**Legal Analysis of the Criminal Act of Extortion Through Cracking**

**Analisis Hukum Tindak Pidana Pemerasan Melalui *Cracking***

**Agam Yudha Herlambang**

**Sekolah Tinggi Ilmu Hukum IBLAM, Jl. Kramat Raya No.25, RT.3/RW.2, Kramat, Kec. Senen, Kota Jakarta Pusat, Daerah Khusus Ibukota Jakarta 10450**

**Sugeng Djatmiko**

**Sekolah Tinggi Ilmu Hukum IBLAM, Jl. Kramat Raya No.25, RT.3/RW.2, Kramat, Kec. Senen, Kota Jakarta Pusat, Daerah Khusus Ibukota Jakarta 10450**

***Abstract***

*Cybercrime crime is growing and out of control. An example is hacking activity which poses a high risk, especially if the hack involves an institutional information network or a vital installation. Of the various cases that occur, it is not uncommon for hackers and crackers to take advantage of these hacks by blackmailing and threatening victims to pay a sum of money if they want the victim's site or website to be returned to its original state. These hacks are often aimed at companies or corporations. However, not many cases are investigated or reported because the victim is afraid of threats from the perpetrator and for the sake of protecting the victim's personal data. This type of legal research is normative legal research. The nature of the research in this study is analytical descriptive in nature. The type of data used in this study is library research. An act of extortion through cracking can be held accountable based on Law no. 19 of 2016 concerning Amendments to Law no. 11 of 2008 concerning Information and Electronic Transactions namely Article 27 paragraph (4) in conjunction with Article 45 paragraph (1), Article 30 in conjunction with Article 46, Article 36 in conjunction with Article 51 paragraph (2), and Article 37 in conjunction with Article 52 paragraph (2). Based on the provisions of these articles, the penalty that can be imposed on the perpetrator is a maximum of 12 years in prison and a minimum of 6 years in prison, as well as a maximum fine of Rp. 12,000,000,000,000 and a minimum fine of Rp. 1,000,000,000,000. And based on the provisions of Article 2 of the ITE Law, it is emphasized that this Law applies to every person who carries out legal actions as stipulated in this Law, both within the jurisdiction of Indonesia and outside the territory of Indonesia, which has legal consequences in the jurisdiction of Indonesia. Indonesia and/or outside the jurisdiction of Indonesia and detrimental to Indonesia's interests. The perpetrators of the crime of extortion through cracking can also be charged with criminal liability based on the provisions of the Criminal Code, namely Article 335 paragraph (1), Article 368 paragraph (1), Article 369 and Article 406 of the Criminal Code. Article 335 paragraph (1) of the Criminal Code is punishable by a maximum penalty of one (1) year imprisonment or a maximum fine of Rp. 4,500 (four thousand and five hundred rupiahs), Article 368 paragraph (1) of the Criminal Code is punishable by a maximum imprisonment of eight (8) years, and a maximum of four (4) years of imprisonment under the provisions of Article 369 of the Criminal Code*

***Keywords***: *Criminal, Extortion, Cracking*

**Abstrak**

Kejahatan cybercrime semakin berkembang dan tidak terkendali. Sebagai contoh adalah aktifitas hacking yang menimbulkan risiko yang tinggi, apalagi jika yang di-hack itu menyangkut jaringan informasi institusi atau instalasi vital. Dari berbagai kasus yang terjadi tak jarang para hacker dan cracker memanfaatkan peretasaan tersebut dengan melakukan pemerasan dan mengancam korban agar membayarkan sejumlah uang jika ingin situs atau website korban dikembalikan seperti semula. Peretasan tersebut sering ditujukan pada perusahaan atau korporasi. Namun tidak banyak kasus yang diusut atau dilaporkan karena korban takut dengan ancaman dari pelaku dan demi menjaga data pribadi korban.Jenis penelitian hukum ini merupakan penelitian hukum normatif. Sifat penelitian dalam penelitian ini adalah bersifat deskriptif analitis. Jenis data yang digunakan dalam penelitian ini adalah penelitian kepustakaan (library research).Suatu Tindak Pidana Pemerasan Melalui Cracking dapat dibebani pertanggungjawaban berdasarkan Undang-Undang No. 19 Tahun 2016 tentang Perubahan Atas Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yaitu Pasal 27 ayat (4) jo Pasal 45 ayat (1), Pasal 30 jo Pasal 46, Pasal 36 jo Pasal 51 ayat (2), dan Pasal 37 jo Pasal 52 ayat (2). Berdasarkan ketentuan pasal-pasal tersebut, ancaman hukuman yang dapat dijatuhkan kepada pelaku adalah maksimal 12 tahun pidana penjara dan minimal 6 tahun pidana penjara, serta denda maksimal Rp. 12.000.000.000.000 dan denda minimal Rp. 1.000.000.000.000. Dan berdasarkan ketentuan Pasal 2 UU ITE ditegaskan bahwa Undang-Undang ini berlaku untuk setiap Orang yang melakukan perbuatan hukum sebagaimana diatur dalam Undang-Undang ini, 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. Adapun Pelaku Tindak Pidana Pemerasan Melalui Cracking juga dapat dibebani pertanggungjawaban pidana berdasarkan ketentuan dalam KUHP yaitu Pasal 335 ayat (1), Pasal 368 ayat (1), Pasal 369, dan Pasal 406 KUHP. Pada Pasal 335 ayat (1) KUHP diancam dengan hukuman maksimal satu (1) tahun pidana penjara atau denda sebanyak-banyaknya Rp. 4.500 (empat ribu kima ratus rupiah), Pada Pasal 368 ayat (1) KUHP diancam dengan hukuman penjara maksimal delapan (8) tahun, dan maksimal empat (4) tahun pidana penjara berdasarkan ketentuan Pasal 369 KUHP

**Kata Kunci**: Pidana, Pemerasan, Cracking.

### PENDAHULUAN

Cikal bakal internet dikenal pertamakali pada tahun 1969 oleh Departemen Pertahanan Amerika Serikat dengan nama ARPAnet (*Advanced Research Projects Agency Network*). ARPAnet dibangun dengan sasaran untuk membuat suatu jaringan komputer yang tersebar, untuk menghindari pemusatan informasi di satu titik yang dipandang rawan untuk dihancurkan bila terjadi peperangan. Dengan cara ini diharapkan apabila satu jaringan terputus, maka jalur yang melalui jaringan tersebut dapat secara otomatis dipindahkan ke saluran lainnya (Arifin & Muthia, 2019). Yang kemudian jaringan ini berkembang menjadi internet dan terbentuklah dunia baru yang disebut sebagai *Cyberspace*. *Cyberspace* menawarkan manusia untuk “hidup” dalam dunia alternatif. Sebuah dunia yang dapat mengambil alih dan menggantikan realitas yang ada, yang lebih menyenangkan dari kesenangan yang ada, yang lebih menggairahkan dari kegairahan yang ada (Raodia, 2019). Jagat raya *cyberspace* telah membawa masyarakat dalam berbagai sisi realitas baru yang tidak pernah dibayangkan sebelumnya, yang penuh dengan harapan, kesenangan, kemudahan dan pengembaraan, seperti *Teleshoping, Teleconference, Teledildonic, Virtual Cafe, Virtual Architecture, Virtual Museum, Cybersex, Cyberparty* Dan *Cyberorgasm* (Abdul & Mohammad, 2005). Perkembangan yang pesat dalam teknologi internet menyebabkan kejahatan di bidang itu juga muncul, misalnya kejahatan manipulasi data, spionase, sabotase, provokasi, *money laundering*, *hacking*, pencurian *software* maupun perusakan *hardware* dan berbagai macam lainnya, yang kemudian sering disebut sebagai kejahatan dalam dunia maya atau *Cybercrime* (Bunga, 2019)*.*

*Cybercrime* dalam pengertian sempit (Kejahatan Komputer), apapun prilaku yang tidak sah yang diarahkan atas bantuan operasi elektronik dengan sasaran keamanan sistem komputer dan data yang diprosesnya. Dalam pengertian luasnya (Kejahatan yang berkaitan dengan komputer), apapun perilaku yang dilakukan atas bantuan atau dalam hubungan dengan suatu sistem komputer atau jaringan, mencakup kejahatan pemilikan tidak sah dan menawarkan atau membagi-bagikan informasi atau bantuan suatu sistem komputer atau jaringan (IMAM SUJONO MH CPL, 2019). Internet atau jaringan komputer yang besar sesungguhnya tidak mengganggu manusia, justru membantu manusia dalam mencapai tujuan-tujuan yang bersifat positif, seperti dalam bidang bisnis ada *e-commerce* atau *e-trade*, sebagai media pendidikan politik dan sebagainya. Faktor manusia yang menggunakan internet dengan tujuan jahat yang membuat pemakai internet lainnya tidak nyaman. Manusia inilah yang dalam dunia *cyberspace* dinamakan *hacker* hitam/*cracker* (Arifah, 2011)*.*

Permasalahan keamanan jaringan atau keamanan informasi berbasis internet dalam era global ini menempati kedudukan yang sangat penting, apalagi jika dihubungkan dengan persoalan informasi sebagai komoditi. Informasi sebagai komoditi memerlukan kehandalan pelayanan agar apa yang disajikan tidak mengecewakan pelanggannya. Untuk mencapai tingkat kehandalan tentunya informasi itu sendiri harus selalu dimutakhirkan sehingga informasi yang diberikan tidak ketinggalan zaman. Disamping itu, menjaga keamanan sistem informasi yang dijual itu sama pentingnya dengan menjaga kemutakhiran informasi. Keamanan sistem informasi berbasis internet juga selalu harus dimutakhirkan untuk mencegah serangan atau perusakan yang dilakukan oleh *cracker* maupun *vandal* computer (Nyoman Triana Suskendariani & Sabri Guntur, 2022). Peringkat Indonesia dalam kejahatan di dunia maya (menggunakan internet) telah menggantikan posisi Ukraina yang sebelumnya menduduki posisi pertama. Indonesia menempati presentase tertinggi di dunia maya. Data tersebut berasal dari penelitian *Verisign*, perusahaan yang memberikan pelayanan intelijen di dunia maya yang berpusat di California Amerika Serikat (Singgi et al., 2020). Hal ini mengakibatkan kejahatan *cybercrime* semakin berkembang dan tidak terkendali. Sebagai contoh adalah aktifitas *hacking* yang menimbulkan risiko yang tinggi, apalagi jika yang di-*hack* itu menyangkut jaringan informasi institusi atau instalasi vital seperti halnya pusat-pusat penelitian, jaringan sistem informasi bisnis keuangan dan perbankan, reaktor nuklir, sistem pertahanan keamanan negara, pengawas penerbangan pesawat udara atau jaringan-jaringan komputer rumah sakit medis (Sari, 2017).

Berikut ini beberapa kejadian yang menimpa beberapa situs milik pemerintah dan perusahaan di Indonesia yang telah menjadi korban *cracker*, antara lain (Sa’diyah, 2012):

1. Situs Departemen Luar Negeri dan ABRI dijebol oleh *cracker* Porto (Portugis) yang pro kemerdekaan Timor-Timur.
2. September dan Oktober 2000, seorang *cracker* dengan julukan Fabian Clone berhasil menjebol *web* milik Bank Bali. Sebelumnya mereka juga berhasil menjebol *web* milik Bank Lippo.
3. April 2001, situs *web* milik Departemen Agama dan Departemen Perindustrian dan Perdagangan dirusak oleh *cracker*. *File-file* penting dan *Log file*-nya dihapus.

Kasus lainnya yaitu *website* milik KPU yang berhasil dibobol oleh Dani Firmansyah, seorang konsultan Teknologi Informasi di PT. Danareksa Jakarta yang diputus dengan Putusan No: 1322/Pid.B/2004/PN.Jkt.Pst, Kasus 3 Komputer Milik PT. Bumi Resources Tbk (BUMI) berupa 1,5 *Terrabyte* data berbentuk *Microsoft Office*, *Portabel Document Format* (PDF), Gambar, dan jenis data lainnya yang berhasil dicuri oleh *cracker*, kemudian yang baru saja terjadi di tahun 2018 adalah kasus Surabaya *Black Hat* (SBH) yang meretas ribuan situs dari 40 Negara, yang tersangkanya adalah 3 orang mahasiswa dari Surabaya mereka terjerat Pasal 30 jo. Pasal 46 atau Pasal 29 jo. Pasal 45B dan atau Pasal 32 jo. Pasal 48 UU ITE dan/atau Pasal 3, 4, dan 5 UU RI No. 8 Tahun 2010 tentang Tindak Pidana Pencucian Uang (hukumonline.com, 2004).

Dari berbagai kasus yang terjadi tak jarang para *hacker* dan *cracker* memanfaatkan peretasaan tersebut dengan melakukan pemerasan dan mengancam korban agar membayarkan sejumlah uang jika ingin situs atau *website* korban dikembalikan seperti semula. Peretasan tersebut sering ditujukan pada perusahaan atau korporasi. Namun tidak banyak kasus yang diusut atau dilaporkan karena korban takut dengan ancaman dari pelaku dan demi menjaga data pribadi korban. Contoh kasus tindak pidana pemerasan melalui *cracking* yaitu kasus seorang bekas Pegawai Negeri Sipil (PNS) berinisial BA (32), menjadi seorang pembajak *e-mail*, sekaligus melakukan pemerasan terhadap pemilik emailnya. BA melakukan perbuatannya di sebuah warnet yang terletak di Wonosobo, Jawa Tengah. BA terlebih dahulu membajak *e-mail* Mr. X kemudian mengirimkan *e-mail* kepada korbannya dengan mengancam akan mempublikasikan foto-foto *hot* sang pemilik *e-mail* ke jejaring sosial. "Bilamana korban tidak menyerahkan uang Rp 500 juta, maka dia (BA) akan menyebarluaskan foto-foto pribadi korban melalui internet," kata Kepala Divisi Humas Polri Irjen Polisi, Saud Usman Nasution, di Mabes Polri, Jakarta Selatan, Selasa (21/2/2012). Foto-foto pribadi korban yang akan disebarkan BA merupakan foto yang ada di dalam *folde*r *e-mail* korban yang dibajak. Setelah mendapatkan ancaman, Mr. X pun langsung melaporkan kejadian tersebut ke Bareskrim Mabes Polri pada 6 Februari 2012 lalu. Tidak butuh waktu lama untuk menangkap BA, Direktorat I Tindak Pidana Khusus Mabes Polri, Unit *Cyber Crime* langsung melakukan pelacakan terhadap sang pembajak melalui internet sampai akhirnya diketahui petunjuk-petunjuk bahwa pelaku berada di Wonosobo. Kemudian pada 8 Februari 2012, polisi berhasil menangkap BA di sebuah warung internet. Kini BA mendekam di tahanan Bareskrim Polri untuk mempertanggungjawabkan perbuatannya, tersangka dijerat dengan pasal perusakan, pemerasan, dan Undang-Undang ITE (Adi Suhendi dan Taryono, 2018).

Jika dilihat dalam Kitab Undang-Undang Hukum Pidana KUHP dan dalam Undang-Undang No.19 Tahun 2016 tentang Perubahan Atas Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), contoh kasus tersebut dapat dikategorikan sebagai suatu perbuatan yang melanggar hukum dan dapat dijerat dengan pasal berlapis atau *samenloop* (Agung et al., 2023). Pasal yang dilanggar yaitu pasal yang mengatur tentang pemerasan dan pasal yang mengatur tentang *hacking/cracking,* yaitu Pasal 335 Ayat (1), 368 ayat (1), Pasal 406 ayat (1) KUHP, Pasal 27 Ayat (4) UU ITE, Pasal 30 UU ITE, Pasal 45 ayat (1) ITE, dan Pasal 46 UU ITE.

Ketentuan pertanggungjawaban pidana adalah kesalahan, maka suatu pertanggungjawaban pidana dapat dilakukan apabila seseorang telah melakukan kesalahan dan kesalahan tersebut juga telah memenuhi unsur-unsur tindak pidana yang diatur dalam peraturan perundang-undangan. Dasar pertanggung jawaban adalah kesalahan, dalam arti sempit kesalahan dapat berbentuk sengaja (*opzet*) atau lalai (*culpa*). Membicarakan kesalahan berarti juga membicarakan pertanggungjawaban. Sehingga dengan demikian pertanggungjawaban pidana merupakan dasar fundamental hukum pidana (Teguh Prasetyo, 2017). Dimana kesalahan merupakan jantungnya hukum pidana. Konsepsi yang melatarbelakangi pemikiran pertanggungjawaban pidana itu dapat dilakukan apabila unsur-unsur tindak pidana tersebut terbukti atau pertanggungjawaban pidana dilekatkan kepada unsur-unsur tindak pidana adalah suatu pemikiran yang berangkat dari suatu perdebatan panjang dianutnya aliran *monistis* yang berorientasi kepada perbuatan sebagai konsekuensi dianutnya asas legalitas formal dalam Pasal 1 KUHP (Utrecht, 2000). Bukti yuridis bahwa konsep demikian dianut oleh hukum pidana terletak dalam rumusan Pasal 1 KUHP yang merumuskan bahwa tiada suatu perbuatan dapat dipidana kecuali ditentukan terlebih dahulu dalam peraturan perundang-undangan. Dengan demikian yang dilarang dan diancam dengan pidana adalah dilarangnya melakukan perbuatan yang disertai dengan ancaman terhadap perbuatan itu sendiri. Secara umum hukum pidana merupakan peraturan yang mengatur tentang perbuatan-perbuatan yang dilarang oleh Undang-Undang beserta ancaman pidana yang dapat dijatuhkan terhadap pelanggarnya (Hakim, 2020). Dalam hukum pidana ada dua hal penting yang perlu mendapat perhatian, yaitu tentang melakukan perbuatan pidana (*actus reus*) yang berkaitan dengan subjek atau pelaku tindak pidana dan mengenai kesalahan (*mens rea*) yang berkaitan dengan masalah pertanggungjawaban pidana (Atmasasmita, 1989).

Subjek atau pelaku tindak pidana secara umum dalam hukum pidana hanya mengakui orang sebagai pelaku, sedangkan pertanggungjawaban pidana menganut asas kesalahan (*culpabilitas*) yang berarti untuk dapat menjatuhkan sanksi pidana pada pelaku tindak pidana, selain memenuhi unsur-unsur rumusan tindak pidana juga harus adanya unsur-unsur kesalahan. Dalam menentukan dapat dipidananya seseorang ada dua pendapat yang dianut yaitu aliran monistis dan aliran dualistis. Aliran monistis memandang bahwa seseorang yang melakukan tindak pidana dan telah memenuhi unsur-unsur dari tindak pidana tersebut, sudah pasti dapat dipidana. Dikarenakan dalam aliran ini menggabungkan antara kesalahan dan unsur-unsur dari suatu tindak pidana. Sehingga, unsur kesalahan itu sendiri tidak perlu dibuktikan lagi, sedangkan dalam aliran dualistis, terdapat perbedaan antara kesalahan dengan unsur-unsur dari suatu tindak pidana (Marwan Effendy, 2014). Jadi, selain terpenuhinya unsur-unsur dari suatu tindak pidana, harus juga dibuktikan unsur kesalahannya. Dari uraian tersebut dapat dikatakan bahwa pedoman pemidanaan bagi pelaku tindak pidana masih berpegang pada asas “tiada pemidanaan tanpa kesalahan” yang artinya bahwa seseorang tidak mungkin dipidana apabila tidak mempunyai kesalahan, atau meskipun telah melakukan tindak pidana, tidak selalu seseorang dapat dipidana.

Keinginan untuk menganalisis mengenai pertanggungjawaban suatu tindak pidana *cyber crime* terhadap pelanggaran Pasal 335, 368 dan 406 KUHP, serta pelanggaran Pasal 27 ayat (4) dan Pasal 30 UU ITE dianggap telah mengganggu ketertiban kehidupan bermasyarakat. Dikatakan mengganggu ketertiban kehidupan bermasyarakat karena tindak pidana ini bisa menimbulkan kerugian berupa materil maupun immateril. Kerugian materil dapat berupa hilangnya uang, sedangkan kerugian immateril dapat berupa tercemarnya nama baik seseorang maupun instansi tertentu (Abidin, 2015).

Untuk membahas permasalahan yang telah dirumuskan dan dibatasi sebagaimana tersebut diatas, maka dalam metode penyusunan dan penyelesaian peneliti dalam penelitian ini, akan dipergunakan metode dan Teknik penelitian sebagaimana dibawah ini. Jenis penelitian yang dilakukan adalah penelitian hukum normatif (Suteki dan Galang Taufani, 2018). Sifat penelitian dalam penelitian ini adalah bersifat deskriptif analitis. Jenis data yang digunakan dalam penelitian ini adalah penelitian kepustakaan (*library research*).Sumber data yang digunakan dalam penelitian ini adalah data sekunder yang berupa bahan hukum primer: Kitab Undang - Undang Hukum Pidana (KUHP) dan Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik. Bahan hukum sekunder: yaitu bahan-bahan hukum yang diperoleh buku - buku bacaan dan laporan-laporan hasil penelitian hukum yang ada hubungannya dengan masalah yang diteliti dan bahan hukum tersier yaitu bahan hukum yang pelengkap sifatnya memberikan petunjuk atau penjelasantambahan terhadap bahan hukum primer dan bahan hukum sekunder. Bahan hukum tersier ini terdapat dalam penelitian misalnya kamus hukum, kamus bahasa, ensiklopedia dan lain sebagainya (Soerjono Soekanto & Sri Mamudji, 2001).

### PERTANGGUNGJAWABAN PIDANA PELAKU TINDAK PIDANA PEMERASAN MELALUI *CRACKING* BERDASARKAN KITAB UNDANG – UNDANG HUKUM PIDANA

Perbuatan pidana hanya menunjukkan kepada dilarang dan diancamnya perbuatan dengan suatu pidana. Apakah orang yang melakukan perbuatan kemudian juga di jatuhkan pidana, sebagaimana telah diancam, ini tergantung dari soal apakah dalam melakukan perbuatan ini dia mempunyai kesalahan, sebab asas dalam pertanggungjawaban dalam hukum pidana ialah tidak dipidana jika tidak ada kesalahan (*Geen Straf Zonder Schuld: Actus non facit reum nisi mens sir rea*) (Moelijatno, 2015). Pertanggungjawaban tanpa adanya kesalahan dari pihak yang melanggar, dinamakan *leer van het materiele fei*t (*fait materielle*).

Kemampuan bertanggung jawab merupakan salah satu unsur dalam hukum pidana untuk menentukan apakah si pembuat tindak pidana itu dapat dituntut atau tidak, masalah kemampuan bertanggung jawab dalam KUHP dirumuskan secara negatif, seperti yang dicantumkan di dalam Pasal 44 KUHP tentang tidak mampu bertanggung jawab. Dalam Pasal 44 KUHP seseorang dinyatakan tidak mampu bertanggung jawab apabila jiwanya cacat dalam pertumbuhan (kurang sempurna akalnya) dan terganggu karena penyakitnya (sakit ingatan). Dalam teori lain dijelaskan bahwa, seseorang dapat dimintakan pertanggungjawaban atas perbuatan pidanayang dilakukannya apabila memenuhi syarat-syarat berikut (Remmelink, 2014): (1) kemampuan untuk membeda-bedakan antara perbuatan yang baik dan yang buruk yang sesuai dengan hukum yang melawan hukum; (2)kemampuan untuk menentukan kehendaknya menurut keinsyafan tentang baik dan buruknya perbuatan tadi

Moeljatno kemudian menjelaskan, yang pertama merupakan faktor akal (*intelectual factor*) yaitu dapat memperbeda-bedakan antara perbuatan yang diperbolehkan dan yang tidak. Yang kedua adalah faktor perasaan atau kehendak (*volitional factor*) yaitu dapat menyesuaikan tingkah lakunya dengan keinsyafan atas nama yang diperbolehkan dan mana yang baik (Moelijatno, 2015). Dengan kemajuan teknologi yang semakin berkembang, suatu tindak pidana ataupun kejahatan semakin sulit untuk dijangkau. Apalagi kejahatan yang berkaitan dengan dunia maya atau biasa disebut dengan istilah *cyber crime.* Dan bentuk kejahatannyapun bermacam-macam, salah satunya adalah kejahatan pemerasan yang didahului dengan kejahatan *cracking* (Sa’diyah, 2012). Berdasarkan peraturan perundang-undangan yang berlaku di Indonesia ada dua peraturan yang mengatur tentang tindak pemerasan yaitu Kitab Undang-Undang Hukum Pidana (KUHP) dan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE).

Tindak Pidana *Cracking* dalam KUHP tidak diatur dalam delik khusus, karena jenis tindak pidana ini termasuk ke dalam jenis tindak pidana baru. Namun tindak pidana *cracking* dapat dikenakan ketentuan dalam Pasal 406 ayat (1) KUHP atas delik pengrusakan dimana pasal ini yang menyatakan bahwa barangsiapa dengan sengaja dan dengan melawan hak membinasakan, merusakkan, membuat sehingga tidak dapat dipakai lagi atau menghilangkan sesuatu barang yang sama sekali atau sebagiannya kepunyaan orang lain (Tajriyani, 2021).

Pasal 406 ayat (1) KUHP:

“Barangsiapa dengan sengaja dan dengan melawan hak membinasakan, merusakkan, membuat sehingga tidak dapat dipakai lagi atau menghilangkan sesuatu barang yang sama sekali atau sebagiannya kepunyaan orang lain, dihukum penjara selama-lamanya dua tahun delapan bulan atau denda sebanyak-banyaknya Rp. 4.500,--“

Penjelasan R. Soesilo antara lain:

1. Supaya dapat dihukum menurut pasal ini harus dibuktikan:
2. bahwa terdakwa telah *membinasakan, merusakkan, membuat sehingga ridak dapat dipakai lagi* atau *menghilangkan sesuatu barang*;
3. bahwa pembinasaan dsb. tersebut itu harus dilakukan dengan *sengaja* dan dengan *melawan hak*;
4. bahwa barang itu harus *sama sekali* atau *sebagian kepunyaan orang lain*.
5. Yang dihukum menurut pasal ini tidak saja mengenai barang, tetapi juga menganai binatang.
6. Pembinasaan atau perusakan dsb. Barang disini hanya mengenai barang-barang biasa kepunyaan orang lain.
7. Jika pengrusakan barang itu dilakukan oleh dua orang atau lebih, diancam dengan hukuman yang lebih berat (Pasal 412)
8. Pada waktu mengusut perkara perusakan ini oleh polisi senantiasa harus menyelidiki berpakah uang kerugian yang diderita pemilik barang yang telah dirusak tersebut. Dst.[[1]](#footnote-0)

Jadi pelaku tindak pidana *cracking* dapat dibebani pertanggungjawaban pidana atas pengrusakan sistem komputer atau *website* milik orang lain, dan di dakwa dengan dakwaan alternatif bersamaan dengan UU ITE (Talinusa, 2015).

1. **PERTANGGUNGJAWABAN PIDANA PELAKU TINDAK PIDANA PEMERASAN MELALUI *CRACKING* BERDASARKAN UNDANG-UNDANG NOMOR 19 TAHUN 2016 TENTANG PERUBAHAN ATAS UNDANG-UNDANG NOMOR 11 TAHUN 2008 TENTANG INFORMASI**

Dalam ketentuan UU ITE perumusan tindak pidana selalu diawali dengan kata-kata “Setiap Orang”, hal ini menunjuk kepada pengertian orang. Namun pada Pasal 1 angka 21 UU ITE ditegaskan bahwa yang dimaksud dengan “orang” adalah orang perorangan, baik warga negara Indonesia, warga negara asing, maupun badan hukum. Pasal 1 angka 21 UU ITE menyebutkan Orang adalah orang perseorangan, baik warga negara Indonesia, warga negara asing, maupun badan hukum (Budoyo et al., 2021). Tindak pidana pemerasan dalam UU ITE diatur dalam Pasal 27 Ayat (4) UU ITE yang menyebutkan Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elekronik yang memiliki muatan pemerasaan dan/atau pengancaman. Terdapat 2 Unsur dalam Pasal 27 ayat (4) tersebut, yaiitu Unsur Obyektif dan Unsur Subyektif. Unsur-Unsur Obyektif antara lain: (1) perbuatannya, adalah mendistribusikan, mentransmisikan dan membuat dapat diaksesnya; (2) melawan hukum, adalah yang dimaksud dengan “tanpa hak”; (3) objeknya, adalah informasi elektronik dan/atau dokumen elektronik yang memiliki muatan pemerasan dan/atau pengancaman. Unsur Subyektifnya yaitu berupa kesalahan atau “dengan sengaja” (Budoyo et al., 2021).

Dengan demikian pelaku dapat dibebani pertanggungjawaban pidana berdasarkan Pasal 27 ayat (4) apabila pelaku terbukti dengan sengaja dan dengan penuh kesadaran telah melakukan pemerasan dan/atau pengancaman melalui media elektronik (Suparman et al., 2023). Jenis tindak pidana ini juga diatur dalam KUHP namun di dalam KUHP tidak menyebutkan mengenai media yang digunakan yaitu media elektronik, jadi tindak pidana yang dapat dipertanggungjawabkan berdasarkan pasal ini adalah jika media yang digunakan adalah media elektronik dan bukan dengan fisik seperti yang disebutkan dalam KUHP (Luthfi, 2021). Semua unsur di dalam ketentuan pasal ini harus terpenuhi dan dibuktikan dalam peradilan, apabila tidak terbukti maka tidak dapat dituntut atau diminta pertanggungjawaban pidana berdasarkan pasal ini . Adapun untuk ancaman pidananya tindak pidana pemerasan diatur dalam UU ITE Pasal 45 ayat (1), yang menyebutkan Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 27 ayat (1), ayat (2), ayat (3), atau ayat (4) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp. 1.000.000.000,00 (satu miliar rupiah).

Ada beberapa tahap *Hacking* yang selanjutnya akan digunakan sebagai langkah untuk menentukan tahap-tahap *Hacking* yang dapat dikategorikan sebagai kejahatan. Tahap-tahap *Hacking* seperti yang dimaksud adalah (Khalisah & Kirana, 2022):

1. mengumpulkan dan mempelajari informasi yang ada mengenai sistem operasi komputer atau jaringan kompuetr yang dipakai pada target sasaran;
2. menyusup atau mengakses jaringan komputer target sasaran;
3. menjelajahi sistem komputer dan mencari akses yang lebih tinggi;
4. membuat backdoor dan menghilangkan jejak.

Tidak setiap tahap dari *hacking* dapat disebut sebagai kejahatan. Tahap pertama dari hacking tidak dapat disebut sebagai kejahatan karena belum dapat dikatakan ada bahaya serius yang mengancam. Tahap kedua sampai keempat, dapat disebut sebagai kejahatan. Tahap kedua merupakan tahap yang paling ringan karena dalam tahap ini hanya bersifat masuk atau menyusup dan belum ada tindakan destruktif. Tahap ketiga dan keempat sudah mengandung unsur destruktif sehingga akibat yang ditimbulkan lebih buruk dibandingkan dengan tahap kedua (Hartanto, 2021). Tahap ketiga dan keempat inilah yang disebut dengan *cracking*, dimana perbuatannya dapat berupa merubah tampilan komputer atau website yang di *hack;* dan mengakses dan/atau mengambil *file-file* rahasia dalam sistem komputer. Dalam UU ITE telah diatur mengenai perbuatan peretasan kedalam Pasal 30. Pasal 30 UU ITE mengatur perbuatan yang meliputi: a. mengakses Komputer dan/atau Sistem Elektronik milik orang lain dengan cara apa pun; b. mengakses Komputer dan/atau Sistem Elektronik milik orang lain dengan cara apa pun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik; dan c. mengakses Komputer dan/atau Sistem Elektronik milik orang lain dengan cara apa pun dengan melanggar, menerobos, melampui, atau menjebol sistem pengamanan.

Pasal 30 UU ITE:

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 milik orang lain 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 milik orang lain dengan cara apa pun dengan melanggar, menerobos, melampui, atau menjebol sistem pengamanan.

Berdasarkan Pasal 30 ini dapat dijelaskan bahwa unsur-unsur yang termuat dalam tindak pidana peretasan *(hacking)* tersebut antara lain (Oktaviani, 2023):

1. Pasal 30 ayat (1) UU ITE

Unsur-unsurnya yaitu:

1. unsur “setiap orang”, yaitu setiap orang sebagai subjek hukum dapat bertanggungjawab baik orang perorangan maupun suatu badan hukum;
2. unsur “dengan sengaja, dan tanpa hak atau melawan hukum”, yaitu bahwa perbuatan tersebut dilakukan dengan sengaja dan pelaku mempunyai kesadaran penuh atas apa yang dilakukannya. Untuk unsur melawan hukum berarti bahwa perbuatan tersebut telah dilarang dan telah diatur dalam peraturan perundang-undangan yang berlaku;
3. unsur “mengakses komputer dan/atau sistem elektronik milik orang lain”, yaitu suatu suatu kegiatan melakukan interaksi dengan sistem elektronik yang berdiri sendiri atau dalam jaringan, melalui seperangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisa, menyimpan, menampilkan, mengummkan, mengirimkan, dan/atau menyebarkan informasi elektronik yang dilindungi keberadaannya;
4. unsur “dengan cara apapun”, yaitu dengan berbagai cara yang memungkinkan untuk dapat mengakses komputer dan/atau sistem elektronik milik orang lain, baik secara langsung maupun melalui internet (Singgi et al., 2020).

Seseorang dapat dibebani pertanggungjawaban pidana berdasarkan pasal ini apabila perbuatan yang dilakukan telah memenuhi unsur-unsur tersebut. Dan pasal ini menegaskan bahwa cara apapun yang ditempuh oleh pelaku dalam mengakses komputer dan/atau sistem komputer bukanlah merupakan faktor penentu bagi dapat atau tidak dapatnya pelaku dipertanggungjawaban secara pidana (Tolib Effendi, 2013). Ancaman pidana bagi pelanggar ketentuan dalam pasal ini diatur pada Pasal 46 ayat (1) UU ITE yang menyebutkan 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).

1. Pasal 30 ayat (2) UU ITE

Unsur-unsur pada pasal ini hampir sama dengan unsur yang terdapat Pada Pasal 30 ayat (1) namun ada sedikit penambahan unsur, yaitu unsur dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik. Dalam pasal ini ditegaskan bahwa pelaku tidak hanya sekedar mengakses saja tetapi pelaku mempunyai tujuan dalam perbuatannya yaitu untuk memperoleh suatu informasi elektronik dan/atau dokumen elektronik. Sehingga pelaku hanya dapat dibebani pertanggungjawaban pidana apabila terbukti mempunyai tujuan untuk memperoleh suatu informasi elektronik dan/atau dokumen elektronik (Arifah, 2011). Dan bagi pelaku diancam pidana berrdasarkan ketentuan pidana pada Pasal 46 ayat (2) UU ITE yang menyebutkan 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). Adapun penuntutannya harus dilakukan berdasarkan pasal sebelumnya yaitu, Pasal 30 ayat (1) *jo* Pasal 46 ayat (1). Dengan demikian Pasal 30 ayat (2) *jo* adalah *lex specialis* dari Pasal 30 ayat (1) *jo* Pasal 46 ayat (2).

1. Pasal 30 ayat (3) UU ITE

Unsur yang ditonjolkan dalam ayat (3) ini yaitu unsur dengan melanggar, menerobos, melampaui, atau menjebol sistem keamanan. Dalam unsur ini berarti bahwa pelaku *hacking* melakukan kejahatannya dengan menerobos sistem keamanan atau dalam ilmu komputer disebut *firewall*. Para *hacker* menggunakan berbagai aplikasi *tool hacking* dalam melakukan kejahatannya. Dimana aplikasi tersebut berguna untuk menerobos atau menjebol sistem keamanan suatu sistem elektronik (Aryo & Pakpahan, 2021). Dalam praktek dunia pengamanan sistem komputer, suatu perusahaan biasanya menyewa seorang *hacker* untuk menguji sistem pengamanan pada sistem komputer mereka apakah sudah baik dan tidak ada cela bagi *hacker* untuk mengakses sistem komputer tersebut. Dengan demikian seorang *hacker* tidak dapat dibebani pertanggungjawaban pidana berdasarkan Pasal ini karena ia memiliki izin dari pemilik untuk menerobos, melampui, atau menjebol sistem pengamanan pada sistem komputer tersebut. Dan baru dapat dibebani pertanggungjawaban pidana berdasarkan ketentuan dalam pasal ini apabila ia tidak memiliki izin untuk menerobos, melampui, atau menjebol sistem pengamanan computer (Dermawan Akmal, 2019). Untuk ancaman pidananya itu diatur di dalam Pasal 46 ayat (3) UU ITE menyebutkan 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).

Ketentuan Pasal 30 ayat (2) dan Pasal 30 ayat (3) UU ITE ini adalah apa yang biasa disebut dengan kejahatan atau tindak pidana *cracking.* Dalam UU ITE ini terdapat beberapa aturan tambahan yang mengatur tentang tindak pidana yang telah diatur dalam pasal-pasal sebelumnya (Hamdan Mustameer, 2022). Pasal-pasal ini menjadi aturan tambahan yang dapat dijadikan sebagai pasal penjerat bagi penegak hukum untuk menjerat para pelakuTindak Pidana Pemerasan Melalui *Cracking*, pasal-pasal tersebut diantaranya adalah:

* + - 1. Pasal 36 UU ITE

Pasal ini melarang setiap orang yang dengan sengaja dan tanpa hak atau melawan hukum untuk melakukan suatu perbuatan sebagaimana yang dimaksud dalam ketentuan pada Pasal 27 sampai dengan Pasal 34 yang mengakibatkan kerugian bagi orang lain. Pasal 36 UU ITE menyebutkan Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan perbuatan sebagaimana dimaksud dalam pasal 27 sampai dengan pasal 34 yang mengakibatkan kerugian bagi orang lain. Unsur-unsur yang terdapat di dalam Pasal 36 yaitu:

1. setiap orang;
2. dengan sengaja dan tanpa hak atau melawan hukum;
3. melakukan perbuatan sebagaimana dimaksud dalam Pasal 27 sampai Pasal 34;
4. mengakibatkan kerugian bagi orang lain.

Pengertian setiap orang disini, selain ditafsirkan sebagai individu juga badan hukum yang berbadan hukum sesuai ketentuan perundang-undangan. Pengertian dengan sengaja dan tanpa hak, dapat ditafsirkan sebagai perbuatan yang bertentangan dengan undang-undang dan tindakan melalaikan ancaman hukuman (Raodia, 2019). Serta perbuatan yang dilarang adalah melakukan perbuatan sebagaimana yang dimaksud Pasal 27 sampai dengan Pasal 34, khususnya Pasal 27 ayat (4) tentang Pemerasan dan Pasal 30 tentang *Cracking* dan perbuatan tersebut harus mengakibatkan kerugian bagi orang lain. Maka pelaku dapat dibebani pertanggungjawaban pidana atas Tindak Pidana Pemerasan Melalui *Cracking* berdasarkan ketentuan dalam pasal 36 apabila perbuatan yang dilakukannya menyebabkan kerugian bagi orang lain dan tidak dapat dibebani pertanggungjawaban pidana berdasarkan Pasal 36 apabila perbuatannya tersebut tidak menyebabkan kerugian bagi orang lain. Dan harus dapat dibuktikan unsur merugikan orang lain tersebut.

Pengaturan *hacking* sebagai tindak pidana dalam UU ITE pasal 36 diatas diancam dengan sanksi pidana yang terdapat dalam ketentuan pidana pasal 51 ayat (2) yaitu menyebutkan Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 36 dipidana dengan penjara paling lama 12 (dua belas) tahun dan/atau dengan paling banyak Rp 12.000.000.000,00 (dua belas miliar rupiah).

* + - 1. Pasal 37 UU ITE

Pasal 37 UU ITE melarang setiap orang untuk melakukan perbuatan yang dilarang sebagaimana yang dimaksud dalam Pasal 27 sampai dengan Pasal 36 di luar wilayah Indonesia terhadap Sistem Elektronik yang berada diwilayah yurisdiksi Indonesia. Pasal 37 UU ITE menyebutkan Setiap orang dengan sengaja melakukan perbuatan yang dilarang sebagamana dimaksud dalam pasal 27 sampai dengan pasal 36 di luar wilayah Indonesia terhadap Sistem Elektronik yang berada diwilayah yurisdiksi Indonesia. Hal yang ditonjolkan dalam Pasal 37 UU ITE adalah perbuatan tersebut dilakukan di luar wilayah Indonesia tetapi sasaran atau korbannya berada di wilayah Indonesia. Sehingga hanya dapat dipertanggungjawabkan pidananya apabila pelaku tindak pidana (khususnya pada Tindak Pidana Pemerasan Melalui *Cracking)* adalah orang luar negeri atau berada di luar negeri tetapi sasaran atau korban dari tindak pidana tersebut adalah orang Indonesia atau berada di dalam wilayah *yurisdiksi* Indonesia.

Berkaitan dengan ketentuan pidananya, dalam UU ITE terdapat pemberatan penjatuhan sanksi pidana pokok jika perbuatan-perbuatan yang dilakukan memiliki sifat-sifat yang memberatkan yang berkaitan dengan Tindak Pidana Pemerasan Melalui *Cracking*. Pemberatan tersebut terdapat dalam Pasal 52 ayat (4) UU ITE menyebutkan Dalam hal tindak pidana sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 37 dilakukan oleh korporasi dipidana dengan pidana pokok ditambah dua pertiga. Berdasarkan pasal 52 ayat (4) UU ITE diketahui bahwa pemberatan sanksi pidana didasarkan pada pelaku tindak pidana yang merupakan suatu korporasi (Oktaviani, 2023). Korporasi bisa dikatakan sebagai suatu lembaga atau badan ataupun organisasi yang memiliki struktur kepengurusan baik itu berupa suatu perusahaan ataupun badan hukum lainnya (Liyakasa, 2012). Ketentuan tersebut di atas dimaksudkan untuk menghukum setiap perbuatan yang memenuhi unsur sebagaimana dalam pasal 27 sampai dengan pasal 37 yang dilakukan oleh koorporasi (*corporate crime*) dan/atau staf yang memiliki kapasitas untuk: 1. mewakili korporasi; 2. mengambil keputusan dalam korporasi; 3. melakukan pengawasan dan pengendalian dalam korporasi; dan 4. melakukan kegiatan demi keuntungan korporasi. Apabila pelaku Tindak Pidana Pemerasan Melalui *Cracking* adalah korporasi maka dapat dibebani pertanggungjawaban pidana berdasarkan Pasal 52 ayat (2) UU ITE dan diancam hukuman pidana ditambah dua pertiga dari pidana pokoknya.

Ada beberapa tahap *Hacking* yang selanjutnya akan digunakan sebagai langkah untuk menentukan tahap-tahap *Hacking* yang dapat dikategorikan sebagai kejahatan. Tahap-tahap *Hacking* seperti yang dimaksud adalah (Aditama, 2021):

* 1. mengumpulkan dan mempelajari informasi yang ada mengenai sistem operasi komputer atau jaringan kompuetr yang dipakai pada target sasaran;
  2. menyusup atau mengakses jaringan komputer target sasaran;
  3. menjelajahi sistem komputer dan mencari akses yang lebih tinggi;
  4. membuat backdoor dan menghilangkan jejak.

Tidak setiap tahap dari hacking dapat disebut sebagai kejahatan. Tahap pertama dari hacking tidak dapat disebut sebagai kejahatan karena belum dapat dikatakan ada bahaya serius yang mengancam. Tahap kedua sampai keempat, dapat disebut sebagai kejahatan. Tahap kedua merupakan tahap yang paling ringan karena dalam tahap ini hanya bersifat masuk atau menyusup dan belum ada tindakan destruktif. Tahap ketiga dan keempat sudah mengandung unsur destruktif sehingga akibat yang ditimbulkan lebih buruk dibandingkan dengan tahap kedua. Tahap ketiga dan keempat inilah yang disebut dengan *cracking*, dimana perbuatannya dapat berupa merubah tampilan komputer atau website yang di *hack* dan mengakses dan/atau mengambil *file-file* rahasia dalam sistem computer (Ariyanto & Zeinudin, 2022).

Hal yang ditonjolkan dalam Pasal 37 UU ITE adalah perbuatan tersebut dilakukan di luar wilayah Indonesia tetapi sasaran atau korbannya berada di wilayah Indonesia. Sehingga hanya dapat dipertanggungjawabkan pidananya apabila pelaku tindak pidana (khususnya pada Tindak Pidana Pemerasan Melalui *Cracking)* adalah orang luar negeri atau berada di luar negeri tetapi sasaran atau korban dari tindak pidana tersebut adalah orang Indonesia atau berada di dalam wilayah *yurisdiksi* Indonesia (Singgi et al., 2020). Adapun mengenai yurisdiksi ini dijelaskan juga pada Pasal 2 UU ITE yaitu bahwa undang-undang ini memiliki jangkauan yurisdiksi yang luas yaitu tidak hanya kepada perbuatan hukum yang dilakukan di Indonesia dan/atau dilakukan oleh warga negara Indonesia, tetapi juga berlaku untuk perbuatan yang dilakukan di luar wilayah yurisdiksi Indonesia baik yang dilakukan oleh warga negara indonesia ataupun warga negara asing, badan hukum indonesia maupun badan hukum asing yang memiliki akibat hukum di wilayah yurisdiksi Indonesia.

Berkaitan dengan ketentuan pidananya, dalam UU ITE terdapat pemberatan penjatuhan sanksi pidana pokok jika perbuatan-perbuatan yang dilakukan memiliki sifat-sifat yang memberatkan yang berkaitan dengan Tindak Pidana Pemerasan Melalui *Cracking*. Pemberatan tersebut terdapat dalam Pasal 52 ayat (4) UU ITE menyebutkan Dalam hal tindak pidana sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 37 dilakukan oleh korporasi dipidana dengan pidana pokok ditambah dua pertiga. Berdasarkan pasal 52 ayat (4) UU ITE diketahui bahwa pemberatan sanksi pidana didasarkan pada pelaku tindak pidana yang merupakan suatu korporasi. Korporasi bisa dikatakan sebagai suatu lembaga atau badan ataupun organisasi yang memiliki struktur kepengurusan baik itu berupa suatu perusahaan ataupun badan hukum lainnya (Pease, 2001). Ketentuan tersebut di atas dimaksudkan untuk menghukum setiap perbuatan yang memenuhi unsur sebagaimana dalam pasal 27 sampai dengan pasal 37 yang dilakukan oleh koorporasi (*corporate crime*) dan/atau staf yang memiliki kapasitas untuk: 1. mewakili korporasi; 2. mengambil keputusan dalam korporasi; 3. melakukan pengawasan dan pengendalian dalam korporasi; dan 4. melakukan kegiatan demi keuntungan korporasi. Apabila pelaku Tindak Pidana Pemerasan Melalui *Cracking* adalah korporasi maka dapat dibebani pertanggungjawaban pidana berdasarkan Pasal 52 ayat (2) UU ITE dan diancam hukuman pidana ditambah dua pertiga dari pidana pokoknya.

1. **PENUTUP**
2. **Kesimpulan**

Suatu Tindak Pidana Pemerasan Melalui *Cracking* dapat dibebani pertanggungjawaban berdasarkan Undang-Undang No. 19 Tahun 2016 tentang Perubahan Atas Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yaitu Pasal 27 ayat (4) *jo* Pasal 45 ayat (1), Pasal 30 *jo* Pasal 46, Pasal 36 *jo* Pasal 51 ayat (2), dan Pasal 37 *jo* Pasal 52 ayat (2). Berdasarkan ketentuan pasal-pasal tersebut, ancaman hukuman yang dapat dijatuhkan kepada pelaku adalah maksimal 12 tahun pidana penjara dan minimal 6 tahun pidana penjara, serta denda maksimal Rp. 12.000.000.000.000 dan denda minimal Rp. 1.000.000.000.000. Dan berdasarkan ketentuan Pasal 2 UU ITE ditegaskan bahwa Undang-Undang ini berlaku untuk setiap Orang yang melakukan perbuatan hukum sebagaimana diatur dalam Undang-Undang ini, 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. Adapun Pelaku Tindak Pidana Pemerasan Melalui *Cracking* juga dapat dibebani pertanggungjawaban pidana berdasarkan ketentuan dalam KUHP yaitu Pasal 335 ayat (1), Pasal 368 ayat (1), Pasal 369, dan Pasal 406 KUHP. Pada Pasal 335 ayat (1) KUHP diancam dengan hukuman maksimal satu (1) tahun pidana penjara atau denda sebanyak-banyaknya Rp. 4.500 (empat ribu kima ratus rupiah), Pada Pasal 368 ayat (1) KUHP diancam dengan hukuman penjara maksimal delapan (8) tahun, dan maksimal empat (4) tahun pidana penjara berdasarkan ketentuan Pasal 369 KUHP

1. **Saran**

Setiap kejahatan pasti selalu terjadi karena adanya niat dan kesempatan, maka jangan pernah memberi kesempatan untuk terjadinya kejahatan tersebut. Dimulai dengan cara jangan sembarangan memasukkan informasi pribadi ataupun *file-file* rahasia di dalam media internet. Adapun untuk sistem komputer, mulailah dengan cara jangan men-*download* konten-konten pada halaman atau *website* yang tidak terpercaya, jangan memasang aplikasi ilegal pada sistem komputer, dan jangan membiarkan sembarang orang mengotak atik perangkat komputer yang kita miliki. Dan kita seharusnya lebih bijak dalam menggunakan perkembangan teknologi, jangan menggunakan teknologi sebagai alat untuk melakukan kejahatan. Agar ketentuan pasal-pasal dalam Undang-Undang No. 19 Tahun 2016 tentang Perubahan Atas Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang membahas mengenai Tindak Pidana Pemerasan Melalui *Cracking* di amandemen agar lebih jelas mengenai batasan-batasan yang dimaksud dengan kejahatan pemerasan dan kejahatan *cracking* tersebut.

1. **DAFTAR PUSTAKA**

Abdul, W., & Mohammad, L. (2005). Kejahatan Mayantara (Cyber Crime). *Refika Aditama, Hlm*.

Abidin, D. Z. (2015). Kejahatan dalam Teknologi Informasi dan Komunikasi. *Jurnal Ilmiah Media Processor*, *10*(2).

Adi Suhendi dan Taryono. (2018). *Serahkan Rp 500 Juta atau Saya Publikasikan Foto Hot Anda*. http://www.tribunnews.com/nasional/2012/02/21/serahkan-rp-500-juta-atau-saya-publikasikan-foto-hot-anda

Aditama, R. (2021). Penegakan Hukum Cyber Crime Terhadap Tindak Pidana Pencurian Uang Nasabah Dengan Cara Pembajakan Akun Internet Banking Lewat Media Sosial. *Wajah Hukum*, *5*(1). https://doi.org/10.33087/wjh.v5i1.360

Agung, A., Hafrida, H., & Erwin, E. (2023). Pencegahan Kejahatan Terhadap Cybercrime. *PAMPAS: Journal of Criminal Law*, *3*(2). https://doi.org/10.22437/pampas.v3i2.23367

Arifah, D. A. (2011). KASUS CYBERCRIME DI INDONESIA Indonesia’s Cybercrime Case. *Jurnal Bisnis Dan Ekonomi (JBE)*, *18*(2).

Arifin, R., & Muthia, F. R. (2019). Kajian Hukum Pidana Pada Kasus Kejahatan Mayantara ( Cybercrime ) Dalam Perkara. *RESAM Jurnal Hukum*, *5*(April).

Ariyanto, O., & Zeinudin, M. (2022). LOCUS DELICTIE TINDAK PIDANA HACKING DALAM PERSPEKTIF HUKUM POSITIF INDONESIA. *PROSIDING*.

Aryo, A., & Pakpahan, H. (2021). Tindak Pidana Turut serta Mengakses Komputer dan/atau Sistem Elektronik dengan Modus Skimming. *Bhirawa Law Journal*, *2*(2). https://doi.org/10.26905/blj.v2i2.6822

Atmasasmita, R. (1989). Asas-asas Perbandingan Hukum Pidana. In *Cet. I*.

Budoyo, S., Lathifah Nugraheni, N., & Martomo, M. (2021). ANALISIS SANKSI PIDANA DAN PELANGGARAN TERHADAP UNDANG-UNDANG TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK. *Jurnal Meta-Yuridis*, *4*(2). https://doi.org/10.26877/m-y.v4i2.9411

Bunga, D. (2019). Politik Hukum Pidana Terhadap Penanggulangan Cybercrime. *Jurnal LEGISLASI INDONESIA*, *16*(1).

Dermawan Akmal, A. A. (2019). URGENSI PERLINDUNGAN HUKUM BAGI KORBAN TINDAK PIDANA KEJAHATAN TEKNOLOGI INFORMASI. *JOURNAL OF SCIENCE AND SOCIAL RESEARCH*, *Vol 2*, *No 2 (2019): August 2019*.

Hakim, L. (2020). Asas Asas Hukum PIDANA. In *Deepublish*.

Hamdan Mustameer. (2022). Penegakan Hukum Nasional dan Hukum Internasional Terhadap Kejahatan Cyber Espionage Pada Era Society 5.0. *JURNAL YUSTIKA: MEDIA HUKUM DAN KEADILAN*, *25*(01). https://doi.org/10.24123/yustika.v25i01.5090

Hartanto. (2021). Perlindungan Hukum Pengguna Teknologi Informatika Sebagai Korban Dari Pelaku Cyber Crime Ditinjau Dari Undang-Undang Informasi Dan Transaksi Elektronik (UU ITE). *HERMENEUTIKA: Jurnal Ilmu Hukum*, *5*(2).

hukumonline.com. (2004). *Hacker KPU Dituntut Membayar Denda 10 Juta*.

IMAM SUJONO MH CPL, S. H. I. (2019). Rekonstruksi Hukum Cybercrime Dalam Konsep Cybersecurity National (Cybercrime Law Reconsruction in National Cybersecurity Concept). *Zenodo*.

Khalisah, A. M., & Kirana, P. (2022). Implementasi Norma Hukum Terhadap Tindak Pidana Peretasan (Hacking) di Indonesia. *Jurist-Diction*, *5*(6). https://doi.org/10.20473/jd.v5i6.40073

Liyakasa, K. (2012). Cracking the Code on Cyber Crimes. *CRM Magazine*, *16*(9).

Luthfi, H. (2021). PENERAPAN ASAS ULTIMUM REMIDIUM DALAM PENEGAKAN HUKUM TINDAK PIDANA UNDANG-UNDANG INFORMASI DAN TRANSAKSI ELEKTRONIK. *Yurispruden*, *4*(1). https://doi.org/10.33474/yur.v4i1.9164

Marwan Effendy. (2014). Teori Hukum; dari Perspektif Kebijakan, Perbandingan dan Harmonisasi Hukum Pidana. In *Referensi*.

Moelijatno. (2015). *Asas-asas Hukum Pidana*. PT Rineka Cipta.

Nyoman Triana Suskendariani, N., & Sabri Guntur. (2022). PERKEMBANGAN KEJAHATAN MAYANTARA. *Lakidende Law Review*, *1*(2). https://doi.org/10.47353/delarev.v1i2.15

Oktaviani, A. (2023). ALTERNATIF PIDANA BAGI PELAKU TINDAK PIDANA PERETASAN DI INDONESIA DALAM UNDANG-UNDANG INFORMASI DAN TRANSAKSI ELEKTRONIK. *NOVUM: JURNAL HUKUM*.

Pease, K. (2001). Cracking crime through design. In *Design Council*.

Raodia, R. (2019). Pengaruh Perkembangan Teknologi Terhadap Terjadinya Kejahatan Mayantara (Cybercrime). *Jurisprudentie : Jurusan Ilmu Hukum Fakultas Syariah Dan Hukum*, *6*(2). https://doi.org/10.24252/jurisprudentie.v6i2.11399

Remmelink, J. (2014). Pengantar Hukum Pidana Material. In *Buku Pengantar Hukum Pidana*.

Sa’diyah, N. K. (2012). MODUS OPERANDI TINDAK PIDANA CRACKER MENURUT UNDANG-UNDANG INFORMASI DAN TRANSAKSI ELEKTRONIK. *Perspektif*, *17*(2). https://doi.org/10.30742/perspektif.v17i2.97

Sari, E. O. (2017). Tinjauan Yuridis Tindak Pidana Cybercrime Dalam Perspektif Hukum Pidana. *Cakrawala Hukum*, *XIII No. 0*.

Singgi, I. G. A. S. K., Suryawan, I. G. B., & Sugiartha, I. N. G. (2020). Penegakan Hukum terhadap Tindak Pidana Peretasan sebagai Bentuk Kejahatan Mayantara (Cyber Crime). *Jurnal Konstruksi Hukum*, *1*(2). https://doi.org/10.22225/jkh.2.1.2553.334-339

Soerjono Soekanto & Sri Mamudji. (2001). *Penelitian Hukum Normatif (Suatu Tinjauan Singkat)*. Rajawali Pers.

Suparman, S., Asmara, G., & Zunnuraeni, Z. (2023). Tinjauan Kritis Pasal 27 & Pasal 28 UU ITE Terhadap Kebebasan Pers. *Jurnal Risalah Kenotariatan*, *4*(1). https://doi.org/10.29303/risalahkenotariatan.v4i1.82

Suteki dan Galang Taufani. (2018). Metodologi Penelitian Hukum. In *Metodologi Penelitian Hukum*.

Tajriyani, N. S. (2021). Pertanggungjawaban Pidana Tindak Pidana Pemerasan Dengan Modus Operandi Penyebaran Ransomware Cryptolocker. *Jurist-Diction*, *4*(2). https://doi.org/10.20473/jd.v4i2.25785

Talinusa, S. C. (2015). Tindak Pidana Pemerasan Dan/Atau Pengancaman Melalui Sarana Internet Menurut Undang-Undang Nomor 11 Tahun 2008. *Lex Crimen*, *4*(6).

Teguh Prasetyo. (2017). Hukum Pidana Edisi Revisi. *Pelajaran Hukum Pidana Bagian I*.

Tolib Effendi. (2013). Sistem peradilan pidana : perbandingan komponen dan proses sistem peradilan pidana di beberapa negara. In *hukum pidana*.

Utrecht, E. (2000). Hukum pidana I : rangkaian sari kuliah. In *Hukum pidana - studi dan pengajaran*.

1. R. Soesilo, *Op.Cit.* hlm. 279. [↑](#footnote-ref-0)