilakukan seperti, kejahatan

---

[1] Artikel Skripsi
[2] Mahasiswa Fakultas Hukum Unsrat, NIM 19071101219
[3] Fakultas Hukum Unsrat, Doktor Ilmu Hukum
[4] Fakultas Hukum Unsrat, Magister Ilmu Hukum

[5] Agus Raharjo, *Cybercrime, Pemahaman Dan Upaya Pencegahan Kejahatan Berteknologi.* (Bandung: PT. Aditya. Bakti, 2002). 1.
[6] Ahmad Ramli, *Cyber Law dan HAKI-Dalam System Hukum Indonesia*, (Bandung: Rafika Aditama, 2004), hlm.1s
[7] Penjelasan Undang-Undang Nomor 11 Tahun 2008 *Tentang Informasi dan Transaksi Elektronik, Paragraf 2*

manipulasi data, spionase, sabotase, provokasi, *money laundering, hacking*, pencurian software maupun perusakan *hardware* dan kejahatan judi dengan menggunakan media internet.[8]

Berbicara tentang kerangka hukum dalam suatu konteks sistem telematika adalah salah satu tantangan baru didalam hukum itu sendiri. Adanya keterbatasan aturan-aturan hukum yang ada selama ini membuat para penegak hukum harus mengambil kebijakan untuk melakukan penemuan hukum di bidang ini sehingga yang akan menjadi suatu putusan yang berkaitan dengan masalah telematika dan dapat memenuhi kepastian hukum. Permasalahan kejahatan didunia maya selama ini tidak diatur dalam Kitab Undang- Undang Pidana (KUHP), oleh karena itu untuk mengatasi kekosongan hukum maka pada tahun 2008 dibentuklah Undang-Undang tentang Informasi dan Transaksi Elektronik Nomor 11 tahun 2018. Namun dalam Undang-Undang ini belum mengatur secara jelas mengenai perbuatan dan sanksi terhadap hacking.

Pada bidang Telematika, sangatlah disadari bahwa bidang baru ini terus berkembang dengan tingkat kompleksitas yang sangat tinggi, tentu nya memerlukan suatu payung hukum yang mengatur seluruh permasalahan di bidang telematika. Oleh karena itu, pembentukan kerangka hukumnya harus dilihat dari berbagai aspek seperti *rule of law* dan internet, yuridiksi dan konflik hukum, pengakuan hukum terhadap dokumen serta tanda tangan elektronik *(electronic signature)*, perlindungan dan privasi konsumen, *cyber crime*, pengaturan konten, dan cara-cara penyelesaian sengketa domain.[9]

Kemudahan yang diperoleh melalui internet tentunya tidak menjadi jaminan bahwa aktivitas yang dilakukan di media tersebut adalah aman atau tidak melanggar norma. Di situlah kita harus jeli dalam melihat permasalahan yang berkembang di dalam Masyarakat. Pesatnya perkembangan teknologi, khususnya teknologi informasi dan komunikasi pada saat ini, telah menumbuhkan interkoneksitas antar masyarakat dunia tanpa terhambat oleh batas-batas wilayah negara. Perkembangan dari teknologi informasi dan komunikasi yang berkolaborasi dengan media serta komputer, memunculkan sebuah piranti baru yang dikenal sebagai internet.[10] Penggunaan internet semakin hari semakin meningkat, terkhusus di Indonesia. Berangkat dari data *Internet World Stats* menyebutkan jumlah pengguna internet di Indonesia telah mencapai 212,35 juta jiwa terhitung pada Maret 2021, dan menempati urutan ketiga dengan jumlah pengguna internet terbanyak di Asia.[11]

Perkembangan internet diibaratkan sebagai pedang bermata dua, karena selain memberikan dampak positif bagi kehidupan manusia, internet bisa juga menjadi cara efektif untuk melakukan perbuatan melawan hukum.[12] Salah satu perbuatan melawan hukum akibat perkembangan internet adalah kejahatan *cybercrime* atau yang dikenal sebagai kejahatan yang dilakukan melalui jaringan internet. Berdasarkan *International Telecommunication Union* (ITU) menyatakan bahwa *cybercrime* merupakan kejahatan yang dilakukan melalui komputer baik sebagai alat, target, maupun sarana untuk melakukan kejahatan.[13] Sehingga, pendekatan sistem hukum terhadap pemanfaatan internet tidak dapat lagi dilakukan secara konvensional,[14] mengingat aktivitasnya dilakukan secara lintas negara, mudah memperoleh akses dari lintas negara, serta kerugian dapat terjadi meskipun pelaku dan korban tidak pernah berhubungan sekaligus.[15]

International Criminal Police Organization (Interpol) dalam laman resminya mencatat sebanyak hampir 270 situs web yang disusupi, termasuk portal pemerintah di wilayah Asia Tenggara, serta 26 situs web pemerintah yang terpengaruh oleh enam kelompok peretas dan beberapa peretas individu, khususnya di Indonesia berdasarkan data Badan Siber dan Sandi Negara (BSSN) mencatat serangan siber tahun 2020 angka mencapai angka 495,3 juta atau meningkat 41 persen dari tahun sebelumnya 2019 yang

---

[8] Agus Rahardjo, *Cybercrime-Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi, Citra Aditya Bakti*, Bandung, 2002. Hlm 213

[9] Dikdik M. Arief Mansur dan Elisatris Gultom, *Cyber Law: Aspek Hukum Teknologi Informasi*, (Bandung: PT. Refika Aditama, 2009), hal. 3

[10] Donovan Typhano Rachmadie & Supanto, *"Regulasi Penyimpangan Artificial Intelligence Pada Tindak Pidana Malware Berdasarkan Undang-Undang Republik Indonesia Nomor 1 Tahun 2016"* (2020) 9:2 J Huk Pidana Dan Penanggulangan Kejahatan, Hlm.129.

[11] Viva Budy Kusnandar, "*Pengguna Internet Indonesia Peringkat ke-3 Terbanyak di Asia | Databoks," Katadata*.co.id, 2021,https://databoks.katadata.co.id/datapublish/2021/10/14/pengguna-internetindonesia-peringkat-ke-3-terbanyak-di-asia.

[12] Fiorida Mathilda, *"Cyber Crime Dalam Sistem Hukum Indonesia,"* Sigma-Mu 4, no. 2 (2012), Hlm. 35.

[13] Galuh Kartiko, *"Pengaturan Terhadap Yurisdiksi Cyber Crime Ditinjau dari Hukum Internasional"* (2013) 8:2 Rechtidee,Hlm. 137

[14] Cahyo Handoko, *"Kedudukan Alat Bukti Digital Dalam Pembuktian Cybercrime di Pengadilan"* (2017) 6:1 J Jurisprud, Hlm.14

[15] Raida L Tobing, *Laporan Akhir Penelitian Hukum tentang Efektifitas UU No. 11 Tahun 2008 tetang Informasi dan Transaksi Elektronik* (Jakarta: Badan Pembinaan Hukum Nasional Kementrian Hukum dan HAM RI, 2010), Hlm. 5.

sebesar 290,3 juta. Sama halnya dengan Badan Reserse Kriminal Kepolisian Negara Republik Indonesia (Bareskrim), yang melihat adanya peningkatan laporan kejahatan siber. Dimana pada tahun 2019 terdapat 4.586 laporan polisi diajukan melalui Patroli siber pada Januari sampai Agustus 2020, hampir 190 juta terjadi upaya serangan siber di Indonesia yang dilakukan oleh hacker nasional hingga internasional.[16] Bahkan, Akhman Muqowam, Ketua Komite 1 DPD RI menyatakan tingkat *cybercrime* di Indonesia berada pada peringkat kedua di dunia.[17] Pada tahun 2017 kerugian ekonomi akibat *cybercrime* di Indonesia mencapai Rp.478,8 triliun.[18] Lebih lanjut, disampaikan oleh Direktur Tindak Pidana Siber Bareskrim Polri, Brigadir Jenderal Polisi Slamet Uliandi, S.I.K., menyampaikan sejak 2020 hingga 2021, terjadi 649 laporan penipuan dan 39 kali pencurian data yang masuk Siber Polri. Terjadi juga 18 kali aduan peretasan sistem elektronik.

Pengaturan *cybercrime* tertuang dalam beberapa regulasi, salah satunya adalah Kitab Undang-Undang Hukum Pidana (selanjutnya disebut KUHP) dan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (selanjutnya disebut Undang-Undang Informasi dan Transaksi Elektronik). Menurut pandangan Mardjono Reksodiputro, Kriminolog dari Universitas Indonesia menyatakan *cybercrime* sebenarnya bukanlah kejahatan baru yang masih bisa diakomodir oleh KUHP.[19] Lebih lanjut, meskipun Indonesia belum memiliki regulasi khusus *cybercrime*, namun terdapat Undang-Undang Informasi dan Transaksi Elektronik sebagai *lex specialis* yang mengatur *cybercrime.*

Salah satu bentuk kejahatan yang sering terjadi di dunia maya seperti tindak *Cracking. Cracking* adalah kegiatan membobol sistem komputer yang bertujuan untuk mengambil keuntungan dengan cara merusak dan menghancurkan dengan maksud tertentu.[20] *Cracker* adalah istilah yang diajukan oleh Richard Stallman bagi para peretas yang cenderung melakukan kegiatan *Black Hat Hacker*. *Cracker* merupakan seorang yang masuk tanpa izin atau *Illegal* kedalam suatu sistem komputer. Istilah *Cracker* memiliki kecenderungan *Hacker* pada pengertian *White Hat Hacker*. *Hacker* dan *Cracker* mempunyai persamaan dan perbedaan. Persamaannya adalah sama-sama melakukan kegiatan *Hacking,* tetapi berbeda dalam hal motivasi dan tujuan *Hackingnya. Cracker* lebih cenderung melakukan *Hacking* yang merusak, sedangkan *Hacker* sejatinya merupakan spirit para profesional untuk membantu menyelesaikan suatu masalah pada sistem komputer.[21]

Kejahatan hacking atau peretasan adalah aktivitas mengeksploitasi kelemahan dalam suatu sistem atau jaringan komputer untuk mendapatkan akses tanpa izin, tujuannya adalah mengubah atau mencuri resource yang seharusnya tidak dapat diakses sembarangan. Salah satu contoh serangan hacking ialah *Phising* merupakan teknik pengelabuan mencuri data email dengan membuat situs web palsu yang nampak resmi. Dimana korban mengisi informasi pribadi sesuai permintaan. Sedangkan, *Cracking* merupakan salah satu bentuk kejahatan siber yang berbahaya yang berpotensi menyebabkan kerugian besar, secara finansial maupun non-finansial. Contohnya ialah Membajak situs web. Salah satu kegiatan yang sering dilakukan oleh *cracker* adalah mengubah halaman web, yang dikenal dengan istilah *deface*. Pembajakan dapat dilakukan dengan mengeksploitasi lubang keamanan.

Salah satu kasus hacking yang terjadi di Indonesia yaitu putusan pengadilan Negeri Marisa dengan *Nomor 41/PID. Sus/2020/PN Mar* dengan uraian kasus, kejahatan yang dilakukan oleh terdakwa Yantu berdomisili di Provinsi Gorontalo. Pada bulan Desember 2019 terdakwa melakukan peretasan dengan cara masuk ke dalam website e-dikbang Polri dengan menggunakan NRP anggota polisi secara acak, kemudian terdakwa mengupload/ memasukan file *hypertext preprocecor* ke forum upload pada situs e-dikbang polri kemudian Terdakwa membuat dan merubah file indeks yang baru dengan kata-kata atau kalimat yang dibuat oleh Terdakwa pada tampilan kata-kata atau kalimat pada website e-dikbang Polri dari tampilan yang sebelumnya, yaitu dengan tampilan kata-kata "HACKED BY

[16] Putri Zakia Salsabila, *"Kejahatan Siber di Indonesia Naik 4 Kali Lipat Selama Pandemi,"* Kompas.com, 2020, https://tekno.kompas.com/read/2020/10/12/07020007/kejahatan-siber-di-indonesia-naik-4-kalilipat-selama-pandemi

[17] Dessy Suciati Saputri, *"Indonesia Peringkat ke-2 Dunia Kasus Kejahatan Siber,"* Republika Online, 2015, https://republika.co.id/berita/nasional/umum/15/04/09/nmjajy-indonesia-peringkat-ke2-duniakasus-kejahatan-siber

[18] *Ratna Christianingrum & Ade Nurul Aida, Tantangan Penguatan Keamanan Siber dalam Menjaga Stabilitas Keamanan* (Jakarta: Pusat Kajian Anggaran Badan Keahlian-Sektretariat Jenderal Dewan Perwakilan Rakyat Republik Indonesia, 2021), hlm. 5.

[19] Budi Suhariyanto, *Tindak Pidana Teknologi Informasi (Cybercrime) Urgensi Pengaturan dan Celah Hukumnya* (Jakarta: Rajawali Press, 2013), Hlm. 48

[20] Doni Ariyus, *Kamus Hacker*, (Yogyakarta: Andi Offset, 2005), hal. 86.

[21] Mundzir MF, *Tips Dan Trik Belajar Hacker,* (Yogyakarta: Notebook, 2004), hal. 10.

DEDEN RAMADHAN GOBEL (UP) KASUS NOVEL BASWEDAN HANYA PENGALIHAN ISU DARI KASUS MEGA KORUPSI JIWASRAYA. KETAHUAN BOONGNYA" dimana yang sebelumnya tampilan website e-dikbang Polri adalah website yang menyediakan informasi bagi pendaftaran sekolah pengembangan di Institusi Kepolisian, diantaranya Sekolah Lanjutan Perwira (Sespima), Pendidikan Alih Golongan, Sekolah Inspektur Polisi.

Bahwa akibat perbuatan Terdakwa tanpa hak membuat dan merubah file indeks tampilan pada website e-dikbang Polri mengakibatkan berubahnya tampilan dan tidak bisa dibuka untuk sementara waktu website e-dikbang Polri.

Atas perbuatan tersebut terdakwa dijerat Pasal 32 ayat (1) jo Pasal 48 ayat (1) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana diubah dengan Undang undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik; Mahkamah Agung Republik Indonesia 2. Menjatuhkan pidana terhadap Terdakwa berupa pidana penjara selama 1 (satu) Tahun dengan perintah Terdakwa ditahan, denda Rp50.000.000,00 (lima puluh juta rupiah); subsidair 3 (tiga) bulan kurungan.[22]

B. Rumusan Masalah

1. Bagaimana perbuatan hacking dalam perspektif hukum informasi dan transaksi elektronik ?
2. Bagaimana akibat hukum yang ditimbulkan dari perbuatan hacking dalam perspektif hukum informasi dan transaksi elektronik ?

C**. Metode Penelitian**

Dalam penelitian ini penulis menggunakan penelitian yuridis normatif.

PEMBAHASAN

A. Pengaturan Hacking dan Craking Dalam Perspektif Informasi dan Transaksi Elektronik.

Cracking merupakan aktivitas membobol sesuatu sistem komputer selanjutnya disebut PC dengan tujuan memperoleh. Sebaliknya orang yang melaksanakan *Cracking* diucap Cracker. Crack merupakan sesuatu kegiatan pembobolan sesuatu aplikasi berbayar supaya pada saat pendaftarannya bisa dijalani tidak wajib membeli dan juga pembayaran lisensi formal dari sang pembentuk aplikasi tersebut. Perihal ini memiliki itikad kalau kita dapat mendapatkan sebagian persyaratan supaya aplikasi yang berbayar tersebut bisa bekerja secara maksimal. Umumnya pula wajib didaftarkan ataupun sangat tidak memasukkan nomor pendaftaran untuk dalam aplikasi tersebut. Crack Aplikasi merupakan settingan fitur lunak buat menghapus ataupun menonaktifkan fitur yang dikira tidak diidamkan oleh orang. *Cracking* aplikasi, umumnya berkaitan pada tata cara proteksi yaitu terhadap "manipulasi aplikasi, trial atau demo version, no seri, hardware kunci, bertepatan pada pengecekan, CD cek ataupun fitur lunak kendala semacam layar serta adware."[23]

Jika tetap berpatokan pada asas legalitas, maka akan sulit bagi kita untuk menerapkan peraturan yang ada dalam KUHP terhadap kasus Cracking. Berkaitan dengan itu, perlu suatu penafsiran terhadap undang-undang sehingga suatu perbuatan yang tidak diatur dalam undang-undang tidak begitu saja dikesampingkan karena alasan tidak ada peraturan atau ketentuannya. Keberanian hakim untuk menafsirkan undang-undang merupakan bentuk antisipasi terhadap "CC", khususnya mengenai *Cracking*. Penerapan KUHP terhadap tindak pidana *cracking* memerlukan pemilah-milahan, perbuatan mana yang substansinya hampir sama dengan rumusan tindak pidana biasa dalam KUHP. Dalam KUHP terdapat aturan yang mengatur perihal perusakan atau penghancuran tersebut, yaitu pada Pasal 406 ayat (1) KUHP, yang rumusannya sebagai berikut: "Barangsiapa dengan sengaja dan melawan hukum, menghancurkan merusakkan, membuat tidak dapat dipakai atau menghilangkan barang sesuatu baik seluruhnya atau sebagian adalah kepunyaan orang lain, diancam dengan pidana penjara dua tahun delapan bulan penjara atau denda paling banyak empat ribu lima ratus rupiah." Tanggal 23 April 2008 telah diundangkan Undang- undang Informasi dan Transaksi Elektronik, Undang-Undang ini bukanlah Undang-Undang tindak pidana khusus, selain itu juga terkait mengenai pengaturan tentang pengelolaan Informasi dan Transaksi Elektronik dalam tujuan pembangunan, namun Undang-undang ini juga menjaga dari pengaruh negatif oleh manfaat peningkatan teknologi Informasi dan Transaksi Elektronik. Yakni dalam ditetapkannya

[22] Direktori Putusan Mahkamah Agung Republik Indonesia. Putusan Mahkamah Agung Id.

[23] Cok Rai Kesuma Putra1, I Nyoman Gede Sugiartha2, I Made Minggu Widyantara3. Jurnal *Analisis Yurudis Atas Keabsahan Atas Pertanggungjawaban Pidana Terhadap Pelaku Tindakan Pidana Pembobolan Sistem Data Keamanan Komputer (Craking).* 2024. Hlm 5

hukum pidana khususnya mengenai perbuatan pidana yang menyerang keperluan hukum individu, warga, maupun keperluan hukum negara dalam memakai majunya teknologi Informasi dan Transaksi Elektronik, atau biasa dikatakan dengan perbuatan pidana *Cracking.*

Motivasi pelaku kejahatan dunia maya sangat bervariasi, mulai dari keuntungan finansial, pembalasan pribadi, hingga sekadar tantangan teknis. Ini mencerminkan keragaman latar belakang dan tujuan pelaku. Aktivitas dunia maya, meskipun terjadi di ruang virtual, diakui dan diklasifikasikan sebagai tindakan hukum nyata. Banyak negara, termasuk Indonesia telah memperbarui hukum mereka untuk mencakup kejahatan dunia maya. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Undang-Undang Informasi dan Transaksi Elektronik) sudah mengatur kejahatan dunia maya, termasuk penipuan online, pembajakan, dan penyebaran konten ilegal. (Undang-Undang Informasi dan Transaksi Elektronik, 2008) Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 mengakomodasi perkembangan terbaru dalam teknologi informasi dan kejahatan siber (Undang-Undang Republik Indonesia No 19, 2016). Proses penegakan hukum terhadap kejahatan dunia maya melibatkan penyelidikan dan forensik digital menggunakan alat dan teknik forensik untuk melacak dan menganalisis bukti digital, dan kerjasama internasional dikarenakan kejahatan dunia maya sering melibatkan pelaku lintas negara, penegakan hukum sering melibatkan kerjasama internasional antara lembaga penegak hukum. Dalam implikasi hukum kejahatan dunia maya dapat mengakibatkan berbagai konsekuensi hukum, termasuk denda, hukuman penjara, dan tindakan hukum lainnya, tergantung pada jenis dan dampak kejahatan yang dilakukan. Keputusan hukum juga dapat mencakup kompensasi untuk korban dan perintah untuk mengembalikan atau menghentikan aktivitas ilegal. [24]

Badan Siber dan Sandi Negara (BSSN) berfungsi sebagai lembaga yang mengawasi dan mengkoordinasikan keamanan siber di Indonesia. BSSN juga memberikan panduan dan dukungan teknis dalam penanganan kejahatan dunia maya. Inisiatif dan kebijakan Badan Siber dan Sandi Negara (BSSN) menyusun dan menerapkan kebijakan nasional untuk melindungi infrastruktur siber. Badan Siber dan Sandi Negara (BSSN) menyediakan pelatihan dan edukasi mengenai keamanan siber kepada pemerintah dan sektor swasta (BSSN, 2021b). Kepolisian Republik Indonesia (Polri) memiliki unit khusus, yaitu Direktorat Tindak Pidana Siber, yang menangani penyelidikan dan penegakan hukum terhadap kejahatan dunia maya. Polri melakukan operasi untuk menangkap pelaku kejahatan siber dan mengamankan barang bukti. bekerja sama dengan lembaga internasional dalam menangani kejahatan siber lintas negara (Polisi Republik Indonesia, 2018). Dengan kerangka hukum ini, Indonesia berusaha untuk mengatasi dan menanggulangi kejahatan dunia maya yang terus berkembang dengan pesat.

Kendala terbesar dalam penegakan hukum *cyber crime* adalah literasi digital penegak hukum dan kurangnya fasilitas teknologi forensik. Banyak kasus *cyber crime* sulit ditangani karena kurangnya alat dan keterampilan yang memadai untuk melacak bukti digital. Ia juga menyoroti pentingnya kerja sama internasional mengingat banyak kasus melibatkan pelaku lintas negara. Secara regulasi hukum di Indonesia memang telah ada Undang- Undang Nomor 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik yang mengatur mengenai tindak pidana *cyber* termasuk juga dengan kejahatan *hacking craking*, hanya saja penerapan dan pemahaman apparat penegak hukum yang belum maksimal dalam penanganannya. Karakteristik tindak pidana *hacking* dan *craking* berbeda dengan tindak pidana yang lain. Yang menyebabkan karakteristiknya berbeda karena terdapat modus operandi yang berbeda. Sehingga dengan demikian dalam penegakan hukum dan dalam proses beracaranya dari tahap penyelidikan dan penyedikan memerlukan ketentuan khusus. Ketentuan khusus ini pun terdapat dalam Undang-Undang Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang- Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, yang dijelaskan sebagai berikut:

1. Diakuinya alat bukti elektronik dan dokumen elektronik sebagai alat bukti yang sah dalam pembuktian tindak pidana cyber.
2. Adanya wewenang khusus yang berkaitan kepada pejabat pegawai negeri sipil tertentu dilingkungan pemerintah yang lingkup tugas dan tanggung jawabnya dibidang di bidang Teknologi Informasi dan Transaksi Elektronik sebagai penyidik.
3. Adanya kewenangan penyidik, penutut umum, dan hakim untuk meminta keterangan

[24] Aurelia Penelitian dan Pengabdian Masyarakat Indonesia. *Tindak Pidana Cyber Crime Dalam Hukum Indonesia Serta Upaya Pencegahan Dan Penanganan Kasus Tindak Pidana Cyber Crime.* Volume 4 No 1 Januari 2025. Jakarta. Hlm 340

kepada penyedia jasa dan penyelanggara system elektronik mengenai data- data yang berhubungan dengan tindak pidana, dengan tetap terkait terhadap privasi, kerahasian, dan kelancaran layanan publik, integritas data dan keutuhan data.

4. Adanya wewenang terhadap penyidik untuk melakukan penggeledahan, penyitaan terhadap system elektronik yang terkait dengan dugaan tindak pidana harus dilakukan atas izin ketua pengadilan negeri setempat, hal ini menghindari agar pelacakan pelaku berjalan cepat, sehingga jejak pelaku mudah ditemukan. [25]

Kejahatan *hacking craking* telah diatur dalam Undang- Undang Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang- Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik yang terdapat pada pasal 30 yang berbunyi;

(1) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apa pun.
(2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik.
(3) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.

Pada pasal 30 ayat (1) sudah tertera jelas unsur setiap orang, unsur dengan sengaja dan tanpa hak melawan hukum, unsur mengakses computer atau system elektornik milik orang lain, serta unsur dengan cara apapun.

a. Unsur setiap orang
   Dalam unsur ini setiap orang yang dimaksud adalah orang sebagai subjek hukum yang dapat bertanggungjawab dan cakap hukum berdasarkan atas Perundang-Undangan.
b. Unsur dengan sengaja dan tanpa hak melawan hukum
   Unsur ini merujuk pada niat atau kesengajaan dan penuh dengan keasadaran dari orang tesebut dalam melakukan suatu tindakan yang malawan hukum.
c. Unsur mengakses komputer dan/ atau sistem elektronik milik orang unsur ini memberi gambaran bahwa sistem elektronik milik orang lain itu berarti hal yang bersifat pribadi milik orang lain dan bukan bersifat untuk umum.
d. Unsur dengan cara apapun
   Dengan cara apapun yang dimaksud dalam hal ini adalah baik peretas tersebut masuk menggunakan perangkat milik korban yang diretas atau melalui perangkat atau jaringan internet.[26]

Pembahasan mengenai kejahatan *hacking craking* juga diatur lebih lanjut dalam Pasal 31 sampai Pasal 35 yang berbunyi sebagai berikut;

Pasal 31

(1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atau penyadapan atas Informasi Elektronik dan/atau Dokumen Elektronik dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik Orang lain.
(2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atas transmisi Informasi Elektronik dan/atau Dokumen Elektronik yang tidak bersifat publik dari, ke, dan di dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik Orang lain, baik yang tidak menyebabkan perubahan apa pun maupun yang menyebabkan adanya perubahan, penghilangan, dan/atau penghentian Informasi Elektronik dan/atau Dokumen Elektronik yang sedang ditransmisikan.
(3) Kecuali intersepsi sebagaimana dimaksud pada ayat (1) dan ayat (2), intersepsi yang dilakukan dalam rangka penegakan hukum atas permintaan kepolisian, kejaksaan, dan/atau institusi penegak hukum lainnya yang ditetapkan berdasarkan undang-undang.
(4) Ketentuan lebih lanjut mengenai tata cara intersepsi sebagaimana dimaksud pada ayat (3) diatur dengan Peraturan Pemerintah.

Pasal 32

(1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik publik.
(2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun

[25] Yuli Tasya. Jurnal *Craking Dalam Perspektif Undang-Undang Nomor 11 Tahun 2008 Dan Hukum Pidana Islam* 2020. Hlm 48

[26] *Ibid* Hlm 337

memindahkan atau mentransfer Informasi Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik Orang lain yang tidak berhak.

(3) Terhadap perbuatan sebagaimana dimaksud pada ayat (1) yang mengakibatkan terbukanya suatu Informasi Elektronik dan/atau Dokumen Elektronik yang bersifat rahasia menjadi dapat diakses oleh publik dengan keutuhan data yang tidak sebagaimana mestinya.[27]

Pasal 33

"Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan tindakan apa pun yang berakibat terganggunya Sistem Elektronik dan/atau mengakibatkan Sistem Elektronik menjadi tidak bekerja sebagaimana mestinya."

Pasal 34

(1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum memproduksi, menjual, mengadakan untuk digunakan, mengimpor, mendistribusikan, menyediakan, atau memiliki:
   a. perangkat keras atau perangkat lunak Komputer yang dirancang atau secara khusus dikembangkan untuk memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 33;
   b. sandi lewat Komputer, Kode Akses, atau hal yang sejenis dengan itu yang ditujukan agar Sistem Elektronik menjadi dapat diakses dengan tujuan memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 33.

(2) Tindakan sebagaimana dimaksud pada ayat (1) bukan tindak pidana jika ditujukan untuk melakukan kegiatan penelitian, pengujian Sistem Elektronik, untuk perlindungan Sistem Elektronik itu sendiri secara sah dan tidak melawan hukum.

Pasal 35

"Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik."

Mengenai tindakan perusakan atau penghancuran diatur pada KUHP Pasal 406 ayat (1). Pengaturan tindak pidana Cracking diatur pada Undang-Undang Informasi dan Transaksi Elektronik yang terdapat dalam 9 pasal, yakni dari Pasal 27 sampai dengan Pasal 35. Undang-Undang Informasi dan Transaksi Elektronik telah menetapkan perbuatan-perbuatan mana yang termasuk tindak pidana di bidang Informasi dan Transaksi Elektronik terutama tindak pidana cracking dan telah ditentukan unsur-unsur tindak pidana dan penyerangan terhadap berbagai kepentingan hukum dalam bentuk rumusan-rumusan tindak pidana tertentu.

Pemerintah membuat SKB Undang- Undang Informasi Elektronik untuk membantu penegak hukum menjalankan pekerjaan mereka. Namun, ada beberapa kategori dan kondisi yang memungkinkan pemerintah tak memperhatikan SKB tersebut. Pemerintah harus menyiapkan perubahan pada Undang-undang Informasi Teknologi Elektonik menggunakan pertimbangan semua pendapat masyarakat serta stakeholder dengan efektif. Ini juga harus mempertahankan aspirasi Pasal 28 D ayat (1) Undang-undang Dasar Negara Republik Indonesia Tahun 1945, yang menjelaskan apabila tiap manusia memiliki hak atas pengakuan, jaminan, perlindungan, hingga kepastian juga perlakuan hukum yang adil di hadapan hukum.

Materi Undang- undang Informasi Transaksi Elektronik terbagi dua, yaitu: pengaturan transaksi elektronik dan informasi elektronik, serta pengaturan pelanggaran yang tak diperbolehkan dan diancam hukuman pidana (*cybercrime)*. Selain itu, Undang-Undang Informasi dan Transaksi Elektronik adalah pengaturan tindak pidana siber pada Undang-Undang pertama di Indonesia.

Berbicara mengenai cakupan hukum undang-undang Informasi Dan Transaksi Elektronik perlu diketahui bahwa Undang-Undang Informasi dan Transaksi Elektronik berlaku untuk setiap orang yang melakukan perbuatan hukum sebagaimana diatur dalam Undang-Undang ini (termasuk perbuatan *cracking*), baik yang berada di wilayah hukum Indonesia maupun di luar wilayah hukum Indonesia, yang memiliki akibat hukum di wilayah hukum Indonesia dan/atau di luar wilayah hukum Indonesia dan merugikan kepentingan Indonesia.[28] Hal ini terdapat dalam pasal 37 Undang- Undang Nomor 1 Tahun 2024 Tentang Perubahan Keduan Undang- Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, yang berbunyi;

[27] Undang- Undang Nomor 1 Tahun 2024 *Tentang Perubahan Kedua Atas Undang- Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.*

[28] https://www.hukumonline.com/klinik/a/jangkauan-yurisdiksi-uu-ite-menjerat-pelaku-icracking-server-i-milik-asing-lt517d0337ad845/. Diakses Pada Hari Senin 24 Maret 2025 Pada Pukul 05.14 WITA

Pasal 37 Setiap Orang dengan sengaja melakukan perbuatan yang dilarang sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 36 di luar wilayah Indonesia terhadap Sistem Elektronik yang berada di wilayah yurisdiksi Indonesia.

B. Akibat Hukum yang Ditimbulkan dari Perbuatan *Hacking* dalam Persepktif Hukum Informasi dan Transaksi Elektronik

Kejahatan teknologi Informasi atau *hacking* dan *cracking* memiliki karakter yang berbeda dengan tindak pidana lainnya baik dari segi pelaku, korban, modus operandi dan tempat kejadian perkara sehingga butuh penanganan dan pengaturan khusus di luar Kitab Undang-Undang Hukum Pidana (KUHP) dan juga Kitab Undang-Undang Hukum Acara Pidana (KUHAP). Terkait dengan hukum pembuktian biasanya akan memunculkan sebuah posisi dilema, di salah satu sisi diharapkan agar hukum dapat mengikuti perkembangan zaman dan teknologi, di sisi lain perlu juga pengakuan hukum terhadap berbagai jenis-jenis perkembangan teknologi digital untuk berfungsi sebagai alat bukti di pengadilan. Pembuktian memegang peranan yang penting dalam proses pemeriksaan sidang pengadilan. Pembuktian inilah yang menentukan bersalah atau tidaknya seseorang yang diajukan di muka pengadilan. Apabila hasil pembuktian dengan alat bukti yang ditentukan dengan undang-undang tidak cukup membuktikan kesalahan dari orang tersebut maka akan dilepaskan dari hukuman, sebaliknya apabila kesalahan dapat dibuktikan maka dinyatakan bersalah dan dijatuhi hukuman. Oleh karena itu harus berhati-hati, cermat dan matang dalam menilai dan mempertimbangkan maslah pembuktian.[29]

Salah satu contoh kasus *hacking* yang terjadi di Indonesia yaitu, kasus Tindak Pidana Perdagangan Orang (TPPO) dan penipuan online scam dengan modus lowongan pekerjaan. Dimana, sindikat tersebut telah merugikan sejumlah korban baik ditanah air maupun dari berbagai negara. Hal tersebut, diungkapkan oleh, Direktur Tindak Pidana Siber Bareskrim Polri Brigjen Pol Hilmawan Bayu Uji.

Lebih lanjut ia menuturkan jika pengungkapan kasus tersebut berawal dari adanya informasi yang diterima Polri dari konsul Jendral RI di Timur Tengah terkait pemulangan warga negara Indonesia (WNI) yang dipekerjakan sebagai pelaku penipuan online jaringan Internasional di Dubai pada 31 Mei 2023 lalu.

Pada kasus tersebut, kata Himawan pihaknya telah menetapkan empat tersangka dengan inisial ZS, NSS, M dan H. Dimana, satu dari empat tersangka merupakan warga negara asing (WNA).

Himawan menerangkan, sindikat tersebut melakukan aksinya dari luar wilayah Indonesia. Dimana cara kerjanya yakni, operator yang bertugas mencari calon korban dengan mengirim link-link berisi lowongan pekerjaan paruh waktu melaluli aplikasi baik WhatsApp maupun Telegram.

“Kasus online scam jaringan internasional dengan modus lowongan pekerjaan paruh waktu ini, di tawarkan melalui beberapa platfrom media online seperti Telegram dan WhatsApp yang berisikan link login website terkait dengan tugas yang akan dikerjakan,” ucapnya.

Teknik sosial *engineering*, artinya dia memblasting link website kemudian mempelajari pola-polanya untuk menawarkan investasi ataupun pekerjaan paruh waktu dengan hasil yang direkayasa sehingga korban mendapatkan untung atau komisi pada awalnya mendapatkan untung atau komisi dan kemudian menjadi rugi lebih besar dari pada komisi yang diterima.

Lantaran hal tersebut, terdapat ratusan WNI yang menjadi korban penipuan dari sindikat ini. Tak hanya itu, rupanya korbannya bukan hanya dari dalam negeri melainkan juga berasal dari luar negeri.

Atas perbuatanya, para tersangka dijerat dengan Pasal 45 A ayat 1 juncto Pasal 28 ayat 1 dan atau dan Pasal 51 ayat 2 juncto Pasal 36 Undang-Undang nomor 19 tahun 2016 dan atau Pasal 378 KUHP kemudian Pasal 4 Undang-Undang Nomor 21 Tahun 2007 tentang pemberantasan TPPO. [30]

Uraian kasus diatas merupakan salah satu bukti bahwa tindak pidana siber seringkali melibatkan warga negara asing dan locus kejadian yang tidak hanya di Indonesia. Meski demikian karena korban merupakan warga negara Indonesia maka penerapan hukum yang berlaku adalah Undang-Undang Nomor 1 Tahun 2024 Tentang Perubahan Kedua Undang- Undang nomor 19 tahun 2016 Tentang Informasi dan Transaksi Elektronik. Dapat disimpulkan regulasi Undang-Undang yang diterapkan merupakan aturan atau Undang-Undang yang berlaku di Indonesia.

Muncul kesulitan dalam penerapan hukum dan penegakan hukum terhadap tindak pidana *hacking* dan *cracking* yakni dalam penyelesaian

[29] *Ibid* hlm 44

[30] https://hukum.tvrinews.com/berita/tl8977q-polri-bongkar-kasus-scam-modus-lowongan-pekerjaan-kerugian-mencapai-rp15-triliun. Diakses Pada Hari Jumat 27 Juni Pukul 20.50 WITA.

tindak pidana tersebut, kondisi yang paperless (tidak menggunakan kertas) ini menimbulkan masalah dalam pembuktian mengenai Informasi yang di proses, disimpan, atau dikirim secara elektronik. Mendasar penggunaan bukti elektronik dalam proses pembuktian perkara pidana, khususnya yaitu tidak adanya patokan atau dasar penggunaan bukti elektronik di dalam perundang-undangan kita. Selain itu sulitnya mengungkapkan tindak pidana tersebut baik pelaku, dan kejahatan yang sering sekali sulit untuk dibuktikan sehingga hal tersebut menjadi tantangan tersendiri dalam penegakan hukum tindak pidana *hacking* dan *cracking.*[31]

Setiap penegak hukum diberi kewenangan berdasarkan Peraturan Perundang-Undangan yang berlaku untuk menjelaskan tugasnya. Dalam penanganan tindak pidana *hacking* dan *cracking*, hukum acara yang digunakan yaitu hukum acara berdasarkan KUHAP. Hal tersebut memang tidak disebutkan secara jelas dalam atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, tetapi karena undang-undang tersebut tidak menentukan lain maka KUHAP berlaku bagi tindak pidana yang termuat dalam Undang-Undang Nomor 11 Tahun 2008. Dalam Pasal 42 Undang-Undang Nomor 11 Tahun 2008 46 disebutkan : "Penyidikan terhadap tindak pidana sebagimana dimaksud dalam undang-undang ini dilakukan berdasarkan ketentuan dalam Hukum Acara Pidana dan Ketentuan dalam Undang-Undang ini." Hal tersebut juga ditegaskan dalam Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik bahwa dalam perubahan tersebut sama sekali tidak merubah Pasal 42.

Pertanggungjawaban hukum yang dilakukan oleh pelaku tindak pidana pembobolan sistem data keamanan komputer *(cracking)* sudah diatur pada Undang-Undang Informasi dan Transaksi Elektronik perbuatan pidana *cracking* dan dirumuskan pada berbagai pasal yang bisa mengenai pelaku perbuatan pidana Cracking. Perumusan cracking sebagai perbuatan pidana dalam Undang-Undang Informasi dan Transaksi Elektronik sesuai dengan Pasal 30 diancam dengan "sanksi pidana yang terdapat dalam ketentuan pidana Pasal 46. Pemberian sanksi pidana tersebut merupakan sebagai bentuk pertanggungjawaban yang sah dalam putusan hakim yang diberikan kepada pelaku tindak pidana Cracking sesuai dengan unsur-unsur serta alat bukti persidangan sebagai acuan dalam pemberian hukuman."

Pemberian sanksi bagi pelaku kejahatan *hacking* dan *craking* telah diatur dalam Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan atas Undang- Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik yang terdapat dalam Pasal 45 sampai dengan Pasal 51. Pada Undang- Undang Nomor 1 Tahun 2024 Tentang Perubahan Kedua, terdapat amandemen pada Pasal 45 yang menjelaskan lebih terperinci mengenai tujuan tindakan *hacking* dan *craking* yang dilakukan oleh pelaku.

Dalam hal melaksanakan penegakan hukum khususnya pada bidang kejahatan dunia maya, kejahatan tersebut mempunyai jarak yang amat luas tanpa mengetahui perbatasan wilayah teritorial suatu negara sebab kejahatan ini sifatnya "transnasional". Bentuk kejahatan yang tidak mengetahui perbatasan ini mengwajibkan yurisdiksi suatu negara terhubung langsung di dalamnya sebab sangat jauh dari capaian suatu negara. Jika tidak melakukan hubungan antar negara saat melaksanakan penindakan serta menegakkan hukum yang seharusnya, kejahatan yang sifatnya transnasional tersebut bisa berakibat permasalahan individu terkait pada kekuasaan.[32]

Pemberian sanksi sebagaimana dimaksud terdapat pada Pasal 46 ayat (1), ayat (2), dan ayat (3) Undang-Undang Informasi dan Transaksi Elektronik. Pasal 46 Undang-Undang No 19 tahun 2016 tentang Perubahan atas Undang-Undang No 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, menyatakan;

(1) Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp600.000.000,00 (enam ratus juta rupiah).
(2) Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (2) dipidana dengan pidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp700.000.000,00 (tujuh ratus juta rupiah).
(3) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (3) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp800.000.000,00 (delapan ratus juta rupiah).

Jika diperhatikan dari subtansi atau isi dari pengaturan sanksi tersebut terlihat bahwa tidak

[31] *Ibid* Hlm 45

[32] *Ibid* Hlm 4

hanya pemberian sanksinya berupa sanksi pidana tetapi ada juga sanksi lain yang diatur didalamnya sebagai sanksi tambahan yaitu sanksi denda.

Baik rumusan Pasal 30 ayat (1), ayat (2) dan ayat (3) Undang-Undang Informasi dan Transaksi Elektronik, memiliki perbedaan sanksi yang dijatuhkan kepada pelaku tindak pidana *cracking* baik sanksi pidana atau sanksi berupa denda itu sendiri. Hal ini karena keadaan yang ada pada setiap ayat berbeda-beda.

Pemberian sanksi oleh negara tersebut baik sanksi pidana dan sanksi denda adalah merupakan salah satu Upaya pemerintah dalam melakukan pencegahan terhadap kejahatan-kejahatan dalam dunia maya (*cybercrime)* khususnya kejahatan yang berhubungan tindak pidana cracking. Sehingga dapat memberikan perlindungan hukum kepada masyarakat. Selain salah satu upaya yang disampaikan diatas ada upaya lain yang harus pemerintah gunakan agar dapat memberikan perlindungan hukum kepada masyarakat atau kepada korban tindak pidana cracking.[33]

PENUTUP

A. Kesimpulan

1. Perbuatan hacking dalam prespektif hukum informasi dan transaksi elektronik merupakan perbuatan setiap orang yang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik milik orang lain dengan cara apa pun. Definisi kejahatan hacking telah diatur dalam Undang-Undang Informasi dan Transaksi Elektronik Pasal 40. Permasalahan kejahatan didunia maya selama ini tidak diatur dalam Kitab Undang- Undang Pidana (KUHP), maka dari itu terbentuklah Undang-undang Nomor 1 Tahun 2024 Tentang Perubahan Kedua Undang- undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik yang menjadi lex specialis dalam mengatur tindakan di bidang telematika. Hacking tak selamanya digunakan dalam tindakan kejahatan, namun bisa saja digunakan untuk mengetahui kelemahan suatu system untuk perbaikan jaringan tersebut. Namun tindakan tersebut merupakan suatu tindakan ilegal dan hal tersebut telah diatur dalam Undang-Undang Informasi dan Transaksi Elektronik terdapat dalam Pasal 30.
2. Akibat yang ditimbulkan dari tindakan hacking dan craking merupakan suatu perbuatan melawan hukum tanpa hak membobol dan juga merusak system jaringan computer milik orang/ badan hukum tanpa izin dari pemilik tersebut. Sanksi yang dikenakan akibat tindakan ini adalah sanksi pidana yang telah diatur dalam Undang-Undang Informasi dan Transaksi Elektronik selanjutnya dijelaskan dalam pasal 45 samapai dengan pasal 51. Pemberian sanksi yang diberikan bukan hanya sanksi pidana saja melainkan juga dengan denda, hal ini diterapkan agar menciptakan efek jerah dan juga sebagai perlindungan dan kepastian hukum terhadap Masyarakat. Namun dalam hal penerapan sanksi terhadap pelaku hacking dan craking sering terkendala akan Kerjasama antar negara, karena kejahatan ini tidak hanya ditimbulkan dari pelaku yang berada di Indonesia tapi juga di pelaku diluar wilayah Indonesia.

B. Saran

1. Memberikan penguatan pemahaman kepada aparat penegak hukum terkait regulasi hukum yang diterapkan dalam kejahatan *cyber.* Dengan memeberikan pemahaman ini diharapkan agar aparat penegak hukum tidak lagi multitafsir akan penerapan pasal-pasal dan alur hukum acara dalam menyelesaikan kejahatan *cyber* ini. Selain mempekuat SDM penegak hukum, diperlukan juga laboratorium *cyber* yang canggih dan memadai agar supaya memudahkan dalam proses pembuktian yang bersifat elektronik ini. Penguatan terhadap system pertahanan jaringan juga sangat dibutuhkan untuk mencegah kejahatan-kejahatan *cyber*.
2. Memperluas Kerjasama dengan negara-negara luar agar supaya memudahkan dalam penerapan undang- undang terhadap pelaku yang bukan merupakan warga negara Indonesia.

DAFTAR PUSTAKA

Buku

Arief Mansur Dikdik M. dan Elisatris Gultom, *Cyber Law: Aspek Hukum Teknologi Informasi*, (Bandung: Refika Aditama, 2010).

Ariyus Doni, *Kamus Hacker*, (Yogyakarta: Andi Offset, 2005).

Darma, dkk, *Buku Pintar Menguasai Internet*, (Jakarta: Mediakita, 2010),

Daryanto, *Memahami Kerja Internet*, (Bandung: Rama Widya, 2004.

[33] Mariya Azis dan Muhamad Hasan Rumlus. Jurnal *Perlindungan Hukum Pada Masyarakat Dari Tindakan CrackingPerpektif UUInformasi Dan Transaksi Elektronik Dan Hukum Pidana Islam.* 2021. Hlm 83

Edrisy Ibrahim Fikma, *Pengantar Hukum Siber*, (Lampung: Sai Wawai Publishing, 2019).

Karnasudiraja Eddy Djunedi, *Yurisprudensi Kejahatan Komputer*, (Jakarta: CV Tanjung Agung, 1993).

Kristian dan Yogi Gunawan, Sekelumit Penyadapan dalam Hukum Positif Indonesia, (Jakarta : Nuansa Aulia, 2013), h. 48.

Makarim Edmon, *Pengantar Hukum Telematika (Suatu Kajian Kompilasi)*, (Jakarta: PT Raja Grafindo Persada, 2005).

Marzuki Peter Mahmud, *Penelitian Hukum*, Kencana Prenada Media Group, Jakarta, Tahun 2011.

MF Mundzir, *Tips Dan Trik Belajar Hacker*, (Yogyakarta: Notebook, 2004),

Muhammad, Hukum dan Penelitian Hukum, Citra Aditya Bakti, Bandung, Tahun 2004.

Muladi dan Barda Nawawi Arif, Bunga Rampai Hukum Pidana(Bandung: Alumni Bandung, 1992),

Nitibaskara Ronni R dalam Didik M. Arief Mansur dan Elisatris Gultom, *Cyber Law Aspek Hukum Teknologi Informasi*, (Bandung: PT Refika Aditama, 2005),

Parker Donn B.,*Crime by Computer*,1973.

Rahardjo Agus, *Cybercrime: Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*, (Bandung: PT Citra Aditiya Bakti, 2002).

Ramli Ahmad, *Cyber Law dan HAKI-Dalam System Hukum Indonesia*, (Bandung: Rafika Aditama, 2004).

Sahetapy J. E dalam Abdul Wahid, K*riminologi dan Kejahatan Kontemporer,* Lembaga Penerbitan Fakultas Hukum Unisma, (Malang: 2002).

Situmeang Sahat Maruli T., *CYBER LAW* (Bandung: CV. Cakra, 2020).

Suhariyanto Budi, *Tindak Pidana Teknologi Informasi (Cybercrime) Urgensi Pengaturan dan Celah Hukumnya* (Jakarta: Rajawali Press, 2013).

Suhariyanto Budi, *Tindak Pidana Teknologi Informasi (Cybercrime)*, (Jakarta: PT Rajagrafindo Persada, 2013).

Suteki dan Galang Taufani, 2018, *Metodologi Penelitian Hukum (Filsafat, Teori dan Praktik*, Depok: PT RajaGrafindo Persada.

Soedjono Dirdjosisworo. *Doktrin- Doktrin Kriminologi.*Bandung.1969.

Wahid Abdul dan Mohammad Labib, *Kejahatan Mayaantara (Cybercrime)*, (Bandung: PT Refika Aditama, 2005).

Jurnal Hukum

Aurelia Penelitian dan Pengabdian Masyarakat Indonesia. *Tindak Pidana Cyber Crime Dalam Hukum Indonesia Serta Upaya Pencegahan Dan Penanganan Kasus Tindak Pidana Cyber Crime.* Volume 4 No 1 Januari 2025. Jakarta.

Budiman Maman, *Kejahatan Korporasi Di Indonesia*, Malang, Setara Press, 2020

Cok Rai Kesuma Putra1, I Nyoman Gede Sugiartha2, I Made Minggu Widyantara3. Jurnal *Analisis Yurudis Atas Keabsahan Atas Pertanggungjawaban Pidana Terhadap Pelaku Tindakan Pidana Pembobolan Sistem Data Keamanan Komputer (Craking).* 2024

Handoko Cahyo, *"Kedudukan Alat Bukti Digital Dalam Pembuktian Cybercrime di Pengadilan"* (2017).

Irianto Sulistyowati. *Metode Penelitian Kualitatif dalam Metodologi Penelitian Ilmu Hukum.* Jurnal Hukum dan Pembangunan. Volume 32 Nomor 2. 2002.

I Gusti Ayu Suanti Karnadi Singgi, I Gusti Bagus Suryawan, I Nyoman Gede Sugiartha. Jurnal. *Penegakan Hukum Terhadap Tindak Pidana Peretasan Sebagai Bentuk Kejahatan Mayantara (Cyber crime).* Vol. 1 No 2 Oktober 2020.

Kartiko Galuh, *"Pengaturan Terhadap Yurisdiksi Cyber Crime Ditinjau dari Hukum Internasional"* (2013) 8:2 Rechtidee.

Mathilda Fiorida, *"Cyber Crime Dalam Sistem Hukum Indonesia,"* Sigma-Mu 4, no. 2 (2012).

Mariya Azis dan Muhamad Hasan Rumlus. Jurnal *Perlindungan Hukum Pada Masyarakat Dari Tindakan CrackingPerpektif UUInformasi Dan Transaksi Elektronik Dan Hukum Pidana Islam.* 2021.

Mertukusomo Sudikno, *"Mengenal Hukum",* Liberty Yogyakarta, Yogyakarta :2003.

Muhamad Antony dan Agus Priyambodo. Jurnal *cyber crime dalam sudut pandang hukum pidana.* Vol 6. No 1 Juni 2022.

Nikles Denny Ardiansyah1, Bambang Panji Gunawan2, Djasim Siswono3. Jurnal Hukum *Penerapan UU ITE Dalam Penegakan Hukum Siber Di Indonesia Studi Kasus Pada Pasal 27 Hingga Pasal 37.* Volume 7, Nomor 2, Juli 2024.

Putrananto Widiatmoko Adi, *"Pengelolaan Arsip di Era Digital: Mempertimbangkan Kembali Sudut Pandang Pengguna"*, Diplomatika Vol. 1 No. 1, 2017.

Rachmadie Donovan Typhano & Supanto, *"Regulasi Penyimpangan Artificial Intelligence Pada Tindak Pidana Malware*

Berdasarkan Undang-Undang Republik Indonesia Nomor 1 Tahun 2016" (2020) 9:2 Hukum Pidana Dan Penanggulangan Kejahatan.

Rizky Arafah. *Sanksi Tindak Pidana Hacking (STUDI ANALISIS UNDANG UNDANG ITE DAN HUKUM PIDANA ISLAM).* Sumatera Utara 2019.

Sabillon et al Regner, *"Cybercrime and cybercriminals: A comprehensive study"* , Volume 4, Nomor 6, 2016.

Saleh Muliadi. *Aspek Kriminologis Dalam Penanggulangan Kejahatan.* Volume 6. No 1 Januari-April 2012.

Suharto Miko Aditiya & Maria Novita Apriyani, *"Konsep Cyber Attack, Cyber Crime, Dan Cyber Warfare Dalam Aspek Hukum Internasional"* (2021).

Septiani Maharani. *Manusia sebagai Homo Economicus Refleksi Atas Kasus- Kasus Kejahatan Di Indonesia.* Vol 26, No 1 Tahun 2016

Thackeray Rosemary & MaryAnne Hunter, *"Empowering Youth: Use of Technology in Advocacy to Affect Social Change"*, Volume 15, Nomor 4, 2020.

Widodo, *Hukum Pidana di Bidang Teknologi Informasi, Cybercrime Law: Telaah Teoritik dan Bedah Kasus,* Aswaja Pressindo, Yogyakarta, 2013.

Yuli Tasya. Jurnal *Craking Dalam Prespektif Undang- Undang Nomor 11 Tahun 2008 DAN Hukum Pidana Islam* 2020.

Peraturan Perundang-undangan

Undang-undang Dasar Negara Republik Indonesia Tahun 1945

Kitab Undang-undang Hukum Pidana

Undang-undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik

Artikel/Internet

Dosen Sosiologi. *Pengertian Kejahatan, Jenis, penyebab, dan Contohnya.* https://www.sosiologi79.com/2020/03/pengertian-kejahatan-menurut-para-ahli.html.

Dessy Suciati Saputri, *"Indonesia Peringkat ke-2 Dunia Kasus Kejahatan Siber,"* RepublikaOnline,2015,https://republika.co.id/berita/nasional/umum/15/04/09/nmjajy-indonesia-peringkat-ke2-duniakasus-kejahatan-siber

Direktori Putusan Mahkamah Agung Republik Indonesia. Putusan Mahkamah Agung Id.

Irhan Hisyam Dwi Nugroho. Artikel tentang *Cyber Security.* Dalam https://dibimbing.id/blog/detail/data-forgery-adalah#:~:text=Data%20forgery%20adalah%20tindakan%20memalsukan%20data%20digital%2C%20seperti

Mas Wigrantoro Roes Setiyadi dan Mirna Dian Avanti Siregar, Naskah Akademik Rancangan Undang-Undang Tindak Pidana di Bidang Teknologi Informasi, Global Internet PolicyInitiativeIndonesia bekerja sama dengan Indonesia Media Law and Policy Center, November

Penjelasan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, Paragraf 2

Putri Zakia Salsabila, *"Kejahatan Siber di Indonesia Naik 4 Kali Lipat Selama Pandemi,"*Kompas.com,2020,https://tekno.kompas.com/read/2020/10/12/07020007/kejahatan-siber-di-indonesia-naik-4-kalilipat-selama-pandemi

Raida L Tobing, *Laporan Akhir Penelitian Hukum tentang Efektifitas UU No. 11 Tahun 2008 tetang Informasi dan Transaksi Elektronik* (Jakarta: Badan Pembinaan Hukum Nasional Kementrian Hukum dan HAM RI, 2010)

Ratna Christianingrum & Ade Nurul Aida, Tantangan Penguatan Keamanan Siber dalam Menjaga Stabilitas Keamanan (Jakarta: Pusat Kajian Anggaran Badan Keahlian-Sektretariat Jenderal Dewan Perwakilan Rakyat Republik Indonesia, 2021)

Ridhokudik. ArtikelTentangCyberLawdalamhttp://ridhosukamusik.blogspot.co.id/ 2010/10/ artikel-tentang-cyberlaw.html

TVRI News, Jakarta. *Polri Bongkar Kasus Scam Modus Lowongan Pekerjaan, Kerugian Mencapai Rp. 1,5 Triliun. https://hukum.tvrinews.com/berita/tl8977q-polri-bongkar-kasus-scam-modus-lowongan-pekerjaan-kerugian-mencapai-rp15-triliun*

Viva Budy Kusnandar, "Pengguna Internet Indonesia Peringkat ke-3 Terbanyak di AsiaDataboks,"Katadata.co.id,2021,https://databoks.katadata.co.id/datapublish/2021/10/14/pengguna-internetindonesia-peringkat-ke-3-terbanyak-di-asia.

Hukum Online, "Jangkauan Yuridiksi UU ITE Menherat Pelaku Craking Server Milik Asing". https://www.hukumonline.com/klinik/a/jangkauan-yurisdiksi-uu-ite-menjerat-pelaku-

icracking-server-i-milik-asing-
lt517d0337ad845/.