BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Perkembangan zaman yang semakin mengalami perubahan tidak terlepas dari pengaruh era globalisasi sebagai arah kemajuan suatu bangsa di setiap bangsa. Hal ini sebagai arah dan tuntutan zaman yang semakin maju dan semakin berkembang sesuai dengan perkembangan zaman yang tidak bisa dihindarkan. Globalisasi ditandai dengan adanya keterbukaan dan kebebasan dalam berbagai bidang kehidupan yang mengakibatkan perubahan dalam berbagai aspek kehidupan yang berlangsung dengan sangat cepat. Melalui globalisasi serta adanya keterbukaan teknologi informasi maka kegiatan di segala bidang menjadi bersifat terbuka sehingga mengakibatkan komunikasi dan informasi dapat diakses serta dilakukan dimana saja dan kapan saja.[1]

Kemajuan teknologi informasi yang semakin mengalami peningkatan dan memberikan banyak sekali manfaat didalamnya bisa saja membawa konsekuensi tertentu, dimana semakin mudahnya kejahatan itu dilakukan. Misalkan saja kejahatan siber yang merupakan bentuk dari fenomena terbaru dalam tindak kejahatan yang merupakan dampak langsung dari adanya perkembangan teknologi informasi. Kejahatan dunia maya ini dapat dilakukan tanpa mengenal batasan teritorial dan tidak diperlukan adanya interaksi langsung antara pelaku dan korban kejahatan.

Istilah siber kini menjadi suatu istilah yang seringkali digunakan oleh seluruh lapisan masyarakat sekarang ini. Kata siber telah ditambahkan pada berbagai istilah untuk menggambarkan bentuk masyarakat atau jenis kejahatan yang berbasis siber seperti *cyber society, cyber attack, cyber crime, cyber terrorism,* dan lain sebagainya. Dalam konteks ini yang menjadi penekanan yakni tindakan *cybercrime.*[2] Dalam perkembangannnya,

[1] Rahman Saleh, "*Perlindungan Data Pribadi dalam Perspektif Kebijakan Hukum Pidana",* Jurnal Hukum, Vol.1/No.1/2021, hlm. 95.
[2] Maskun, *et.al, Korelasi Kejahatan Siber dan Kejahatan Agresi dalam Perkembangan Hukum Internasional,* Makasar :Nas Media Pustaka, 2020, hlm. 20.

yang namanya kemajuan teknologi yang dihubungkan ke internet, telah memunculkan suatu kejahatan yang sangat canggih yang disebut dengan *cybercrime.* Kebanyakan orang mengenal *cybercrime* ini dengan kejahatan dalam dunia maya atau melalui jaringan internet.[3] Definisi *cyber crime* menurut Marita adalah tindak kriminal yang dilakukan dengan menggunakan kejahatan yang memanfaatkan perkembangan teknologi komputer khususnya internet. Berdasarkan kutipan tersebut dapat disimpulkan bahwa *cybercrime* atau kejahatan dunia maya merupakan penyalahgunaan teknologi internet untuk sebuah tindak kejahatan.[4]

Penjahat dunia maya seringkali menggunakan sejumlah teknik serangan untuk melakukan serangan *cyber* mereka dan terus mencari metode dan teknik baru untuk mencapai tujuan mereka, sambil menghindari deteksi dan penangkapan oleh pihak berwajib. Terdapat beberapa jenis-jenis serangan *cyber* atau dapat disebut *hacking* (peretasan) yang secara umum sering digunakan, diantaranya berupa *distributed denial of service* (DDOS), *malware, phising, credential attack,* dan *cybercriminals.* Tindakan *cybercrime* dapat dilakukan tanpa memerlukan adanya kontak langsung antara pelaku dan korban, tindakan ini dapat dilakukan dimana saja, kapan saja, tanpa memperhitungkan jarak antara pelaku dan korban, sepanjang ada jaringan internet dan peralatan yang memadai.

Tindakan *hacking* atau peretasan semakin sering terjadi, yang pada umumnya bertujuan untuk mengambil data-data tertentu yang dimiliki target, tapi ada juga peretasan yang bertujuan untuk menghancurkan data atau sistem tertentu sehingga berdampak seperti kerusakan digital. Menurut John. S. Tumiwa pada umumnya tindakan *hacker* Indonesia belum separah aksi di luar negeri. Perilaku *hacker* Indonesia masih sebatas masuk ke suatu situs komputer orang lain yang ternyata rentan penyusupan dan memberitahukan kepada pemiliknya untuk berhati-hati, sedangkan di luar

[3] Oksidelfa Yanto, *Pemidanaan atas Kejahatan yang berhubungan dengan Teknologi Informasi,* Yogyakarta : Samudera Biru, 2021, hlm. 117.
[4] David Eko Setiawan dan Anton Isharjono, *Kabar Baik di Tengah Dunia Maya (Menghadirkan Injil dalam Ruang Virtual,)* Yogyakarta : KBM Indonesia, 2022, hlm. 20.

negeri *hacker* sudah memasuki sistem perbankan dan merusak data *base* bank.[5]

Dalam kasus-kasus yang berhubungan dengan tindak pidana *cybercrime,* tidak sedikit dari pelakunya menggunakan fasilitas umum dalam mengakses media elektronik dengan menggunakan sambungan internet dengan memanfaatkan fasilitas di warung internet (warnet) atau fasilitas umum lainnya, hal ini tentu akan sangat menyulitkan proses penyelidikan untuk mengumpulkan alat bukti, karena untuk melakukan pelacakan pelaku itu dilaksanakan pada alamat server atau informasi IP *Address* dari perangkat yang digunakan. Tindak pidana *cybercrime* sangat berbeda dengan tindak pidana yang terjadi pada umumnya, khususnya yang berkaitan dengan pengumpulan alat-alat bukti yang berkaitan dengan saksi-saksi, karena pada umumnya para saksi belum tentu mengetahui keberadan lokasi dari pelaku.

Menurut Hendy Sumandi, dalam mengungkapkan tindak pidana *cyber crime* maka dibutuhkan fasilitas yang mampu menunjang kinerja aparat kepolisian/penyidik, fasilitas tersebut berupa laboratorium forensik komputer yang digunakan untuk mengungkapkan data-data yang bersifat digital serta merekam dan menyimpan bukti-bukti yang berupa soft copy (gambaran, program, html, suara dan lain sebagainya). Komputer forensik dikenal sebagai digital forensik, tujuannya ialah untuk mengamankan dan menganalisis bukti digital, serta memperoleh berbagai fakta yang objektif dari sebuah kejadian atau pelanggaran keamanan dari sistem informasi, berbagai fakta tersebut akan menjadi bukti yang akan digunakan dalam proses penegakan hukum.[6]

Menurut Sucipto, dengan adanya internet forensik, penyidik dapat mengetahui siapa saja orang yang mengirim email, kapan dan di mana keberadaan alamat pengirim berdasarkan server pengirim, dan dalam contoh lain kita bisa melihat siapa pengunjung websInformasi Transaksi Elektronikr secara lengkap dengan informasi IP *Address,* alat elektronik

[5] Aswan, *Tindak Pidana Penipuan Berbasis Transaksi Elektronik,* Bogor : Guapedia, 2019, hlm. 51.
[6] J. Anhar Rabi Hamsah Tis'ah, *Kejahatan Berbahasa (Language Crime),* Tasikmalaya : Langgam Pustaka, 2022, hlm. 41-42.

yang dipakainya dan keberadaanya serta kegiatan apa yang dilakukan pada websInformasi Transaksi Elektronik tersebut.[7] Lemahnya konsep penegakan hukum merupakan faktor penyebab dari melonjaknya kasus *cybercrime* yang terjadi, sehingga diperlukan produk hukum baru yang bisa digunakan untuk mengatasi semua jenis kejahatan *cybercrime,* untuk memastikan stabilitas global, maka konsep hukum yang akan digunakan sebagai payung hukum dalam mengatasi tindakan *cybercrime* harus dimodifikasi untuk bisa mengkarateristikkan *cybercrime* sebagai suatu kejahatan agresif di tengah kemajuan teknis.[8]

Berdasarkan hal itu, untuk mengatasi melonjaknya tindakan *cybercrime,* pemerintah telah menetapkan Undang-Undang Nomor 8 tahun 2011 tentang Informasi Transaksi Elektronik sebagaimana telah diubah menjadi Undang-Undang Nomor 19 tahun 2016, yang secara khusus mengatur tentang kejahatan *cyber* pada Pasal 27 sampai Pasal 30. Undang-Undang ini memiliki jangkaun yuridiksi yang sangat luas. Pada pokoknya, di dalam ketentuan tersebut telah mengatur mengenai perbuatan hukum yang dilakukan di Indonesia dan/atau dilakukan oleh warga negara Indonesia, tetapi juga dapat berlaku untuk perbuatan hukum yang dilakukan di luar wilayah negara Indonesia dan/atau dilakukan oleh warga negara Indonesia ataupun warga negara asing.[9]

Terdapat beberapa kekurangan dalam Undang-Undang Informasi Transaksi Elektronik yang perlu untuk kembali disempurnakan, mengingat *cybercrime* ini tidak dibatasi oleh teritorial suatu negara. Penegakan hukum bagi kejahatan *hacking* ini memiliki jangkauan yang sangat luas tanoa mengenal batas wilayah teritorial suatu negara dikarenakan kejahatan *hacking* ini bersifat transnasional. Tipe kejahatan semacam ini sama dengan kejahatan-kejahatan lain dalam dunia maya, dimana kejahatan itu tidak mengenal batas dan mengharuskan suatu yuridiksi suatu negara terlibat langsung didalamnya, karena sangat jauh dari jangkauan suatu negara,

[7] *Ibid*
[8] Ardiansyah, *Hukum Administrasi Negara Fenomena Hukum di Ruang Publik,* Yogyakarta : Deepublish, 2022, hlm. 129.
[9] Ardison Asri, *Tindak Pidana Khusus,* Bojong Genteng : Jejak, 2022, hlm. 138.

sehingga diperlukan kerja sama antar negara dalam melakukan pemberantasan serta penegakan hukum yang sesuai karena kejahatan yang bersifat transnasional akan menimbulkan masalahnya sendiri dengan yuridiksinya.[10]

Berdasarkan pengalaman empiris sebelum diberlakukannya Undang-Undang Informasi Transaksi Elektronik, aturan hukum yang paling sering digunakan di Indonesia ketika terjadinya *cybercrime* adalah aturan hukum positif yakni KUHP dan KUHAP. KUHP khususnya masih cukup dipandang sebagai landasan hukum yang cukup memadai. Dalam praktik di Indonesia, tindak pidana dengan menggunakan komputer sejak dahulu merupakan salah satu jenis kejahatan yang sangat sulit untuk diklasifikasikan sebagai tindak pidana, hal ini dikarenakan dengan berlakunya Pasal 1 ayat 1 KUHP yang merupakan asas legalitas bahwa tidak ada satupun perbuatan yang dapat dipidana jika belum da suatu peraturan yang mengaturnya (*nullum delictum noela poena sine pravia lege poenali),* untuk itu ketentuan Pasal 1 ayat 1 KUHP ini menjadi penghambat dalam penegakan hukum di bidang kejahatan siber.[11]

Sebelum diberlakukannya Undang-Undang Informasi Transaksi Elektronik, aparat hukum menggunakan KUHP dalam menangani kasus-kasus kejahatan dunia siber, dimana ketentuan-ketentuan yang terdapat dalam KUHP tentang *cybercrime* tersebut masih bersifat global, adapun dari Teguh Arifiady, mengkategorikan beberapa hal secara khusus diatur dalam KUHP dan disusun berdasarkan tingkat intensitas terjadinya kasus tersebut yaitu. :[12]

1. Ketentuan yang berkaitan dengan delik pencurian Pasal 362 KUHP;
2. Ketentuan yang berkaitan dengan pornografi Pasal 282 KUHP;
3. Ketentuan yang berkaitan dengan penipuan Pasal 378 KUHP;
4. Ketentuan yang berkaitan dengan penghinaan Pasal 311 KUHP;
5. Ketentuan yang berkaitan dengan pembocoran rahasia Pasal 112 KUHP, Pasal 113 KUHP dan Pasal 114 KUHP.

[10] Hardi Fardiansyah, *et.all, Cyber Crime Paling Populer Pada Era Digital,* Bandung : Media Sains Indonesia, 2022, hlm. 57.
[11] Maskun, *Kejahatan Siber (Cyber Crime) Suatu Pengantar,* Jakarta : Kencana, 2013, hlm. 62.
[12] Dicky Nofriansyah, *et.all, Bisnis Online : Strategi dan Peluang Usaha,* Medan : Yayasan Kita Menulis, 2020, hlm. 138.

Salah satu tindakan *cyber crime* yang sangat menimbulkan kerugian adalah tindakan peretasan data seseorang. Sebab tindakan itu bisa sangat memberikan kerugian baik itu berupa materiil dan nonmateril, regulasi mengenai perlindungan data pribadi di Indonesia secara teknis merujuk pada Peraturan Pemerintah Nomor 71 tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PSTE), Peraturan Menteri Kominfo Nomor 20 tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik. Tujuan dari tindakan *hacking* adalah untuk mengambil data-data tertentu yang dimiliki oleh korban tanpa izin, namun ada juga tindakan peretasan data dengan menghancurkan atau merusakan sistem-sistem tertentu sehingga berdampak pada kerusakan digital. Secara eksplisit, tindakan peretasan data telah terlebih dahulu diatur dalam Pasal 28 G ayat 1 Undang-Undang Dasar 1945 dan secara khusus diatur dalam Pasal 30 ayat 1,2, dan 3 Undang-Undang Undang-Undang Nomor 8 tahun 2011 tentang Informasi Transaksi Elektronik sebagaimana telah diubah menjadi Undang-Undang Nomor 19 tahun 2016.

Pelanggaran terhadap Pasal 30 Undang-Undang Informasi Transaksi Elektronik tersebut akan dipidana dengan Pasal 46, Undang-Undang ini juga memberatkan dengan menjatuhkan pidana atas tindakan peretasan, yaitu disesuaikan dengan objek dan subjek tindakan peretasan, jika didasarkan pada objeknya maka akan diberatkan dengan Pasal 52 ayat 2 dan ayat 3, sedangkan pemberatan pidana terhadap subjeknya diatur dalam Pasal 52 ayat 4. Berdasarkan uraian tersebut maka jelas jerat hukuman terhadap kejahatan *hacking* dipertanggungjawabkan berdasarkan ketentuan yang tercantum dalam Pasal 30 Undang-undang Informasi dan Transaksi Elektronik.[13]

Dikarenakan semakin meningkatknya kasus penyalahgunaan dan kebocoran data, pemerintah dirasa perlu membuat suatu aturan baru yang bisa memberi ruang privasi dan perlindungan data sebagai bentuk mekanisme hukum dalam memberikan perlindungan terhadap modus-modus baru kejahatan dunia maya. Kejahatan dengan memanfaatkan teknologi

[13] Hardi Fardiansyah, *Op.Cit,* hlm. 55.

informasi sulit untuk dilakukan penegakan hukum melalui pendekatan sistem hukum konvensional karena berkaitan dengan proses pembuktiaanya, sebab kejahatan dunia maya sangat rentan untuk diubah, disadap, dipalsukan, dan dikirim ke berbagai penjuru dunia dalam waktu yang cepat.

Walaupun dengan hadirnya Undang-Undang Undang-Undang Nomor 8 tahun 2011 tentang Informasi Transaksi Elektronik sebagaimana telah diubah menjadi Undang-Undang Nomor 19 tahun 2016 dan peraturan perundang-undangan lainnya yang bersifat konvensional serta belum diatur secara komprehensif, maka dengan telah disahkannya Undang-Undang Nomor 27 tahun 2022 tentang Perlindungan Data Pribadi (PDP), diharapkan dapat mengatasi permasalahan pencurian data dan memberikan perlindungan data secara komprehensif, dengan adanya aturan baru ini bisa menjadi payung hukum bagi para penegak hukum dalam mengatasi tindakan para pelaku kejahatan siber di Indonesia khususnya dalam perlindungan data pribadi.

Sebagaimana kasus yang terjadi saat ini dan telah menjadi perbincangan publik mengenai kasus *hacker* Bjorka yang dapat mengakses data-data di situs digital dari data Kementrian Kominfo, data-data para pejabat dan Badan Intelejen Negara (BIN). Berikut ini adalah 10 data yang telah di unggah oleh *hacker* Bjorka diantaranya adalah [14]:

1. Indihome, Telkom
2. 1.3 Miliar data sim Card ponsel
3. 105 Juta data WNI dari KPU
4. Surat-surat untuk Presiden Jokowi
5. Data pribadi Menteri Komunikasi dan Informatika (Kominfo) Johnny G. Plate
6. Data pribadi Dirjen Kominfo Semuel Abrijani
7. Data pribadi Mentri Kominfo Luhut Binsar Pandjaitan
8. Data pribadi ketua DPR Puan Maharani
9. Data pribadi Menteri BUMN Erick Thohir

[14] https://www.google.com/amp/s/katadata.co.id/amp/desysetyowati/digital/631ed1b16b6d2/deretan-langkah-pemerintah-untuk-menangkap-hacker-Bjorka diakses pada 10 Oktober 2022

10. Data pribadi pegiat media sosial Denny Siregar.

Adapun dari pihak Telkom telah melakukan investigasi internal terkait adanya dugaan 26.730.797 data histori *browsing* pelanggan Indihome yang bocor termasuk didalamnya mengenai data berupa KTP, Email, nomor ponsel,kata kunci, domain, *platfrom,* dan URL. Terhadap pencurian data tersebut, dijual oleh *hacker* Bjorka di Breanche.to, setelah ditelusuri, hasilnya dari 15%-20% dari dua juta sampel yang diberikan oleh Bjorka ternyata valid.[15] Tindakan *hacker* Bjorka ini dapat dikenakan pasal berlapis karena telah melanggar Pasal 30 ayat 1 sampai ayat 3 Undang-Undang Informasi Tranksasi Elektronik dan Pasal 67 ayat 1 sampai ayat 3 Undang-Undang Perlindungan Data Pribadi. Jika dilihat berdasarkan kajian hukum, tindakan peretasan data pribadi yang dilakukannya sangat jelas telah melanggar hukum, akibat perbuatannya masyarakat kini menjadi korban atas eksploitasi data seperti pembocoran data pengguna layanan internet dan registrasi SIM Card. Untuk mengatasi terulangnya kembali tindakan pencurian data dimasa yang akan mendatang, perlu adanya *emergency response team* yang dapat bertugas cepat untuk menjaga tata kelola data dengan baik serta melakukan pembenahan dalam pertahanan sistem informasi lembaga pemerintah sehingga bisa lebih kokoh dan terintegrasi sebagaimana yang telah diterapkan di beberapa negara maju lainya.

Berdasarkan uraian-uraian yang telah dijelaskan sebelumnya mengenai tindakan peretasan data yang seringkali terjadi membuktikan kelemahan pemerintah dalam menjaga sistem keamanan siber, pemerintah tidak memiliki ketegasan dalam mengatasi kebocoran data dengan belajar dari kasus-kasus sebelumnya, dengan begitu ada kemungkinan kedepannya peristiwa kebocaran data akan terus berulang di Institusi dan lembaga pemerintah lainnya Indonesia. untuk itulah penulis merasa tertarik untuk melakukan suatu penelitian yang disajikan dalam bentuk skripsi yang berjudul "**PENEGAKAN HUKUM TERHADAP KASUS PERETASAN DATA PRIBADI YANG DILAKUKAN OLEH BJORKA"**

[15] *Ibid*

1.2 Rumusan Masalah

Terhadap identifikasi masalah diatas, maka yang akan dInformasi Transaksi Elektronikliti dalam penelitian ini berkaitan dengan :

1. Bagaimana upaya penegakan hukum yang dapat dilakukan dalam menangani kasus peretasan data pribadi yang dilakukan oleh Bjorka ?
2. Bagaimana pertanggungjawaban pidana terhadap kejahatan siber peretasan data yang dilakukan oleh *hacker* Bjorka jika ditinjau dari Undang-Undang Nomor 19 tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi elektronik ?

1.3 Tujuan Penelitian

Suatu penelitian dilakukan karena mempunyai tujuan yang diharapkan dapat menyajikan sejumlah data yang bersifat akurat, sehingga bisa menjadi acuan untuk memberikan solusi bagaimana caranya mengatasi persoalan-persoalan yang relevan dengan masalah yang sedang diteliti, sehingga kedepannya dapat memberikan manfaat dalam menyelesaikan masalah, adapun tujuan dilaksanakan penelitian ini adalah untuk mengetahui:

1. Untuk upaya penegakan hukum yang dapat dilakukan dalam menangani kasus peretasan data pribadi yang dilakukan oleh Bjorka !
2. Untuk mengetahui pertanggungjawaban pidana terhadap kejahatan siber peretasan data yang dilakukan oleh *hacker* Bjorka jika ditinjau dari Undang-Undang Nomor 19 tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi elektronik.

1.4. Manfaat Penelitian

1.4.1. Manfaat Teoritis

1. Diharapkan dari hasil penelitian ini bisa menjadi memberikan wawasan lebih bagi seluruh lapisan masyarakat mengenai

pentingnya perlindungan data pribadi dalam melindungi privasi masing-masing individu;

2. Diharapkan dari hasil penelitian ini dapat menjadi bahan hukum ilmiah yang bisa dipergunakan dikemudian hari dalam rangka menunjang perkembangan serta proses pencegahan dan penegakan hukum terhadap tindakan peretasan data.

1.4.2. Manfaat Praktis

1. Dapat menjadi bahan masukan kepada pemerintah untuk bisa membenahi proses penanganan tindakan peretasan data sehingga tidak akan terulang kembali;
2. Diharapkan dari hasil penelitian ini dapat menjadi bentuk solusi terhadap penanganan tindakan peretasan data di Indonesia yang seringkali terjadi dengan memberikan sumbangan pemikiran dari sudut pandang penulis.

1.5. Kerangka Konseptual

1. Peretasan Data mengacu pada aktivitas yang berupaya mengakses secara ilegal perangkat digital, seperti komputer, ponsel cerdas, tablet, dan bahkan selururh jaringan.[16]
2. Perlindungan data adalah hubungan antara perolehan, pengumpulan, pengolahan, penganalisisan, penyimpanan, penampilan, pengumpulan, pengiriman, penyebarluasan dan pemusnahan data, serta masalah hukum dan politik yang melingkupinya. Perlindungan data juga dikenal sebagai privasi data.[17]
3. *Cybercrime* adalah aktivitas kriminal yang melibatkan komputer, perangkat jaringan atau jaringan. Sementara sebagian besar kejahatan dunia maya dilakukan untuk menghasilkan keuntungan bagi penjahat dunia maya. Beberapa kejahatan dunia maya dilakukan terhadap komputer atau perangkat secara langsung untuk merusak atau menonaktifkannya, sementara yang lain menggunakan komputer atau jaringan untuk menyebarkan malware, informasi ilegal, gambar atau

[16] https:app.nfbsbogor.sch.id/helpdesk/knowledgebase.php?article 5 Oktober 2022
[17] https://id.m.wikipedia.org/wiki/Perlindungan_data diakses pada 5 Oktober 2022

materi lainnya. Beberapa *cybercrime* akan melakukan beberapa hal berupa menargetkan komputer untuk menginfeksinya dengan virus kemudian menyebarkan ke mesin lain dan seluruh jaringan.[18]

4. *Hacker* pada awalnya adalah kata pelengkap untuk penggemar komputer, namun kini mengacu pada suatu perilaku negatif, yakni melakukan pengaksesan komputer atau jaringan secara tidak resmi. Biasanya para *hacker* menganggap bahwa apa yang dilakukan hanya untuk menguji pengamanan.[19]
5. Pertanggungjawaban pidana atau *criminal responsibility* artinya orang yang telah melakukan suatu tindak pidana belum berarti harus dipidana, ia harus mempertanggungjawabkan perbuatan yang telah dilakukannya, jika ditemukan unsur kesalahan padanya.[20]

1.6. Kerangka Teoritis

1.6.1. Teori Penegakan Hukum

Penegakan hukum pada hakikatnya adalah usaha-usaha untuk mewujudkan ide-ide hukum yang abstrak yaitu keadilan, kepastian hukum dan kemanfaatan sosial menjadi suatu kenyataan, di mana usaha tersebut membutuhkan adanya organisasi, badan atau lembaga seperti kepolisian, kejaksaan, pengadilan dan lembaga pemasyarakatan sebagai unsur yang dibentuk oleh negara. Meskipun badan-badan tersebut tampak berdiri sendiri-sendiri namun mengemban tugas yang sama yaitu mewujudkan ide-ide hukum dalam masyarakat.[21]

Penegakan hukum secara konkrit berarti pelaksanaan dan tindaklajut dari adanya ketentuan hukum yang berwujudkan peraturan perUndang-Undangan yang telah dipilih dan ditetapkan sebagai sarana untuk mengatur kehidupan bermasyarakat, bernegara dan berbangsa yang dilaksanakan oleh aparatur negara khususnya penegak hukum, dalam

[18] Hendro Wijayanto, *Op.Cit*, hlm. 6.
[19] Beranda Agency, *Pengamanan Total Data dan Informasi Penting,* Jakarta : Elex Media Komputindo, 2011, hlm. 2.
[20] Hasbullah F. Sjawie, *Loc.Cit*
[21] Rahman Amin, *Perlindungan Hukum Justice Collaborator dalam Sistem Peradilan Pidana di Indonesia : Studi Perkara Tindak Pidana Narkotika,* Yogyakarta : Deepublish, 2020, hlm. 26.

penegakan hukum sangatlah penting memperhatikan komponen-komponen yang terdapat dalam sistem hukum yakni struktur, substansi dan kultur hukum sehingga dalam penegakan hukum dapat terlaksana dengan baik.[22] Penegakan hukum itu merupakan suatu hal yang sangatlah esensial dan subtansial dalam konsep suatu negara hukum seperti Indonesia. Prinsip dasar negara hukum ada tiga yaitu supremasi hukum, persamaan di muka hukum, dan penegakan hukum. Di dalam suatu negara hukum, peran hakim menduduki tempat yang strategis, karena putusan yang dihasilkannya dapat menjadi suatu sumber hukum yang mencerminkan gerak dinamis permasalahan hukum yang tumbuh di masyarakat. [23]

Penegakan hukum pada umumnya dikenal sebagai suatu upaya dalam menegakan suatu ketentuan hukum yang berlaku, yang berkaitan dengan hukum pembuktian sebagai bagian dari hukum acara dalam menegakan ketentuan hukum materil, bahwa dalam melaksanakan penegakan hukum itu tidak terlepas dari upaya pembuktian dengan tujuan agar suatu perkara yang terjadi dapat dijatuhkan putusan yang seadil-adilnya selain memberikan kepastian dan kemanfaatan dari hukum itu sendiri. Jika berbicara mengenai penegakan hukum maka berkaitan erat dengan para penegak hukum dalam menegakan hukum yang berlaku di Indonesia sehingga dapat tercipatanya kehidupan masyarakat yang aman, tentran dan damai. [24]

Jika berbicara mengenai penegakan hukum itu berarti berkaitan dengan proses penegakan ketentuan hukumnya, dimana yang secara umumnya hukum itu merupakan seperangkat aturan yang berisikan perintah-perintah serta larangan yang sifatnya itu mengikat, serta bisa mendapatkan sanksi yang tegas jika dilanggar. Menurut Sajipto Rahardji, penegakan hukum pada hakikatnya adalah usaha-usaha untuk

[22] *Ibid,* hlm. 27.
[23] Siti Chormarijah Lita Samsi, *Integritas Hakim dalam Menghasilkan Putusan Tindak Pidana Korupsi,* Yogyakarta : Deepublish, 2019, hlm. 10.
[24] Rahman Amin, *Hukum Pembuktian dalam Perkara Pidana dan Perdata,* Yogyakarta : Deepublish, 2020, hlm.1.

mewujudkan ide-ide hukum yang abstrak yaitu keadilan, kepastian hukum dan kemanfaatan sosial mejadi suatu kenyataan, dimana usaha tersebut membutuhkan adanya organisasi, badan atau lembaga seperti kepolisian, kejaksaan, pengadilan dan lembaga pemasyarakatan sebagai unsur yang terbentuk oleh negara. Meskipun badan-badan tersebut berdiri sendiri-sendiri namun mengemban tugas yang sama yaitu untuk mewujudkan ide-ide hukum dalam kehidupan masyarakat.[25] Menurut Sajipto Rahardjo bahwa seyogyanya dalam proses praktik penegakan hukum yang sangat perlu untuk dikembangakan adalah penegakan hukum yang mengharuskan aparatur penegak hukum untuk bertumpu pada nilai-nilai keadilan yang berkembang dalam masyarakat, terlebih lagi jika norma hukum positif yang sedang berlaku tidak sesuai dengan rasa keadilan masyarakat yang disebut sebagai model hukum progresif. Menurut Sajipto Rahardjo bahwa model hukum yang progresif akan sangat menuntut keberanian dari aparatur penegak hukum untuk melakukan berbagai terobosan-terobosan hukum (*legal breakthrought),* bukan *law breaking,* dan menurutnya bahwa hukum yang progresif itu bertujuan untuk mencari cara dalam mengatasi kondisi keterpurukan hukum di Indonesia secara lebih bermakna (bermartabat) dengan mengadakan perubahan secara lebih cepat, melakukan pembalikan yang mendasar, melakukan pembebasan, terobosan dan lainnya. [26]

Pada intinya, penegakan hukum sebagaimana yang telah dirumuskan secara sederhana oleh Sajipto Rahardjo, merupakan suatu proses untuk dapat mewujudkan keinginan-keinginan hukum untuk menjadi kenyataan. Keinginan-keinginan hukum yang dimaksudkan yakni pikiran-pikiran dari badan pembentuk Undang-Undang yang dirumuskan dalam setiap peraturan-peraturan hukum itu, dengan adanya perumusan pikiran pembuat yang telah dituangkan dalam peraturan hukum akan turut serta dalam menentukan bagaimana penegakan hukum

[25] *Ibid,* hlm.3
[26] Golkar Pangarso, *Penegakan Hukum Perlindungan Ciptaan Sinematografi di Indonesia,* Bandung : Alumni, 2022, hlm. 70.

itu akan dijalankan, dengan demikian pada gilirannya, proses penegakan hukum itu akan memuncak pada pelaksanaanya oleh para pejabat penegak hukum itu sendiri, sehingga untuk keberhasilan maupun kegagalan para penegak hukum dalam melaksanakan tugasnya sebetulnya sudah dimulai sejak peraturan hukum yang harus dijalankan itu dibuat. Terdapat beberapa unsur yang sangat berpengaruh dalam proses penegakan hukum yang didasarkan kepada derajat kedekatannya pada suatu proses yakni yang agak jauh dan yang agak dekat, berdasarkan kriteria kedekatan tersebut, maka Sajipto Rahardjo telah membedakan tiga unsur utama yang terlibat dalam proses penegakan hukum, yaitu unsur pembuatan Undang-Undang yakni lembaga legistalitif, unsur penegakan hukumnya yakni polisi jaksa dan hakim, dan unsur lingkungan yang meliputi pribadi warga negara dan sosial. [27]

1.6.2. Pertanggungjawaban Pidana

Pertanggungjawaban pidana sangat diperlukan dalam suatu sistem hukum pidana dalam hubungannya dengan prinsip *daad daderstrafs recht.* KUHP Indonesia sebagaimana halnya WvS yang berlaku di negara Belanda tidak mengatur secara khusus tentang pertanggungjawaban pidana, tetapi hanya mengatur tentang keadaan-keadaan yang mengakibatkan tidak dipertanggungjawabkannya pembuat. Tidak dipertanggungjawabkannya pembuat hanya dijelaskan dalam *Memorie van Toelichting (*MvT*)* bahwa seorang pembuat tidak dipertanggungjawabkan apabila memenuhi syarat-syarat tertentu. Ini menandakan bahwa pertanggungjawaban pidana di dalam KUHP diatur secara negatif, yaitu dengan keadaan-keadaan tertentu pada diri pembuat atau perbuatan mengakibatkan tidak dipidananya pembuat.[28]

Syarat tidak dipertanggungjawabkannya pembuat adalah pada saat pembuat melakukan tindak pidana, tetapi karena adanya faktor dalam diri pembuat maupun faktor di luar diri pembuat. Seseorang yang

[27] Erma Rusdiana, *Pertanggunggjawaban Pidna Partai Politik sebagai Badan Hukum,* Surabaya : Scopindo, 2021, hlm. 63.
[28] Agus Rusianto, *Tindak Pidana dan Pertanggungjawaban Pidana Tinjauan Kritis Melalui Konsistensi Antara Asas, Teori dan Penerapannya,* Jakarta : Kencana, 2016, hlm. 1.

telah melakukan tindak pidana tidak akan dipidana apabila dalam keadaan yang sedemikian rupa sebagaimana yang dijelaskan di dalam MvT. Apabila pada diri seorang pembuat tidak terdapat keadaan sebagaimana yang diatur dalam MvT tersebut, pembuat adalah orang yang dipertanggungjawabkan dan dijatuhi pidana.[29]

Kesalahan dan pertanggungjawaban pidana, masih menyisakan berbagai persoalan dalam hukum pidana karena belum adanya kesamaan pola dalam menentukan kesalahan dan pertanggungjawaban pembuat tindak pidana. Menurut Schaffmeister bahwa penggunaan kesalahan sebagai dasar pemidanaan bukan keharusan menurut Undang-Undang yang empiris, tetapi asas normatif. Konsekuensinya seolah-olah memang tidak ada standar dalam menentukan kesalahan dan pertanggungjawaban pidana, sedangkan menurut Curzon bahwa untuk dapat mempertanggungjawabkan seseorang dan karenanya mengenakan pidana terhadapnya tidak boleh ada keraguan sedikitpun pada diri hakim tentang kesalahan terdakwa.[30]

Adanya kesalahan merupakan unsur mutlak yang bisa mengakibatkan dimintakannya pertanggungjawaban pidana dari di pelaku delik. Pertanggungjawaban atas tindak pidana yang dilakukan oleh seseorang itu adalah untuk menentukan kesalahan dari tindak pidana yang ia lakukan. Pertanggungjawaban pidana hanya dapat terjadi setelah sebelumnya dia melakukan tindak pidana. Jadi, tindak pidana dipisahkan dari pertanggungjawaban pidana, atau dipisahkan dari unsur kesalahan. Berkaitan dengan pertanggungjawaban pidana, seseorang hanya dapat dibebani tanggungjawab pidana bukan hanya karena dia telah melakukan perbuatan yang dilarang atau melanggar kewajiban yang dipersyaratkan Undang-Undang, yang harus dibuktikan penuntut umum, tetapi juga bahwa pada saat perbuatan itu dilakukan, pelakunya harus memiliki *mens rea,* atau sikap kalbu. Hal ini merupakan salah satu ciri dari hampir semua sistem hukum, dimana tanggung jawab pelaku atas tindak pidana

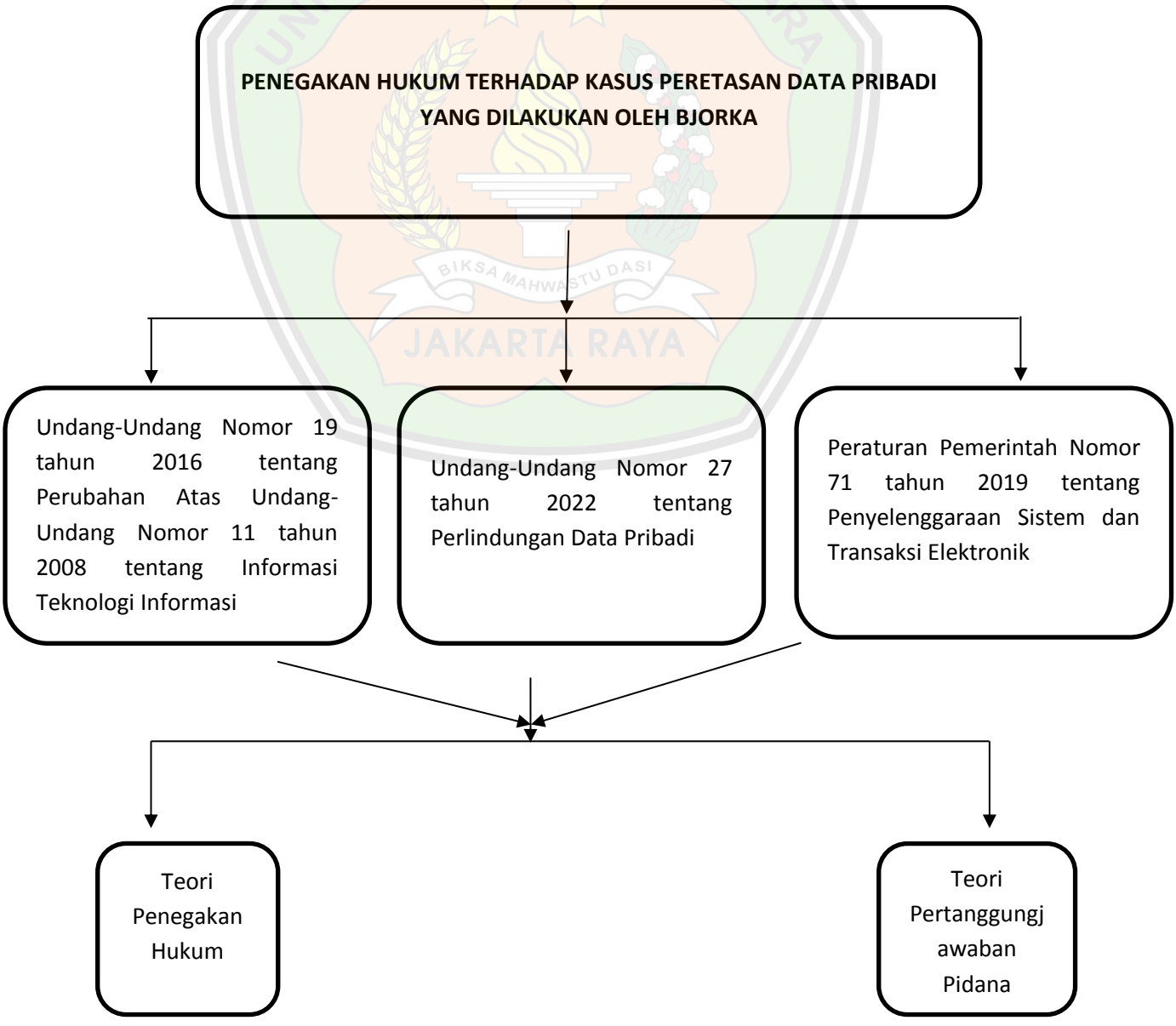
[29] *Ibid,* hlm. 2.
[30] Chairul Huda, *Dari Tiada Pidana Tanpa Kesalahan Menuju Kepada Tiada Pertanggungjawaban Pidana tanpa Kesalahan,* Jakarta : Kencana, 2015, hlm. 2.

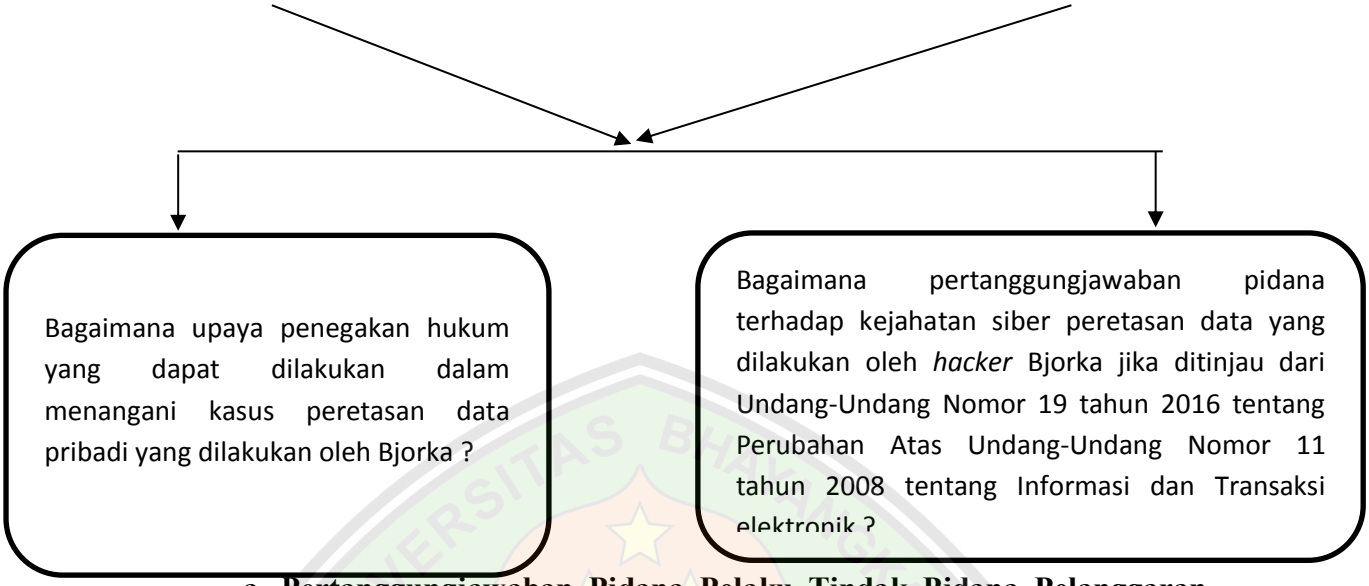
yang telah dilakukannya selalu dikaitkan pada keadaan-keadaan tertentu dari mentalnya.[31]

Menurut Jan Remmeink, persyaratan yang harus dipenuhi untuk menghukum seseorang sekaligus memenuhi tuntutan keadilan dan kemanusiaan, harus ada suatu perbuatan yang bertentangan dengan hukum dan dipersalahkan kepada pelakunya. Tambahan pada syarat-syarat ini adalah pembuat harus merupakan seseorang yang mampu bertanggungjawab (*toerekeningsvatbaar)* atau *schuldfahig.* Syarat-syarat mampu bertanggungjawab diabstraksikan bahwa tindak pidana merupakan perilaku manusia. Menurut pandangan teori dualistis, kemampuan bertanggungjawab hanya disyaratkan apabila pembuat tindak pidana adalah seorang manusia. Syarat-syarat ini merupakan syarat yang umum merupakan pengertian tindak pidana, karena dalam tindak pidana semua syarat termasuk sebagai unsur tindak pidana. Hanya saja untuk menjatuhkan pidana kepada pembuat harus memenuhi syarat-syarat umum tersebut berupa unsur-unsur perbuatan yang bersifat melawan hukum dan kesalahan, serta adanya kemampuan bertanggungjawab, namun demikian dalam merumuskan unsur dalam Undang-Undang tidak selalu menyinggung syarat-syarat umum tersebut.[32]

[31] Hasbullah F. Swajie, *Direksi Perseroan Terbatas Serta Pertanggungjawaban Pidana Korporasi,* Jakarta : Kencana, 2017, hlm. 258.
[32] Agus Rusianto, *Op.Cit,* hlm. 67.

1.7. Kerangka Konseptual





a. Pertanggungjawaban Pidana Pelaku Tindak Pidana Pelanggaran Pasal 30 Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik

Oleh Kartika Ulan Sari, Fakultas Hukum Universitas Sriwijaya Indralaya 2020

Tindak pidana merupakan tindakan yang dilarang oleh suatu aturan hukum yang disertai dengan ancaman sanksi berupa pidana tertentu bagi pelanggarnya. Peretasan yang dilakukan dengan menjebol, melampaui atau menerobos sistem elektronik yang digunakan oleh pemerintah atau untuk informasi publik merupakan tindak pidana yang dilakukan untuk ketenaran maupun keisengan hacker, yang diakomodir dalam Pasal 46 Ayat (3) Jo Pasal 30 Ayat (3) Undang-Undang RI No. 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang RI No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. Dengan latar belakang tersebut penulis mengangkat judul tentang Pertanggungjawaban Pidana Pelaku Tindak Pidana Pelanggaran Pasal 30 Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. Dengan rumusan masalah Bagaimana pertanggungjawaban pidana dan Bagaimana penerapan unsur-unsur

pertanggungjawaban pidana dalam tindak pidana pelanggaran Pasal 30 Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. Untuk menjawab masalah tersebut penulis menggunakan metode

penelitian normatif, hasil dari penelitian ini menyatakan kesimpulan bahwa pertangungjawaban pidana pelaku penjebolan keamanan sistem elektronik dalam bentuk pertanggungjawaban pidana atas dasar kesalahan didasarkan pada Undang-Undang Informasi dan Transaksi Elektronik serta penerapan unsur-unsur pertanggungjawaban pidana meliputi unsur subjektif dan unsur objektif dari tindak pidana tersebut telah terpenuhi sehingga hakim menjatuhkan putusan pidana penjara dan pidana denda kepada pelaku dengan pemberatan berupa pidana pokok ditambah sepertiga karena dilakukan terhadap sistem elektronik milik pemerintah.

b. **Pertanggungjawaban Pidana Terhadap Cyber Crime Berupa Penyebaran Virus Yang Mengakibatkan Terganggunya Sistem Elektronik**

Oleh Dhenok Qonita Zanuba, Fakultas Hukum Universitas Sriwijaya Indralaya 2021

eiring berkembangnya zaman, manusia dan teknologi sudah dapat dikatakan seperti hidup berdampingan. Semakin maju suatu teknologi tidak menutup kemungkinan bahwa akan semakin berkembang pula tingkat cyber crime atau kejahatan siber. Cyber crime sendiri memiliki berbagai jenis mulai dari peretasan, pencurian data, sampai dengan penyebaran virus. Pada penulisan skripsi ini, permasalahan yang akan dibahas adalah: 1. Bagaimana pertanggungjawaban pidana terhadap kasus cyber crime berupa penyebaran virus yang mengakibatkan terganggunya sistem elektronik dalam putusan nomor 730/Pid.Sus/2018/PN.JKT.PST. 2. Bagaimana pula pertimbangan hakim terhadap kasus cyber crime berupa penyebaran virus yang mengakibatkan terganggunya sistem elektronik dalam putusan nomor 730/Pid.Sus/2018/PN.JKT.PST tersebut. Dengan demikian metode

penelitian yang digunakan dalam penulisan skripsi ini yaitu yuridis normatif. Hasil penelitian skripsi ini dapat dapat menunjukkan bahwa Terdakwa terbukti secara sah dan meyakinkan telah melakukan suatu tindak pidana yang dengan sengaja dan melawan hukum berupa menyebarkan virus yang dapat mengakibatkan terganggunya sistem elektronik sehingga dapat dipidana.

c. **Sanksi Tindak Pidana *Hacking* (Studi Analisis Undang Undang Ite Dan Hukum Pidana Islam)**

Oleh Rizki Arfah, Fakultas Syari'ah Dan Hukum Universitas Islam Negeri Sumatera Utara Medan 2019

Tindak pidana penyadapan informasi elektronik menurut UU ITE adalah kegiatan untuk mendengarkan, merekam, membelokkan, mengubah, menghambat, dan/atau mencatat transmisi Informasi Elektronik dan/atau Dokumen Elektronik yang tidak bersifat publik, baik menggunakan jaringan kabel komunikasi maupun jaringan nirkabel, seperti pancaran elektromagnetis atau radio frekuensi. Peraturan yang mengatur perbuatan tersebut adalah Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik pada Pasal 31 ayat (1) sampai ayat (2) dengan sanksi pidana yang dimuat dalam Pasal 47 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Menurut Hukum Pidana Islam kejahatan hacking adalah kejahatan yang baru sehingga kejahatan hacking secara mendasar tidak ada aturan hukum islam yang mengatur, sehingga penulis menggunakan qiyas (salah satu sumber hukum islam) yaitu Ilegal akses dengan surah An-Nur ayat 27 yang intinya melarang orang memasuki rumah milik orang lain tanpa izin dari pemilik rumah dan surah Al-Maidah ayat 38 untuk pencurian data.

d. **Pertanggungjawaban Pidana Cracker Yang Melakukan Peretasan Website Presiden Ditinjau Dari Undang-Undang No. 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik (Studi Kasus Putusan Pengadilan Negeri Jember Nomor: 253/Pid.B/2013/PN JR)**

Oleh Fildza Ramadiansyah, Universitas Pembangunan Nasional Veteran Jakarta, 2016

Cyber Crime berkembang di Indonesia dikarenakan teknologi yang berkembang sangat pesatnya, tindak pidana cyber crime di Indonesia bukanlah suatu hal yang baru, dikarenakan semakin pesatnya teknologi maka cyber crime pun semakin beragam, hal ini yang menjadi alasan Indonesia pada tahun 2008 mengganti UU Telekomunikasi menjadi UU ITE. Oleh karena semakin berkembangnya kejahatan tersebut. Oleh karena itu dalam penelitian ini mengangkat tentang bagaimana pertanggungjawaban pelaku tindak pidana cyber crime serta unsur-unsur kejahatan tersebut didalam UU ITE dan KUHP. Untuk mengatasi masalah ini penulis menggunakan teori pertanggungjawaban pidana. Penelitian ini menggunakan penelitian juridicial normative dengansumber utama adalah data sekunder. Kesimpulan dari penelitian ini adalah unsur-unsur cracking sebelum adanya UU ITE juga diatur dalam UU Telekomunikasi dan KUHP, Majelis Hakim dalam menjatuhkan pidana terhadap terdakwa dalam kasus ini dijatuhi pidana dengan pasal 46 ayat (1) jo. Pasal 30 ayat (1) UU ITE sebagai bentuk pertanggungjawaban pidana atas tindakannya tersebut.

e. **Tinjauan Yuridis Tindak Pidana Memindahkan Atau Mentransfer Informasi Elektronik Dan/Atau Dokumen Elektronik Milik Pemerintah Secara Melawan Hukum (Studi Putusan No. 527/Pid.Sus/2020/PN.SMN)**

Oleh: Putri Afifah Yushalia Faisal, Fakultas Hukum Universitas Hasanuddin Makassar 2022

Penelitian ini bertujuan untuk mengetahui kualifikasi tindak pidana memindahkan atau mentransfer informasi elektronik dan/atau dokumen elektronik milik pemerintah secara melawan hukum dan untuk mengetahui pertanggungjawaban pidana pelaku tindak pidana memindahkan atau mentransfer informasi elektronik dan/atau dokumen elektronik milik pemerintah secara melawan hukum berdasarkan pertimbangan hakim dalam putusan nomor

527/Pid.Sus/2020/Pn.Smn. Jenis penelitian yang digunakan adalah penelitian hukum normatif dengan pendekatan perundang-undangan dan pendekatan kasus. Bahan hukum yang digunakan terdiri dari peraturan perundang-undangan, buku hukum, jurnal, pandangan para ahli, dan hasil penelitian hukum yang kemudian dianalisis secara preskriptif. Hasil penelitian ini menunjukkan bahwa (1) Tindak pidana memindahkan atau mentransfer informasi elektronik dan/atau dokumen elektronik milik pemerintah secara melawan hukum diatur dalam Pasal 32 ayat (2) jo. Pasal 48 ayat (2) jo. Pasal 52 ayat (2) Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik (UU ITE). Tindak pidana tersebut dapat dikualifikasikan sebagai delik kejahatan, delik formil, delik komisionis, delik dolus, delik biasa, dan delik khusus. (2) Terdakwa mampu mempertanggungjawabkan perbuatannya mengingat Terdakwa tidak mengalami gangguan jiwa, seperti diatur pada Pasal 44 ayat (1) KUHPidana sehingga terbukti ada kemampuan untuk bertanggung jawab atas perbuatan pidana yang dilakukannya dan tidak ada alasan pemaaf , serta tidak adanya error in persona (syarat subjektif terpenuhi). Meskipun demikian, penulis memandang bahwasanya penerapan unsur pasal pada Tindak Pidana memindahkan atau mentransfer informasi elektronik dan/atau dokumen elektronik milik pemerintah secara melawan hukum pada Putusan Nomor 527/Pid.Sus/2020/Pn.Smn tidak tepat (syarat objektif tidak terpenuhi).

1.9. Metode Penelitian

1. Jenis Penelitian

Mengadakan suatu penelitian ilmiah harus menggunakan metode, karena ciri khas ilmu adalah dengan menggunakan metode. Metode berarti penyelidikan yang berlangsung menurut suatu rencana tertentu. Adapun metode penelitian yang digunakan oleh penulis adalah yuridis normatif yang merupakan suatu penelitian yang

difokuskan untuk mengkaji penerapan kaidah-kaidah atau norma-norma dalam hukum positif.[33]

Penggunaan jenis penelitian yuridis normatif atau biasa disebut doktrinal ini disebabkan dari landasan pada sifat atau karakter dari ilmu hukum yang bersifat spesifik atau khas yang terdapat dalam metode penelitiannya yang sifatnya normatif, dimana penelitian akan dilakukan dengan menganalisis prinsip-prinsip hukum yang merupakan pendapat atau pandangan para ahli hukum yang berkualifikasi tinggi, sehingga sifat dari penelitian ini adalah menggabungkan dua unsur pokok sebagai faktor analisis dalam suatu penelitian hukum, yaitu unsur norma atau kaidah dan unsur doktrin atau pendapat para ahli yang dapat disebut seabagai konsep hukum.[34]

2. Pendekatan Penelitian

Metode pendekatan yang digunakan dalam proses penelitian ini adalah yuridis normatif yang dilakukan melalui dua bentuk varian pendekatan, yang berupa :

1. Pendekatan Perundang-undangan

   Pendekatan Perundang-undangan (*statute approach)* merupakan penelitian yang mengutamakan bahan hukum yang berupa peraturan Perundang-undangan sebagai bahan acuan dasar dalam melakukan penelitian.[35] Dalam melakukan penelitian ini, penelitian dilaksanakan dengan melakukan pengkajian secara keseluruhan dari peraturan Perundang-undangan yang kemudian dilihat bagaimana implementasi aturan tersebut dalam menangani permasalahan yang sedang dikaji oleh peneliti sehingga bisa mendapatkan solusi atas permasalahan hukum yang sedang diteliti.

2. Pendekatan kasus

[33] Andriensjah, *Hak Desain Industri Berdasarkan Penilaian Kebaruan Desain Industri,* Bandung : Alumni, 2021, hlm. 40.

[34] Andika Persada Putra, *Hukum Perbankan Analisa Mengenai Perjanjian Kredit dan Keterkaitannya dengan Batalnya Perkawinan Debitur Serta Alternatif Penyelesaiannya,* Surabaya : Scopindo Media Pustaka, 2021, hlm. 12.

[35] Kadarudin, *Penelitian di Bidang Ilmu Hukum (Sebuah Pemahaman Awal),* Semarang : Formaci, 2021, hlm. 106.

Pendekatan kasus dilakukan dengan cara melakukan telaah terhadap kasus-kasus yang berkaitan dengan isu hukum yang sedang dihadapi yang telah mejadi putusan pengadilan dan telah mempunyai kekuatan hukum tetap.[36]

Tujuan dari menggunakan pendekatan Undang-Undang dan pendekatan kasus karena penulis akan melakukan pengkajian terhadap data sekunder berupa berbagai bahan kepustakaan yang terbagi atas bahan hukum primer, bahan sekunder dan bahan hukum tersier yang berkaitan dengan konsep hukum yang sedang diteliti oleh penulis. Selain itu, dengan menggunakan dua varian pendekatan ini dapat saling melengkapi antara satu pendekatan dengan pendekatan yang lainnya sehingga bisa melengkapi dan memperkaya hasil analisa kasus yang sedang dikaji.

3. Sumber Bahan Hukum

Sumber bahan hukum yang digunakan oleh penulis untuk mendukung penelitianini adalah data sekunder yang diperoleh dari data kepustakaan (*library research)* untuk bisa mendapatkan landasan teoritis terhadap objek permasalahan yang sedang diteliti, yang dimana dalam proses pengumpulan bahan hukumnya ini dilakukan dengan cara membaca, mempelajari, menganalisis, serta menelaah data-data yang masih relevan dengan objek permasalahan. Berikut ini adalah penggunaan sumber bahan hukum yang terdiri atas :

1. Bahan hukum primer :
    a. Kitab Undang-Undang Hukum Pidana
    b. Undang-Undang Nomor 19 tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 tahun 2008 tentang Informasi Teknologi Informasi;
    c. Undang-Undang Nomor 27 tahun 2022 tentang Perlindungan Data Pribadi

[36] Suharyono, *Hukum Pertahanan di Indonesia Progresifitas Sistem Publikasi Positif Terbatas dalam Pendaftaran tanah di Indonesia,* Malang : Cita Intrans Selaras, 2018, hlm. 45.

d. Peraturan Pemerintah Nomor 71 tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik;
e. Peraturan Pemerintah Nomor 82 tahun 2012 tentang Penyelenggara Sistem dan Transaksi Elektronik.

2. Bahan hukum sekunder yang berupa suatu publikasi atau karya ilmiah yang terdiri atas buku referensi, doktrin, jurnal, makalah, artikel dan berbagai bahan hukum sekunder lainnya yang bisa diperoleh berdasarkan studi kepustakaan (*library research).*
3. Bahan hukum tersier ini dapat dikatakan sebagai bahan hukum pelengkap yang memberikan petunjuk serta penjelasan terhadap bahan hukum primer dan juga sekunder. Untuk bahan hukum tersiernya ini diperoleh dari bahan-bahan yang menunjang bahan hukum primer dan sekunder, yang dapat berupa buku-buku, kamus hukum, ensiklopedia, dan lain sebagainya.

4. Metode Pengumpulan Bahan Hukum

Tenik pengumpulan bahan hukumnya itu berupa studi kepustakaan (*library research),* yang dapat dikatakan sebagai suatu kegiatan pengumpulan data serta informasi dari berbagai sumber, seperti buku yang memuat berbagai ragam kajian teori yang sangat dibutuhkan peneliti. Penggunaan studi kepustakaan ini didapatkan dengan cara membaca, mempelajari dan menganalisis berbagai aturan hukum dari bahan hukum yang relevan dengan objek permasalahan dengan menggunakan berbagai teori-teori pendukung atau pendapat para ahli hukum, sehingga bisa mendapatkan kesimpulan akhir atas landasan teoritis permasalahan yang sedang di teliti.

5. Metode Pengolahan dan Analisis Bahan Hukum

Terhadap semua kumpulan data-data yang telah diperoleh dalam penelitian ini selanjutnya akan dianalisa secara kualitatif dengan melakukan pengelompokan dan juga penyesuaian data-data yang telah didapatkan untuk bisa mendapatkan gambaran secara sistematis dengan didasarkan pada teori-teori yang digunakan,

sehingga bisa mendapatkan kesimpulan akhir yang dapat dipertanggungjawabkan secara ilmiah.