

**PERTANGGUNGJAWABAN PIDANA PELAKU *CRACKING*
PERSPEKTIF UNDANG UNDANG NOMOR 27 TAHUN 2022 TENTANG
PERLINDUNGAN DATA PRIBADI DAN UNDANG UNDANG NOMOR
19 TAHUN 2016 TENTANG INFORMASI DAN TRANSAKSI
ELEKTRONIK**



Oleh :

M. ALI PAMUNGKAS

502019260

PEMBIMBING SKRIPSI

1. Dr. Helwan Kasra, S.H., M.Hum

2. Dr. Hasanul Mulkan, S.H., M.H

PROGRAM STUDI HUKUM PROGRAM SARJANA

FAKULTAS HUKUM

UNIVERSITAS MUHAMMADIYAH PALEMBANG

2023

UNIVERSITAS MUHAMMADIYAH PALEMBANG

FAKULTAS HUKUM

PERSETUJUAN DAN PENGESAHAN

**JUDUL SKRIPSI : PERTANGGUNGJAWABAN PIDANA PELAKU
CRACKING PRESPEKTIF UNDANG-UNDANG
NOMOR 27 TAHUN 2022 DAN UNDANG -UNDANG
NOMOR 19 TAHUN 2016 TENTANG INFORMASI
DAN TRANSAKSI ELEKTRONIK**



NAMA : M. ALI PAMUNGKAS
NIM : 502019260
PROGRAM STUDI : Hukum Program Sarjana
PROGRAM KEKHUSUSAN : Hukum Pidana

Pembimbing :

1. DR. HELWAN KASRA, S.H., M.HUM (Helwan Kasra)

2. DR. HASANAL MULKAN, S.H., M.H (Hasanal Mulkan)

Palembang, 31 Januari 2023

PERSETUJUAN OLEH TIM PENGUJI :

Ketua : Dr. Mulyadi Tanzil, S.H., M.H (Mulyadi Tanzil)

Anggota : 1. Mona Wulandari, S.H., M.H (Mona Wulandari)

2. Dr. Hasanal Mulkan, S.H., M.H (Hasanal Mulkan)

**DISAHKAN OLEH
DEKAN FAKULTAS HUKUM
UNIVERSITAS MUHAMMADIYAH PALEMBANG**



Dr. Nur Husni Emilson, SH., Sp.N., MH
NBM/NIDN : 858994/0217086201

SURAT PERNYATAAN ORISINALITAS SKRIPSI

Yang bertanda tangan di bawah ini :

Nama : M. Ali Pamungkas
NIM : 502019260
Program Studi : Hukum Program Sarjana
Program Kekhususan : Hukum Pidana

Menyatakan bahwa karya ilmiah / skripsi saya yang berjudul :
PERTANGGUNGJAWABAN PIDANA PELAKU *CRACKING* PRESPEKTIF
UNDANG-UNDANG NOMOR 27 TAHUN 2022 DAN UNDANG -UNDANG
NOMOR 19 TAHUN 2016 TENTANG INFORMASI DAN TRANSAKSI
ELEKTRONIK

Adalah bukan merupakan karya tulis orang lain, baik sebagian maupun
keseluruhan, kecuali dalam bentuk kutipan yang telah kami sebutkan sumbernya.

Demikian surat pernyataan ini saya buat dengan sebenar-benarnya dan
apabila pernyataan ini tidak benar, kami bersedia mendapatkan sanksi akademis.

Palembang, 30 Agustus 2023

Yang menyatakan,



M. Ali Pamungkas

Motto :

“Karunia Allah yang paling lengkap adalah kehidupan yang didasarkan pada ilmu pengetahuan.”

(Ali bin Abi Thalib)

Ku Persembahkan untuk :

- *Kepada Ayahanda Mirza Hasra dan Ibunda Novianti tercinta yang tanpa lelah penuh kasih sayang memanjatkan doa yang luar biasa untuk anaknya terimakasih atas pengorbanan dan kerja keras dalam mendidik saya*
- *Kepada Kakak dan Adik Adikku terimakasih atas semangat dan pengertiannya*
- *Seluruh keluarga besarku yang tidak bisa kusebutkan satu persatu, terima kasih atas dukungannya.*
- *Teruntuk partner sekaligus kekasih saya, Rika Apriyani. S.E yang selalu mendukung dan membantu agar skripsi ini terselesaikan*
- *Teruntuk temanku Nugrata Redo dan Mutiara terimakasih sudah menemani dan berjuang*

*bersama sama selama 4 tahun dalam
perkuliahan ini*
➤ *Almamaterku tercinta*

ABSTRAK

PERTANGGUNGJAWABAN PIDANA PELAKU *CRACKING* PRESPEKTIF UNDANG-UNDANG NOMOR 27 TAHUN 2022 DAN UNDANG -UNDANG NOMOR 19 TAHUN 2016 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK

M. Ali Pamungkas

Adapun permasalahan dalam skripsi ini adalah Bagaimana pengaturan tindak pidana *cracking* dalam sistem hukum pidana di Indonesia? Bagaimana pertanggungjawaban pidana menurut Undang-Undang PDP dan Undang-Undang ITE? Jenis penelitian hukum ini adalah penelitian hukum normatif yang dimaksudkan objek kerjanya meliputi data-data sekunder yang ada di perpustakaan.

Ilmu pengetahuan dalam bidang teknologi telah berkembang dengan sangat pesat setiap informasi dalam bentuk tanda-tanda, isyarat, tulisan, gambar, suara dan bunyi melalui sistem kawat, optik, radio atau sistem elektronik lainnya. Berdasarkan penelitian dan hasil pembahasan, dapat disimpulkan bahwa : dapat dibebani pertanggungjawaban berdasarkan Pasal 27 ayat (4) jo Pasal 45 ayat (1), Pasal 30 jo Pasal 46, Pasal 46 jo Pasal 51 ayat (2), dan Pasal 37 jo pasal Pasal 52 ayat (2). Yang diatur dalam UU ITE. Pertanggungjawaban Undang-Undang Perlindungan Data Pribadi dan Informasi dan Transaksi Elektronik yaitu Sanksi pidana untuk pelaku penyebaran data pribadi sudah diatur di dalam Pasal 67 Ayat 1-3 Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, sebagaimana diatur dalam Pasal 28G UUD 1945, hal itu merupakan hak asasi manusia yang mana merupakan bagian dari perlindungan diri pribadi.

Kata Kunci : Pertanggungjawaban pidana, *cracking*, Perlindungan Data Pribadi

KATA PENGANTAR



Assalamu'alaikum Wr.Wb.

Segala puji dan syukur senantiasa dipanjatkan kehadirat Allah SWT, serta sholawat dan salam kepada nabi Muhammad Saw., karena atas rahmat dan nikmat Nya skripsi dengan judul :PERTANGGUNGJAWABAN PIDANA PELAKUCRACKING PRESPEKTIF UNDANG UNDANG NOMOR 27 TAHUN 2022 TENTANG PERLINDUNGAN DATA PRIBADI DAN UNDANG UNDANGNOMOR 19 TAHUN 2016 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK.

Dengan segala kerendahan hati diakui bahwa skripsi ini masih banyak mengandung kelemahan dan kekurangan. semua itu adalah disebabkan masih kurangnya pengetahuan dan pengalaman penulis, karenanya mohon dimaklumi.

Kesempatan yang baik ini penulis ucapkan terima kasih kepada semua pihak yang telah memberikan dorongan dan bantuan, khususnya terhadap:

1. Bapak Dr. AbidDjazuli, SE., MM., Rektor Universitas Muhammadiyah Palembang beserta jajarannya;
2. Bapak Dr. Nur Husni Emilson, SH, SpN, MH..., Dekan Fakultas Hukum Universitas Muhammadiyah Palembang beserta stafnya;
3. Bapak/Ibu Wakil Dekan I, II, III dan IV, Fakultas Hukum Universitas Muhammadiyah Palembang;
4. Bapak Yudistira Rusydi, SH., M.Hum. selaku Ketua Prodi Hukum Program Sarjana Fakultas Hukum Universitas Muhammadiyah Palembang.

5. Bapak Dr. Helwan Kasra, S.H., M.Hum. Selaku Pembimbing I, dalam penulisan skripsi ini;
6. Bapak Dr. Hasanul Mulkan, S.H., M.H. Pembimbing II, dalam penulisan skripsi ini;
7. Seluruh Bapak dan Ibu Dosen Fakultas Hukum Universitas Muhammadiyah Palembang;

Semoga segala bantuan materil dan moril yang telah menjadikan skripsi ini dapat selesai dengan baik sebagai salah satu persyaratan untuk menempuh ujian skripsi, semoga kiranya Allah Swt., melimpahkan pahala dan rahmat kepada mereka.

Wassalamu'alaikum wr.wb.

Palembang, Agustus 2023

Penulis,

M. Ali Pamungkas

DAFTAR ISI

	Halaman
HALAMAN JUDUL	i
LEMBAR PERSETUJUAN PEMBIMBING	Error! Bookmark not defined.
PENDAFTARAN UJIAN SKRIPSI	Error! Bookmark not defined.
SURAT PERNYATAAN ORISINALITAS SKRIPSI	ii
HALAMAN MOTTO DAN PERSEMBAHAN	iii
ABSTRAK	v
KATA PENGANTAR	vi
DAFTAR ISI	viii
BAB I :PENDAHULUAN	1
A. Latar Belakang	1
B. Rumusan Masalah.....	9
C. Ruang Lingkup dan Tujuan.....	9
D. Definisi Konseptual.....	10
E. Metode Penelitian	11
F. Sistematika Penulisan	13
BAB II : TINJAUAN PUSTAKA	14
A. Tinjauan Umum Tentang Tindak Pidana	15

1. Pengertian Tindak Pidana	15
2. Unsur-Unsur Tindak Pidana	16
3. Jenis-Jenis Tindak Pidana	17
B. Tinjauan Umum Tentang Tindak Pidana <i>Cracking</i>	19
1. Pengertian Tindak Pidana <i>Cracking</i>	19
C. Tinjauan Umum Tentang Pelaku	26
D. Tinjauan Umum Tentang Pertanggungjawaban Pidana.....	27
1. Perbuatan Melawan Hukum.....	29
2. Unsur Kesalahan Melawan Hukum.....	29
3. Kemampuan Bertanggung Jawab.	30
4. Tidak Ada Alasan Pemaaf.....	31
E. Tinjauan Umum Tentang Perlindungan Data Pribadi	31
BAB III : HASIL DAN PEMBAHASAN.....	34
A. Pengaturan Tindak Pidana <i>Cracking</i> Dalam Sistem Hukum Pidana Di Indonesia Pasal 30 Ayat (2)	34
B. Pertanggungjawaban Menurut Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi Dan Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik	41
1. Pertanggungjawaban Pidana Menurut Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi	41

2. Pertanggungjawaban Pidana Menurut Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik	47
BAB IV: PENUTUP	52
A. Kesimpulan	52
B. Saran	53
DAFTAR PUSTAKA	54
LAMPIRAN	

BAB I

PENDAHULUAN

A. Latar Belakang

Indonesia adalah negara hukum bermaksud bahwa walaupun rakyat memegang kekuasaan tertinggi terhadap negara, namun tetap dibatasi oleh adanya hukum. Indonesia adalah suatu negara yang memiliki dua sistem kedaulatan, yaitu sebagai negara kedaulatan rakyat dan negara kedaulatan hukum. Pasal 1 ayat (3) berbunyi "Negara Indonesia adalah negara hukum". Hal ini berarti bahwa Indonesia juga merupakan negara kedaulatan hukum dimana rakyat di Indonesia melaksanakan kewajibannya terhadap negara dengan menaati hukum yang berlaku. Hal ini dikarenakan tidak ada hukum yang akan melenceng dari Undang-Undang Dasar.

Internet pertama kali dibuat oleh *Advanced Research Projects Agency* (ARPA) pada tahun 1969. Pada saat itu, internet masih berupa sebuah jaringan komputer yang kemudian diberi nama ARPANET. Istilah inilah yang menjadi cikal bakal terbentuknya jaringan internet yang populer hingga saat ini.

Perkembangan internet saat ini telah membentuk karakter masyarakat dan kebudayaan yang baru, masyarakat yang tidak lagi terhalang oleh batas-batas teritorial jarak, ruang, dan waktu karena internet merupakan sarana untuk menyalurkan suatu informasi maupun sistem yang lainnya kepada khalayak luas. Perkembangan yang pesat dalam bidang teknologi internet menyebabkan

kejahatan baru di bidang itu juga muncul, Misalnya kejahatan manipulasi data, spionase, sabotase, provokasi, *money laundry*, *hacking*, pencurian *software* maupun perusakan *hardware*, pemerasan dan berbagai macam lainnya, Bahkan laju kejahatan melalui jaringan internet (*cybercrime*) tidak diikuti dengan kemampuan pemerintah untuk mengimbangnya sehingga sulit untuk mengimbangnya.¹

Cybercrime adalah tindak pidana yang dilakukan dengan memanfaatkan teknologi informasi. Istilah “Hukum Siber” diartikan sebagai padanan kata dari *Cyber Law*, yang saat ini secara internasional digunakan untuk istilah hukum yang terkait dengan pemanfaatan teknologi informasi. Istilah lain yang juga digunakan adalah hukum Teknologi Informasi (*Law Of 2 Information Technology*) Hukum Dunia Maya (*Virtual World Law*) dan Hukum Mayantara. Istilah-istilah tersebut lahir mengingat kegiatan internet dan pemanfaatan teknologi informasi berbasis virtual.²

Perkembangan teknologi informasi di Indonesia cukup signifikan dan tidak terlepas dibarengi oleh beberapa dampak yang kurang baik antara lain ancaman terhadap hak perlindungan data pribadi. Salah satu hal yang perlu diperhatikan ialah ketika menggunakan internet ialah seluruh aktivitas yang dilakukan otomatis akan terekam dan informasi tadi akan menjadi riwayat digital yang akan disimpan. Maka perlindungan data pribadi terhadap kesewenangan oleh pihak yang tidak

¹ Budi Suhariyanto, 2012, *Tindak Pidana Teknologi Informasi (Cybercrime)*, PT Raja Grafindo Persada, Jakarta, hlm. 3

² Adami Chazawi, 2015, Ardi Ferdian, *Tindak Pidana Informasi & Transaksi Elektronik*, Media Nusa Creative, Malang, hlm. 121

diketahui dan kemudian itu akan menjadi masalah yang serius dan sulit untuk diselesaikan.³

Tujuan dari dibuatnya aturan mengenai Perlindungan Data Pribadi tentunya untuk mengingatkan kesadaran akan pentingnya perlindungan data pribadi serta untuk melindungi hak warga negara atas data pribadi. Untuk mencegah individu menyalahgunakan data, penting untuk memastikan bahwa data yang telah mereka kumpulkan hanya dapat digunakan untuk tujuan yang dimaksudkan.

Kepastian peraturan data pribadi belum dimaknai secara mendalam seperti di beberapa peraturan, salah satunya Peraturan Nomor 11 Tahun 2008 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik. Sesungguhnya dalam perlindungan data pribadi tidak sepenuhnya diatur oleh hukum. Pengaturan yang lengkap ini sangat diperlukan sebagai landasan yang sah dalam memberikan keamanan, pedoman dan persetujuan atas penyalahgunaan informasi individu sebagaimana yang diarahkan dalam peraturan.

Di Indonesia kasus pelanggaran data pribadi sering terjadi pada aplikasi pinjaman online, kebocoran data pada e-commerce, hingga kasus transfer data pribadi yang dilakukan oleh pihak korporat tanpa izin. Kasus pelanggaran data pribadi di Indonesia yaitu:

1. Seperti yang pernah terjadi pada tahun 2021 dimana tersebar data penduduk yang tersimpan di Badan Penyelenggara Jaminan Sosial (BPJS), dimana ratusan juta data pribadi warga negara Indonesia tersebar pada forum di internet,

³kepaniteraan dan sekretariat jenderal mahkamah konstitusi, <https://www.mkri.id/index.php?page=download.Penelitian&id=123>, diakses pada tanggal 22 Agustus 2023 Pukul 17.00.

diperkirakan data pribadi tersebut berjumlah 279 juta, meliputi data warga yang masih hidup maupun yang sudah meninggal.⁴ Dan pada tahun sebelumnya juga terjadi penyebaran data pribadi yang tersimpan pada Komisi Pemilihan Umum (KPU) yaitu sebesar 2,3 juta data WNI tersebar.⁵

2. Kasus kebocoran data pribadi juga terjadi pada e-commerce, seperti pada tahun 2020 terjadi kebocoran data pribadi e-commerce bukalapak, dimana 13 juta data pribadi pengguna bukalapak yang bocor tersebut dijual belikan, padahal pada data tersebut berisi informasi penting seperti nama, alamat tempat tinggal, email, tanggal lahir, dan nomor handphone.⁶

RUU Perlindungan Data Pribadi merupakan inisiatif pemerintah mulai tahun 2016 dan kemudian menjadi prioritas untuk dibahas tahun 2019 untuk RUU Perlindungan Data Pribadi ditanda tangani, dan ditetapkan pada 20 September 2022.⁷ Terlepas dari kenyataan bahwa RUU Perlindungan Data Pribadi itu sendiri menganut panji-panji internasional serta menggunakan prinsip umum perlindungan data pribadi, makna data pribadi, subyek serta bagaimana ruang lingkup informasi yang mengikat entitas publik dan swasta, dan perlindungan data khusus semuanya diklarifikasi dalam formulasi.

⁴ Andita Rahma dan Syailendra Persada, *Data Penduduk di BPJS Kesehatan Bocor, Bukti Lemahnya Perlindungan Data Pribadi*, www.tempo.com, diakses pada tanggal 22 Agustus 2023 Pukul 18.00.

⁵ Fira Nursyabani, *2,3 Juta Data WNI Bocor di Pasar Gelap, Diduga Milik KPU*, www.ayobandung.com, diakses pada tanggal 22 Agustus Pukul 18.20.

⁶ CNN Indonesia, *13 Juta Data Bocor Bukalapak Dijual di Forum Hacker*, www.bukalapak.com, diakses pada tanggal 22 Agustus Pukul 19.00.

⁷ <https://tekno.kompas.com/read/2022/09/20/11210337/ruu-pdp-resmi-disahkan-jadi-undang-undang-perlindungan-data-pribadi>, diakses pada tanggal 22 Agustus pukul 19.10.

Perlindungan terhadap data diri seseorang telah dijamin dalam amandemen konstitusi Undang-Undang Dasar 1945, yaitu terkait hak asasi manusia, dimana hak asasi manusia di atur pada pasal 28G ayat 1 UUD 1945, yang berisi:

“Setiap orang berhak atas perlindungan atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi”

Selain berdasarkan UUD 1945, Indonesia juga harus melindungi privasi dan data pribadi warga negara Indonesia karena terlibat dengan *International Covenant on Civil and Political Rights (ICCPR)* yang sudah disahkan dengan disahkannya Undang-Undang Nomor 12 tahun 2005. Aturan ini sesuai dengan Undang-Undang Nomor 39 tahun 1999 tentang Hak Asasi Manusia, yaitu pada pasal 29 ayat (1) menyatakan bahwa:

“Pengakuan akan hak setiap orang atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan hak miliknya. Perlindungan tersebut tidak hanya dalam konteks hubungan langsung, melainkan atas informasi atau data pribadi”.

Sehingga dibentuk lah suatu aturan khusus untuk mengatur terkait pengaturan perlindungan data pribadi, maka lahir lah Undang-Undang nomor 27 tahun 2022 tentang perlindungan data pribadi (UU PDP) untuk memberikan perlindungan kepada masyarakat dan meningkatkan efektivitas dalam perlindungan data pribadi.

Pasal yang dilanggaryaitu pasal yang mengatur tentang Perlindungan Data Pribadi dan pasal UU ITE , yang berbunyi sebagai berikut:

1. Pasal 65 UU PDP

- (1) Setiap orang dilarang secara melawan hukum memperoleh atau mengumpulkan data pribadi yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian subjek data pribadi.
- (2) Setiap orang dilarang secara melawan hukum mengungkapkan data pribadi yang bukan miliknya.
- (3) Setiap orang dilarang secara melawan hukum menggunakan data pribadi yang bukan miliknya.

2. Pasal 30 UU ITE yang menyatakan:

- (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."

Maka pelaku harus bertanggung jawab sesuai dengan tindak pidana yang telah dilakukannya, yang ketentuan pidananya tercantum dalam pasal berikut:

1. Pasal 67 UU PDP:

- “(1) Setiap Orang yang dengan sengaja dan melawan hukum memperoleh atau mengumpulkan Data Pribadi yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian Subjek Data Pribadi sebagaimana dimaksud dalam Pasal 65 ayat (1) dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau pidana denda paling banyak Rp5.000.000.000,00 (lima miliar rupiah).
- (2) Setiap Orang yang dengan sengaja dan melawan hukum mengungkapkan Data Pribadi yang bukan miliknya sebagaimana dimaksud dalam Pasal 65 ayat (2) dipidana dengan pidana penjara paling lama 4 (empat) tahun dan/atau pidana denda paling banyak Rp4.000.000.000,00 (empat miliar rupiah).
- (3) Setiap Orang yang dengan sengaja dan melawan hukum menggunakan Data Pribadi yang bukan miliknya sebagaimana dimaksud dalam Pasal 65 ayat (3) dipidana dengan pidana penjara paling lama 5 (lima) tahun

dan/atau pidana denda paling banyak Rp5.000.000.000,00 (lima miliar rupiah).”

2. Pasal 46 UU ITE:

“(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).”

Dapat dipidananya seseorang tidak terlepas dari suatu tindakan melanggar hukum, baik dilakukannya dengan sengaja maupun tidak dengan sengaja. Tindakan melanggar hukum itu menunjukkan kepada sifat perbuatannya, yaitu sifat perbuatan yang dilarang dengan ancaman pidana apabila melanggar suatu aturan yang berlaku.⁸

Pertanggungjawaban dalam hukum pidana bukan hanya berarti menjatuhkan pidana terhadap seseorang, tetapi yang perlu diyakini apakah sudah tepat meminta pertanggungjawaban atas tindak pidana yang dilakukannya. Pertanggungjawaban pidana ini merupakan suatu keadaan yang terdapat pada diri si pembuat saat melakukan tindak pidana, dan pertanggungjawaban pidana ini juga menghubungkan antara si pembuat dengan perbuatan yang telah dilakukannya. Karena ketentuan pertanggungjawaban pidana adalah kesalahan, maka suatu pertanggungjawaban pidana dapat dibebankan apabila seseorang telah

⁸ Soerjono Soekanto, 2002, *Faktor-faktor yang Mempengaruhi Penegakan Hukum*, Raja Grafindo, Jakarta, hlm. 15

melakukan kesalahan dan kesalahan tersebut juga telah memenuhi unsur-unsur suatu tindak pidana yang diatur dalam peraturan perundang-undangan.

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.⁹

Sedangkan dalam aliran dualistis, terdapat perbedaan antara kesalahan dengan unsur-unsur dari suatu tindak pidana. 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.¹⁰

⁹ Rasyid Ariman, 2006, *Kapita Selekta Perbandingan Hukum Pidana*, Universitas Sriwijaya, Palembang, hlm 1.

¹⁰*Ibid.*

Walaupun perkembangan teknologi dan digital sangat pesat namun penelitian terkait Data Pribadi dalam kajian hukum masih belum banyak. Dari latar belakang yang dijabarkan peneliti bermaksud menjalankan penelitian dengan pokok pikiran Berdasarkan uraian dari data di atas, maka penulis tertarik untuk menulis penelitian dalam skripsi yang berjudul: **“PERTANGGUNGJAWABAN PIDANA PELAKU *CRACKING* PRESPEKTIF UNDANG UNDANG NOMOR 27 TAHUN 2022 TENTANG PERLINDUNGAN DATA PRIBADI DAN UNDANG UNDANG NOMOR 19 TAHUN 2016 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK”**

B. Rumusan Masalah

Berdasarkan latar belakang yang ada, maka dapat di identifikasikan pokok permasalahan dalam rumusan sebagai berikut:

1. Bagaimana pengaturan tindak pidana *cracking* dalam sistem hukum pidana di Indonesia?
2. Bagaimana pertanggungjawaban pidana pelaku *cracking* menurut Undang-Undang Perlindungan Data Pribadi dan Undang-Undang Informasi dan Transaksi Elektronik?

C. Ruang Lingkup dan Tujuan

Dalam penelitian ini penulis melakukan pembahasan terhadap masalah dengan menitik beratkan pertanggungjawaban pidana pelaku *cracking* prespektif Undang Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi dan

Undang Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik.

Adapun tujuan penelitian ini adalah:

1. Untuk mengetahui pengaturan tindak pidana *cracking* dalam sistem hukum pidana di Indonesia.
2. Untuk mengetahui pertanggungjawaban menurut Undang Undang Perlindungan Data Pribadi dan Undang Undang Informasi dan Transaksi Elektronik.

Penelitian ini diharapkan menjadi khasanah perkembangan ilmu Hukum sebagai studi difakultas hukum di Universitas Muhammadiyah Palembang. Selain itu, diharapkan juga hasil penelitian ini dapat memberikan penelitian yang bermanfaat bagi almamater, akademisi, biokrasi pemerintahan, serta bagi masyarakat pada umumnya.

D. Definisi Konseptual

1. Pengertian tindak pidana yaitu tindak pidana merupakan gangguan terhadap keseimbangan, keselarasan dan keserasian dalam kehidupan masyarakat yang mengakibatkan gangguan individual ataupun masyarakat.¹¹
2. Pengertian *cracking* yaitu merupakan keseluruhan bentuk kejahatan yang ditunjukkan terhadap komputer, jaringan komputer dan para penggunanya,

¹¹ Muladi, 2002, *Lembaga Pidana Bersyarat*, Alumni, Bandung, hlm. 61

dan bentuk-bentuk kejahatan tradisional yang menggunakan atau dengan bantuan peralatan komputer.¹²

3. Pengertian Data Pribadi adalah data perseorangan tertentu yang disimpan, dirawat, dan dijaga kebenaran serta dilindungi kerahasiaannya.¹³
4. Pertanggungjawaban pidana adalah diteruskannya celaan yang secara objektif ada pada tindak pidana, secara subjektif terhadap pembuatnya.¹⁴
5. Pelaku adalah orang yang melakukan tindak pidana yang bersangkutan, dalam arti orang yang dengan suatu kesengajaan atau suatu tidak sengaja seperti yang diisyaratkan oleh Undang-Undang telah menimbulkan suatu akibat yang tidak dikehendaki oleh Undang-Undang, baik itu merupakan unsur-unsur subjektif maupun unsur-unsur obyektif, tanpa memandang apakah keputusan untuk melakukan tindak pidana tersebut timbul dari dirinya sendiri atau tidak karena gerakkan oleh pihak ketiga.¹⁵

E. Metode Penelitian

Metode penelitian yang digunakan oleh penulis adalah penelitian hukum normatif, yang berarti penelitian ini menggunakan bahan-bahan kepustakaan.

1. Jenis Penelitian

Penelitian Hukum Normatif terdapat beberapa pendekatan yang digunakan. Pendekatan perundang-undangan (*normative approach*) dengan cara meneliti

¹² Widodo, 2011, *Aspek Hukum Kejahatan Mayantara*, Yogyakarta: Aswindo, hlm. 7.

¹³ Pengertian Data Pribadi, https://www.hukumonline.com/klinik/detail/ulasan/lt5c498fb94dc87/perlindungan-data-pribadi-dalam-penyelenggaraan-fintech/#_ftn5, diakses pada tanggal 22 Agustus 2023 Pukul 19.50.

¹⁴ Roeslan Saleh, 1983, *Perbuatan Pidana dan Pertanggungjawaban Pidana; Dua Pengertian Dasar dalam Hukum Pidana*, Jakarta: Aksara Baru, hlm. 89

¹⁵ Sudarto, 1996, *Hukum dan Hukum Pidana*, Bandung, Alumni, hlm 115

ketentuan-ketentuan yang terkandung dalam Undang-undang. Dengan pendekatan ini akan diketahui aspek-aspek apa saja yang termasuk dalam tindak pidana pemerasan.

2. Sumber Data

Data Sekunder data yang diperoleh dengan melakukan penelitian kepustakaan (*library research*), yaitu data yang diperoleh dari bahan hukum, yaitu:

a. Bahan hukum primer yaitu bahan hukum yang mempunyai kekuatan mengikat peraturan perundang-undangan dan peraturan pemerintah yang berkaitan dengan pokok masalah di skripsi ini, terdiri dari:

1. Pancasila dan Undang-Undang Dasar 1945.
2. Kitab Undang-Undang Hukum Pidana
3. Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi
4. Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik

b. Bahan Hukum Sekunder, yaitu bahan hukum yang menjelaskan mengenai bahan hukum primer yang terdiri dari:

1. Hasil penelitian;
2. Jurnal ilmiah;
3. Pendapat para pakar yang relevan dengan pembahasan permasalahan dalam penelitian ini; dan
4. Internet.

c. Bahan Hukum Tersier, yaitu bahan hukum penunjang yang memberikan petunjuk serta penjelasan bahan hukum primer dan bahan hukum sekunder, yang terdiri dari:

1. Kamus Hukum;
2. Ensiklopedia,
3. Majalah, dan
4. Surat Kabar, dan sebagainya.

3. Pengelolaan Data

Setelah data-data dikumpulkan, selanjutnya penulis mengelola data tersebut dengan cara

- a. Induktif, yakni suatu metode analisis data yang dimulai dari penarikan kesimpulan dari fakta-fakta khusus, yang kemudian ditarik kesimpulan secara umum.
- b. Komperatif, yakni membandingkan antara data yang berlainan untuk mendapatkan suatu pendapat yang logis dan untuk dijadikan rujukan dan menjadi suatu pedoman.

4. Analisis Data Penelitian

Dalam penulisan skripsi ini, penulis menggunakan analisis kualitatif yaitu data yang diperoleh dari penelitian kepustakaan akan dianalisis dengan pembahasan dan penjabaran hasil-hasil penelitian dengan mendasarkan pada norma-norma dan doktrin-doktrin yang berkaitan dengan materi yang diteliti.

F. Sistematika Penulisan

Rencana penulisan skripsi ini akan disusun secara keseluruhan yang terdiri dari empat bab yaitu:

BAB I : Pendahuluan

Pada bab ini terdiri dari latar belakang, permasalahan, ruang lingkup dan tujuan, kerangka konseptual, metode penelitian, serta sistematika penulisan.

BAB II : Tinjauan Pustaka

Pada bab ini disajikan tentang kerangka teori yang erat kaitannya dengan permasalahan yang akan dibahas dengan bahan hukum primier dan sekunder

BAB III : Pembahasan

Pengaturan Tindak Pidana *cracking* dalam sistem Hukum Pidana di Indonesia 30 ayat (2).

Pertanggungjawaban pidana pelaku *cracking* prespektif Undang Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi dan Undang Undang Nomor 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik.

BAB IV : Penutup

Bab ini penulis menarik kesimpulan dari uraian-uraian yang dijabarkan pada skripsi ini serta memberikan saran.

BAB II

TINJAUAN PUSTAKA

A. Tinjauan Umum Tentang Tindak Pidana

1. Pengertian Tindak Pidana

Pengertian tindak pidana dalam Kitab Undang-undang Hukum Pidana (KUHP) dikenal dengan istilah *strafbaar feit* dan dalam kepustakaan tentang hukum pidana sering mempergunakan istilah delik, sedangkan pembuat undang-undang merumuskan suatu undang-undang mempergunakan istilah peristiwa pidana atau perbuatan pidana atau tindak pidana.¹⁶

Tindak Pidana merupakan suatu perbuatan, baik itu secara aktif maupun pasif yang mengakibatkan unsur kesalahan sebagai perbuatan yang dilarang serta dapat diancamkan pidana. Dijatuhkan sanksi pidana tersebut agar tegaknya hukum dan merasakan hidup yang aman dan tertib.¹⁷

Para sarjana Indonesia mengistilahkan *strafbaarfeit* itu dalam arti yang berbeda diantaranya Moeljato menggunakan istilah perbuatan pidana, “yaitu suatu perbuatan yang dilarang oleh suatu aturan hukum, larangan nama disertai ancaman sanksi yang berupa pidana tertentu, bagi barang siapa larangan tersebut”.¹⁸ Sementara perumusan *strafbaarfeit* menurut Van Hamel dalam buku saku Satochid Kartanegara adalah orang yang dirumuskan undang-undang bersifat melawan hukum yang patut dipidana dan dilakukan dengan kesalahan.¹⁹

¹⁶ Amir Ilyas, 2012, *Asas-Asas Hukum Pidana : Memahami Tindak Pidana dan Pertanggungjawaban Pidana sebagai Syarat Pidanaaan*, Yogyakarta, hlm. 20

¹⁷ P.A.F. Lamintang, 1996, *Dasar-dasar hukum pidana Indonesia*, PT Citra Aditya Bakti, Bandung, hlm. 7

¹⁸ S.S.T Kansil dan Christine S.T. Kansil, 2004, *Pokok-Pokok Hukum Pidana*, Pradnya Paramita, hlm. 54

¹⁹ Satochid Kartanegara, 1995, *Hukum Pidana Bagian Pertama*, Balai Lektur Mahasiswa, Jakarta, hlm. 4

Dengan memperhatikan definisi diatas, maka ada beberapa syarat untuk menentukan perbuatan itu sebagai tindak pidana, syarat tersebut adalah sebagai berikut:

1. harus ada perbuatan manusia
2. perbuatan manusia itu bertentangan dengan hukum
3. perbuatan itu dilarang berdasarkan ketentuan peraturan perundang-undang dan diancam dengan pidana
4. perbuatan itu dilakukan oleh orang yang dapat dipertanggungjawabkan
5. perbuatan itu harus dapat dipertanggungjawabkan kepada si pembuat.²⁰

2. Unsur-Unsur Tindak Pidana

Unsur-unsur Tindak Pidana antara lain:

a. Unsur Objektif

Unsur objektif yaitu unsur yang berasal dari luar si pelaku, unsur-unsur yang ada hubungannya dengan keadaan di mana tindakan-tindakan si pelaku itu harus dilakukan. Unsur objektif terdiri dari:

- 1) Sifat melanggar hukum
- 2) Kualitas dari pelaku
- 3) Kualitas yaitu hubungan antara suatu tindakan sebagai penyebab dengan suatu kenyataan sebagai akibat.

b. Unsur Subjektif

Unsur subjektif adalah unsur yang terdapat atau melekat pada diri si pelaku, atau yang dihubungkan dengan diri si pelaku dan termasuk

²⁰M. Rasyid Ariman dan M. Fahmi Raghieb, 2013, *Hukum Pidana Fundamental*, Unsri Press, Palembang, hlm. 85

didalamnya segala sesuatu yang terkandung di dalam hatinya. Unsur ini terdiri atas:

- 1) Kesengajaan atau ketidaksengajaan (*dolus* atau *culpa*)
- 2) Maksud pada suatu percobaan, seperti ditentukan dalam Pasal 53 ayat (1) KUHP
- 3) Macam-macam maksud seperti terdapat dalam kejahatan , pencurian, penipuan, pemerasan dan sebagainya
- 4) Merencanakan terlebih dahulu, seperti yang tercantum di dalam Pasal 340 KUHP yaitu pembunuhan yang direncanakan terlebih dahulu
- 5) Perasaan takut, seperti yang terdapat di dalam Pasal 308 KUHP.²¹

3. Jenis-Jenis Tindak Pidana

Tindak pidana dibedakan dalam beberapa jenis, antara lain:

1. Tindak pidana kejahatan dan pelanggaran

Dalam *Weetboek Van Strafecht* (WVS) Belanda, telah terdapat pembagian tindak pidana antara kejahatan dan pelanggaran, yang berdasarkan asas *concordantie* masuk ke dalam WVS Hindia Belanda yang sekarang disebut KUHP. Dalam sistem KUHP, kejahatan (*misdriften*) dimuat dalam Buku II dan pelanggaran (*overtredingen*) dimuat dalam Buku III.

2. Tindak Pidana Formil dan Tindak Pidana Materil

Tindak pidana formil adalah tindak pidana yang penekanannya pada dilarangnya suatu perbuatan, contohnya Pasal 160,209, 210,242, 263,

²¹Teguh Prasetyo, 2010, *Hukum Pidana*, Rajawali Pers, Jakarta, hlm. 48

362KUHP. Sedangkan tindak pidana materil adalah tindak pidana yang tekanannya pada dilarangnya akibat; dalam hal ini bila akibat tidak terjadi maka perbuatan tersebut hanya berupa percobaan tindak pidana saja, contohnya Pasal 187, 378, 338 KUHP.

3. Tindak Pidana *Commissionis*, Tindak Pidana *Omissionis*, dan Tindak Pidana *Commissionis Per Omissionem Commissa*.

Tindak Pidana *Commissionis* adalah tindak pidana yang berupa pelanggaran terhadap larangan. Tindak pidana ini dilakukan dengan tindakan aktif, baik tindak pidana tersebut dirumuskan secara materil maupun formil, contohnya Pasal 362 KUHP. Sedangkan tindak pidana *Omissionis* adalah tindak pidana yang berupa pelanggaran terhadap perintah. Tindak pidana ini merupakan perbuatan yang dilarang justru karena tidak melakukan sesuatu (mengabaikan, membiarkan), contoh: Pasal 522 KUHP tentang tidak hadir sebagai saksi, Pasal 531 KUHP tentang tidak menolong orang yang perlu pertolongan. Tindak pidana *Commissionis Per Omissionem Comissa* adalah tindak pidana yang berupa pelanggaran terhadap larangan tetapi dilakukan dengan pasif (tidak berbuat), contohnya: seorang ibu yang membunuh anaknya dengan tidak memberikan air susu (Pasak 338, 340 KUHP).

4. Tindak Pidana Dolus dan Tindak Pidana Culpa

Tindak pidana dolus adalah tindak pidana yang mengandung unsur kesengajaan, contohnya: Pasal 17, 197, 245, 263, 310, 338 KUHP.

Sedangkan tindak pidana culpa adalah tindak pidana yang mengandung unsur kealpaan, contohnya: Pasal 195, 197, 201, 203, 231 ayat (4), 359, 360 KUHP.

5. Tindak Pidana Tunggal dan Tindak Pidana Berganda

Tindak pidana tunggal yaitu tindak pidana seputar perbuatan yang dilakukan satu kali saja. Sedangkan tindak pidana berganda adalah perbuatan yang baru menjadi tindak pidana bila dilakukan berulang kali. Misalnya, Pasal 481 KUHP tentang Penadahan.

6. Tindak Pidana Aduan dan Tindak Pidana Biasa

Tindak pidana aduan merupakan tindak pidana yang penuntutannya didasari oleh adanya pengaduan dari pihak korban. Inisiatif untuk dituntutnya tindak pidana tidak diletakkan pada penuntut umum, tetapi tergantung dari adanya pengaduan korban (pihak yang dirugikan). Apabila tidak ada pengaduan dari pihak yang dirugikan, jaksa tidak memiliki kewenangan melakukan penuntutan. Pertimbangan yang mendasari diaturnya delik aduan dalam KUHP terhadap beberapa hal adalah lebih besar kepentingan pihak yang dirugikan agar perkaranya tidak dituntut daripada kepentingan negara untuk menuntut perkara tersebut.

B. Tinjauan Umum Tentang Tindak Pidana *Cracking*

1. Pengertian Tindak Pidana *Cracking*

Perlindungan masyarakat dengan harta bendanya merupakan kewajiban pemerintah dari kejahatan dapat dilakukan melalui dua pendekatan, yaitu pendekatan penal (pendekatan hukum pidana) dan pendekatan non penal

(pendekatan di luar hukum pidana). Di dalam ketentuan Pasal 4 ayat (2) UU ITE disebutkan bahwa Pemerintah melindungi kepentingan umum dari segala jenis gangguan sebagai akibat penyalahgunaan Informasi Elektronik dan Transaksi Elektronik yang mengganggu ketertiban umum, sesuai dengan ketentuan Peraturan Perundang-undangan.

Pemerintah melalui UU ITE Dalam memberikan perlindungan hukum dari kejahatan *cracking* kepada warga negara yaitu dengan melakukan pencegahan atau penanganan kejahatan dalam dunia maya (*cybercrime*) khususnya kejahatan Cracking yang kemudian diatur didalam UU No. 19 tahun 2016 tentang perubahan atas UU No 11 tahun 2008 tentang Informasi dan transaksi elektronik Pasal 30 ayat (1), ayat (2) dan ayat (3) UU ITE sedangkan Pemberian Saksi tersebut diatur pada Pasal 46 ayat (1), ayat (2) dan ayat (3). Namun secara Pendefinisian terhadap kejahatan cracking tidaklah disampaikan secara jelas dalam Undang-Undang 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik yang kemudian diubah dengan Undang-Undang No 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik. Pada Undang-Undang tersebut hanya berisi larangan dan Sanksi. Walaupun seperti itu dibentuknya Undang-Undang Nomor 19 tahun 2016 tentang Perubahan atas Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) oleh pemerintah diharapkan dapat mampu mengakomodir kasus kejahatan Cracking tersebut. Kejahatan Cracking secara

eksplisit diatur dalam Pasal 30 ayat (1), ayat (2) dan ayat (3) UU ITE, Pasal tersebut menyatakan :²²

1. Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik milik orang lain dengan cara apapun.
2. setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan atau sistem elektronik dengan cara apapun 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 apapun dengan melanggar, menerobos, melampau, atau menjebol sistem pengamanan.

Cracking adalah sebuah kegiatan meretas suatu sistem elektronik milik orang lain secara melawan hukum dengan tujuan untuk menikmati hasil dari apa yang telah pelaku lakukan yaitu meretas sistem elektronik orang lain dengan cara illegal. Dapat diketahui bahwa *Cracking* merupakan tindak pidana yang memiliki sanksi dan hukum yang jelas. perbuatan ini tentunya dapat dikaitkan dengan delik pencurian, karena pelaku *Cracking* tidak hanya memiliki niat untuk memasuki sistem elektronik milik orang lain tapi juga ingin mengambil apa yang ada didalam sistem elektronik tersebut. Pasal 30 UU ITE adalah Pasal yang membahas mengenai *illegal access* yang merupakan awal terjadinya suatu tindak pidana pencurian, Sedangkan *Cracking* yang dikategorikan sebagai pencurian diatur dalam Pasal 32 ayat (2) UU ITE menyatakan :

“setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan atau sistem elektronik dengan cara apapun dengan tujuan untuk memperoleh informasi elektronik dan/atau dokumen elektronik”

²²Republik Indonesia, “Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik”, No. 1

Pengertian *hacking* menurut para ahli bernama Sutan Remy Syahdeini, Hacking adalah perbuatan membobol sistem komputer. Dia menggunakan istilah "membobol" sistem komputer karena perbuatan tersebut adalah menasuki sistem komputer orang lain tanpa izin atau otorisasi dari pemiliknya. Orang yang melakukan hacking disebut sebagai *Hacker*.²³

Dan adapun pengertian dari istilah "*Hacker*" antara lain sebagai berikut: Secara Harfiah Istilah Hacker berarti mencincang atau membacok. Dalam arti luas adalah mereka yang menyusup atau melakukan perusakan melalui komputer. Hacker dapat juga didefinisikan sebagai orang-orang yang mempelajari seluk beluk sistem komputer dan bereksperimen dengannya.²⁴

Sedangkan menurut seorang Edmon Makarim, *Hacker* secara umum adalah orang yang mengakses suatu sistem komputer dengan suatu cara yang tidak sah atau salah. Perbuatan ini biasanya dilakukan dengan diawali rasa keingintahuan kekaguman dan terakhir adalah adanya suatu tantangan yang ditujukan terhadap suatu sistem komputer.²⁵

Hacker dan *Cracker* adalah sikembar yang mempunyai karakter dan kepribadian yang berbeda. Si *Hacker* biasanya mempunyai sifat yang positif kalau si *Cracker* memiliki sifat sebaliknya dari si *Hacker*. Namun keduanya selalu ada di jagad maya yang dinamakan Internet ini.²⁶

²³ Sutan Remy Syahdeini, *Op.Cit.*, hlm.118.

²⁴ Agus Raharjo, *Op.Cit.*, hlm.132.

²⁵ Abdul Wahid dan Muhammad Labib, *Op.Cit.*, hlm.89.

²⁶ Fadjar Efendy Rasyid, *Hacker Dan Cracker*,

http://www.ubaya.ac.id/2014/content/articles_detail/148/Hacker-dan-Cracker.html, diakses pada 22 Agustus 2023 Pukul 22.00.

Hacker mempunyai keinginan untuk mengetahui secara mendalam mengenai kerja suatu sistem, komputer atau jaringan komputer, sehingga menjadi orang yang ahli dalam bidang penguasaan sistem, komputer atau jaringan komputer. Istilah *hacker* sering disalah artikan menjadi hal-hal yang merusak atau hack, seperti *hack facebook*, *hack email*, *hack* jaringan dan lain-lainnya. tetapi sebetulnya *hacking* adalah ilmu seni, yaitu seni keamanan jaringan komputer.²⁷

Sifat-sifat *Hacker* terdiri atas:²⁸

- a. Mempunyai kemampuan menganalisis kelemahan suatu sistem atau situs. Sebagai contoh: jika seorang *hacker* mencoba menguji suatu situs dipastikan situs tersebut akan berantakan dan mengganggu yang lain. Biasanya *hacker* melaporkan kejadian ini untuk diperbaiki menjadi sempurna. Bahkan seorang *hacker* akan memberikan masukan dan saran yang bisa memperbaiki kebobolan *system* yang ia masuki.
- b. *Hacker* mempunyai etika serta kreatif dalam merancang suatu program yang berguna bagi siapa saja.
- c. Seorang *hacker* tidak pelit berbagi ilmunya kepada orang-orang yang serius atas nama ilmu pengetahuan dan kebaikan
- d. Seorang *hacker* akan selalu memperdalam ilmunya dan memperbanyak pemahaman tentang sistem operasi.

Menurut Fajar Efendy Rasjid, seorang *hacker* juga memiliki etika dalam

²⁷ Fajar Efendy Rasyid, *Hacker Dan Cracker*, http://www.ubaya.ac.id/2014/content/articles_detail/148/Hacker-dan-Cracker.html, diakses pada 22 Agustus 2023 Pukul 22.00.

²⁸ Fajar Efendy Rasyid, *Hacker Dan Cracker*, http://www.ubaya.ac.id/2014/content/articles_detail/148/Hacker-dan-Cracker.html, diakses pada 22 Agustus 2023 Pukul 22.00.

beraktivitas di dunia maya, etika *Hacker* tersebut antara lain:

- (1) di atas segalanya, menghormati pengetahuan dan kebebasan informasi;
- (2) memberitahukan sistem administrator akan adanya pelanggaran keamanan atau lubang di keamanan yang dilihat;
- (3) tidak mengambil keuntungan yang tidak *fair* dari *hack*;
- (4) tidak mendistribusikan dan mengumpulkan *software* bajakan;
- (5) tidak pernah mengambil risiko yang bodoh;
- (6) selalu mengetahui kemampuan sendiri;
- (7) selalu bersedia untuk secara terbuka, bebas dan gratis memberitahukan serta mengajarkan berbagai informasi dan metode yang diperoleh;
- (8) tidak pernah meng-*hack* sebuah sistem untuk mencuri uang;
- (9) tidak pernah memberikan akses ke seseorang yang akan membuat kerusakan;
- (10) tidak pernah secara sengaja menghapus dan merusak file di komputer yang di-*hack*;
- (11) menghormati mesin yang di-*hack*, dan memperlakukan mesin yang di-*hack* seperti mesin sendiri.²⁹

Sedangkan saudara kembar si *Hacker* adalah si *Cracker*. *Cracker* adalah sebutan untuk mereka yang masuk ke sistem orang lain dan *cracker* lebih bersifat destruktif, biasanya di jaringan komputer, mem-*bypass password* atau lisensi program komputer, secara sengaja melawan keamanan komputer, men-

²⁹ Fadjar Efendy Rasyid, *Hacker Dan Cracker*,
http://www.ubaya.ac.id/2014/content/articles_detail/148/Hacker-dan-Cracker.html, diakses pada 14 juni 2023 Pukul 23.11

deface (merubah halaman muka web) milik orang lain bahkan hingga men- *delete* data orang lain, dan mencuri data dari sistem.³⁰

Seorang *Cracker* memiliki sifat yang sangat berbeda dengan *Hacker*. Sifat- sifat Cracker tersebut antara lain:³¹

1. Mampu membuat suatu program bagi kepentingan dirinya sendiri dan bersifat destruktif atau merusak dan menjadikannya suatu keuntungan Sebagai contoh: Virus, Pencurian Kartu Kredit, Pembobolan Rekening Bank, Pencurian *PasswordE-mail* atau *Web Server*, dan sebagainya.
2. Bisa berdiri sendiri atau berkelompok dalam bertindak.
3. Wempunyai website atau *channel* dalam IRC yang tersembunyi, hanya orang-orang tertentu yang bisa mengaksesnya.
4. Mempunyai IP *address* yang tidak bisa dilacak.
5. Kasus yang paling sering terjadi ialah *Carding* yaitu pencurian kartu kredit, kemudian *Cracking* yaitu perbuatan pembobolan situs dan mengubah segala isinya menjadi berantakan.

Adapun akibat yang ditimbulkan antara keduanya adalah:³²

1. Hacker

Membuat teknologi internet semakin maju karena hacker menggunakan keahliannya dalam hal komputer untuk melihat, menemukan, dan memperbaiki

³⁰ Fadjar Efendy Rasyid, *Hacker Dan Cracker*, http://www.ubaya.ac.id/2014/content/articles_detail/148/Hacker-dan-Cracker.html, diakses pada 14 juni 2023 Pukul 23.11

³¹ Fadjar Efendy Rasyid, *Hacker Dan Cracker*, http://www.ubaya.ac.id/2014/content/articles_detail/148/Hacker-dan-Cracker.html, diakses pada 14 juni 2023 Pukul 23.11

³² Apazhadechh, *Hacker Dan Cracker 2*, [blogkucybercrime.blogspot.com/2013/05/hacker- dan-cracker-2.html](http://blogkucybercrime.blogspot.com/2013/05/hacker-dan-cracker-2.html), diakses pada pada 16 juni 2023 Pukul 21.00

kelemahan sistem keamanan dalam sebuah sistem komputer ataupun dalam sebuah software, membuat gairah bekerja seorang administrator kembali hidup karena hacker membantu administrator untuk memperkuat jaringan mereka.

2. Cracker

Merusak dan melumpuhkan keseluruhan sistem komputer, sehingga data-data pengguna jaringan rusak, hilang ataupun berubah.

C. Tinjauan Umum Tentang Pelaku

Pelaku adalah orang yang melakukan tindak pidana yang bersangkutan, dalam arti orang yang dengan suatu kesengajaan atau suatu tidak sengaja seperti yang diisyaratkan oleh Undang-Undang telah menimbulkan suatu akibat yang tidak dikehendaki oleh Undang-Undang, baik itu merupakan unsur-unsur subjektif maupun unsur-unsur obyektif, tanpa memandang apakah keputusan untuk melakukan tindak pidana tersebut timbul dari dirinya sendiri atau tidak karena gerakkan oleh pihak ketiga. Melihat batasan dan uraian diatas, dapat dikatakan bahwa orang yang dapat dinyatakan sebagai pelaku tindak pidana dapat dikelompokkan kedalam beberapa macam antara lain :

1. Orang yang melakukan (*dader plagen*) Orang ini bertindak sendiri untuk mewujudkan segala maksud suatu tindak pidana.
2. Orang yang menyuruh melakukan (*doen plagen*) Dalam tindak pidana ini perlu paling sedikit dua orang, yakni orang yang menyuruh melakukan dan yang menyuruh melakukan, jadi bukan pelaku utama yang melakukan

tindak pidana, tetapi dengan bantuan orang lain yang hanya merupakan alat saja.

3. Orang yang turut melakukan (*mede plagen*) Turut melakukan artinya disini ialah melakukan bersama-sama. Dalam tindak pidana ini pelakunya paling sedikit harus ada dua orang yaitu yang melakukan (*dader plagen*) dan orang yang turut melakukan (*mede plagen*).

D. Tinjauan Umum Tentang Pertanggungjawaban Pidana

Konsep "pertanggungjawaban" dalam hukum pidana, merupakan konsep sentral yang dikenal dengan ajaran kesalahan. Dalam bahasa latin ajaran kesalahan dikenal dengan sebutan *mens rea*. Doktrin *mens rea* dilandaskan pada suatu perbuatan yang tidak mengakibatkan seseorang bersalah kecuali jika pikiran orang itu jahat. Dalam bahasa Inggris doktrin tersebut dirumuskan dengan *an act does not make a person guilty, unless the mind is legally blameworthy*. Berdasarkan asas tersebut ada dua syarat yang harus terpenuhi untuk dapat memidana seseorang, yaitu perbuatan Jahiria yang terlarang atau perbuatan pidana (*actus reus*), dan ada sikap batin jahat atau tercela (*mens rea*).³³

Roeslan Saleh menyatakan bahwa pertanggungjawaban pidana diartikan sebagai diteruskannya celaan yang objektif yang ada pada perbuatan pidana dan secara subjektif memenuhi syarat untuk dapat dipidana

³³ Hanafi Amrani dan Mahrus Ali, 2015, *Sistem Pertanggungjawaban Pidana Perkembangan dan Penerapan*, PT RajaGrafindo Persada, Jakarta, hlm. 20

karena perbuatannya itu.³⁴ Maksud celaan objektif adalah bahwa perbuatan yang dilakukan oleh seseorang memang merupakan suatu perbuatan yang dilarang. Indikatornya adalah perbuatan tersebut melawan hukum baik dalam arti melawan hukum materil. Sedangkan maksud celaan subjektif menunjuk kepada orang yang melakukan perbuatan yang dilarang tadi. Sekalipun menunjuk kepada orang yang melakukan perbuatan yang dilarang tadi, sekalipun perbuatan yang dilarang telah dilakukan oleh seseorang, namun jika orang tersebut tidak dapat dicela karena pada dirinya tidak terdapat kesalahan, maka pertanggungjawaban pidana tidak mungkin ada.³⁵

Perbuatan pidana hanya menunjukkan kepada dilarang dan diancamnyaperbuatan dengan suatu pidana. Apakah orang yang melakukan perbuatan kemudian juga dijatuhkan 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 Zorden Schuld non facit reum nisi mens sir rea*).³⁶

Dilihat dari sudut pandang bertanggungjawab, dikatakan seseorang mampu bertanggungjawab (*toerekeningsvatbaar*) pada umumnya seseorang yang bisabertanggungjawab lah yang dapat dimintai pertanggungjawaban

³⁴ Roeslan Saleh, 1983, *Perbuatan Pidana dan Pertanggungjawaban Pidana (Dua Pengertian Dasar Dalam Hukum Pidana)*, Aksara Baru, Jakarta, hlm. 75

³⁵ Hanafi Amrani dan Mahrus Ali, *Op.Cit.* hlm 21

³⁶ Moeljatno, 2002, *Asas-asas Hukum Pidana*, cet. 7 PT Renaka Cipta, Jakarta, hlm. 153

atastindakan/perbuatan itu. Adapun unsur-unsur pertanggungjawaban pidana ialah:³⁷

1. Melakukan perbuatan yang melawan hukum.
2. Adanya unsur kesalahan.
3. Kemampuan bertanggung jawab.
4. Tidak ada alasan pemaaf.

1. Perbuatan Melawan Hukum

Setiap perbuatan yang dilakukan seseorang segalanya memiliki konsekuensi bagi dirinya ataupun orang lain, baik itu perbuatan yang baik ataupun yang buruk dan setiap konsekuensi atau tindakannya harus dipertanggungjawabkan sesuai dengan peraturan-peraturan yang berlaku. Disebut sebagai perbuatan melawan hukum, hal ini dapat dijelaskan sebagai suatu sifat melawan hukum dalam artiumum yang dimaksudkan adalah karena dapat dirumuskan sebagai suatu perbuatan hukum subjektif yang secara yuridis adalah bertentangan dengan norma hukum yang berlaku, dan yang karenanya dapat dicela.³⁸

2. Unsur Kesalahan Melawan Hukum.

Menurut Simons kesalahan dalam arti luas yaitu meliputi dolus (sengaja) dan culpa late (alpa dan lalai). Dari rumus tersebut Simons mencampurkan unsur-

³⁷ Moeljatno, 2001, *Asas-asas Hukum Pidana*, PT Reneka Cipta, Jakarta, hlm. 166

³⁸ Roeslan Saleh, 1987, *Sifat Melawan Hukum Dari Perbuatan Pidana*, Aksara Baru, Jakarta, hlm. 27

unsur perbuatan pidana (*criminal act*) yang meliputi perbuatan dan sifat melawanhukum perbuatan dan pertanggungjawaban pidana (*criminal liability*) yang mencakup kesengajaan, kealpaan serta kelalaian dan kemampuan bertanggungjawab³⁹

Istilah kesalahan mempunyai dua arti yang masing-masing berbeda jangkauan dan isinya, yaitu:

a. Pengertian kesalahan dipakai sebagai syarat umum untuk dapat dipidanya perbuatan di samping sifat melawan hukum. Kesalahan didefinisikan sebagai sifat dapat dicela. Sifat dapat dicela ini digunakan kalau kita berbicara tentang taripa sila" atau tentang alasan-alasan penghapus pidana.

b. Pengertian kesalahan dipakai juga untuk bagian khusus rumusan delik, yaitu sebagai sinonim dari kata tidak berhati-hati misalnya Pasal 359 KUHP yang menyebutkan:

"karena kesalahan/kealpaannya, menyebabkan matinya orang lain."

Sekalipun mirip, kealpaan di sini tidak dipakai dalam arti pertama. Jadi, bukan sebagai sifat dicela, melainkan sebagai sifat kurang berhati- hati.

3. Kemampuan Bertanggung Jawab.

Kemampuan bertanggung jawab merupakan unsur yang diwajibkan gunamemenuhi suatu pertanggungjawaban perbuatan pidana.

³⁹ Zainal Abidin Farid, 2010, *Hukum Pidana 1*, Sinar Grafika, Jakarta, hlm. 224

Moeljatno menyimpulkan bahwa untuk adanya kemampuan bertanggung jawab harus ada⁴⁰

1. Kemampuan untuk membedakan antara perbuatan yang baik dan yang buruk yang merupakan faktor akal.
2. Kemampuan untuk menentukan kehendaknya menurut keinsyafan tentang baik dan buruknya perbuatan tersebut yang merupakan faktor perasaan kehendak.

4. Tidak Ada Alasan Pemaaf.

Pertanggungjawaban pidana seseorang yang melakukan perbuatan pidana dapat dibatalkan demi hukum jika terdapat alasan pemaaf. Yang dimaksud alasan pemaaf menurut teori hukum adalah alasan yang menghapuskan kesalahan (alasan pemaaf), maka masih ada perbuatan pidana, maka orang tersebut tidak dapat dipidana (tidak dapat dipertanggungjawabkan).⁴¹ Alasan pemaaf atau *schulduitsluitingsgrond* ini menyangkut pertanggungjawaban seseorang terhadap perbuatan pidana yang telah dilakukannya atau *criminal responsibility*. Alasan yang melakukan delik atas dasar pemaaf ini menghapuskan kesalahan orang yang beberapa hal.⁴²

E. Tinjauan Umum Tentang Perlindungan Data Pribadi

Konsep perlindungan data pribadi menekankan bahwa setiap orang berhak menentukan nasibnya sendiri seperti apakah dirinya akan melakukan sharing data

⁴⁰ Moeljatno, 2008, *Asas-asas Hukum Pidana*, Rineka Cipta, Jakarta, hlm. 178

⁴¹ Moeljatno, *Op.Cit*, hlm. 137

⁴² Teguh Prasetyo, *Op.Cit*, hlm. 126

atau tidak dan apabila sharing data dilakukan maka ia berhak juga menentukan syarat yang hendak dipenuhi dalam suatu komunitas masyarakat.⁴³

Data pribadi ialah keterangan data tunggal atau gabungan bersifat tertutup ataupun umum, kemudian diserahkan oleh subyek data dan disatukan dalam sistem elektronik kemudian dikerjakan oleh pengelola untuk dimanfaatkan sesuai tujuan serta kegunaannya, kemudian jika diselewengkan subyek data boleh menuntaskannya lewat ranah hukum.⁴⁴

Kemudian berdasarkan Pasal 1 ayat (1) Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, yang berbunyi Data Pribadi adalah data tentang orang perseorangan yang teridentifikasi atau dapat diidentifikasi secara tersendiri atau kombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik atau nonelektronik.⁴⁵

Perlindungan data pribadi ialah langkah-langkah cepat guna menjaga kerahasiaan informasi privasi perseorangan dari eksploitasi yang tidak legal atau akses yang tidak diizinkan oleh pihak lain. Data pribadi mencakup berbagai jenis informasi, seperti identitas pribadi seperti nama lengkap, lokasi, telepon, lahir, kartu tanda atau paspor, informasi keuangan, informasi kesehatan, dan sejenisnya.⁴⁶

1. Jenis Data Pribadi

⁴³ Fanny, P , 2019, *Perlindungan Privasi data Pribadi Perspektif Perbandingan Hukum*, Jatiswara, hlm. 239.

⁴⁴ Rizky P.P. Karo Karo, 2020, *Pengaturan Perlindungan Data Pribadi Di Indonesia; Perspektif Teori Keadilan Bermartabat*, Nusa Media, Bandung: Nusa, hlm. 50.

⁴⁵ Lembaran Negara Republik Indonesia, 2022, *Nomor 196, Tambahan Lembaran Negara Republik Indonesia Nomor 6820*.

⁴⁶ Maharani P Maulina, 2020, *Perlindungan data pribadi dalam perspektif Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE)*. Jurnal Kajian Informasi dan Perpustakaan, hlm. 8.

a) Data Pribadi yang bersifat spesifik, meliputi:

1)Data informasi kesehatan.

2)Data biometrik.

3)Data genetika.

4)Catatan kesehatan.

5)Data anak.

6)Data keuangan pribadi; dan/ atau.

7)Data lainnya sesuai dengan ketentuan sebagaimana perundang -
undangan.

2. Hak Subjek Data Pribadi

a. Mendapatkan informasi.

b. Menunda atau membatasi pemrosesan data.

c. Menggugat dan menerima ganti rugi atas pelanggaran data pribadi.

d. Mengajukan keberatan.⁴⁷

⁴⁷ Lembaran Negara Republik Indonesian, 2022, *Nomor196, Tambahan Lembaran Negara Republik Indonesia Nomor6820.*

BAB III

HASIL DAN PEMBAHASAN

A. Pengaturan Tindak Pidana *Cracking* Dalam Sistem Hukum Pidana Di Indonesia Pasal 30 Ayat (2)

Data pribadi atau suatu privasi seseorang itu mempunyai hak privasi sendiri untuk dilindungi baik secara pribadi maupun secara umum. Baik secara pribadi adalah melindungi dari diri pribadi agar tidak dapat secara mudah diketahui orang lain dan tidak di salah gunakan. Dan secara umum ialah melindungi dalam suatu kumpulan data seseorang agar tidak bocor. Dalam situasi ini bukan dalam elektronik saja dan masih dapat dilakukan pula dalam di kehidupan nyata dengan alibi perjanjian atau yang lain dari suatu perkara penipuan dan masih banyak lainnya.⁴⁸

Pelindungan terhadap data pribadi berkaitan dengan konsep privasi, konsep privasi sendiri adalah merupakan sebuah gagasan untuk memelihara integritas dan martabat setiap orang secara pribadi. Privasi adalah istilah lain yang kemudian digunakan oleh negara-negara maju yang berkaitan dengan data pribadi sebagai hak yang harus dilindungi, yaitu hak seseorang untuk tidak diganggu kehidupan pribadinya.⁴⁹

⁴⁸ Oktaviani Sugiarto, 2019, *Tinjauan Hukum Internasional terkait Perlindungan Data Pribadi*, Fakultas Hukum Universitas Hasanuddin, Makassar, hlm. 28

⁴⁹ Muhamad Hasan Rumlus, Hanif Hartadi, 2020, *Kebijakan Penanggulangan Pencurian Data Pribadi dalam Media Elektronik*, Malang, hlm. 290

Perihal perlindungan Data Pribadi ini Indonesia sudah mempunyai suatu undang –undang yang dapat membahas secara komprehensif dan sudah sah untuk diberlakukannya perlindungan data pribadi itu untuk memenuhi hak privasi seseorang sebagaimana diatas yang sudah yang sudah memenuhi dalam Undang – Undang Dasar pasal 28G ayat (1) yang menjelaskan untuk setiap seseorang mempunyai perlindungan secara pribadi. Undang –Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi.

Undang–Undang Nomor 27 tahun 2022 ini yang isinya menjelaskan dari pengertian data pribadi di Pasal –Pasal awal dan yang menjelaskan tentang Sanksi terdapat pada Pasal 57 dan yang menjelaskan dalam ketentuan pidananya dari suatu kasus mencakup perlindungan data pribadi diatur mulai Pasal 67. Sudah secara komprehensif membahas perlindungan data pribadi itu dalam Hukum yang mengayomi dari data pribadi setiap warga Negara..

Kejahatan dunia maya (*Cybercrime*) adalah kejahatan yang dilakukan oleh seseorang atau sekelompok orang atau korporasi dengan cara menggunakan atau dengan sasaran komputer atau sistem komputer atau jaringan komputer. Kejahatan ini terjadi pada dunia maya sehingga mempunyai karakteristik yang berbeda dengan kejahatan tradisional.⁵⁰

Kemajuan teknologi informasi pada masa kini ditandai dengan meningkatnya penggunaan teknologi dalam setiap aspek kehidupan manusia. Teknologi seperti internet, komputer dan perangkat lainnya banyak memberikan kemudahan bagi manusia untuk dapat melakukan aktivitas yang bermanfaat

⁵⁰ Anggia Dasa Putri, Dapit Pratama, 2017, *Sistem Pakar Mendeteksi Tindak Pidana cybercrime menggunakan Metode forward Chaining berbasis Web di Kota Batam*, Batam, hlm. 198

namun di sisi lain juga dapat memberikan kemudahan akses bagi pihak tertentu untuk melakukan suatu tindak pidana, salah satunya adalah *cracking*.⁵¹

Contoh kasus yang pernah terjadi di Indonesia yaitu Penyerangan terhadap jaringan internet KPU, Jaringan internet di Pusat Tabulasi Nasional Komisi Pemilihan Umum sempat down (terganggu) beberapa kali. KPU menggandeng kepolisian untuk mengatasi hal tersebut. *Cybercrime* kepolisian juga sudah membantu. Domain kerjasamanya antara KPU dengan kepolisian, kata Ketua Tim Teknologi Informasi KPU, Husni Fahmi di Kantor KPU, Jalan Imam Bonjol, Menteng , Jakarta Pusat. Menurut Husni, tim kepolisian pun sudah mendatangi Pusat Tabulasi Nasional KPU di Hotel Brobudur di Hotel Brobudur, Jakarta Pusat. Mereka akan mengusut adanya dugaan kriminal dalam kasus kejahatan dunia maya dengan cara meretas. Husni menyebut sejak tiga hari dibuka, Pusat Tabulasi berkali-kali diserang oleh peretas. Sejak hari lalu dimulainya perhitungan tabulasi. Seluruh penyerang itu sekarang, kata Husni, sudah diblokir alamat IP-nya oleh PT. Telkom. Tim TI KPU bisa mengatasi serangan karena belajar dari pengalaman yang lalu.⁵²

Beberapa cara untuk menanggulangi dari kasustersebut ialah :

1. Kriptografi : seni menyandikan data. Data yang dikirimkan disandikan terlebih dahulu sebelum dikirim melalui internet.

⁵¹ Christiara Febriliani, Ismunarno, Diana Lukitasari, 2019, *Kajian Etiologi Kriminal Tindak Pidana Cracking Sistem Operasi Windows Di Provinsi Daerah Istimewa Yogyakarta*, Yogyakarta, hlm. 221

⁵²Yulianti, Farida, 2021, *Contoh Kasus Cyber Crime Dan Penyelesaiannya*, Bandung, hlm. 12

2. Internet Farewell: untuk mencegah akses dari pihak luar ke sistem internal. Firewall dapat bekerja dengan 2 cara, yaitu menggunakan filter dan proxy
3. Menutup service yang tidak digunakan.

Kejahatan yang dilakukan oleh cracker adalah produk manusia modern, yang tidak memerlukan kekerasan fisik, namun dapat dikendalikan melalui suatu ruangan tertentu. Modalnya juga tidak terlalu besar, namun dapat menghasilkan uang yang cukup banyak dari hasil kejahatan tersebut. Di Indonesia, kejahatan yang menggunakan sarana komputer sebenarnya sudah lama terjadi, namun pada saat ini sangat sulit di deteksi karena berbagai hal, baik lihat dari sumber daya manusianya, maupun dari sisi hukum yang memayunginya. Dari tahun ke tahun usaha untuk melakukan kejahatan ini terus meningkat, seiring dengan kemajuan teknologi dan kemajuan berfikir manusia. Di sisi lain, usaha-usaha untuk melakukan penegakan hukum masih belum ada perkembangannya.⁵³

Berdasarkan peraturan perundang-undangan yang berlaku di Indonesia ada peraturan yang mengatur tentang tindak *cracking* yaitu Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Dalam UU ITE telah diatur mengenai perbuatan peretasan kedalam Pasal 30. Pasal 30 UU ITE mengatur perbuatan yang meliputi:

⁵³ Nur Khalimatus Sa'diyah, 2013, *Modus Operandi Tindak Pidana Cracker Menurut Undang-Undang Informasi Dan Transaksi Elektronik*, Universitas Wijaya Kusuma Surabaya, Surabaya, hlm. 89

- 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 komputer 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 antar lain:

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; komputer dan/atau sistem elektronik milik orang suatu kegiatan melakukan interaksi dengan sistem
3. unsur "mengakses elektronik yang berdiri sendiri atau dalam jaringan, melalui seperangkat lain"
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.

2.) 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.

Dan bagi pelaku diancam pidana berdasarkan ketentuan pidana pada Pasal

46 ayat (2) UU ITE, yaitu:

"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)."

Dan penuntutannya harus dilakukan berdasarkan pasal sebelumnya yaitu, Pasal 30 ayat (1) jo Pasal 46 ayat (1). Dengan demikian Pasal 30 ayat (2) adalah *lex specialis* dari Pasal 30 ayat (1) jo Pasal 46 ayat (2).

3) 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.⁵⁴

Untuk ancaman pidananya itu diatur di dalam Pasal 46 ayat (3) UU ITE, yaitu:

"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 kita sebut dengan kejahatan atau tindak pidana *cracking*.

⁵⁴ Marina Raisa Theodora Napitupulu, *Op.Cit*, hlm. 56

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 sit rea*).⁵⁵Pertanggungjawaban tanpa adanya kesalahan dari pihak yang melanggar, dinamakan *leer van het materiele feit (fait materielle)*.⁵⁶

B. Pertanggungjawaban Menurut Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi Dan Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik

1. Pertanggungjawaban Pidana Menurut Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi

Pelaku usaha atau penyelenggara sistem elektronik bisa mengumpulkan data pribadi dari pelanggan atau calon pelanggan secara luring atau daring, dimana data digital dapat diperjualbelikan tanpa sepengetahuan dan seizin pemilik data atau disalahgunakan (untuk tujuan di luar pemberian, penyerahan data pribadi digital), bisa juga terjadi data pribadi yang terkoneksi dibajak, dicuri (hack) oleh pihak ketiga.⁵⁷

⁵⁵ Moeljatno, 2002, *Asas-asas Pidana*, PT Rineka Cipta, Jakarta, hlm. 153

⁵⁶ *Ibid*, hlm. 153

⁵⁷ Sahat Maruli Tua Situmeang, 2021, *Penyalahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna Dalam Perspektif Hukum Siber*, Bandung, hlm. 39.

Perlindungan data pribadi ialah upaya untuk mengamankan data pribadi seseorang dari penyelewengan, pengumpulan, dan pengolahan tanpa sepengetahuan dan persetujuannya. Konsep ini erat kaitannya dengan hak privasi individu, di mana setiap orang berhak atas kebebasan untuk menentukan penggunaan data pribadinya.

Perlindungan data pribadi sangat esensial dan diperlukan karena data pribadi mencakup identitas seseorang, dimiliki oleh individu tersebut, dan digunakan untuk melakukan “perbuatan hukum” selanjutnya menyebabkan kedaulatan serta tanggung jawab dalam berbagai bentuk.⁵⁸Perlindungan data pribadi merupakan hak pribadi yang mencakup hak menikmati kehidupan pribadi dan bebas dari segala macam gangguan, Hak berkomunikasi dengan orang lain tanpa bermaksud memata matai, dan hak mengawasi akses informasi tentang kehidupan pribadi dan data seseorang.⁵⁹

Dengan adanya penyalahgunaan data pribadi, maka dapat terlihat adanya kelemahan sistem, kurangnya pengawasan, sehingga data pribadi dapat disalahgunakan dan mengakibatkan kerugian bagi pemilik data tersebut. Penyalahgunaan, pencurian, penjualan data pribadi merupakan suatu pelanggaran hukum dalam bidang teknologi informasi dan juga dapat dikategorikan sebagai pelanggaran atas hak asasi manusia, karena data pribadi merupakan bagian dari hak asasi manusia yang harus dilindungi. Berkaitan hal tersebut, terdapat beberapa contoh kasus dalam penyalahgunaan data pribadi, diantaranya yaitu:

⁵⁸ Rizky P.P. Karo Karo, 2020, *Pengaturan Perlindungan Data Pribadi Di Indonesia; Perspektif Teori Keadilan Bermartabat*, Nusa Media, Bandung, hlm. 47.

⁵⁹ Nurhidayati, Sugiyah, Kartika Yuliantari, 2021, *Pengaturan Perlindungan Data Pribadi dalam Penggunaan Aplikasi PeduliLindungi*, Jakarta, hlm. 43.

1. Penyalinan data dan informasi kartu ATM nasabah (skimming) dimana pelaku skimming melakukan penarikan dana di tempat lain.
2. Pinjaman online, dimana mekanisme transaksinya mengisi data secara online akan tetapi dalam hal keterlambatan pembayaran tidak jarang menggunakan kolektor untuk melakukan intimidasi kepada nasabah, keluarga nasabah, pimpinan tempat nasabah bekerja dan bahkan dapat mengakses data dari handphone nasabah.
3. Transportasi online, dimana konsumen mengalami pelecehan seksual melalui nomor whatsapp.⁶⁰

Berdasarkan peristiwa tersebut dapat disimpulkan bahwa terdapat metadata berupa data pribadi yang diberikan untuk berbagai kepentingan (perbankan, *e-commerce*, dll.), diserahkan secara sukarela dan disimpan sebagai data digital oleh pelaku usaha atau siapapun yang menerima dan menyimpan data pribadi, metadata rentan untuk disalahgunakan penerima-penyimpan data atau dicuri (*hack*) pihak ketiga dan terbuka untuk disalahgunakan, digunakan untuk tujuan-tujuan lain di luar kesepakatan.

Apabila terjadi suatu peristiwa pidana atau ada laporan terjadinya tindak pidana, maka petugas yang menerima laporan segera mengadakan penyelidikan untuk menentukan sampai dimana kebenaran peristiwa tersebut. Laporan tersebut dapat dilakukan secara tertulis yang harus ditandatangani oleh si pelapor dan dapat juga diajukan secara lisan. Sehingga bila terjadi penyalahgunaan data pribadi yang sama-sama merupakan warga negara Indonesia maka akan

⁶⁰*Ibid*, hlm. 39.

diselesaikan melalui hukum Indonesia serta dilaksanakan di Pengadilan yang ada di wilayah hukum Indonesia.

Tindakan pemerintah dalam penanggulangan kebocoran data pribadi Berdasarkan alinea ke-4 Pembukaan Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, menyebutkan Pemerintah Negara Indonesia mempunyai kewajiban konstitusional melindungi segenap bangsa Indonesia dan seluruh tumpah darah Indonesia dan untuk memajukan kesejahteraan umum, mencerdaskan kehidupan bangsa, dan ikut melaksanakan ketertiban dunia yang berdasarkan kemerdekaan, perdamaian abadi, dan keadilan sosial. Secara umum dapat diterima bahwa UUD1945 selaku Konstitusi memberikan kebijakan dalam menaggulangi pencurian data pribadi dengan cara melindungi kepemilikan pribadi dari para pihak yang mencoba melakukan pembobolan atau pencurian data pribadi milik seseorang dalam media elektronik.⁶¹

Regulasi yang secara lebih spesifik meletakkan hak pemilik data adalah Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dalam Undang-Undang No. 19 Tahun 2016 (UU ITE). UU ITE memberikan landasan perlindungan data pribadi yang diperoleh dengan menggunakan sistem elektronik sebagaimana dinyatakan dalam Pasal 26 UU ITE. Persetujuan pemilik data merupakan kata kunci dalam penggunaan data pribadi seseorang sebagaimana dinyatakan dalam Pasal 26 ayat (1) UU ITE yang mana pelanggaran terhadap hal tersebut menyebabkan timbulnya hak hukum keperdataan bagi pihak yang digunakan datanya untuk mengajukan gugatan

⁶¹ Akbari Amarul Zaman, Jumadi Anwar, Aryo Fadlian, 2021, *Pertanggungjawaban Pidana Kebocoran Data Bpjs Dalam Perspektif UU ITE*, Karawang hlm. 153

sebagaimana dinyatakan dalam Pasal 26 ayat (2) UU ITE. UU ITE mengakomodir pula konsep *right to be forgotten* melalui ketentuan dalam Pasal 26 ayat (3) yang memberikan hak kepada pemilik data untuk meminta penghapusan data pribadi yang tidak relevan kepada penyelenggara sistem elektronik.⁶²

Pasal 67 Undang-Undang Nomor 27 Tahun 2022 berisi sanksi administratif yaitu:

- (1) Setiap Orang yang dengan sengaja dan melawan hukum memperoleh atau mengumpulkan Data Pribadi yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian Subjek Data Pribadi sebagaimana dimaksud dalam Pasal 65 ayat (1) dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau pidana denda paling banyak Rp5.000.000.000,00 (lima miliar rupiah).
- (2) Setiap Orang yang dengan sengaja dan melawan hukum mengungkapkan Data Pribadi yang bukan miliknya sebagaimana dimaksud dalam Pasal 65 ayat (2) dipidana dengan pidana penjara paling lama 4 (empat) tahun dan/atau pidana denda paling banyak Rp4.000.000.000,00 (empat miliar rupiah).
- (3) Setiap Orang yang dengan sengaja dan melawan hukum menggunakan Data Pribadi yang bukan miliknya sebagaimana dimaksud dalam Pasal 65 ayat (3) dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau pidana denda paling banyak Rp5.000.000.000,00 (lima miliar rupiah).

Ketentuan ini dapat dijelaskan sebagai berikut:

a. Setiap orang

Ketentuan ini menunjukkan bahwa siapapun baik perseorangan ataupun lembaga hukum, termasuk organisasi pemerintah atau swasta, harus mematuhi ketentuan ini.

b. Dilarang secara melawan Hukum

⁶²Siti Yuniarti, 2019, *Perlindungan Hukum Data Pribadi Di Indonesia*, Jakarta, hlm. 152

Ketentuan ini menunjukkan bahwa tindakan mengungkapkan atau menunjukkan data yang bersifat pribadi atau privasi bukan miliknya harus dianggap sebagai pelanggaran hukum. Tindakan melanggar ketentuan ini dapat dikenakan sanksi pidana dan/atau perdata.

c. Mengungkapkan data pribadi yang bukan miliknya

Ketentuan ini menunjukkan bahwa tindakan mengungkapkan data pribadi yang bukan milik seseorang, walaupun itu dengan sengaja atau tidak, merupakan tindakan dilarang.

d. Data pribadi

Ketentuan ini menunjukkan bahwa ketentuan ini berkenaan dengan data pribadi yang dimiliki oleh perseorangan, termasuk informasi tentang identitas, pekerjaan, keuangan, kesehatan, pendidikan, dan lain sebagainya.

Setiap orang harus memahami bahwa data pribadi adalah hak privasi yang harus dilindungi. Karena itu, penggunaan, pengungkapan, dan pemrosesan data pribadi harus dijalankan dengan langkah yang sah serta wajar, kemudian tidak merugikan pemilik data pribadi. Ketentuan ini juga menunjukkan bahwa setiap tindakan dilarang terhadap ketentuan ini bisa dikenai sebuah sanksi pidana dan/atau perdata. Hal ini menunjukkan betapa pentingnya hak privasi dan keamanan data pribadi bagi masyarakat dan negara, sehingga diperlukan perlindungan yang kuat untuk menghindari penyalahgunaan dan pelanggaran atas data pribadi ini.

2. Pertanggungjawaban Pidana Menurut Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik

Undang-undang Informasi dan Teknologi Elektronik disusun untuk mendukung pertumbuhan ekonomi di Indonesia melalui ekonomi digital dan perdagangan di dunia maya (*e-commerce*) di Indonesia. Kemudian di tengah perjalanan terjadi banyak polemik dan kasus yang menimbulkan pro kontra terhadap pasal-pasal di Undang-undang Informasi dan Teknologi Elektronik, terutama terkait dengan penggunaan media sosial. Merespon perkembangan modus operandi suatu tindak pidana yang dilakukan melalui media elektronik, sejak tahun 2008 telah diatur melalui Undang-undang Nomor 11 tahun 2008 Tentang Informasi dan Transaksi Elektronik (selanjutnya disebut UU ITE) sebagaimana telah dirubah dengan Undang-undang No. 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik bertujuan agar pemanfaatan teknologi lebih dipergunakan sesuai dengan ketentuan peraturan perundang-undangan.⁶³

Dalam UU ITE ini terdapat beberapa aturan tambahan yang mengatur tentangtindak pidana yang telah diatur dalam pasal-pasal sebelumnya. Pasal-pasal ini menjadi aturan tambahan yang dapat dijadikan sebagai pasal penjerat bagi penegak hukum untuk menjerat para pelaku Tindak Pidana Melalui *Cracking*, pasal-pasal tersebut diantaranya adalah:

1. Pasal 36 UU ITE

⁶³ L. Heru Sujamawardi, 2018, *Analisis Yuridis Pasal 27 ayat (1) Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*, Bandung, hlm. 86.

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:

“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 dengan ketentuan peraturan perundang-undangan. Pengertian dengan sengaja dan tanpa hak, dapat ditafsirkan sebagai perbuatan yang bertentangan dengan undang-undang dan tindakan melalaikan ancaman hukuman.⁶⁴ 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 Melalui *Cracking* berdasarkan ketentuan dalam pasal 36 apabila perbuatan

⁶⁴Marina Raisa Theodora Napitupulu, *Op.Cit*, hlm. 58

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 di atas diancam dengan sanksi pidana yang terdapat dalam ketentuan pidana pasal 51 ayat (2) yaitu:

"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)".

2. 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 wilayah Indonesia terhadap Sistem Elektronik yang berada di wilayah yurisdiksi Indonesia.

Pasal 37 UU ITE:

"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".

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 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.

Dan 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.

Pasal 2 UU ITE:

“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.”

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 Cracking. Pemberatan tersebut terdapat dalam Pasal 52 ayat (4) UU ITE mengatakan bahwa:

"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.

Apabila pelaku Tindak Pidana 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.

Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik adalah salah satu bentuk upaya dalam perkembangan teknologi elektronik. Di dalam undang-undang ini telah diatur berbagai hal yang berkaitan dengan suatu informasi elektronik beserta kriteria-kriterianya. Seseorang dapat disebut pelaku apabila telah melakukan tindak pidana dan perbuatannya terbukti sebagai tindak pidana seperti yang telah diatur dalam Undang-undang Informasi dan Transaksi Elektronik.⁶⁵

Pertanggungjawaban pidana yang diatur di dalam Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik juncto Undang-Undang No. 19 Tahun 2016 tentang Perubahan atas Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik Pasal 45A ayat (1) dan ayat (2) sebagai berikut :

⁶⁵Annisa Nur Afni, 2022, *Pertanggungjawaban Pidana Terhadap Pelaku Tindak Pidana Menyebarkan Berita Bohong Dalam Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik*, Aceh, hlm. 10.

1)Setiap orang yang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik sebagaimana dimaksud dalam Pasal 28 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp 1.000.000.000,00 (satu miliar rupiah).

2)Setiap orang dengan sengaja dan tanpa hak menyebarkan informasi yang ditujukan untuk menimbulkan rasa kebencian atau permusuhan individu dan/atau kelompok masyarakat tertentu berdasarkan atas suku, agama, ras, dan antar golongan (SARA) sebagaimana dimaksud dalam Pasal 28 ayat (2) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp 1.000.000.000,00, (satu miliar rupiah).

Untuk membuktikan telah terjadinya pelanggaran dalam Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik terdapat pada Pasal 45A ayat (1).

BAB IV

PENUTUP

A. Kesimpulan

Berdasarkan uraian pada bab-bab terdahulu, maka dapat disimpulkan sebagai berikut :

1. Pengesahan RUU Perlindungan Data Pribadi dapat dikatakan sebagai solusi kebocoran data pribadi konsumen terutama konsumen e-commerce yang mana pendaftaran penggunaan e-commerce mengharuskan mengisi

data-data yang menyinggung data pribadi, yang mana hal ini akan sering kita temui di dalam internet. Semenjak kemunculan COVID-19 membuat peningkatan penggunaan internet naik. Hal tersebut justru membuat sistem keamanan internet semakin rentan dan mudah disusupi oleh oknum jahat untuk melakukan peretasan dan kebocoran data. Dengan pengesahan RUU Perlindungan Data Pribadi diharapkan dapat menjadi solusi kebocoran data pribadi.

2. Indonesia mengakui bahwa perlindungan data pribadi sebagai bagian dari privasi merupakan hak asasi manusia. Pengakuan tersebut terefleksi, baik dalam konstitusi maupun beragam peraturan selevel undang-undang. Kebutuhan pengaturan perlindungan data pribadi pada level undang-undang dibutuhkan karena perlindungan data pribadi sebagai bagian dari privasi merupakan hak asasi warga negara. pasal 65 jo. Pasal 67 UU PDP. Sehingga selain UU ITE dan perubahannya, tindakan *cracking* juga dapat dijerat menggunakan UU PDP sepanjang memenuhi unsur perbuatan yang disebut dalam pasal di atas. Dapat dipertanggungjawabkan secara pidana dan dapat dikenakan hukuman penjara atau denda, atau keduanya.

B. Saran

1. Ketentuan hukum tindak pidana cyber crime pada dasarnya sudah diatur dalam Undang-undang Nomor 19 Tahun 2016 tentang Perubahan Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik. Untuk mencegah terjadinya pelanggaran data pribadi,

disarankan untuk menghindari penggunaan layanan pinjaman berbasis online apabila tidak dalam keadaan yang sangat membutuhkan.

2. Masyarakat secara luas perlu mengetahui cara perlindungan diri terhadap data pribadinya di dunia maya. Dengan tidak secara cuma-cuma membagikan informasi mengenai dirinya sendiri. Secara langsung mengedukasi masyarakat sekitarnya secara bijak penggunaan media sosial dan internet.

DAFTAR PUSTAKA

A. Buku

Abidin, Zainal Farid. 2010. *Hukum Pidana 1*. Sinar Grafika. Jakarta.

Amrani, Hanafi & Mahrus Ali. 2015. *Sistem Pertanggungjawaban Pidana Perkembangan dan Penerapan*, PT RajaGrafindo Persada, Jakarta.

Ariman, Rasyid. 2006. *Kapita Selekta Perbandingan Hukum Pidana*. Universitas Sriwijaya. Palembang.

- Ariman, M. Rasyid & M. Fahmi Raghieb. 2013. *Hukum Pidana Fundamental (Tindak Pidana, Pertanggungjawaban Pidana, Pidana & Pemidanaan)*. Unsri Press. Palembang.
- Chazawi, Adami&Ardi Ferdian. 2015.*Tindak Pidana Informasi & Transaksi Elektronik*. Media Nusa Creative. Malang.
- Ilyas Amir, 2012, *Asas-Asas Hukum Pidana : Memahami Tindak Pidana dan Pertanggungjawaban Pidana sebagai Syarat Pemidanaan*. Yogyakarta.
- Indonesia Kejaksaan Republik. 2010. *Asas-asas Hukum Pidana, Modul untuk Diklat Pendahuluan Pendidikan dan Pelatihan Pembentukan Jaksa (PPPJ)*, Pusat Pendidikan dan Pelatihan Kejaksaan Republik Indonesia, Jakarta.
- Kartanegara, Satochid. 1995.*Hukum Pidana Bagian Pertama*. Balai Lektor Mahasiswa. Jakarta.
- Lamintang, P.A.F. 2009. *Delik-Delik Khusus Kejahatan Terhadap Harta Kekayaan*. Sinar Grafika. Jakarta.
- Mansur, M Arief dan Elisatris Gultom. 2009. *CYBER LAW: Aspek Hukum Teknologi Informasi*,PT Refika Aditama. Bandung.
- Muladi. 2002.*Lembaga Pidana Bersyarat*. Alumni. Bandung.
- Moeljatno. 2001.*Asas-asas Hukum Pidana*. PT Renaka Cipta. Jakarta.
- Moeljatno. 2002.*Asas-asas Pidana*.PT Rineka Cipta. Jakarta.
- Moeljatno. 2002.*Asas-asas Hukum Pidana*. PT Renaka Cipta. Jakarta.
- Moeljatno. 2008.*Asas-asas Hukum Pidana*. PTRineka Cipta. Jakarta.

- Napitupulu, Marina Raisa Theodora. 2018. *Pertanggungjawaban Pidana Terhadap Pelaku Tindak Pidana Peretasan (Hacking)*, Universitas Sumatera Utara.
- Pendidikan, Departemen& Kebudayaan, 1990, *Kamus Besar Bahasa Indonesia*, Jakarta.
- P, Fanny. 2019.*Perlindungan Privasi data Pribadi Perspektif Perbandingan Hukum*. Jatiswara. Mataram.
- P, Maharani Maulina. 2020.*Perlindungan data pribadi dalam perspektif Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE)*. Jurnal Kajian Informasi dan Perpustakaan.
- P, Rizky Karo Karo. 2020.*Pengaturan Perlindungan Data Pribadi Di Indonesia Perspektif Teori Keadilan Bermartabat*. Nusa Media. Bandung.
- Prasetyo, Teguh. 2010, *Hukum Pidana*. Rajawali Pers. Jakarta.
- Raisa, Marina Theodora Napitupulu. 2018. *Pertanggungjawaban Pidana Terhadap Pelaku Tindak Pidana Peretasan (Hacking)*, Universitas Sumatera Utara.
- Saleh, Roeslan. 1983.*Perbuatan Pidana dan Pertanggungjawaban Pidana; Dua Pengertian Dasar dalam Hukum Pidana*. Aksara Baru. Jakarta.
- Saleh, Roeslan. 1987.*Sifat Melawan Hukum Dari Perbuatan Pidana*. Aksara Baru. Jakarta.
- Soesilo, R. 1998.*Kitab Undang-Undang Hukum Pidana (KUHP) Serta Komentar-Komentarnya Lengkap Pasal Demi Pasal*. Politiea. Bogor.

- Soekanto, Soerjono. 2002. *Faktor-faktor yang Mempengaruhi Penegakan Hukum*. Raja Grafindo. Jakarta.
- S.S.T, Kansil dan Christine S.T. Kansil. 2004. *Pokok-Pokok Hukum Pidana*. Pradnya Paramita. Jakarta.
- Sudarto, 1996. *Hukum dan Hukum Pidana*, Bandung, Alumni.
- Sugiarto, Oktaviani. 2019. *Tinjauan Hukum Internasional terkait Perlindungan Data Pribadi*. Fakultas Hukum Universitas Hasanuddin. Makassar. hlm. 28
- Suhariyanto, Budi. 2012. *Tindak Pidana Teknologi Informasi (Cybercrime)*, PT Raja Grafindo Persada. Jakarta.
- Yulianti, Farida. 2021. *Contoh Kasus Cyber Crime Dan Penyelesaiannya*. Universitas Komputer Indonesia. Bandung.
- Widodo. 2011. *Aspek Hukum Kejahatan Mayantara*. Aswaja Presindo. Yogyakarta.

B. Undang-Undang

Undang-Undang Dasar 1945.

Kitab Undang-Undang Hukum Pidana.

Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi.

Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik

C. Jurnal

Akbari Amarul Zaman, Jumadi Anwar, Aryo Fadlian, 2021, "Pertanggungjawaban Pidana Kebocoran Data Bpjs Dalam Perspektif UU ITE", *Jurnal Fakultas Hukum Universitas Singaperbangsa*, Vol. 1, No. 2, November 2021

Anggia Dasa Putri, Dapit Pratama, 2017, "Sistem Pakar Mendeteksi Tindak Pidana cybercrime menggunakan Metode forward Chaining berbasis Web di Kota Batam", *Jurnal Edik Informatika*, Vol.3, No. 2, Maret 2017

Annisa Nur Afni, 2022, "Pertanggungjawaban Pidana Terhadap Pelaku Tindak Pidana Menyebarkan Berita Bohong Dalam Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik", *Jurnal Pengabdian Cendikia*, Vol. 1, No. 1, Mei 2022

Christiara Febriliani, Ismunarno, Diana Lukitasari, 2019, "Kajian Etiologi Kriminal Tindak Pidana Cracking Sistem Operasi Windows Di Provinsi Daerah Istimewa Yogyakarta", *Jurnal Kajian Etiologi Kriminal Tindak Pidana*, Vol. 8, No. 3, Desember 2019

L. Heru Sujamawardi, 2018, "Analisis Yuridis Pasal 27 ayat (1) Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik", *Jurnal Universitas Maranatha Christian*, Vol. 9, No.2, April 2018

- Nurhidayati, Sugiyah, Kartika Yuliantari, 2021, “Pengaturan Perlindungan Data Pribadi dalam Penggunaan Aplikasi PeduliLindungi”, *Jurnal Universitas Bina Sarana Informatika*, Vol. 5, No.1, Maret 2021
- Nur Khalimatus Sa’diyah, 2013, “Modus Operandi Tindak Pidana Cracker Menurut Undang-Undang Informasi Dan Transaksi Elektronik”, *Jurnal Universitas Wijaya Kusuma Surabaya*, Vol. 17, No. 2, Mei 2013
- Muhamad Hasan Rumlus, Hanif Hartadi, 2020, “Kebijakan Penanggulangan Pencurian Data Pribadi dalam Media Elektronik”, *Jurnal Fakultas Hukum Universitas Brawijaya*, Vol. 11, No. 2, Agustus 2022
- Sahat Maruli Tua Situmeang, 2021, “Penyalahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna Dalam Perspektif Hukum Siber”, *Jurnal Fakultas Hukum Universitas Komputer*, Vol. 27, No. 1, Maret 2021
- Siti Yuniarti, 2019, “Perlindungan Hukum Data Pribadi Di Indonesia”, *Jurnal Bina Nusantara University*, Vol. 1, No.1, September 2019

D. Internet

- Apazhadechh. *Hacker Dan Cracker*
2, <http://blogkucybercrime.blogspot.com/2013/05/hacker-dan-cracker-2.html>, diakses pada pada 16 juni 2023.
- Data, *Pengertian Pribadi*,
https://www.hukumonline.com/klinik/detail/ulasan/lt5c498fb94dc87/perlindungan-data-pribadi-dalam-penyelenggaraan-fintech/#_ftn5,
diakses pada tanggal 22 Agusuts 2023 Pukul 19.50.

<https://tekno.kompas.com/read/2022/09/20/11210337/ruu-pdp-resmi-disahkan-jadi-undang-undang-perlindungan-data-pribadi>, diakses pada tanggal 22 Agustus pukul 19.10.

Indonesia, CNN. *13 Juta Data Bocor Bukalapak Dijual di Forum Hacker*, www.bukalapak.com, diakses pada tanggal 22 Agustus Pukul 19.00.

Kamus Besar Bahasa Indonesia, <https://kbbi.web.id/>, diakses pada tanggal 2 Juni 2023 pukul 21.00.

Kepaniteraan dan sekretariat jenderal mahkamah konstitusi, <https://www.mkri.id/index.php?page=download.Penelitian&id=123>, diakses pada tanggal 22 Agustus 2023 Pukul 17.00.

Nursyabani, Fira. *2,3 Juta Data WNI Bocor di Pasar Gelap, Diduga Milik KPU*, www.ayobandung.com, diakses pada tanggal 22 Agustus Pukul 18.20.

Peretas, Anonim. <https://id.wikipedia.org/wiki/Peretas>, diakses pada 11 juni 2023.

Pomalingo, Suwito. *Tentang Pasal 27 UU ITE Nomor 11 Tahun 2008*, <https://suwitopoms.id/tentang-pasal-27-uu-ite-nomor-11-tahun-2008.html>, diakses pada 14 Juni 2023.

Rahma, Andita dan Syailendra Persada, *Data Penduduk di BPJS Kesehatan Bocor, Bukti Lemahnya Perlindungan Data Pribadi*, www.tempo.com, diakses pada tanggal 22 Agustus 2023 Pukul 18.00.

E. Makalah

Annisa, *Hacker dan Cracker*. <http://ilmuti.org/wp-content/uploads/2014/04/Annisa-Hacker-dan-Cracker.pdf>. Diakses pada 12 juni 2023.

Firman, Yogi Efendi. *Analisis tindak pidana cracking menurut hukum positif dan Hukum Pidana Islam*, <https://eprints.walisongo.ac.id/id/eprint/14227/>. Diakses pada 14 Desember 2022.

Rasyid, Fadjar Efendy. *Hacker Dan Cracker*. http://www.ubaya.ac.id/2014/content/articles_detail/148/Hacker-dan-Cracker.html. diakses pada 14 juni 2023.

Yuli, Tasya. *Cracking Dalam Prespektif Undang-Undang Nomor 11 Tahun 2008 Hukum Pidana Islam*. <http://repository.uinsu.ac.id/13540/>. diakses pada 14 Desember 2022.