BAB I
PENDAHULUAN

A. Latar Belakang

Negara Indonesia adalah salah satu negara di dunia yang sedang mengalami perkembangan. Salah satu ciri perkembangan ini adalah dengan banyaknya program pembangunan di berbagai bidang kehidupan berbangsa, bernegara, dan bermasyarakat salah satunya perkembangan dalam dunia teknologi dan telekomunikasi.

Dewasa ini teknologi informasi dan komunikasi telah mengalami perkembangan yang begitu pesat di dunia, terutama di Indonesia yang tidak mau ketinggalan dalam hal penggunaan dan pemanfaatan kemajuan dibidang teknologi informasi dan komunikasi, hal ini dapat dilihat dari banyaknya masyarakat yang telah menggunakan alat komunikasi dan teknologi seperti komputer atau laptop, handphone, dan internet. Kemajuan teknologi ini telah membantu masyarakat dalam hal berkomunikasi lebih efektif dan memudahkan pekerjaan yang sulit menjadi lebih sederhana, sehingga penggunaan dan pemanfaatan teknologi informasi dan komunikasi hampir seluruh bidang kehidupan manusia telah menggunakan teknologi.[1]

Perkembangan dan kemajuan teknologi komputer dan telekomunikasi berupa media internet sebagai salah satu penyebaran informasi dalam kehidupan seharihari membawa dampak buruk berupa penyalahgunaan

[1] Ahmad, Amar. 2012. *Perkembangan Teknologi Komunikasi Dan Informasi: Akar Revolusi Dan Berbagai Standarnya.* Universitas Indonesia, Jakarta, hlm.11

media internet. Kecanggihan teknologi informasi dan komunikasi saat ini telah berkembang dengan cepat, sehingga memudahkan setiap orang untuk berkomunikasi, mencari informasi ataupun bersosialisasi. Dengan berbagai alat komunikasi yang semakin canggih seperti smartphone, laptop, atau personal komputer yang kini hadir di tengah-tengah masyarakat dapat mengefisienkan waktu dan juga tempat, karena alat komunikasi tersebut mudah diakses kapanpun dan dimanapun.

Teknologi merupakan sebuah sarana prasarana yang dibuat untuk menyediakan suatu barang atau komponen yang dibutuhkan setiap orang, teknologi tentu memiliki tujuan yaitu memecahkan suatu permasalahan, membuka kreativitas oleh karenanya teknologi berperan penting bagi setiap orang untuk menghasilkan sebuah informasi yang akurat.[2]

Di era globalisasi ini peranan teknologi dan komunikasi telah menghadirkan suatu yang menjadi dampak dengan meningkatnya produktivitas dan efisiensi. Adanya globalisasi ini sangat berpengaruh pada masyarakat dan telah mengubah pola hidup mereka dengan penggunaan sarana teknologi informasi dan komunikasi membuat tatanan kehidupan yang berkemang terjadinya perubahan sosial, budaya, ekonomi, pertahanan, keamanan, dan penegakan hukum. Salah satu pilar globalisasi yaitu penggunaan komunikasi yang merupakan suatu pilar

[2] Nudirman Munir, 2017, *Pengantar Hukum Siber*, Rajawali Press, Jakarta, hlm. 10.

utama dalam hubungan internasional dengan adanya kemajuan teknologi.[3]

Sebagai sebuah jaringan dalam komputer yang mampu tersalurkan ke seluruh dunia, internet disebut sebagai jalur transportasi segala informasi yang berbentuk file atau data pada komputer lain. [4] Dengan kata lain, tanpa adanya jaringan internet segala bentuk informasi atau dokumen yang tersimpan dalam sebuah komputer tidak dapat digunakan demi penyebaran informasi ke dalam komputer yang lain.

Manusia yang berada hampir di seluruh belahan dunia sangat bergantung dengan keberadaan internet bahkan dengan menggunakan jaringan internet, telah mampu membentuk budaya baru di dalam kehidupan. Internet merubah pekerjaan sehari-hari menjadi lebih mudah dalam berbagai sektor mulai dari kegiatan perdagangan, bisnis, pembayaran atau transaksi perbankan yang dapat dimanfaatkan untuk kepentingan pribadi, instansi/perusahaan atau pun pemerintahan.

Semakin banyaknya aktifitas yang dimanfaatkan oleh internet ini, mengakibatkan peningkatan pengguna internet di seluruh dunia. Oleh karena itu, berkenaan dengan pembangunan, kemajuan dan perkembangan teknologi informasi melalui internet, peradaban manusia

---

[3] Siswanto Sunarso, 2009, *Hukum Informasi dan Transaksi Elekronik Studi Kasus Prita Mulyas*ari, Rineka Cipta, Jakarta, hlm. 39

[4] Y. Maryono, B. Patmi Istiana, 2008, *Teknologi Informasi & Komunikasi 3,* Quadra, Jakarta, hlm. 3

diperhadapkan pada fenomena-fenomena baru yang mampu mengubah hampir setiap aspek kehidupan manusia.[5]

Istilah kejahatan yang terjadi dalam sebuah transaksi elektronik ini biasa dikenal dengan *cybercrime*. Bentuk kejahatan ini mengkhawatirkan sampai ke berbagai negara di dunia karena segala perkara yang terjadi berbeda ruang maupun waktu sehingga kebanyakan korban maupun penegak hukum harus mempunyai kemampuan ekstra untuk menyikapi kejahatan ini. Phising merupakan salah satu bentuk kejahatan yang juga harus di waspadai karena ketelitian dalam penggunaan media elektronik merupakan faktor utama agar tidak terjerat phising ini.

Di Indonesia juga banyak memanfaatkan jaringan internet mengikuti perkembangan global mulai dari penggunaan media sosial sampai transaksi perbankan menggunakan media elektronik yang paling banyak dijadikan sasaran oleh pelaku *cybercrime* dalam bentuk phising ini. Contoh pada umumnya yaitu dalam penggunaan internet banking sehingga pelaku dapat memanfaatkan untuk mengambil keuntungan di dalamnya secara melawan hukum. Sehingga menyebabkan hubungan dunia menjadi *boardless* (tanpa batas) serta berpengaruh dalam perubahan sosial, ekonomi dan budaya yang secara signifikan berlangsung demikian cepat.[6]

---

[5] Dikdik M, Elisatris Gultom, 2009, *Cyber Law Aspek Hukum dan Teknologi Informasi,* PT. Refika Aditama, Bandung, hlm.2

[6] Maskun, 2013,*Kejahatan Siber Cybercrime : Suatu Pengantar,* Kencana, Jakarta, hlm.29.

Dalam perkembangannnya teknologi informasi mendorong negara-negara lain untuk berkompetisi pada sektor komunikasi yang nantinya akan memberikan kemajuan pada bidang ekonomi[7] ditambah dengan semakin berkembangnya jaringan internet di seluruh dunia.

Jaringan internet saat ini sudah menjadi hal yang primer karena setiap orang memakainya, sebagian besar orang pasti mengetahui apa manfaat dari internet bagi kehidupannya, yaitu untuk saling berkomunikasi dengan internet bisa menghubungkan orang-orang dari berbagai negara yang berbeda, dengan internet juga setiap orang bisa mengakses ilmu pengetahuan apapun melalui adanya google, selain itu internet juga mempermudah pelaksanaan sistem akademik, tidak hanya itu bahkan dalam bidang bisnis internet sangatlah penting untuk digunakan apalagi dengan internet kini setiap orang bisa membeli barang melalui *online shop*. Begitu banyak manfaat dari jaringan internet yang memudahkan kehidupan manusia, namun di balik manfaat tersebut justru memberikan peluang kepada oknum untuk melakukan kejahatan yang disebut dengan *cybercrime* [8] Kejahatan *cyber* sudah sering terdengar di kalangan masyarakat. *Cybercrime* adalah salah satu bentuk atau dimensi baru dari kejahatan masa kini yang mendapat perhatian luas di dunia Internasional.

Cybercrime timbul dari dua penyebab, yang pertama adalah dalam hal teknis, kemajuan teknologi yang semakin pesat menjadikan dunia yang

---

[7] Sinta Dewi, 2009, *Cyber Law I: Perlindungan Privasi Atas Informasi Pribadi Dalam E-Commerce Menurut Hukum Internasional*, Widya Padjajaran, Bandung, hlm. 2.

Maidin Gultom, 2021, *Suatu tinjauan tentang tindak pidana yang berkaitan dengan informasi dan transaksi elektronik cybercrime,* Bina Media Perintis, Medan, hlm. 12

luas ini menjadi tanpa jarak, menghilangkan batas wilayah negara yang dapat memberikan peluang dnegan mudah bagi pelaku untuk melakukan aksinya, dan tidak meratanya penyebaran teknologi ini menyebabkan kelemahan yang dapat dimanfaatkan oleh oknum yang tidak bertanggung jawab melakukan kejahatan. Yang kedua adalah dalam bidang sosial dan ekonomi dimana keamanan jaringan menjadi isu global yang kemudian dihubungkan dengan tidak pidana yaitu tentang keamanan jaringan, selaras dengan jaringan internet yang sangat dibutuhkan banyak orang tentu setiap negara membutuhkan keamanan jaringan. Tindak pidana di dunia maya berada dalam skenario besar dari kegiatan ekonomi dunia.[9] Dalam lngkungan masyarakat modern, kejahatan sudah semakin canggih dan mudah. Kejahatan di dunia maya saat ini semakin hari semakin banyak jumlahnya dan modusnya pun semakin canggih pula, bervariasi karakteristik pelakunya dan akibat yang didapat juga semakin serius.[10] Keamanan di dunia *cyber* masih sangat rentan dikarenakan mudahnya mengakses teknologi yang menyebabkan banyak peretas dapat dengan mudah menjangkau sebuah sistem keamanan yang dibuat sedemikian rupa, ada saja celah untuk menembus sistem keamaan dari internet. *Bug* merupakan kecacatan dalam perangkat dan hal ini akan sangat membahayakan karena berhubungan dengan celah pada sistem

[9] Sahuri Lasmadi, *Tindak PIdana Dunia Maya dalam Perspektif Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik* , Jurnal Ilmu hukum, 2012, hlm.40-41.

[10] Widodo, 2013, *Memerangi Cybercrime Karakteristik, Motivasi dan Strategi Penanganannya Dalam Perspektif Kriminologi,* Asswaja Pressindo, Yogyakarta, hlm. 1.

keamanan dengan begitu peretas akan masuk dan menguasai sistem tersebut nantinya.

Dengan telah adanya phising di Indonesia, membuat aktifitas dalam sebuah transaksi elektronik sangat rentan dan memprihatinkan untuk dilakukan seperti sebelumnya. Apalagi ditunjang dengan pengguna internet yang ada di Indonesia tersebar dari beberapa kalangan masyarakat, sehingga pemahaman terhadap apa saja yang sebenarnya ada di internet, salah satunya dengan telah lahirnya kejahatan di internet, dikarenakan *cybercrime* terlebih khusus phising adalah jenis kejahatan yang dilakukan dengan tipu muslihat sehingga tidak semua pengguna dapat menyadari sebelumnya. Oleh karena itu, tentunya pelaku *cybercrime* berbentuk phising yang berkeliaran di dunia maya harus diberikan sanksi berupa pertanggungjawaban pidana atas kesalahan yang telah ia perbuat. Seperti dalam UU ITE sebagaimana sebagai peraturan perundang-undangan di Indonesia yang mengatur mengenai kejahatan menggunakan media elektronik atau *cybercrime* ini, yang menggunakan bentuk pemidanaan berupa pidana penjara dan/atau denda dimana agar dapat diketahui apakah pemidanaan atau pemberian sanksi bagi pelaku phising yang termasuk di dalamnya, telah efektif untuk mengurangi kejahatan yang berkembang serta mengurangi residivis terhadap pelaku itu sendiri atau tidak. Selanjutnya, yang perlu diperhatikan adalah korban phising yang merupakan pihak yang paling dirugikan. Dimana korban phising yaitu korban yang mengalami kerugian materiil, sehingga demi

kesejahteraan hidup bagi korban phising maupun korban phising tidak langsung (suami/istri, anak atau sanak saudara) atas dampak kerugian materiil seperti kekurangan perekonomian yang seharusnya tidak mereka terima menjadi sumber dasar atas bagaimana negara harus memberikan kembali pada korban phising apa yang seharusnya mereka miliki. Dimana hal ini pun termasuk dalam hak warga negara untuk mendapat jaminan, perlindungan serta kepastian hukum yang seadil-adilnya.

Phising memiliki arti yaitu kejahatan dunia maya (*cybercrime*) dimana seseorang menyamar sebagai lembaga yang sah menghubungi target atau korban melalui email, telepon atau pesan teks, agar ia memberikan data sensitive seperti informasi identitas pribadi, detail perbankan atau kartu kredit serta kata sandi. Setelah korban atau target memberikan informasi tersebut kemudian nantinya akan digunakan untuk mengakses akan pentingnya yang dapat mengakibatkan pencurian identitas dan kerugian finansial.

Phising sendiri berasal dari kata "*passwod, harvest* dan *fishing*" yakni memanen *password* seperti halnya kegiatan memancing. Phising adalah kejahatan dengan cara memanfaatkan umpan. Umpan yang tepat sasaran adalah faktor penentu keberhasilan phising. Kehadiran akun phising adalah kunci, sebab menyerupai akun resmi. Jika dilihat dari definisinya phising adalah kejahatan yang menggunakan rekayasa sosial dan dalih teknis mencuri data identitas pribadi dan akun keuangan dengan skema mamangsa korban yang tidak waspada atau lalai dengan membodohi

mereka agar mereka percaya bahwa mereka berurusan dengan pihak terpercaya dan sah, seperti menggunakan alamat email yang menipu, hal ini direncanakan untuk mengarahkan korban ke situs web palsu yang menipu korbannya sehingga data akun yang berhubungan dengan keuangan, nama pengguna serta kata sandi itu dibocorkan.[11]

Saat ada celah pada sistem keamanan disitulah peretas memanfaatkan momen yang sering terdengar dengan sebutan *hacking* maupun *hacker*, kemudian ada juga istilah *cracking* dan *cracker* yang mana kejahatan yang dilakukan oleh cracking salah satunya adalah Phising karena memiliki tujuan yaitu untuk menguntungkan diri sendiri dan tentunya akan ada pihak yang dirugikan dan menjadi korban dari tindak pidana *cybercrime* ini. Phising merupakan salah satu kejahatan elektronik dalam lingkup penipuan dimana proses phising ini memiliki tujuan untuk mengambil informasi yang sangat sensitif seperti *username*, *password*, dan detail kartu kredit dalam bentuk meniru sebagai sebuah lembaga yang dipercaya dan biasanya berkomunikasi secara elektronik. [12]

Phising juga dilakukan dengan berbagai media yang terhubung ke jaringan internet seperti melalui email atau sms dan website. Dan modusnya adalah dengan menawarkan hadiah kepada target dan

---

[11] Phising melalui Situs web Palsu: Penyerang menciptakan situs web palsu yang meniru tampilan dan nuansa situs resmi untuk meminta pengguna memasukkan informasi pribadi mereka, https://www.google.com/search?q=arti+phising&rlz=1C1GCEA_enID1082ID1082&oq=arti+phising&gs_lcrp=EgZjaHJvbWUyCQgAEEUYORiABDIHCAEQABiABDIHCAIQABiABDIHCAMQABiABDIHCAQQABiABDIGCAUQRRg8MgYIBhBFGDwyBggHEEUYPNIBCDUwMzJqMGo3qAIAsAIA&sourceid=chrome&ie=UTF-8, diakses 09 Februari 2024

[12] Dian Rachmawati, *Phising Sebagai Salah Satu Bentuk Ancaman dalam Dunia Cyber*, Jurnal Saintkom, Volume 13, Nomor 3 Tahun 2014, hlm. 211.

memberikan link dari website dengan begitu ketiga seseorang mengklik link tersebut maka datanya akan diretas, ataupun memasukkan data pribadi pada sebuah website tertentu sebagai pemancingan.

Penyalahgunaan itu untuk melakukan perbuatan memperoleh data identitas diri seperti user id dan password dengan menggunakan teknik phising. Indonesia sendiri telah memliki Undang-Undang khusus mengenai transaksi yang berbasis elektronik yaitu Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. Namun yang menjadi dilema regulasi saat ini bahwa apakah aturan-aturan tersebut, baik tingkat nasional maupun internasional mampu menjangkau dan mengikuti kemajuan dari pola perubahan *cybercrime* itu sendiri seiring dengan pesatnya perkembangan kecanggihan teknologi berinternet hingga saat ini. Semakin mutakhir perkembangan teknologi informasi, maka akan semakin mutakhir pula bentuk dan modus pelaku melakukan kejahatan. [13] Di dalam jaringan komputer seperti internet, masalah kriminalitas menjadi semakin kompleks karena ruang lingkupnya yang luas. Fenomena *cybercrime* memang harus diwaspadai karena kejahatan ini agak berbeda dengan kejahatan lain pada umumnya.

Cybercrime dapat dilakukan tanpa mengenal batas teritorial dan tidak diperlukan interaksi langsung antara pelaku dengan korban kejahatan. Bisa dipastikan dengan sifat global internet, semua negara yang

[13] Maskun, 2013, *Kejahatan Siber (Cybercrime) Suatu Pengantar*, Kencana Prenada Media Group, Jakarta, hlm. 44.

melakukan kegiatan internet hampir pasti akan terkena dampak dari perkembangan *cybercrime* ini.

Cybercrime dengan modus phisisng saat ini di Indonesia dimungkinkan dapat dikenakan Pasal 378 KUHP karena termasuk ke dalam tindakan penipuan yang mengarahkan korbannya untuk mengakses situs palsu. *Cybercrime* dalam bentuk Phising ini juga dapat dikenakan Pasal 28 ayat (1) jo Pasal 45 ayat (1) UU ITE karena pelaku phising melakukan kebohongan untuk menyesatkan orang lain dimana mengarahkan orang yang dibohongi untuk mengakses sebuah link yang ditujukan ke situs palsu dan memberikan suatu perintah untuk memperbaharui informasi pribadinya yang rahasia ke dalam situs palsu tersebut sehingga informasi pribadinya itu dapat diketahui oleh pelaku dan menyebabkan orang tersebut mengalami kerugian. Serta tindakan kejahatan phising ini dapat dikenakan Pasal 35 jo Pasal 51 ayat (1) ayat (1) UU ITE karena phising merupakan kejahatan siber yang memanipulasi korbannya dengan membuat situs yang menyerupai situs asli yang resmi padahal situs tersebut adalah situs palsu.

Pasal 378 KUHP yang menegaskan sebagai berikut :

> “Barangsiapa dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum dengan memakai nama palsu atau martabat palsu, dengan tipu muslihat ataupu rangkaian kebohongan, menggerakkan orang lain untuk menyerahkan barang sesuatu kepadanya. Atau supaya memberi hutang maupun menghapuskan piutang diancam karena penipuan dengan pidana penjara paling lama empat tahun”.

Pasal 35 jo Pasal 51 ayat (1) berdasarkan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang menegaskan:

> Pasal 35
>
> "Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan,perubahan, penghilangan, pengrusakan informasi Elektronik dan/atau dokumen elektronik dengan tujuan agar informasi elektronik dan/atau dokumen elektronik tersebut dianggap seolah-olah data otentik".
>
> Pasal 51 ayat (1)
>
> "Setiap orang yang memenuhi unsur sebagaimana dimaksud Pasal 35 dipidana dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp 12.000.000.000 (dua belas milliar rupiah)".

Kebijakan dalam perundang-undangan mutlak diperlukan oleh para penegak hukum dan pemerintah untuk menanggulangi dan menindak pelaku kejahatan, sama halnya dengan tindak kejahatan mayantara (*cybercrime*), tentunya jenis hukum perundang-undangan haruslah sesuai dengan jenis kejahatan dan cara untuk mengungkap kasus kejahtan dunia maya. Pemerintah republik Indonesia sudah berkomitmen untuk memerangi kejahatan dunia maya.

Berdasarkan latar belakang masalah di atas, penulis tertarik untuk melakukan penelitian tentang Perlindungan hukum terhadap korban tindak pidana phising menurut Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang_undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

B. Perumusan Masalah

Berdasarkan uraian latar belakang masalah di atas, maka yang menjadi permasalahan dalam tesis ini adalah :

1. Bagaimana pemidanaan terhadap pelaku tindak pidana *cybercrime* berbentuk phising?
2. Bagaimana pembuktian terjadinya tindak pidana phising?
3. Bagaimana perlindungan hukum terhadap korban tindak pidana phising?

C.Tujuan Penelitian

Adapun yang menjadi tujuan dalam penelitian adalah :

1. Untuk mengetahui pemidanaan terhadap pelaku tindak pidana phising
2. Untuk mengetahui Pembuktian terjadinya tindak pidana phising
3. Untuk mengetahui perlindungan Hukum terhadap korban tindak pidana phising

D. Manfaat Penelitian

Penelitian ini diharapkan dapat memberikan manfaat baik secara teoretis maupun praktis

1. Secara Teoritis

Penulisan ini diharapkan dapat menambah wawasan dan memberikan sumbangan dalam memberikan perlindungan terhadap korban tindak pidana phising serta penulisan ini dapat menjadi rujukan ilmiah bagi penelitian-penelitian selanjutnya tentang perlindungan hukum terhadap

korban-korban kejahatan *cybercrime*, khususnya korban tindak pidana phising.

2. Secara Praktis

Untuk memberikan pengetahuan kepada penulis tentang korban tindak pidana phising. Dalam hal ini perlindungan terhadap seluruh warga negara khususnya korban tindak pidana phising dituangkan dalam Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik Dilihat dari ketentuan tersebut maka diketahui bahwa korban tindak pidana phising mendapat perlindungan hukum sesuai dengan undang-undang tersebut.

E. Kerangka Teori dan Kerangka Konsep

1. Kerangka Teori

a. Teori Perlindungan Hukum

Dalam Penulisan ini penulis menggunakan *Grand Teori* yaitu *Teori Perlindungan Hukum.* Menurut Satjipto Raharjo, perlindungan hukum adalah memberikan pengayoman terhadap Hak Asasi Manusia (HAM) yang dirugikan orang lain dan perlindungan itu diberikan kepada masyarakat agar dapat menikmati semua hak-hak yang diberikan oleh hukum. Hukum dapat difungsikan untuk mewujudkan perlindungan yang sifatnya tidak sekedar adaptif dan fleksibel, melainkan juga prediktif dan antisipatif. Hukum dibutuhkan untuk mereka yang lemah

dan belum kuat secara sosial, ekonomi, dan politik untuk memperoleh keadilan sosial.[14]

Perlindungan Hukum adalah suatu perlindungan yang diberikan kepada subyek hukum yang sesuai dengan aturan hukum, baik itu yang bersifat preventif (pencegahan) maupun dalam bentuk yang bersifat represif (pemaksaan) baik yang secara tertulis mapupun tidak tertulis dalam rangka menegakkan peraturan hukum.Perlindungan hukum bagi rakyat meliputi dua hal, yakni :

a. Perlindungan hukum preventif, yakni bentuk perlindungan hukum dimana kepada rakyat diberi kesempatan untuk mengajukkan keberatan atau pendapat sebelum suatu keputusan pemerintah mendapat bentuk yang definitif.
b. Perlindungan hukum represif, yakni bentuk perlindungan hukum dimana lebih ditujukan dalam penyelesaian sengketa.

Unsur-unsur yang tercantum dalam definisi teori perlindungan hukum, meliputi:

1. Adanya wujud atau bentuk perlindungan atau tujuan perlindungan;
2. Subjek hukum dan;
3. Subjek perlindungan hukum.

Pada dasarnya, teori perlindungan hukum merupakan teori yang berkaitan pemberian pelaayanan kepada masyarakat. Roscoe Pound mengemukakan hukum merupakan alat rekayasa sosial (*law as tool of*

[14] Satjipto Rahardjo, 2000*, Ilmu Hukum,* Citra Aditya Bakti, Bandung, hlm. 54

social engginering). Kepentingan manusia, adalah suatu tuntutan yang dilindungi dan dipenuhi manusia dalam bidang hukum.

Roscoe Pound membagi kepentingan manusia yang dilindungi hukum menjadi tiga macam, yang meliputi:

1. *Public Interest* (kepentingan umum);
2. *Social Interest* (kepentingan masyarakat); dan
3. *Privat Intetest* (kepentingan individual).[15]

Hukum sebagai perlindungan kepentingan manusia berbeda dengan norma-norma yang lain. Karena hukum itu berisi perintah dan/atau larangan, serta membagi hak dan kewajiban.

b. Teori Kepastian Hukum

Sebagai *Middle Teori* dalam penelitian ini, penulis menggunakan *Teori Kepastian Hukum.* Menurut Utrecht, kepastian hukum mengandung dua pengertian, yaitu pertama, adanya aturan yang bersifat umum membuat individu mengetahui perbuatan apa yang boleh atau tidak boleh dilakukan dan kedua, berupa keamanan hukum bagi individu dari kesewenangan pemerintah karena dengan adanya aturan yang bersifat umum itu individu dapat mengetahui apa saja yang boleh dibebankan atau dilakukan oleh negara terhadap individu.[16] Menurut Sudikno Mertukusumo, kepastian hukum merupakan jaminan bahwa hukum tersebut dapat dijalankan dengan baik. Sudah tentu kepastian hukum sudah menjadi bagian yang tidak terpisahkan hal ini lebih

[15] Lili Rasyidi, 1998, *Filsafat Hukum*, Remadja Karya, Bandung, hlm. .228-231.
[16] Riduan Syahrani*, 1999, Rangkuman Intisari Ilmu Hukum*, Citra Aditya Bakti, Bandung, hal.23

diutamakan untuk norma hukum tertulis. Karena kepastian sendiri hakikatnya merupakan tujuan utama dari hukum. Kepastian hukum ini menjadi keteraturan masyarakat berkaitan erat dengan kepastian itu sendiri karena esensi dari keteraturan akan menyebabkan seseorang hidup secara berkepastian dalam melakukan aktivitas kehidupan masyarakat itu sendiri. [17] Sedangkan menurut Gustav Radbruch keadilan dan kepastian hukum merupakan bagian-bagian yang tetap dari hukum. Beliau berpendapat bahwa keadilan dan kepastian hukum harus diperhatikan, kepastian hukum harus dijaga demi keamanan dan ketertiban suatu negara. Akhirnya hukum positif harus selalu ditaati. Berdasarkan teori kepastian hukum dan nilai yang ingin dicapai yaitu nilai keadilan dan kebahagiaan.[18]

Kepastian hukum lahir atas adanya suatu konflik norma, sehingga terbentuknya suatu aturan yang dibuat untuk mengatur masyarakat tanpa adanya keraguan. Kepastian hukum merujuk kepada suatu keadilan dimana hukum ditegakkan secara jelas, tetap, dan konsisten pada setiap pelaksanaannya.

c. Teori Penegakan Hukum

Sebagai Applied Teori dalam penelitian ini penulis menggunakan *Teori Penegakan Hukum,* Hukum sebagai *social engineering atau social planning* berarti bahwa hukum sebagai alat yang digunakan oleh

[17] Sudikno Mertukusumo, 2017, *Mengenal Hukum Suatu Pengantar*, Liberty, Yogyakartahal, hlm. 160

[18] Achmad Ali, 2002, *Menguak Tabir Hukum (Suatu Kajian Filosofis dan Sosiologis)*, Gunung Agung, Jakarta, hal.95

agent of change atau pelopor perubahan yang diberi kepercayaan oleh masyarakat sebagai pemimpin untuk mengubah masyarakat seperti yang dikehendaki atau direncanakan. [19] Hukum sebagai tatanan perilaku yang mengatur manusia dan merupakan tatanan pemaksa, maka agar hukum dapat berfungsi efektif mengubah perilaku dan memaksa manusia untuk melaksanakan nilai-nilai yang ada dalam kaedah hukum, maka hukum tersebut harus disebarluaskan sehingga dapat melembaga dalam masyarakat.

Di samping pelembagaan hukum dalam masyarakat, perlu dilakukan penegakan hukum *(law enforcement*) sebagai bagian dari rangkaian proses hukum yang meliputi pembuatan hukum, penegakan hukum, peradilan serta administrasi keadilan. [20] Menyampaikan pendapatnya mengenai penegakan hukum (*law enforcement)* adalah pelaksanaan hukum secara konkrit dalam kehidupan masyarakat. Setelah pembuatan hukum dilakukan, maka harus dilakukan pelaksanaan konkrit dalam kehidupan masyarakat sehari-hari, hal tersebut merupakan penegakan hukum. Namun dalam istilah lain sering disebut penerapan hukum, atau dalam istilah bahasa asing sering disebut *rechistoepassing dan rechtshandhaving* (Belanda)*, law enforcement* dan *application* (Amerika)*.*

[20] Satjipto Rahardjo, 2009, Penegakan Hukum Suatu Tinjauan Sosiologis, GEnta Publishing, Yogyakarta, hlm. 175

Penegakan hukum[21] merupakan suatu proses untuk terciptanya suatu ide-ide atau berfungsinya aturan hukum secara fakta sebagai pedoman prilaku dalam lintasan hubungan hukum bermasyarakat dan berbangsa. Penegakkan hukum adalah suatu usaha yang bertujuan untuk membuat konsep hukum serta ide - ide yang diharapkan oleh masyarakat menjadi suatu kenyataan yang melibatkan banyak hal dalam prosesnya. Soerjono Soekanto menjelaskan bahwa penegakkan hukum ialah suatu kegiatan untuk menyelerasakan hubungan antara nilai - nilai yang terdapat dalam kaidah-kaidah atau pandangan yang mantap dan mengejewantah serta sikap sebagai suatu rangkaian nilai tahap akhir agar terciptanya, terpeliharanya dan mempertahankan kedamaian dalam pergaulan hidup masyarakat.[22]

Penegakan Hukum Pidana atau disingkat dengan PHP ialah suatu bagian sistem dari keseluruhan sistem penegakkan hukum positif di Indonesia, yang dimana masih merupakan suatu kesatuan dari sistem pembangunan nasional, baik secara *in abstracto* maupun secara *in concreto*. Sistem penegakkan hukum pidana secara integral harus dilihat secara *in abstracto* (pembuatan hukumnya) dikarenakan penegakkan hukum pidana merupakan tahap pembuatan hukum atau peraturannya dirumuskan oleh legislatif. Menurut Barda Nawawi Arief, menjelaskan bahwa penegakkan hukum secara *in abstracto* dilakukan

[21] Sukardi, 2020, *Restorative Justice dalam Penegakan Hukum Pidana Indonesia,* Raja Grafindo Persada, Jakarta, hlm. 70-71

[22] Soerjono Soekanto,2013, *Faktor-Faktor yang Mempengaruhi Penegakan Hukum*, Raja Grafindo Persada, , Jakarta. hlm. 42

dengan tahapan formulasi yang sangat penting dimana di dalam tahap tersebut adalah permulaan dari suatu proses hukum secara *in concreto*. Sistem Penegakkan Hukum Pidana yang ada pada saat ini masih sama sekali belum berkesinambungan secara *in abstracto* atau perumusan hukumnya, hal tersebut dikarenakan masih tidak tersinkronisasi antara hukum pidana materil dan formil serta dalam pengaplikasiannya.

Faktor – faktor yang mempengaruhi penegakkan hukum dalam pengaplikasiannya antara lain :

a. *Faktor Segi Hukum*.

   Praktik penerapan hukum yang terjadi di masyarakat seringkali timbul pertentangan antara suatu nilai keadilan dan juga mengenai jaminan kepastian hukum. Pertentangan tersebut dilandaskan nilai keadilan yang ada merupakan suatu rumusan yang masih bersifat abstrak atau tidak pasti, sedangkan kepastian hukum yang dimaksud adalah kepastian hukum yang telah ditentukan secara normatif di dalam peraturan. Suatu kebijakan yang tidak berasaskan hukum ialah kebijakan yang bisa dibenarkan sepanjang kebijakan atau tindakan tersebut tidak bersinggungan dengan peraturan yang tercipta terlebih dahulu. Penyelenggaraan aturan hukum tidak hanya masuk kedalam *law enforcement*, namun juga harus masuk kedalam *peace mantenance*, sebab penerapan hukum adalah proses sinkronisasi atau proses penyelerasan nilai sosial yang

nyata dan norma hukum yang memiliki tujuan yang sama yaitu terciptanya keserasian serta perdamaian.

b. *Faktor Penegakkan Hukum.*

Penyelenggaran hukum dalam proses penegakkan nya tidak terlepas dari faktor penggeraknya. Fungsi hukum, mental kepribadian aparat penegak hukum memiliki peran penting dalam permainan penegakkan hukum. Apabila peraturan fungsi hukum sudah baik, tetapi kualitas dan integritas aparat penegak hukum masih kurang, pasti akan timbul permasalah dalam penegakkan hukum.Kepribadian atau integritas penegak hukum dalam pengyelenggaraan hukum sangat penting sekali untuk suksesnya suatu aturan hukum sesuai dengan fungsi hukumnya.

c. *Faktor Fasilitas Pendukung / Sarana Prasarana*.

Pendidikan yang dimiliki aparat penegak hukum sangat mendukung dalam penyelenggaraan hukum. Pendidikan sebagai perangkat lunak aparat penegak hukum dewasa ini lebih menjurus kepada hal – hal yang bersifat praktis konvensional, sehingga hal tersebut berujung pada hambatan yang dialami oleh aparat penegak hukum, diantaranya ialah minimnya pengetahuan mengenai *cybercrime*. *Cybercrime* sebagai tindak pidana khusus dalam penegakkannya masih berwenang kejaksaan, hal tersebut disebabkan kepolisian secara teknis yuridis masih dianggap belum memenuhi syarat dan belum siap.

d. *Faktor Masyarakat.*

Masyarakat sebagai tujuan utama alasan peyelenggaraan penegakkan hukum. Menciptakan perdamaian dan ketentraman dalam masyarakat merupakan alasan penegakkan hukum wajib dilaksanakan secara maksimal. Setiap warga masyarakat mempunyai kesadaran akan hukum. Permasalahan yang seringkali timbul adalah kurangnya rasa kepatuhan yang ada akan hukum. Prosentasi kepatuhan hukum masyarakat terhadap aturan hukum yang ada merupakan indikator untuk terciptanya dan berfungsinya hukum secara baik.

e. *Faktor Kebudayaan.*

Konsep kebudayaan menurut Soerjono Soekanto mempunyai fungsi yang sangat penting bagi prilaku masyarakat. Kebudayaan mengatur prilaku masyarakat untuk bertindak, berbuat serta menentukan sikap dalam interaksi dengan masyarakat lainnya. Kebudayaan yang ada pada saat ini dan atran hukum seringkali tidak berjalan dengan serasi. Kebudayaan yang dimilik masyarakat dalam menilai serta memahami suatu hal menjadikan faktor penting lainnya dalam terciptanya kelancaraan penegakaan hukum.[23]

[23] *Ibid.*

2. Kerangka Konsep

a. Perlindungan Hukum

Perlindungan Hukum adalah memberikan pengayoman kepada hak asasi manusia yang dirugikan orang lain dari perlindungan tersebut diberikan kepada masyarakat agar mereka dapat menikmati semua hak-hak yang diberikan oleh hukum.

b. Korban

Korban adalah mereka yang menderita jasmaniah dan rohaniah sebagai akibat tindakan orang lain yang mencari pemenuhan kepentingan diri sendiri atau orang lain yang bertentangan dengan kepentingan hak asasi pihak yang di rugikan.

c. Tindak Pidana

Perbuatan yang oleh aturan hukum dilarang dan diancam dengan pidana, dimana pengertian perbuatan di sini selain perbuatan yang bersifat aktif (melakukan sesuatu yang sebenarnya dilarang oleh hukum) juga perbuatan yang bersifat pasif (tidak berbuat sesuatu yang sebenarnya diharuskan oleh hukum).

d. Phising

Teknik penipuan yang dilakukan dengan cara memancing orang lain untuk memberikan informasi sensitive seperti data pribadi, data akun, data finansial, data Perusahaan, data Kesehatan, dan data yang sensitif lainnya.

F. Keaslian Penelitian

Sepanjang pengetahuan penulis dan berdasarkan pengamatan serta penelurusan yang penulis lakukan judul dan permasalahan ini belum pernah diteliti, akan tetapi terdapat judul tentang perlindungan terhadap korban phising yaitu antara lain yang pernah ditulis oleh :

1. Leticia M. Malunsenge, Cornelis Dj. Massie, Ronald E. Rorie dengan Judul “Penegakan Hukum Terhadap Pelaku dan Korban Tindak PIdana *Cybercrime* Berbentuk Phising di Indonesia”., Fakultas Hukum Unsrat, Tahun 2020.
2. Tuti Warsiti, dengan judul “Perlindungan Hukum Terhadap Korban Kejahatan *Cybercrime* berbentuk Phising dalam Transaksi Perdagangan Internasional” Fakultas Hukum Universitas Esa Unggul, Tahun 2023.
3. Faiz Emery Muhammad, Beniharmoni Harefa, dengan judul “Pengaturan Tindak Pidana Bagi Pelaku Penipuan Phisning Berbasis Web”, Fakultas Hukum Universitas Pembangunan Nasional Veteran Jakarta, Tahun 2023.

G. Metode Penelitian

1. Spesifikasi Penelitian

Jenis penelitian ini secara spesifik bersifat deskriptif analitis. Metode deskriptif analitis ini dimaksudkan untuk memperoleh gambaran yang baik, jelas, dan dapat memberikan data seteliti mungkin tentang objek yang diteliti dalam hal ini untuk

menggambarkan tentang Perlindungan Hukum Terhadap Korban Tindak Pidana Phising Menurut Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

2. Metode Pendekatan

Penelitian ini menggunakan pendekatan perundang-undangan *(statue approach*), pendekatan in imerupakan penelitian yang mengutamakan bahan hukum yang berupa peraturan perundang-undangan sebagai bahan acuan dasar dalam melakukan penelitian. Pendekatan ini dilakukan dengan menelaah semua peraturan perundang-undangan yang bersangkut paut dengan permasalahan (isu hukum) yang sedang dihadapi. Pendekatan konseptual (*conceptual approach*) merupakan jenis pendekatan dalam penelitian hukum yang memberikan sudut pandang analisa penyelesaian permasalahan dalam penelitian hukum dilihat dari aspek konsep-konsep hukum yang melatarbelakanginya, atau bahkan dapat dilihat dari nilai-nilai yang terkandung dalam penormaan sebuah peraturan kaitannya dengan konsep-konsep yang digunakan.[24]

3. Teknik Pengumpulan Data dan Alat Pengumpulan Data

Teknik pengumpulan data sekunder dilakukan melalui studi dokumen yaitu penelitian yang dilakukan dengan mencari bahan-bahan, baik dari buku-buku ilmiah, jurnal maupun peraturan

[24] Saifulanam, and Partners. 2017 *Pendekatan Perundang-Undangan (Statute Approach) Dalam Penelitian Hukum*, Jurnal Multidisplin Indonesia, Universitas Esa Unggul, Volume X, Nomor X, Januari 2022

perundang-undangan,khususnya yang berhubungan dengan permasalahan yang dibahas. Data tersebut kemudian dianalisis dan dirumuskan sebagai bahan penunjang dalam penelitian.

4. Analisis Data

Analisis data merupakan langkah yang selanjutnya untuk mengolah hasil peneltiian menjadi sebuah laporan. Data yang telah terkumpul dalam penelitian ini dianalisis secara kualitatif yuridis artinya penelitian mengacu kenyataan yang ada dan dihubungkan dengan studi kepustakaan yang ada maupun terhadap data sekunder yang digunakan dan juga secara yuridis normatif yaitu dengan mengadakan analisis terhadap pelaksanaan perundang-undangan yang berlaku dan menghubungkan dengan kenyataan di lapangan dan penerapannya dalam praktik. Data yang diperoleh diolah dan dianalisis secara deskriptif, normatif, logis dan sistematis.

Deskriptif merupakan data yang diperoleh dari lapangan tertulis sebagai kenyataan yang sebenarnya. Pendekatan normatif dilakukan dengan menggunakan bahan pustaka dan dihubungkan dengan permasalahan yang diteliti. Logis berarti bahwa dalam melakukan analitis tidak bertentangan dengan akal sehat dan ilmu pengetahuan. Sistematis yaitu bahwa setiap bagian yang dianalitis berkaitan satu sama lain dan saling mempengaruhi. Penarikan kesimpulan dilakukan dengan menggunakan metode berpikir deduktif yang merupakan metode penarikan kesimpulan dari yang bersifat umum terhadap

kesimpulan yang bersifat khusus dengan berpangkal dengan pengajuan premis mayor, kemudian diajukan premis minor dari kedua premis ini ditarik sebuah kesimpulan, artinya penarikan kesimpulan dari permasalahan yang bersifat umum terhadap permasalahan konkrit yang sedang diteliti dan berdasarkan kesimpulan tersebut dirumuskanlah sejumlah saran.

H. Sistematika Penulisan

Bab I memuat Pendahuluan, yang berisikan latar belakang, perumusan masalah, tujuan penelitian, manfaat penelitian, kerangka teori dan kerangka konsep, keaslian penelitian dan metode penelitian serta sistematika penulisan

Bab II memuat tentang Pemidanaan Terhadap Pelaku Tindak Pidana *Cybercrime* dalam bentuk Phising, yang berisikan tentang Pengertian dan Sejarah *Cybercrime*, Bentuk-bentuk Tindak Pidana *Cybercrime*, serta Penegakan Hukum Terhadap Pelaku Tindak Pidana *Cybercrime*

Bab III memuat tentang Pembuktian terjadinya tindak pidana phising yang berisikan tentang Pengertian Tindak Pidana Phising, Pengaturan Tindak Pidana Phising, Pertanggungjawaban Pidana Terhadap Pelaku Tindak Pidana *Cybercrime* daslam Bentuk Phising, serta Pembuktian Tindak Pidana Phising

Bab IV memuat tentang perlindungan hukum terhadap korban tindak pidana *cybercrime* yang berisikan Pengaturan hukum

terhadap *Cybercrime* dalam bentuk Phising, Kebijakan Hukum terhadap *Cyber* Crime dalam bentuk Phising, serta Perlindungan hukum terhadap Korban Tindak Pidana *Cybercrime* Phising.

Bab V berisikan tentang Kesimpulan dan Saran dan terakhir berisikan Daftar Pustaka

BAB II
PEMIDANAAN TERHADAP PELAKU TINDAK PIDANA *CYBERCRIME* BERBENTUK PHISING

A. Pengertian dan Sejarah *Cybercrime*

Teknologi telekomunikasi telah membawa manusia kepada suatu peradaban baru dengan struktur sosial beserta tata nilainya. Artinya, masyarakat berkembang menuju masyarakat baru yang berstruktur global. Sistem tata nilai dalam suatu masyarakat berubah, dari yang bersifat lokal-partikular menjadi global universal. Hal ini pada akhirnya akan membawa dampak pada pergeseran nilai, norma, moral, dan kesusilaan[25] Dampak pergeseran tersebut ditemukanya perkembangan dan kemajuan ilmu pengetahuan dan teknologi, terjadilah konvergensi antara keduanya.

Kemajuan teknologi yang merupakan hasil budaya manusia di samping membawa dampak positif, dalam arti dapat diperdayagunakan untuk kepentingan umat manusia juga membawa dampak negatif terhadap perkembangan manusia dan peradabannya. Dampak negatif yang dimaksud adalah yang berkaitan dengan dunia kejahatan. J. E Sahetapy telah menyatakan dalam tulisannya, bahwa kejahatan erat kaitanya dan bahkan menjadi sebagian dari hasil budaya itu sendiri. Ini berarti semakin tinggi tingkat budaya dan semakin modern suatu bangsa, maka semakin modern pula kejahatan itu dalam bentuk, sifat dan cara pelaksanaanya [26]

---

[25] Abdul Wahid dan Mohammad Labib, 2005, *Kejahatan Mayaantara (Cybercrime),* PT Refika Aditama, Bandung, hlm. 23.

[26] J. E Sahetapy dalam Abdul Wahid, 2002, K*riminologi dan Kejahatan Kontemporer,* Lembaga Penerbitan Fakultas Hukum Unisma, Malang.

Perkembangan teknologi komputer, teknologi informasi, dan teknologi komunikasi juga menyebabkan munculnya tindak pidana baru yang memiliki karakteristik yang berbeda dengan tindak pidana konvensional. Penyalahgunaan komputer sebagai salah satu dampak dari ketiga perkembangan teknologi tersebut itu tidak terlepas dari sifatnya yang khas sehingga membawa persoalan yang rumit dipecahkan berkenaan dengan masalah penanggulangannya (penyelidikan, penyidikan hingga dengan penuntutan).[27] Salah satu kejahatan yang ditimbulkan oleh perkembangan dan kemajuan teknologi informasi atau telekomunikasi adalah kejahatan yang berkaitan dengan aplikasi internet. Kejahatan ini dalam istilah asing sering disebut dengan *cybercrime*.

Cybercrime merupakan bentuk kejahatan yang relatif baru apabila dibandingkan dengan bentuk-bentuk kejahatan lain yang sifatnya konvensional (*street crime). Cybercrime* muncul bersamaan dengan lahirnya revolusi teknologi informasi. Sebagaimana dikemukakan oleh Ronni R. Nitibaskara bahwa: “Interaksi sosial yang meminimalisir kehadiran secara fisik, merupakan ciri lain revolusi teknologi informasi. Dengan interaksi semacam ini, penyimpangan hubungan sosial yang berupa kejahatan (*crime*) akan menyesuaiakan bentuknya dengan karakter baru tersebut.”[28]

---

[27] Edmon Makarim, 2005, Pengantar Hukum Telematika (Suatu Kajian Kompilasi), PT Raja Grafindo Persada, Jakarta, hlm. 426.

[28] Ronni R Nitibaskara dalam Didik M. Arief Mansur dan Elisatris Gultom, 2005, *Cyber Law Aspek Hukum Teknologi Informasi,* PT Refika Aditama, Bandung, hlm. 25.

Ringkasnya, sesuai dengan ungkapan “kejahatan merupakan produk dari masyarakat sendiri” (*crime is a product of society its self*), “habitat” baru ini, dengan segala bentuk pola interaksi yang ada didalamya, akan menghasilkan jenis-jenis kejahatan yang berbeda dengan kejahatan-kejahatan lain yang sebelumnya telah dikenal. Kejahatan-kejahatan ini berada dalam satu kelompok besar yang dikenal dengan istilah *cybercrime.*

Pada masa awalnya, *cybercrime* didefinisikan sebagai kejahatan komputer. Mengenai definisi kejahatan komputer sendiri, sampai sekarang para sarjana belum sependapat mengenai pengertian atau definisi dari kejahatan komputer. Bahkan penggunaan istilah tindak pidana untuk kejahatan komputer dalam bahasa Inggris pun masih belum seragam. Beberapa sarjana menggunakan istilah *computer misuse, computer abuse, computer fraud, computer related crime, computer assistend crime, atau computer crime*. Namun para sarjana pada waktu itu, pada umumnya lebih menerima pemakaian istilah computer crime oleh karena dianggap lebih luas dan bias dipergunakan dalam hubungan internasional.

Dua dokumen Konferensi Perserikatan Bangsa-bangsa (PBB) tentang The Prevention of Crime and The Treatment of Offenders di Havana (Cuba) tahun 1990, dan di Wina (Austria) tahun 2000, memang ada dua istilah yang digunakan: *cybercrime*, dan computerrelated crime. Laporan Dokumen Kongres PBB ke-10 di Wina, tanggal 19 Juli 2000

menggunakan istilah *computer-related crime*, dengan pengertian 2 bentuk berikut:

> *The term computer-related crime had been developed encompass both the entirely new formst of crime that were directed at computer, networks and their users, and the more traditional from crime that were now being commited with the use or assistance of computer equipment.*
> a. *Cybercrime in narrow sense (computer crime); any illegal beheviour directed by means of electronic operations that targets the security of computer system and the data processed by them.*
> b. *Cybercrime in broader sense (computer-related crime); any illegal behavior commited by means of, or in relation to, a computer system network, including such crimes as illegal possession, offering or distributing information by means of computer system an network.*[29]

Berdasarkan laporan tersebut dapat dimengerti bahwa *cybercrime* dibedakan menjadi 2 pengertian, yaitu dalam pengertian sempit dan luas. Dalam pengertian sempit, *cybercrime* adalah perbuatan yang tidak sah yang menjadikan komputer sebagi sasaran atau target kejahatan, baik pada keamanan sistem maupan datanya. Sedangkan *cybercrime* dalam arti luas merupakan keseluruhan bentuk kejahatan yang ditunjukan terhadap komputer, jaringan komputer dan para penggunanya, dan bentuk-bentuk kejahatan tradisional yang menggunakan atau dengan bantuan peralatan komputer. Pengertian yang digunakan dalam istilah *cybercrime* adalah dalam pengertian luas.

Pengkategorian jenis *cybercrime* menjadi dua tersebut selaras dengan The Encyelopedia of Crime and Justice yang menjelaskan bahwa ada dua kategori kejahatan yang *cybercrime*, yaitu:

---

[29] Agus Rahardjo, 2002*, Cybercrime: Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi,* PT Citra Aditiya Bakti, Bandung, hlm 32 dalam Widodo, 2011, *Aspek Hukum Kejahatan Mayantara,* , Aswindo, Yogyakarta, hlm. 7

a. *In the first, computer is a tool of a crime, such as froud, embezzlement, and thieft of property, or is used to plan manage a crime.*
b. *In the second, the computer is aobject of a crime, such as sabotage, theft or alteration of storage data, or theft of it service*[30]

Dari definisi yang diberikan oleh departemen kehakiman Amerika, penyalahgunaan komputer dibagi atas dua bidang utama. Pertama, adalah penggunaan komputer sebagia alat untuk melakukan kejahatan, contoh kasusnya adalah pencurian. Kemudian, yang kedua adalah komputer tersebut merupakan objek atau sasaran dari tindak kejahatan tersebut, contoh kasusnya adalah sabotase komputer sehingga tidak dapat berfungsi sebagimana mestinya.

Pengertian *cybercrime* menurut Widodo adalah setiap aktivitas seseorang, sekelompok orang, badan hukum yang menggunakan komputer sebagai sarana melakukan kejahatan, atau menjadikan komputer sebagai sasaran kejahatan. Semua kejahatan tersebut adalah bentuk-bentuk perbuatan yang bertentangan dengan peraturan perundang-undangan, baik dalam arti melawan hukum secara material maupun melawan hukum secara formal. [31] Kemudian, definisi lain mengenai kejahatan komputer ini dikeluarkan oleh *Organization of European Community Development (OECD) yaitu sebagai berikut: " any illegal, unethicall or unauthorized behavior relating to the authomathic*

[30] Widodo, 2011*, Aspek Hukum Kejahatan Mayantara*, Aswindo,Yogyakarta, hlm. 7

[31] *Ibid.*

processing and/or the transmission of data". [32] Dari definisi tersebut, kejahatan komputer ini termasuk segala akses illegal atau akses secara tidak sah terhadap suatu transmisi data. Sehingga telihat bahwa segala aktivitas yang tidak sah dalam suatu system komputer merupakan suatu kejahatan.

Batasan atau definisi dari kejahatan komputer juga diberikan oleh Andi Hamzah, menurut Andi Hamzah, bahwa "kejahatan di bidang komputer secara umum dapat diartikan sebagai penggunaan komputer secara illegal."[33] Dari pengertian yang diberikan oleh Andi Hamzah dapat disimpulkan bahwa beliau memperluas pengertian kejahatan komputer, yaitu segala aktivitas tidak sah yang memanfaatkan komputer untuk tindak pidana. Sekecil apapun dampak atau akibat yang ditimbulkan dari penggunaan komputer secara tidak sah atau illegal merupakan suatu kejahatan.

Cybercrime memiliki beberapa karakteristik, yaitu:[34]

a. Perbuatan yang dilakukan secara illegal, tanpa hak atau tidak etis tersebut terjadi dalam ruang/wilayah siber/*cyber* (*cyber*space), sehingga tidak dapat dipastikan yurisdiksi negara mana yang berlaku terhadapnya.

---

[32] Eddy Djunedi Karnasudiraja, 1993, *Yurisprudensi Kejahatan Komputer,* CV Tanjung Agung, Jakarta, hlm. 3

[33] Andi Hamzah, 1989, *Aspek-aspek Pidana di Bidang Komputer*, Sinar Grafika, Jakarta, hlm. 26.

[34] Abdul Wahid dan M. Labib, 2005, *Kejahatan Mayantara (Cybercrime),* Rafika Aditama,Bandung, hlm. 76 dalam Budi Suhariyanto, 2013, *Tindak Pidana Teknologi Informasi (Cybercrime) : Urgensi Pengaturan dan Celah Hukumnya*, PT Raja Grafindo Persada, Jakarta, hlm. 13.

b. Perbuatan tersebut dilakukan dengan menggunakan peralatan apa pun yang terhubung dengan internet.
c. Perbuatan tersebut mengakibatkan kerugian materill maupun immaterial (waktu, nilai, jasa, uang, barang, harga diri, martabat, kerahasian informasi) yang cenderung lebih besar dibandingkan dengan kejahatan konvensional.
d. Pelakunya adalah orang yang menguasai penggunaan internet beserta aplikasinya.
e. Perbuatan tersebut sering dilakukan secara transnasional/melintas batas negara.

Cybercrime atau kejahatan dunia maya dalam peraturan Perundang-undangan di Indonesia juga sering disebut dengan kejahatan tindak pidana yang berkaitan dengan teknologi informasi, hal ini sejalan dengan pengertian yang diberikan oleh Donn B. Parker yang memberikan definisi mengenai penyalahgunaan komputer :"*Computer abuse is broadly defined to be any incident associated with computer technology in which a victim suffered or could suffered loss and a perpetrator by intention made or could have gain*", dan diterjemahkan oleh Andi Hamzah sebagai "penyalahgunaan computer didefinisikan secara luas sebagai suatu kejadian yang berhubungan dengan teknologi komputer yang seorang korban menderita atau akan telah menderita kerugian dan seorang pelaku

dengan sengaja memperoleh keuntungan atau akan telah memperoleh keuntungan"[35]

Kejahatan dalam bidang teknologi informasi secara umum terdiri dari dua kelompok, yaitu :

a. Kejahatan konvensional yang menggunakan bidang teknologi informasi sebagai alat bantunya, contohnya pembelian barang dengan menggunakan nomor kartu kredit curian melalui media internet;
b. Kejahatan timbul setelah adanya internet, dengan menggunakan sistem komputer sebagai korbannya, contoh kejahatan ini ialah perusak situs internet (*cracking*), pengiriman virus atau program-program komputer yang bertujuan untuk merusak sistem kerja computer

Menurut Petrus Reinhard Golose, dalam kasus kejahatan dunia maya, baik korban maupun pelaku tidak berhadapan langsung dalam 1 (satu) tempat kejadian perkara. Dalam beberapa kasus, baik korban maupun pelaku dapat berada pada negara yang berbeda. Hal tersebut menggambarkan bahwa kejahatan dunia maya merupakan salah satu bentuk kejahatan lintas negara (*transnational crime),* dan tak berbatas (*borderless*), tanpa kekerasan *(non violence*), tidak ada kontak fisik *(no phisically contact)* dan tanpa nama (a*nonimity*)[36]

Kejahatan komputer atau kejahatan *cyber* atau kejahatan dunia maya *(cybercrime*) adalah sebuah bentuk kriminal yang mana menjadikan

---

[35] Donn B.Parker, 1976, *Crime by Computer*, hlm.12, „Andi Hamzah, 1993, *Hukum Pidana yang berkaitan dengan komputer,* Sinar Grafika Offset, Jakarta, hlm. 18

[36] Petrus Reinhard Golose, 2007*, Penegakan Hukum Cybercrime dalam Sistem Hukum Indonesia dalam Seminar Pembuktian dan Penanganan Cybercrime di Indonesia*, FHUI, Jakarta, hlm. 19

internet dan komputer sebagai medium melakukan tindakan kriminal. Masalah yang berkaitan dengan kejahatan jenis ini misalnya *hacking*, pelanggaran hak cipta, pornografi anak, dan eksploitasi anak. Juga termasuk pelanggaran terhadap privasi ketika informasi rahasia hilang atau dicuri, dan lainnya.

Dalam definisi lain, kejahatan dunia maya adalah istilah yang mengacu kepada aktivitas kejahatan dengan komputer atau jaringan komputer menjadi alat, sasaran atau tempat terjadinya kejahatan. Termasuk ke dalam kejahatan dunia maya antara lain adalah penipuan lelang secara online, pemalsuan cek, penipuan kartu kredit, *confidence fraud*, penipuan identitas, pornografi anak, dan lain-lain. Walaupun kejahatan dunia maya atau *cybercrime* umumnya mengacu kepada aktivitas kejahatan dengan komputer atau jaringan komputer sebagai unsur utamanya, istilah ini juga digunakan untuk kegiatan kejahatan tradisional dimana komputer atau jaringan komputer digunakan untuk mempermudah atau memungkinkan kejahatan itu terjadi.[37]

Kejahatan komputer mencakup berbagai potensi kegiatan ilegal. Umumnya, kejahatan ini dibagi menjadi dua kategori: (1) kejahatan yang menjadikan jaringan komputer dan *device* secara langsung menjadi target; (2) Kejahatan yang terfasilitasi jaringan komputer atau *device*, dan target utamanya adalah jaringan komputer independen atau *device*.

[37] Muhammad Zaidun , 2018, *Penegakan Hukum Tindak Pidana Cybercrime di Indonesia,* MNC, Malang, hlm. 25-28

Contoh kejahatan yang target utamanya adalah jaringan komputer atau *device* yaitu:

1*). Malware (malicious software / code)*

Malware (berasal dari singkatan kata malicious dan software) adalah perangkat lunak yang diciptakan untuk menyusup atau merusak sistem komputer, server atau jaringan komputer tanpa izin (*informed consent*) dari pemilik. Istilah ini adalah istilah umum yang dipakai oleh pakar komputer untuk mengartikan berbagai macam perangkat lunak atau kode perangkat lunak yang mengganggu atau mengusik.Istilah „*virus computer*" terkadang dipakai sebagai frasa pemikat *(catch phrase*) untuk mencakup semua jenis perangkat perusak, termasuk virus murni (*true virus*).

2). *Denial-of-service (DOS) attacks*

Denial of service attack atau serangan *DoS* adalah jenis serangan terhadap sebuah komputer atau server di dalam jaringan internet dengan cara menghabiskan sumber (*resource)* yang dimiliki oleh komputer tersebut sampai komputer tersebut tidak dapat menjalankan fungsinya dengan benar sehingga secara tidak langsung mencegah pengguna lain untuk memperoleh akses layanan dari komputer yang diserang tersebut.

3). *Computer viruses*

Virus komputer merupakan program komputer yang dapat menggandakan atau menyalin dirinya sendiri dan menyebar dengan cara menyisipkan salinan dirinya ke dalam program atau dokumen lain. Virus

murni hanya dapat menyebar dari sebuah komputer ke komputer lainnya (dalam sebuah bentuk kode yang bisa dieksekusi).ketika inangnya diambil ke komputer target, contohnya ketika user mengirimnya melalui jaringan atau internet, atau membawanya dengan media lepas (*floppy disk, cd, dvd, atau usb drive*). Virus bisa bertambah dengan menyebar ke komputer lain dengan menginfeksi file pada network *file system* (sistem file jaringan) atau sistem file yang diakses oleh komputer lain.

Contoh kejahatan yang menjadikan jaringan komputer atau *device* sebagai alat yaitu:

1) Cyber stalking (Pencurian dunia maya)

*Cyber*stalking adalah penggunaan internet atau alat elektronik lainnya untuk menghina atau melecehkan seseorang, sekelompok orang, atau organisasi. Hal ini termasuk tuduhan palsu, memata-matai, membuat ancaman, pencurian identitas, pengerusakan data atau peralatan, penghasutan anak di bawah umur untuk seks, atau mengumpulkan informasi untuk mengganggu. Definisi dari “pelecehan” harus memenuhi kriteria bahwa seseorang secara wajar, dalam kepemilikan informasi yang sama, akan menganggap itu cukup untuk menyebabkan kesulitan orang lain secara masuk akal.

2) Penipuan dan pencurian identitas

Pencurian identitas adalah menggunakan identitas orang lain seperti KTP, SIM, atau paspor untuk kepentingan pribadinya, dan biasanya digunakan untuk tujuan penipuan. Umumnya penipuan ini

berhubungan dengan Internet, namun sering juga terjadi di kehidupan sehari-hari. Misalnya penggunaan data yang ada dalam kartu identitas orang lain untuk melakukan suatu kejahatan. Pencuri identitas dapat menggunakan identitas orang lain untuk suatu transaksi atau kegiatan, sehingga pemilik identitas yang aslilah yang kemudian dianggap melakukan kegiatan atau transaksi tersebut.

3) Phishing scam

Dalam sekuriti komputer, phising (pengelabuan) adalah suatu bentuk penipuan yang dicirikan dengan percobaan untuk mendapatkan informasi peka, seperti kata sandi dan kartu kredit, dengan menyamar sebagai orang atau bisnis yang terpercaya dalam sebuah komunikasi elektronik resmi, seperti surat elektronik atau pesan instan. Istilah phishing dalam bahasa Inggris berasal dari kata *password*, *harvesting* dan *fishing*, dalam hal ini berarti memancing informasi keuangan dan kata sandi pengguna.

4) Perang informasi (Information warfare)

Perang Informasi adalah penggunaan dan pengelolaan informasi dalam mengejar keunggulan kompetitif atas lawan. Perang Informasi dapat melibatkan pengumpulan informasi taktis, jaminan bahwa informasi sendiri adalah sah, penyebaran propaganda atau disinformasi untuk menurunkan moral musuh dan masyarakat, merusak kualitas yang menentang kekuatan informasi dan penolakan peluang pengumpulan-informasi.

Contohnya ketika seseorang mencuri informasi dari situs, atau menyebabkan kerusakan komputer atau jaringan komputer. Semua tindakan ini adalah virtual (tidak nyata) terhadap informasi tersebut – hanya ada dalam dunia digital, dan kerusakannya – dalam kenyataan, tidak ada kerusakan fisik nyata kecuali hanya fungsi mesin yang bermasalah.Komputer dapat dijadikan sumber bukti. Bahkan ketika komputer tidak secara langsung digunakan untuk kegiatan kriminal, komputer merupakan alat yang sempurna untuk menjaga record atau catatan, khususnya ketika diberikan tenaga untuk mengenkripsi data. Jika bukti ini bisa diambil dan didekripsi, ini bisa menjadi nilai bagi para investigator kriminal untuk menentang kekuatan. Informasi perang berhubungan erat dengan perang psikologis.

Tindak pidana *cybercrime* dalam peraturan Perundang-undangan di Indonesia juga sering disebut dengan kejahatan tindak pidana yang berkaitan dengan teknologi informasi. Terdapat suatu definisi tindak pidana *cybercrime* sebagai berikut, *computer abuse is broadly defined to be any incident associated with computer technology in which a victim suffered or could suffered loss and aperpetrator by intention made or could have gain*.[38]

Hal tersebut dapat diartikan sebagai penyalahgunaan komputer didefinisikan secara luas sebagai suatu kejadian yang berhubungan dengan teknologi komputer yang seorang korban menderita atau akan

[38] 0 Suresh T. Viswanathan, *The Indian Cyber Laws with Cyber Glossary,* Bharat Law House, New Delhi, 2001, hlm. 81

telah menderita kerugian dan seorang pelaku dengan sengaja memperoleh keuntungan atau akan telah memperoleh keuntungan.[39]

Kejahatan *Cyber* atau tindak pidana *cyber* merupakan perbuatan malawan hukum yang memanfaatkan media komputer yang terhubung ke internet dan mengeksploitasi komputer lain, adapun bentuk-bentuk kejahatan *cybercrime* yaitu :[40]

a. Tindak pidana *cybercrime* berdasarkan sifat kejahatan

Terdapat dua klasifikasi tindak pidana *cybercrime* berdasarkan sifat kejahatan. Pertama, tindak pidana *cybercrime* sebagai tindakan kriminal yang merupakan kejahatan yang dilakukan dengan motif kriminalitas. Kedua, tindak pidana *cybercrime* sebagai kejahatan abu-abu karena sulit menentukan apakah tindakan ini merupakan tindak kriminal atau bukan mengingat motif kegiatannya terkadang bukan untuk kejahatan.

b. Tindak pidana *cybercrime* berdasarkan modus kejahatan

Terdapat tujuh klasifikasi tindak pidana *cybercrime* berdasarkan modus kejahatan. Pertama, *unauthorized access to computer system and service* yang terjadi ketika seseorang menyusup ke dalam suatu sistem jaringan komputer milik orang lain secara tidak sah, tanpa izin atau tanpa sepengetahuan dari pemilik sistem jaringan komputer yang dimasukinya. Kedua, *illegal contents* yang memasukkan data atau informasi ke internet tentang suatu hal yang tidak benar dan dapat dianggap melanggar hukum. Ketiga, *data forgery* yang dilakukan dengan tujuan memalsukan data pada

[39] *Ibid.*

[40] Florida Mathilda, *Cybercrime dalam Sistem Hukum Indonesia*, Sigma-Mu, Edisi No. 04 Vol. 04 2012, hlm. 35.

dokumen-dokumen penting yang ada di internet. Keempat, *cyber espionage, sabotage,* dan *extortion* yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata pada pihak lain. Kelima, *data theft* yang mengambil data komputer milik orang lain secara tidak sah, baik untuk digunakan sendiri atau digunakan untuk orang lain. Keenam, *infringements of privacy* yang biasanya ditujukan kepada keterangan pribadi seseorang pada formulir data pribadi yang tersimpan secara *computerized*. Ketujuh, *cyber terrorism* yang merupakan suatu tindakan tindak pidana *cybercrime* yang mengancam pemerintah atau warga negara.

c. Tindak pidana *cybercrime* berdasarkan sasaran kejahatan

Terdapat lima klasifikasi tindak pidana *cybercrime* berdasarkan sasaran kejahatan. Pertama, *cybercrime* yang menyerang individu yang ditujukan kepada perorangan atau individu yang memiliki sifat atau kriteria tertentu sesuai tujuan penyerangan tersebut. Kedua, *cyber*stalking yang dilakukan untuk mengganggu atau melecehkan seseorang dengan masuk menggunakan *e-mail* yang dilakukan secara berulang-ulang. Ketiga, *cyber-trespass* yang dilakukan melanggar area privasi orang lain. Keempat, *cybercrime* menyerang hak milik yang mengganggu atau menyerang hak milik orang lain, seperti mengakses komputer secara tidak sah. Kelima, *cybercrime* menyerang pemerintah yang memiliki tujuan khusus penyerangan terhadap pemerintah, seperti mengancam melalui situs resmi pemerintah.

Kemudian, terdapat juga beberapa jenis-jenis tindak pidana *cybercrime* apabila dilihat dari aktivitasnya sebagai berikut:[41]

a. *Carding* Merupakan aktifitas berbelanja menggunakan nomor dan identitas kartu kredit orang lain, yang diperoleh secara ilegal, biasanya dengan mencuri data di internet.
b. *Hacking* Merupakan aktifitas menerobos program komputer milik pihak lain.
c. *Cracking* Merupakan aktifitas *hacking* untuk tujuan jahat. Sebutan untuk *cracker* adalah *hacker* bertopi hitam. Berbeda dengan *carder* yang hanya mengintip kartu kredit, cracker mengintip simpanan para nasabah di berbagai bank atau pusat data sensitif lainnya untuk keuntungan diri sendiri. Meski sama-sama menerobos keamanan komputer orang lain, *hacker* lebih fokus pada prosesnya. Sedangkan *cracker* lebih fokus untuk menikmati hasilnya.
d. *Defacing* Merupakan aktifitas mengubah halaman situs pihak lain. Tindakan *deface* ada yang semata-mata iseng, unjuk kebolehan, pamer kemampuan membuat program, tapi ada juga yang jahat mencuri data dan dijual kepada pihak lain.
e. *Phising* Merupakan aktifitas memancing pemakai komputer di internet agar mau memberikan informasi data diri pemakai dan kata sandinya pada suatu situs yang sudah di-*deface*. Phising biasanya diarahkan kepada pengguna *online banking*.

[41] Nunuk Sulisrudatin, *Analisa Kasus Cybercrime Bidang Perbankan Berupa Modus Pencurian Data Kartu Kredit*, Jurnal Ilmiah Hukum Dirgantara, Edisi No. 01 Vol. 09 2018, hlm. 31.

f. *Spamming* Merupakan aktifitas pengiriman berita atau iklan lewat *e-mail* yang tidak dikehendaki.

g. *Malware* Merupakan program komputer yang mencari kelemahan dari suatu *software*. Umumnya *malware* diciptakan untuk membobol atau merusak suatu *software* atau *operating system*. *Malware* terdiri dari berbagai macam seperti *virus, worm, trojan horse, adware*, hingga *browser hijacker*.

Bentuk-bentuk kejahatan *cybercrime* atau kejahatan di dunia maya kini hampir menyerupai kejahatan di dunia nyata seperti seorang kriminal yang melakukan kejahatan dengan melakukan pencurian dan menggunakan hal yang dicuri tersebut secara ilegal. [42] Namun, terdapat perbedaan pencurian yang dilakukan di dunia maya, di mana umumnya diawali dengan pencurian data. [43] Data yang dicuri ini kemudian digunakan untuk melakukan tindakan yang merugikan korban. Bentuk yang paling umum dari penggunaan data korban ini yakni untuk melakukan pembobolan dana di bank milik korban.[44]

Data yang dicuri tersebut dapat digunakan oleh pelaku kejahatan untuk melakukan pelanggaran terhadap norma kesusilaan, seperti membuka situs pornografi, prostitusi, dan lain sebagainya. Sementara bentuk kejahatan *cybercrime* dalam lingkup yang lebih luas dapat

---

[42] Barda Nawawi Arief, *Kapita Selekta Hukum Pidana*, Citra Aditya Bhakti, Bandung, 2003, hlm. 239.

[43] *Ibid.*

[44] Alexander Anggono, Tarjo, dan Moh. Riskiyadi, *Cyber*crime dan *Cyber*security pada Fintech: Sebuah Tinjauan Pustaka Sistematis, Jurnal Manajemen dan Organisasi (JMO), Edisi No. 3 Vol. 12 2021, hlm. 241.

berbentuk pencurian data yang terintegrasi dalam situs pemerintah atau lembaga negara, pembajakan situs milik perusahaan, melakukan penyebaran virus, dan lain sebagainya.

Salah satu bentuk *cybercrime* yang harus diwaspadai oleh masyarakat yakni metode phising. *Cybercrime* metode phising adalah *password harvesting fishing* atau penipuan yang dilakukan dengan memalsukan e-mail atau situs sehingga seolah-olah asli dengan maksud mengelabui pengguna dan memperoleh data pribadi pengguna tersebut[45]

Cybercrime metode phising memanfaatkan situs palsu atau e-mail palsu untuk memperoleh data pengguna internet yang dituju. Pelaku *cybercrime* metode phising yang disebut sebagai pisher seringkali mengelabui pengguna internet dengan mengirimkan e-mail palsu dengan meniru e-mail yang dikirimkan oleh perusahaan resmi. E-mail tersebut berisi perintah agar pengguna membuka link atau tautan lain yang dikirimkan oleh pisher tersebut. *Cybercrime* metode phising umumnya dilakukan dengan melakukan penyamaran sebagai orang lain, baik sebagai situs web palsu maupun dengan tautan palsu. Situs palsu dan tautan palsu ini dapat digunakan pisher untuk mendapatkan data pengguna yang mengunjungi laman dan mengklik suatu pop-up di situs palsu atau tautan palsu tersebut.

Tautan lain yang dikirimkan oleh pisher umumnya bertuliskan beberapa baris subjek seperti, “silahkan masukan user ID/password anda”

[45] Dian Rachmawati, Phising Sebagai Salah Satu Bentuk Ancaman dalam Dunia *Cyber*, Jurnal Saintkom, Edisi No. 3 Vol. 13 2014, hlm. 211.

atau dapat pula berisikan, “silahkan kirim kode OTP anda”. Dengan data-data yang dikirimkan oleh pengguna, maka pisher dapat melakukan kejahatan yang dapat merugikan korban seperti memperoleh keuntungan dengan mengambil uang yang terdapat pada ewallet korban, bank, dan lain sebagainya. *Cybercrime* metode phising dapat memakan banyak korban dikarenakan masih banyak masyarakat yang belum memiliki pengetahuan yang memadai mengenai teknologi, sehingga tidak menyadari bahwa tindakan-tindakan seperti membuka tautan dan situs palsu dapat menyebabkan pencurian data.[46]

Selain itu, masyarakat Indonesia juga belum mengetahui bahwa melakukan pemalsuan situs dapat dengan mudah dilakukan. Internet memungkinkan pengguna untuk melakukan copy dan paste, serta membuat suatu situs mirip dengan aslinya. Dengan tampilan yang terlihat seperti asli tersebut, maka pengguna tidak mengetahui bahwa *cybercrime* metode phising telah terjadi. *Cybercrime* metode phising sangat marak terjadi, tercatat secara global, jumlah *cybercrime* metode phising adalah 42% dari modus selain *cybercrime* metode phising yang dinyatakan dalam website Anti-Phising Working Group (APWG) dalam laporan bulannya, mencatat terdapat 12.845 e-mail baru dan unik serta 2.560 situs palsu yang digunakan sebagai sarana *cybercrime* metode phising.[47]

---

[46] Handrini Ardiyanti, *Cyber*-Security dan Tantangan Pengembangannya di Indonesia, Jurnal Politica, Edisi No. 01 Vol. 05 2014, hlm. 98

[47] Suhardi Rustam, *Analisa Clustering Phising dengan K-Means dalam Meningkatkan Keamanan Komputer*, Ilkom Jurnal Ilimiah, Edisi No. 02 Vol. 10 2018, hlm. 175

Berdasarkan laporan Indonesia *Anti Phising Data Exchange* (IDADX) menunjukkan bahwa pada kuartal pertama tahun 2023, kurang lebih terdapat 26.675 laporan *cybercrime* metode phising di Indonesia, dan pada kuartal kedua tahun 2023 sebanyak 20.330 laporan. Angka tersebut merupakan kelanjutan dari kuartal ke 4 tahun 2022 yang hanya terdapat 6.106 laporan *cybercrime* metode phising, hal tersebut menandakan adanya peningkatan yang sangat signifikan sebanyak 20.569 laporan. Apabila dilihat dalam kurun waktu lima tahun terakhir sebanyak 69.117 laporan *cybercrime* metode phising yang masuk.[48]

Contoh kasus *cybercrime* metode phising di Yogyakarta yang baru saja terjadi, pada tanggal 30 April 2023, seorang Pegawai Negri Sipil (PNS) di Yogyakarta tertipu hingga Rp.600.000.000,00 (enam ratus juta rupiah) setelah ia diundang masuk ke grup aplikasi telegram, kemudian pelaku meminta korban untuk menyelesaikan beberapa misi di aplikasi tiktok dengan mengikuti dan memberikan like beberapa akun yang sudah di tentukan, lalu korban diarahkan untuk melakukan top up di situs yang menyerupai aplikasi tiktok, total dana yang di transfer senilai Rp.600.000.000,00 (enam ratus juta rupiah) namun, ketika korban ingin melakukan pencairan dana selalu dibuat gagal. [49] Kemudian, pada tanggal 25 Mei 2023, seorang pengusaha yang bertempat tinggal di Malang telah mengaku kehilangan uang di rekening bank miliknya sebesar

[48] Indonesia Anti-Phishing Data Exchange, 2023, Laporan Aktivitas Phishing Domain .ID Periode Q2 2023, Jakarta, hlm. 2-3.

[49] Andi Saputra, Gadaikan SK Ratusan Juta, PNS Ini Malah Jadi Korban Phising, terdapat dalam https://news.detik.com/berita/d-6696948/gadaikan-sk-ratusan-juta-pns-ini-malah-jadi-korban-phising, diakses tanggal 8 April 2024 pukul 18.00 WIB.

Rp.1.400.000.000 (satu miliar empat ratus juta rupiah) setelah ia tertipu sebuah file undangan pernikahan yang dikirim melalui Whatsapp dari nomor tidak dikenal.[50]

Dengan banyaknya *cybercrime* metode phising yang merugikan pengguna internet, maka perlu dilakukan pencegahan dan penegakan terhadap phiser. Penegakan hukum *cybercrime* di Indonesia diatur dalam Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik (UU ITE). Berdasarkan UU ITE, maka pelaku *cybercrime* metode phising dapat diancam dengan Pasal 35 dikarenakan dilakukan dengan menggunakan situs palsu yang menyerupai asli. Selain itu, *cybercrime* metode phising juga dapat diancam dengan Pasal 28 ayat (1) dikarenakan termasuk dalam perbuatan yang dilakukan dengan membohongi pengguna untuk menyesatkan pengguna tersebut. Pisher membohongi pengguna dan mengarahkan pengguna menuju situs palsu yang memberikan perintah untuk memberikan data pribadi pengguna kepada pisher tersebut. [51] Dengan demikian, pisher mendapatkan keuntungan dari data pribadi tersebut dan merugikan pengguna yang mengalami kebocoran data.

Cybercrime metode phising tidak hanya melakukan pemalsuan data dengan menyamarkannya sebagai situs asli, namun juga memiliki

---

[50] Tim detikJatim, Unduh File 'Undangan' di WA, Nasabah Kehilangan Duit Tabungan Rp 1,4 M, terdapat dalam https://www.detik.com/jateng/berita/d-6810966/unduh-file-undangan-di-wanasabah-kehilangan-duit-tabungan-rp-14-m., diakses tanggal 8 April 2024 pukul 18.00 WIB.

[51] Ardi Saputra Gulo, Sahuri Lasmadi, dan Khabib Nawawi, *Cybercrime* dalam Bentuk Phising Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik, PAMPAS: Journal of Criminal Law, Edisi No. 02 Vol. 01 2021, hlm. 70.

maksud untuk memperoleh data pribadi pengguna internet untuk digunakan secara ilegal. Sementara, dalam Pasal 35 UU ITE hanya mengandung unsur pemalsuan data tanpa adanya unsur maksud dan tujuan untuk melakukan tindak kejahatan yang merugikan korban.

5) Sejarah Cybercrime

Sejarah *Cybercrime*Awal mula penyerangan didunia *Cyber* pada tahun 1988 yang lebih dikenal dengan istilah *Cyber* Attack.Pada saat itu ada seorang mahasiswa yang berhasil menciptakan sebuah *worm* atau virus yang menyerang program computer dan mematikan sekitar 10% dari seluruh jumlah komputer di dunia yang terhubung ke internet Pada tahun 1994 seorang anak sekolah musik yang berusia 16 tahun yang bernama RichardPryce, atau yang lebih dikenal sebagai "*the hacker*" alias "*Datastream Cowboy*"(liran data cowboy), ditahan lantaran masuk secara ilegal ke dalam ratusan sistem komputer rahasia termasuk pusat data dari Griffits AirForce, NASA(National Aeronautics and Space Administration) dan Korean Atomic Research Institute atau badan penelitian atom Korea Dalam interogasinya dengan FBI, ia mengaku belajar *hacking* dan *cracking* dari seseorang yang dikenalnya lewat internet dan menjadikannya seorang mentor, yang memiliki julukan "Kuji". Hebatnya, hingga saat ini sang mentor pun tidak pernah diketahui keberadaannya. Hingga akhirnya, pada bulan Februari 1995, giliran Kevin Mitnick diganjar hukuman penjara untukyang kedua kalinya. Dia dituntut dengan tuduhan telah mencuri sekitar 20.000 nomor kartu kredit. Bahkan, ketika ia bebas,

ia menceritakan kondisinya di penjara yang tidak boleh menyentuh komputer atau telepon.

B. Bentuk-Bentuk Tindak Pidana *Cybercrime*

Cybercrime mempunyai bentuk beragam, karena setiap negara tidak selalu sama dalam melakukan krimininalisasi. Begitu pula, dalam setiap negara dalam menyebut apakah suatu perbuatan tergolong kejahatan *cybercrime* atau bukan kejahatan *cybercrime* juga belum tentu sama. Secara teoritik, berkaitan dengan konsepsi kejahatan. Muladi mengemukakan bahwa asas *mala in se* mengajarkan bahwa suatu perbuatan dikategorikan sebagai kejahatan karena masyarakat dengan sendirinya menganggap perbuatan tersebut jahat. Sedangkan berdasarkan asas mala prohibita, suatau perbuatan dianggap jahat karena melanggar peraturan perundang-undangan. [52] Asas *Mala Prohibita* menghasilkan konsepsi kejahatan dalam arti yuridis (yaitu sebagaimana diatur dalam peraturan perundang-undangan tertulis). Jonathan Rosenoer menjelaskan tentang bentuk-bentuk *cybercrime* sebagai berikut:

1. *Copright, include exclutive right, subject matter of copyright, formalities, infringement, source of risk, word wide web sites, hypertext link, graphical element, e-mail, criminal liability, fair use, first amandment, and softwere rental.*
2. *Trademark*
3. *Defamation*
4. *Privacy, include common law privacy, constitutinal law, anonymity, and technology expanding privacy right.*
5. *Duty of care*
   a) *Negligence*

[52] Muladi, 2002, *Demokratisasi , Hak Asasi Manusia, dan Reformasi Hukum di Indonesia,* Habibie Center, Jakarta, hlm. 196

b) Negligent misstatement
c) Equipment malfunctions
d) Economic loss may not be recoverable
e) Contractural limitations of liability.

6. *Criminal liability; such as; computer fraud and abuse act, wire fraund. Electronic communication privacy act, extortion and threats, expose, sexual exploitation of children, obscene and indent telephone call, copyright stalking.*
7. *Procedural issues, include jurisdiction, venue and conflict of law.*
8. *Electronic contract and digital signature, include electronic agreement enforceable, public key encryption and digital signature.*[53]

Cybercrime meliputi pelanggaran hak kekayaan intelektual, fitnah atau pencemaran nama baik, pelanggaran terhadap kebebasan pribadi (privacy), ancaman dan pemerasan, ekploitasi seksual anak-anak dan pencabulan, perusakan sistem komputer, pembobolan kode akses, dan pemalsuan tanda tangan digital. Semua perbuatan tersebut dapat dipertanggungjawabkan secara pidana sesuai dengan yurisdiksinya. *Cybercrime* juga dapat berbentuk pemalsuan data, penyebaran virus komputer ke jaringan komputer atau sistem komputer, penambahan atau pengurangan sistem instruksi dalam jaringan komputer, pembulatan angka, perusakan data, dan pembocoran data rahasia. Ini diuraikan oleh Sue Titus Reid, bahwa *cybercrime* meliputi "*data diddling, the Trojan horse, the salami technique, superzapping, and date leakgage".*[54]

The International *Handbook on Computer Crime* mengklasifikasikan bentuk-bentuk *cybercrime* sebagai berikut.

1. *Computer-related Economic Crimes*

---

[53] Jonathan Rosenoer, 1997, *Cyberlaw: The Law of the Internet,* SpringVerlag, New York, hlm. 45

[54] Sue Titus Reid, 1985*, Crime and Criminology*, CBS College Publishing, New York, hlm. 56

   a. *Fraund by Computer Manipulation*
   b. *Computer Espionage and Software Piracy*
   c. *Computer Sabotage*
   d. *Theft of Services*
   e. *Unauthorized Access to DP Systems and Hacking*
   f. *The Computer as a Tool for traditional Business Offences*
2. *Computer-related Infrigements of Privacy*
   a. *Use of Incorrect Data*
   b. *Illegal Collection and Storage of Correct Data*
   c. *Illegal Disclosure and Misuse of data*
   d. *Infrigments of Formalities of Privancy Laws*
3. *Further Abuses*
   a. *Offences Against State and Political Interests*
   b. *The Extension to Offences Against Personal Intergity*[55]

Berdasarkan uraian *Handbook on Computer Crime, cybercrime* dikategorikan menjadi tiga. Kategori pertama, *cybercrime* adalah kejahatan ekonomi yang terkait dengan komputer, meliputi penipuan dengan manipulasi komputer, pembajakan perangkat lunak komputer, spionase komputer, sabotase, pencurian jasa, akses tidak sah ke dalam sistem atau jaringan komputer, komputer sebagai alat untuk menyerang bisnis tradisional. Kategori ke dua, adalah pelanggaran terhadap keleluasaan pribadi, yaitu penggunaan data yang tidak benar, pengumpulan data secara tidak sah, penyalahgunaan data, pelanggaran rahasia perusahaan. Sedangkan kategori ketiga, misalnya melakukan penyerangan terhadap dan kepentingan politik, dan penyerangan terhadap kebebasan pribadi orang per orang.

Selain penggolongan *cybercrime* sebagaimana terjabar di atas, Donn Parker mengklasifikasikan bentuk-bentuk *cybercrime* ke dalam empat klarifikasi berikut.

---

[55] *Ibid.*

1. Komputer sebagai Objek

   Dalam kategori ini, bentuk-bentuk *cybercrime* termasuk kasus-kasus perusakan terhadap komputer, data atau program yang terdapat di dalamnya atau perusakan terhadap sarana-sarana komputer seperti *Air Condutouring* (AC) dan peralatan yang menunjang pengoprasian komputer.

2. Komputer sebagai Subjek

   Komputer dapat pula menimbulkan tempat atau lingkungan untuk melakukan kejahatan, misalnya pencurian, penipuan, dan pemalsuan yang menyangkut harta benda dalam bentuk baru yang tidak dapat disentuh (*intangible*), misalnya pulsa elektronis dan guratan-guratan magnetis.

3. Komputer sebagai Alat

   Komputer digunakan sebagai alat melakukan kejahatan sehingga sifat peristiwa kejahatan tersebut adalah sangat kompleks dan sulit diketahui. Salah satu contoh adalah seseorang pelaku kejahatan yang mengambil warkat-warkat setoran darai suatu bank dan menulis nomor rekening pelaku dengan tinta magnetis pada warkat-warkat tersebut kemudian melaetakkan kembali ke tempat semula. Nasabah yang akan memasukkan uang akan mengambil dan mengisi warkat yang sudah dibubuhi nomor rekening pelaku kejahatan memroseswarkat-warkat nasabah, komputer secara otomatis akan mengredit sejumlah uang pada rekening pelaku kejahatan. Salah iyu,

pelaku kejahatan menarik uang dengan cek dari rekeningnya sebelum peran nasabah yang menyetor mengajukan complain ke bank.

4. Komputer sebagai simbol

   Suatu komputer dapat digunakan sebagai simbol untuk melakukan penipuan atau ancaman, dalam kategori ini termasuk penipuan “Biro Jodoh” yang menyatakan bahwa biro jodoh tersebut memakai komputer untuk membantu si koraban mencari jodoh, akan tetapi ternyata birojodoh tersebut sama sekali tidak memakai komputer untuk keperluan tersebut.

Kejahatan yang berhubungan dengan komputer (*cybercrime*) sudah diatur oleh istrumen internasional. Satu-satunya instrument internasional yang mengatur kejahtan yang berhubungan dengan komputer adalah *Convention on Cybercrime*. Dalam Bab II konvensi tersebut diatur tentang hukum pidana substantive, yaitu sebagiaman terjabar dalam Pasal (article) 2 sampai dengan Pasal 11. Sedangkan Pasal 12-13 mengatur mengenai ketentuan pemidanaan. Ketentuan tersebut adalah seabagai berikut:

1. *Title 1, offences against the confidentiality, integrity and availability of computer data and system*
   a. *Illegal access (article 2);*
   b. *Illegal interception (article 3);*
   c. *Data interference,*
   d. *Damaging, deleting, deterioration, alteration or suppression of computer data without right (article 4);*
   e. *System interference (article 5);*
   f. *Misuse of devices (access code) (article 6).*

2. *Title 2, Computer Related Offences:*
   a. *Computer related forgery (article 7);*

b. Computer related fraud (article 8).
   1) Title 3, Content Related Offences:
   2) Title 4, Offences Related to Infringement of Copyright and Related Right (article 10).
   3) Title 5, Ancillary laiability and sanction (article 11); (article 12, (article 13).

Berdasarkan ringkasan ketentuan dalam *Convention on Cybercrime* dapat dipahami bahwa dalam bagian 1, Pelanggaran terhadap kerahasiaan, ketersediaan dan integeritas sistem dan data komputer, terdiri atas perbutan berikut:

1. Akses tidak sah, yaitu sengaja memasuki atau mengakses komputer tanpa hak (Pasal 2);
2. Intersepsi tidak sah, yaitu sengaja dan tanpa hak mendengar atau menangkap secara diam-diam pengiriman transmisi dan pemancaran (emisi) data komputer yang tidak bersifat publik ke, dari atau di dalam sistem komputer dengan menggunakan alat bantu teknis (Pasal 3);
3. Gangguan atau perusakan data, yaitu sengaja dan tanpa hak melakukan perusakan.
4. Penghapusan, perubahan atau penghapusan data komputer (Pasal 4);
5. Gangguan atau perusakan sistem, yaitu sengaja melakukan gangguan atau rintangan secara serius tanpa hak terhadap berfungsinya sistem komputer (Pasal 5);
6. Penyalahgunaan peralatan, yaitu penyalahgunaan perlengkapan komputer, termasuk program komputer, password komputer, kode masuk (access code) (Pasal 6).

Kemudian dalam bagian 2, diatur tentang pelanggaran yang berhubungan dengan komputer, yaitu dalam bentuk berikut.

1. Pemalsuan yang berhubungan dengan komputer (Pasal 7), yaitu pemalsuan (dengan sengaja dan tanpa hak memasukkan, mengubah, menghapus data otentik menjadi tidak otentik dengan maksud untuk digunakan sebagai data otentik);
2. Penipuan yang berhubungan dengan komputer (Pasal 8), yaitu penipuan (dengan sengaja dan tanpa hak menyebabkan hilangnya barang atau kekayaan orang lain dengan cara memasukkan, mengubah, menghapus data komputer, atau dengan mengganggu berfungsinya komputer, dengan tujuan untuk memperoleh keuntungan ekonomi bagi dirinya sendiri atau orang lain).

Selanjutnya dalam bagian 3 tentang Pelanggaran yang berhubungan dengan isi, yaitu berkaitan dengan delik-delik yang berhubungan dengan pornografi anak (Pasal 9), yaitu meliputi perbuatan:

1. Memproduksi dengan tujuan mendistribusikan melalui sistem komputer;
2. Menawarkan melalui sistem komputer;
3. Mendistribusikan atau mengirim melaui sistem komputer;
4. Memperoleh melalui sistem komputer;
5. Memiliki dalam sistem komputer atau di dalam media penyimpanan data.

Akhirnya dalam bagian 4 tentang Pelanggaran yang berhubungan dengan Hak Cipta (Pasal 10), yaitu delik-delik yang terkait dengan pelanggaran hak cipta. Sedangkan pada bagian 5, diatur tentang pertanggungjawabkan pidana dan sanksi; Percobaan dan Pembantuan (Pasal 11); Pertanggungjawaban Korporasi (Pasal 12); Sanksi dan tindakan (Pasal 13).

Berdasarkan ketentuan-ketentuan dalam konvensi tersebut dapat disimpulkan bahwa delik-delik *cybercrime* suadah diatur secara umum dalam konvensi. Meskipun demikian, setiap Negara diberi peluang untuk mengembangkan dan mengharmonisasikan dengan kebutuhan Negara yang bersangkutan tanpa mengesampingkan kepentingan masyarakat internasional. Karena itu, bahasa yang digunakan bersifat netral, dan bentuk-bentuk kejahatan yang diatur dalam konvensi adalah ketentuan setandar minimum.

Modus Operandi dan berkembangnya tindak pidana *cybercrime* sehingga bentuk-bentuk tindak pidana *cybercrime* semakin banyak. Hal ini dipengaruhi oleh beberapa faktor. Faktor-Faktor Terjadinya Tindak Pidana *Cybercrime*:

1. Kesadaran Hukum Masyarakat

Proses penegakan hukum pada dasarnya adalah upaya mewujudkan keadilan dan ketertiban di dalam kehidupan bermasyarakat. *Cybercrime* adalah sebuah perbuatan yang tercela dan melanggar kepatutan di dalam masyarakat serta melanggar hukum. Sampai saat ini,

kesadaran hukum masyarakat Indonesia dalam merespon aktivitas *cybercrime* kurang. Hal ini disebabkan anatara lain oleh kurangnya pemahaman dan pengetahuan masyarakat terhadap jenis kejahtan *cybercrime*. Kurangnya perhatian masyarakat. Masyarakat dan penegak hukum saat ini masih memberi perhatian yang sangat besar terhadap kejahatan konvesional. Pada kenyataannya para pelaku kejahatan komputer masih terus melakukan aksi kejahatannya. Sehingga hal tersebut membuat kejahatan tersebut meningkatn dan meluas akibatnya.

2. Faktor Keamanan

Rasa aman tentunya akan dirasakan oleh pelaku kejahatan *Cybercrime* pada saat sedang menjalankan aksinya. Hal ini tidak lain karena internet lazim dipergunakan di tempat-tempat yang relatif tertutup, seperti di rumah, kamar, tempat kerja, perpustakaan dan warung internet. Aktivitas yang dilakukan oleh pelaku di tempat-tempat tersebut sulit untuk diketahui oleh pihak luar. Akibatnya pada saat pelaku sedang melakukan tindak pidana sangat jarang orang luar mengetahuinya. Hal ini, sangat berbeda dengan kejahatan-kejahtan yang sifatnya konvensional, yang mana pelaku akan mudah diketahui secara fisik ketika sedang melakukan aksinya. Sehingga rasa aman yang diperoleh dalam melakukan tindak pidana tersebut membuat tindak pidana *cybercrime* terjadi terus menerus dan meningkat.

3. Faktor Penegak Hukum

Faktor penegak hukum sering menjadi penyebab maraknya kejahatan siber (*cybercrime*). Hal ini dilatarbelakangi masih sedikitnya aparat penegak hukum yang memahami seluk beluk teknologi informasi (internet), sehingga pada saat pelaku tindak pidana ditangkap, aparat penegak hukum mengalami kesulitan untuk menemukan alat bukti yang dapat dipakai menjerat pelaku. Sehingga tak jarang jika pelaku dapat lolos dari jeratan hukum dan tindak pidana tersebut semakin banyak.

4. Faktor Sosial Ekonomi

Faktor ini juga mempengaruhi maraknya tindak pidana *cybercrime* karena Isu global yang kemudian dihubungkan dengan kejahatan tersebut sebenarnya merupakan masalah keamanan jaringan (*security network*). Keamanan jaringan merupakan isu global yang muncul bersamaan dengan internet. Sebagai komoditi ekonomi, banyak negara yang sangat membutuhkan perangkat keamanan jaringan. *Cybercrime* berada dalam skenario besar dalam kegiatan ekonomi dunia, sosial ekonomi yang meningkat membuat celah-celah pelaku dalam menjalankan aksinya.

5. Faktor Globalisasi

Adanya teknologi internet akan menghilangkan batas wilayah negara yang menjadikan dunia ini menjadi begitu dekat dan sempit. Saling terhubungnya antara jaringan yang satu dengan jaringan yang lain sehingga memudahkan pelaku kejahatan untuk melakukan aksinya. Kemudian, tidak meratanya penyebaran teknologi menjadikan yang satu

lebih kuat dari pada yang lain. Akses internet yang tidak terbatas. Dengan akses internet yang tidak terbatas pengguna internet dengan bebas mengakses situs-situs yang ada di internet sehingga hal ini menimbulkan adanya pelaku *cybercrime* dengan cara download, upload dan lain sebagainya secara illegal atau tidak sah.

C. Penegakan Hukum Terhadap Pelaku Tindak Pidana *Cybercrime*

Penegakan hukum merupakan suatu proses untuk mewujudkan keinginan-keinginan hukum menjadi kenyataan. Keinginan hukum inilah yang nantinya menjadi pikiran badan pembuat undang-undang yang dirumuskan dalam peraturan-peraturan hukum. Perumusan pikiran pembuat hukum dituangkan dalam peraturan hukum yang nantinya menentukan bagaimana penegakan hukum itu dijalankan. Pada kenyataannya proses penegakan hukum memuncak pada pelaksanaannya oleh para pejabat penegak hukum.[56]

Aparat penegak hukum di Indonesia adalah hakim, jaksa, polisi. Hakim adalah salah satu aparat penegak hukum yang melaksanakan suatu sistem peradilan yang mempunyai tugas untuk menerima dan memutus perkara dengan seadil-adilnya. Hakim adalah pejabat yang melakukan kekuasaan kehakiman yang diatur dalam undang-undang Nomor 48 Tahun 2009 tentang kekuasaan kehakiman. Dalam rangka penegakan hukum di Indonesia tugas hakim adalah menegakkan hukum

[56] Satjipto Rahardjo, 2009, *Penegakan Hukum Suatu Tinjauan Sosiologis*, Genta Publishing, Cetakan 1, Yogyakarta, hlm. 24.

dan keadilan melalui perkara-perkara yang dihadapkan kepadanya. Jaksa adalah aparat penegak hukum yang merupakan pejabat fungsional yang diberikan wewenang oleh undangundang dan pelasanaan putusan pengadilan. Selanjutnya adalah Polisi, polisi sebagai penegak hukum dituntut melaksanakan profesinya secara baik dengan dilandasi etika profesi. Etika profesi tersebut berpokok pangkal pada ketentuan yang menentukan peranan polisi sebagai penegak hukum. Polisi dituntut untuk melaksanakan profesinya dengan adil dan bijaksana, serta mendatangkan keamanan dan ketenteraman.

Penegakan hukum selalu akan melibatkan manusia di dalamnya dan dengan demikian hal tersebut tingkah laku manusia terlibat di dalamnya. Hukum tidak bias tegak dengan sendirinya sehingga melibatkan aparat penegak hukum, dan aparat dalam mewujudkan tegaknya hukum harus dengan undang-undang, sarana, dan kultur, sehingga hukum dapat ditegakkan dengan seadil-adilnya sesuai dengan cita hukum itu sendiri.

Hal ini menunjukan bahwa tantangan yang dihadapi oleh aparat penegak hukum bukan tidak mungkin sangatlah banyak Penegak hukum tidak hanya dituntut untuk professional dan tepat dalam menerapkan normanya akan tetapi juga dituntut dapat membuktikan kebenaran atas dakwaan kejahatan yang terkadang dipengaruhi oleh rangsangan dari prilaku masyrakat untuk sama-sama menjadi pelanggar hukum.

Pendapat Soerjono Soekanto mengatakan bahwa pokok penegakan hukum terletak pada faktor-faktor yang mempengaruhinya. Faktor-faktor tersebut, adalah sebagai berikut:[57]

1. Faktor hukumnya sendiri, yaitu peraturan perundang-undangan yang berlaku di Indonesia.
2. Faktor penegak hukum, yakni pihak-pihak yang membentuk maupun menerapkan hukum.
3. Faktor sarana atau fasilitas yang mendukung penegakan hukum
4. Faktor masyarakat, yakni lingkungan dimana hukum tersebut berlaku atau diterapkan.
5. Faktor kebudayaan, yakni sebagai hasil karya, cipta dan rasa yang didasarkan pada karsa manusia didalam pergaulan hidup

Dari kelima faktor tersebut saling berkaitan dengan eratnya karena antara yang satu dengan yang lainnya saling mempengaruhi. Kelima faktor tersebut dapat dikatakan esensi dari penegakan hukum, dan dapat dijadikan tolok ukur daripada keefektifitasan penegak hukum di Indonesia.

Kejahatan teknologi informasi atau *cybercrime* memiliki karakter yang berbeda dengan tindak pidana lainnya baik dari segi pelaku, korban, modus operandi dan tempat kejadian perkara sehingga butuh penanganan dan pengaturan khusus di luar Kitab Undang-Undang Hukum Pidana (KUHP) dan juga Kitab Undang-Undang Hukum Acara Pidana (KUHAP). Terkait dengan hukum pembuktian biasanya akan

memunculkan sebuah posisi dilema, di salah satu sisi diharapkan agar hukum dapat mengikuti perkembangan zaman dan teknologi, di sisi yang lain perlu juga pengakuan hukum terhadap berbagai jenis-jenis perkembangan teknologi digital untuk berfungsi sebagai alat bukti di pengadilan. Pembuktian memegang peranan yang penting dalam proses pemeriksaan sidang pengadilan. Pembuktian inilah yang menentukan bersalah atau tidaknya seseorang yang diajukan di muka pengadilan. Apabila hasil pembuktian dengan alat bukti yang ditentukan dengan undang-undang tidak cukup membuktikan kesalahan dari orang tersebut maka akan dilepaskan dari hukuman, sebaliknya apabila kesalahan dapat dibuktikan maka dinyatakan bersalah dan dijatuhi hukuman. Oleh karena itu harus berhati-hati, cermat dan matang dalam menilai dan mempertimbangkan masalah pembuktian.

Muncul kesulitan dalam penerapan hukum dan penegakan hukum terhadap tindak pidana *cybercrime* yakni dalam penyelesaian tindak pidana tersebut , kondisi yang paperless (tidak menggunakan kertas) ini menimbulkan masalah dalam pembuktian mengenai informasi yang diproses, disimpan, atau dikirim secara elektronik. mendasar penggunaan bukti elektronik dalam proses pembuktian perkara pidana, khususnya yaitu tidak adanya patokan atau dasar penggunaan bukti elektronik di dalam perundang-undangan kita. Selain itu sulitnya mengungkap tindak pidana tersebut baik pelaku, dan kejahtan yang sering sekali sulit untuk

dibuktikan sehingga hal tersebut menjadi tantangan tersendiri dalam penegakan hukum tindak pidana *cybercrime.*

Setiap penegak hukum diberi kewenangan berdasarkan Peraturan Perundang-undangan yang berlaku untuk menjelaskan tugasnya. Dalam penanganan tindak pidana *cybercrime*, hukum acara yang digunakan yaitu hukum acara berdasarkan KUHAP. Hal tersebut memang tidak disebutkan secara jelas dalam atas Undang-undan Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik, tetapi karena undang-undang tersebut tidak menetukan lain maka KUHAP berlaku bagi tindak pidana yang termuat dalam Undang-undan Nomor 11 tahun 2008. Dalam Pasal 42 UU Undang-undang Nomor 11 tahun 2008 disebutkan : “Penyidikan terhadap tindak pidana sebagimana dimaksud dalam undang-undang ini dilakukan berdasarkan ketentuan dalam Hukum Acara Pidana dan Ketentuan dalam Undang-undang ini.” Hal tersebut juga ditegaskan dalam UU No 19 Tahun 2016 tentang perubahan atas UU No 11 tahun 2008 tentang Informasi dan Transaksi Elektronik, bahwa dalam perubahan tersebut sama sekali tidak merubah Pasal 43.

Berdasarkan pasal tersebut sehingga dapat ditafsirkan bahwa Hukum Acara Pidana yang diatur dalam KUHAP merupakan lex genaralis, sedangkan ketentuan acara dalam UU No 11 tahun 2008 tentang Informasi dan Transaksi Elektronik dan UU No 19 Tahun 2016 tentang perubahan atas UU No 11 tahun 2008 tentang Informasi dan Transaksi Elektronik, ini merupakan lex specialis. Dengan demikian sepanjang tidak

terdapat ketentuan lain maka ketentuan hukum acara yang digunakan seperti yang terdapat dalam KUHAP. Ketentuan yang diatur lain dalam UU ITE ini yaitu menyangkut proses penyidikan dan penambahan satu alat bukti lain dalam penanganan tindak pidana yang diatur dalam UU ITE.

Pelaksanaan penyelidikan tindak pidana *cybercrime* agak sedikit berbeda dengan penyelidikan tindak pidana lainya, pejabat dalam hal ini adalah pejabat polisi Negara Republik Indonesia yang diberi wewenang oleh undang-undang ini untuk melakukan penyelidikan (Pasal 1 angka 4 KUHAP) dihadapkan pada masalah dari mana dan dimana penyelidikan harus dimulai. Akibat perbuatan tindak pidana *cybercrime* seperti *cyber porno, cyber terrorism, hacking* , dll baik yang diketahui pertama kali oleh penyelidik yang sedang melukan *cyber*-patroling maupun berdasarkan laporan dari korban tindak pidana *cybercrime*, diketahui melalui layar monitor suatu komputer yang terhubung dengan jaringan melalui koneksi internet, ataupun terjun langsung ke warnet-warnet.

Proses awal penyelidikan harus melibatkan komputer, alat elektronik seperti handphone maupun android, tablet, dan jaringannya yang terkoneksi dengan suatu jaringan dan terkoneksi melalui internet. Bukti-bukti dalam suatu tindak pidan *cybercrime* biasanya selalu dapat tersimpan di dalam sistem alat alat elektronik tersebut ataupun sistem komputer. Dengan Demikian inti dari suatu proses penyelidikan adalah bagaimana menemukan dan selanjutnya menyita alat alat atau barang

elektronik maupun komputer milik tersangka. Dari komputer tersebutlah penyelidikan dapat menentukan apakah ada bukti-bukti tindak pidana.

Karakteristik tindak pidana *cybercrime* berbeda dengan tindak pidana yang lain , karakteristik bentuk tindak pidana *cybercrime* antara yang satu dengan yang lain pun berbeda hal ini dikarenakan modus operandi yang digunakan berbeda. Sehingga dengan demikian dalam penegakan hukum dan dalam proses beracaranya dari tahap penyelidikan dan penyidikan memerlukan ketentuan khusus. Ketentuan khusus yang berkaitan dengan acara pidana yang terdapat dalam Undang-undang Nomor 11 Tahun 2008, yang telah dirubah oleh Undang-undang Nomor 19 Tahun 2016 tentang perubahan atas Undang-undang Nomor 11 Tahun 2008 tentang informasi dan transaksi elektronik adalah sebagai berikut;

1. Diakuinya alat bukti elektronik yang berupa informasi elektronik dan dokumen elektronik sebagai alat bukti yang sah dalam pembuktian tindak pidana *cybercrime*.
2. Adanya wewenang khusus yang diberiakan kepada Pejabat Pegawai Negeri Sipil tertentu dilingkungan Pemerintah yang lingkup tugas dan tanggungjawabnya di bidang Teknologi Informasi dan transaksi elektronik sebagai penyidik
3. Adanya kewenangan penyidik, penuntut umum, dan hakim untuk meminta keterangan kepada penyedia jasa dan penyelenggara sistem elektronik mengenai data-data yang berhubungan dengan tindak

pidana, dengan tetap terikat terhadap privasi, kerahasian, dan kelancaran layanan publik, integritas data dan keutuhan data.

4. Adanya wewenang terhadap penyidik untuk melakukan penggeledahan, penyitaan terhadap sistem elektronik yang terkait dengan dugaan tindak pidana harus dilakukan atas izin ketua pengadilan negeri setempat, hal ini menghindari agar sistem elektronik tersebut tidak bias hapus oleh pelaku dan menghindari agar pelacakan pelaku berjalan cepat, sehingga jejak pelaku mudah untuk ditemukan.

Upaya penegakan hukum terhadap tindak pidana *cybercrime* selain dengan aturan-aturan tersebut seharusnya juga diimbangi dengan skill dan kemampuan penegak hukumnya dalam pemberantasan tindak pidana *cybercrime*. Hal ini dikarenakan modus-modus tindak pidana *cybercrime* semakin hari semakin berkembang dikhawatirkan kejahatan tersebut akan merajalela dan pelaku-pelaku sulit untuk dilacak dan ditangkap, sehingga dapat merugikan masyarakat dan Negara dan bahkan dunia luas.

Indonesia sebagaimana tercantum dalam Pasal 1 ayat (3) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 dengan tegas menyebutkan bahwa “Negara Indonesia adalah negara hukum”. Maka dengan diadakannya hukum di tengah-tengah kehidupan bermasyarakat dalam suatu negara membuat semakin dipermudah upaya dalam pencapaian tujuan hidup bagi masyarakat itu sendiri yaitu hidup dengan aman dan tenteram. Dalam kehidupan di tengah-tengah masyarakat, banyak dirangkaikan dengan kehadiran tindak pidana sehingga

mengharuskan untuk diadakannya pemidanaan agar upaya penegakan dan pemeliharan tujuan hidup masyarakat dapat diperhatikan dengan baik. Pemidanaan terhadap pelaku kejahatan tentunya menjadi hal yang sepatutnya dilakukan agar selain memberikan efek jera terhadap pelaku juga menjadi bagian dari upaya yang dilakukan oleh negara terhadap penegakan keadilan di dalam negeri.

Suatu perbuatan dapat disebut sebagai suatu tindak pidana jika perbuatan tersebut dilarang serta diancam pidana menurut peraturan perundang-undangan yang berlaku, dan sebuah tindak pidana dapat diberikan pemidanaan jika perbuatan tersebut terdapat unsur kesalahan sehingga pelaku dapat mempertanggungjawabkan perbuatannya tersebut dengan pemberian pidana atau hukuman. Peraturan perundang-undangan tentang Hukum Pidana di Indonesia menyebutkan jenis-jenis pidana yang ada dan berlaku di Indonesia, sebagaimana yang diatur dalam Pasal 10 KUHP, antara lain: 1. Pidana Pokok: a. Pidana mati; b. Pidana penjara; c. Pidana kurungan; d. Pidana denda; e. Pidana tutupan. 2. Pidana tambahan: a. Pencabutan hak-hak tertentu; b. Perampasan barang-barang tertentu; c. Pengumuman putusan hakim. Sebelum adanya UU ITE, kasus *cybercrime* di Indonesia diadili menggunakan analogi terhadap pasal yang memiliki kesesuaian unsur dalam Kitab Undang-Undang Hukum Pidana sehingga pemidanaan kepada para pelaku *cybercrime* menggunakan Kitab Undang-Undang Hukum Pidana atau disingkat dengan KUHP ini. Dalam KUHP, ketentuan pidana pada kasus *cybercrime*

berbentuk phising dapat digunakan berdasarkan pasal 378 KUHP, sebagaimana berbunyi:

> "Barangsiapa dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum, dengan memakai nama palsu atau martabat palsu, dengan tipu muslihat, ataupun rangkaian kebohongan, menggerakan orang lain untuk menyerahkan barang sesuatu kepadanya, atau supaya memberi hutang maupun menghapuskan piutang diancam karena penipuan dengan penjara paling lama empat tahun". Terhadap pasal tersebut, sama seperti dalam putusan di Pengadilan Negeri Sleman, Yogyakarta dengan terdakwa atas nama Petrus Angkur dipidana dengan secara sah terbukti melakukan tindak pidana pemalsuan di internet berdasarkan Pasal 378 KUHP. Pelaku melakukan transaksi pembelian sebuah barang di e-commerce menggunakan kartu kredit milik warga negara Amerika Serikat senilai Rp. 4.000.000,00 (empat juta rupiah) secara melawan hukum sehingga pelaku dipidana penjara selama 15 bulan[58]

Penggunaan Pasal KUHP dalam pemidanaan pada kasus *cybercrime* hanya dilakukan berdasarkan penafsiran dikarenakan terdapat perbedaan terhadap jenis tindak pidana *cybercrime* dengan tindak pidana konvensional yang ada, walaupun metode phising dan penipuan dalam KUHP memiliki kesamaan unsur perbuatannya akan tetapi tetap memiliki perbedaan mulai dari mulai dari bentuk tindak pidana, penentuan locus delicti sampai tempos delicti-nya. Oleh karena itu, tindak pidana *cybercrime* merupakan pengelompokkan dari jenis tindak pidana yang tergolong baru, dikarenakan *cybercrime* hadir mengikuti perkembangan teknologi yang baru berkembang pesat.

Pasal 492 Undang-Undang Nomor 1 tahun 2003 tentang Kitab Undang-Undang Hukum Pidana (KUHP Baru) menegaskan bahwa :"

---

[58] Andri Winjata Laksana, *"Pemidanaan Cybercrime Dalam Perspektif Hukum Pidana Positif*", Jurnal Hukum Unissula, Vol.35 No.1, 2019, hlm.60-61.

setiap orang dengan maksud menguntungkan diri sendiri atau orang lain secara melawan hukum dengan memakai nama palsu atau kedudukan palsu, menggunakan tipu muslihat atau rangkaian kata bohong, menggerakkan orang supaya menyerahkan suatu barang, memberi utang, membuat pengakuan utang, atau menghapus piutang, dipidana karena penipuan dengan pidana penajra paling lama 4 tahun atau pidana denda paling banyak kategori V, yaitu Rp. 500.000.000 (lima ratus juta rupiah).”

Tujuan perbuatan dalam sebuah penipuan dibagi menjadi 2 (dua) unsur,yakni:

a. Menyerahkan benda, dalam hal ini pengertian benda dalam penipuan memiliki arti yang sama dengan benda dalam pencurian dan penggelapan, yakni sebagai benda yang berwujud dan bergerak. Pada penipuan benda yang diserahkan dapat terjadi terhadap benda miliknya sendiri asalkan di dalam hal ini terkandung maksud pelaku untuk menguntungkan diri sendiri atau orang lain. Pendapat ini didasarkan pada ketentuan bahwa dalam penipuan menguntungkan diri tidak perlu menjadi kenyataan, karena dalam hal ini hanya unsur maksudnya saja yang ditujukan untuk menambah kekayaan.

b. Memberi hutang dan menghapuskan piutang, dalam hal ini perkataan hutang tidak sama artinya dengan hutang piutang, melainkan diartikan sebagai suatu perjanjian atau perikatan. Hoge Raad menyatakan bahwa yang dimaksud dengan hutang adalah suatu perikatan, misalnya

menyetor sejumlah uang jaminan. Oleh karenanya memberi hutang tidak dapat diartikan sebagai memberi pinjaman uang belaka, melainkan diberi pengertian yang lebih luas sebagai membuat suatu perikatan hukum yang membawa akibat timbulnya kewajiban bagi orang lain untuk menyerahkan atau membayar sejumlah uang tertentu. Demikian juga dengan istilah utang, dalam kalimat menghapuskan piutang mempunyai arti suatu perikatan.

Hal tersebut membuat diperlukan adanya suatu aturan khusus yang jelas menangani tindak pidana *cybercrime* ini. Karena jika hanya mengandalkan penafsiran saja akan membuat berbenturnya suatu tatanan hukum sehingga membuat praktik penegakan hukum kurang maksimal. Mengingat juga kaitannya dengan asas legalitas, yaitu tidak ada suatu perbuatan dapat dipidana kecuali berdasarkan ketentuan pidana yang mengatur sebelumnya sehingga ancaman pemidanaan terhadap *cybercrime* dapat diketahui jauh sebelumnya oleh seluruh masyarakat melalui peraturan tersebut.

Terhadap penafsirannya, dikemukakan oleh Andi Hamzah bahwa penafsiran hukum terbagi atas 5 (lima) jenis penafsiran, antara lain:

1. Penafsiran gramatikal, yaitu penafsiran pada setiap kata dalam sebuah undang-undang.
2. Penafsiran sistematis, yaitu penafsiran kepada hubungan dalam suatu aturan pidana secara umum.

3. Penafsiran historis, yaitu penafsiran pada maksud dari pembuat undang-undang ketika undang-undang tersebut diciptakan.
4. Penafsiran teologis, yaitu penafsiran pada tujuan dari sebuah undang-undang.
5. Penafsiran ekstensif, dimana penafsiran ini dilakukan dengan memperluas makna dari sebuah ketentuan. [59] Dari kutipan Paul Scholten, Moeljatno menyampaikan bahwa penafsiran eksentif ini selalu dikaitkan dengan analogi, dikarenakan keduanya mempunyai kesamaan dasar yaitu untuk menemukan norma yang lebih tinggi dari norma yang ada. Sehingga, dapat memperluas suatu aturan yang ada dan akhirnya melahirkan aturan yang baru. Moeljatno mendukung penggunaan penafsiran ekstensif akan tetapi ia menolak penerapan analogi pada hukum pidana.[60]

Pada asas legalitas, Moeljatno juga memberikan pendapat bahwa asas legalitas terkandung tiga pengertian, yaitu:

1. Tiada perbuatan yang dilarang dapat diancam dengan pidana jika belum dinyatakan dalam suatu aturan perundang-undangan.
2. Agar dapat menentukan adanya suatu perbuatan pidana tidak boleh menggunakan analogi (kias). 3. Aturan-aturan hukum pidana yang tidak berlaku surut.[61]

---

[59] Dion Valerian, 2017, *"Penerapan Analogi Dalam Hukum Pidana Indonesia*", Ruas Media,Yogyakarta, 2017, hlm.3-4.

[60] *Ibid*.hlm. 4

[61] *Ibid*, hlm. 3

Jika penggunaan Pasal dalam KUHP terhadap kasus *cybercrime* terus berlanjut maka beberapa hal yang berpeluang terjadi, seperti contohnya dalam putusan PN Bandung No. 162/Pid.B/2004/PN.BDG dengan terdakwa atas nama Harry Parlindungan Samosir dinyatakan melakukan transaksi pembelian sebuah barang di internet dengan melakukan pembayaran menggunakan kartu kredit orang lain tanpa izin serta membuat identitas palsu agar dapat mengambil barang tersebut. Sehingga, diputuskan bahwa terdakwa terbukti melakukan tindak pidana pemalsuan surat dan pencurian dengan pidana penjara selama 3 (tiga) bulan dengan dakwaan Jaksa Penuntut Umum yaitu Kesatu Primair Pasal 263 ayat (1) Subsidair Pasal 263 ayat (2) KUHP dan Kedua Pasal 362 jo. Pasal 55 Ayat (1) ke-1e KUHP. Kemudian, pada akhirnya kasus ini dilanjutkan lagi pada tingkat banding dalam putusan Nomor 181/PID/2004/PT.Bdg di Pengadilan Tinggi Bandung dengan memutuskan untuk menguatkan dan memperbaiki jangka waktu pemidanaan terhadap putusan Pengadilan Negeri Bandung dari awalnya 3 (tiga) bulan penjara menjadi 5 (lima) bulan penjara.[62]

Pada tahun 2008, akhirnya disahkannya sebuah peraturan perundang-undangan di Indonesia tentang Informasi dan Transaksi Elektronik yang dalam bagiannya terdapat larangan atas sebagaimana yang dicantumkan dalam undang-undang ini terhadap transaksi-transaksi elektronik dengan disertai ketentuan pidananya. Seiring berkembangnya zaman, ketika

[62] Sahuri Lasmadi, "*Tindak Pidana Dunia Maya Dalam Perspektif Undang-Undang Nomor 11 Tahun 2008 Tentang Infomarasi Dan Transaksi Elektronik*", Jurnal Ilmu Hukum, Vol.2 No.4, 2010, hlm.39-40.

internet masuk kedalam bagian dari sebuah jaringan komputer, perbuatan-perbuatan hukum yang berkembang di dalamnya menjadi pengelompokkan penanganan menggunakan undang-undang ini, salah satunya yaitu phising. Berdasarkan unsur phising dan dalam putusan-putusan pengadilan, peraturan mengenai *cybercrime* berbentuk phising ini tercantum dalam Undang-Undang Negara Republik Indonesia No. 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dalam beberapa pasal yang dapat dikenakan, antara lain:

1. Pasal 28 ayat (1) menyebutkan bahwa “Setiap Orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik.” jo. Pasal 45 ayat (2) sebagai ketentuan pidananya bahwa “Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 28 ayat (1) atau ayat (2) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah)”.
2. Pasal 35 menyebutkan bahwa “Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik” jo. Pasal 51 sebagai ketentuan pidananya bahwa “Setiap Orang yang

memenuhi unsur sebagaimana dimaksud dalam Pasal 35 dipidana dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp12.000.000.000,00 (dua belas miliar rupiah)".

Dari ketentuan tersebut dapat dilihat bahwa jenis hukuman yang diberikan adalah pidana pokok berupa pidana penjara dan pidana denda dengan menggunakan stelsel straf maksimum, seperti yang digunakan dalam KUHP. Hakim menentukan hukuman yang akan dikenakan (berapa tahun lamanya pidana penjara dan jumlah banyaknya denda) dengan berdasarkan apa yang tercantum dalam UU ITE. Ketentuan dalam pemidanaan ini juga dilakukan dengan cara menggabungkan sistem alternatif dan sistem kumulatif, dimana hakim mempunyai pilihan apakah dapat dijatuhkan pidana penjara atau pidana denda ataupun kedua-duanya.[63]

Terhadap pidana penjara bagi pelaku tindak pidana *cybercrime* berbentuk phising dilakukan dengan memberikan pembatasan kebebasan bergerak seperti pelaku tindak pidana lainnya yang selanjutnya ditampung dalam lembaga pemasyarakatan dengan diwajibkan menaati segala peraturan yang berlaku di dalamnya dikaitkan dengan tata tertib bagi para narapidana jika melanggar peraturan. [64]

Sebagaimana yang tercantum dalam Pasal 1 angka 3 Undang-Undang Negara Republik Indonesia Nomor 12 Tahun 1995 tentang Pemasyarakatan menyatakan bahwa "Lembaga Pemasyarakatan yang

[63] Andri Winjata Laksana*, Op. Cit*., hlm.63-64

[64] P.A.F. Lamintang, 1984, *"Hukum Penitensier Indonesia*", Armico: Bandung, hlm.69.

selanjutnya disebut lapas adalah tempat untuk melaksanakan pembinaan narapidana dan anak didik pemasyarakatan". Oleh karena itu, pidana penjara yang selanjutnya disebut kepada terpidana atau narapidana, diberikan hukuman atas kejahatan yang telah dilakukannya dengan dibatasi kebebasan bergeraknya di dalam lapas sambil diberikan pembinaan dan pengawasan agar para narapidana dapat memperbaiki diri menjadi manusia yang lebih baik.

Dalam sistem kepenjaraan di dunia, terdapat 3 (tiga) jenis sistem kepenjaraan yang populer, antara lain:

1. Sistem Pensylvania: Sistem ini banyak dianut dan berkembang di negara-negara Eropa dengan menekankan pada metode dengan mengasingkan para narapidana di dalam sel serta para narapidana diberikan pekerjaan masing-masing di dalam sel dan mendapat bacaan kitab Injil dan tidak diberikan kesempatan menerima pengunjung ataupun berbicara dengan orang lain dengan tujuan agar para narapidana bertobat dan menyesal atas perbuatannya.
2. Sistem Auburn: Dari penjara Negara Bagian New York sistem ini terus digunakan sampai di penjara Sing Sing pada tahun 1925 dan sampai banyak dipraktikkan di Amerika. Keberhasilan dari sistem ini karena mengharuskan para narapidana untuk tinggal di dalam sel pada malam hari dan diharuskan bekerja secara bersama-sama di siang hari. Akan tetapi, yang membuat lebih ketatnya sistem ini karena para narapidana dilarang berbicara satu sama lain.

3. Sistem Irlandia: Dalam sistem ini, dikehendaki bagi para narapidana untuk pada awalnya ditempatkan di dalam sel terus-menerus akan tetapi pada akhirnya dipekerjakan bersamasama. Berbeda dengan sistem Auburn, dalam sistem Irlandia ini diberikan kelonggaran bagi para narapidana satu sama lain untuk bergaul, dan pada akhirnya dibebaskan dengan syarat setelah mereka menjalani ¾ (tiga per empat) dari lamanya pidana yang harus dijalani.[65]

Akan tetapi, di Indonesia tidak menganut satupun dari tiga jenis sistem kepenjaraan tersebut sehingga perbaikan terhadap fungsi pidana kepenjaraan pun terus dilakukan. Sampai pada tahun 1918, “Reglement Penjara Baru” (Gestichten Reglement) mulai berlaku. Dalam reglemen ini membuat keharusan serta kewajiban bagi pihak yang berwajib untuk menyusun reglemen penjara yang baru dengan berisi aturan bagaimana para narapidana diperbaiki dan menjadi manusia yang susila. Sehingga dalam sistem pemenjaraan ini menjadikan pembinaan sebagai fungsi utama dari pemenjaraan itu sendiri.

Di Indonesia, pidana penjara menjadi jenis pidana yang populer dan sering dipakai oleh hakim dalam mengadili suatu perkara, bahkan tidak sedikit dari semua jenis-jenis tindak pidana yang ada diatur dengan ancaman pidana penjara. Dari perumusan terhadap ancaman pidana

[65] I Wayan P. S. Aryana, “*Efektivitas Pidana Penjara Dalam Membina Narapidana”*, Jurnal Ilmu Hukum, Vol.11 No.21, hlm.40-41

penjara yang bersifat imperatif tersebut merupakan warisan pemikiran aliran klasik yang menentukan pidana dengan definite sentence.[66]

Akan tetapi, Barda Nawawi Arief berpendapat bahwa akibat dari pidana penjara bukan hanya perampasan kemerdekaan, melainkan menimbulkan dampak-dampak negatif bahkan narapidana bisa menjadi lebih jahat setelah bebas dari penjara. Kemudian, Muladi pun menambahkan dalam bukunya yang berjudul Kapita Selekta Sistem Peradilan Pidana (1992) bahwa akibat dari pidana penjara mampu menyebabkan dehumanisasi, beresiko terjadinya prisonisasi serta dapat menimbulkan "cap jahat" (stigma).

Dehumanisasi, prisonisasi, dan stigma tentunya akan lahir ketika seseorang dinyatakan sebagai seorang terpidana sehingga harus mendekam di dalam penjara. Hal tersebut akan terjadi secara langsung terhadap para narapidana, karena:

1. Dehumanisasi: Menurut Kamus Besar Bahasa Indonesia, kata dehumanisasi adalah penghilang harkat manusia. Sehingga, dapat diartikan bahwa dehumanisasi terhadap narapidana di dalam penjara adalah bentuk penghilang harkat manusia yaitu dengan menghilangkan kebebasan bergerak mereka antara lain dengan mendekam di dalam sel.
2. Prisonisasi: adalah suatu bentuk penyesuaian diri narapidana mulai pertama kali masuk ke dalam penjara dari belajar menyesuaikan diri

[66] Sudarsono, 2002. "*Kasus Hukum*", Rineka Cipta, Jakatta,hlm., hlm.16.

dengan peraturan di dalam lapas maupun interaksi dengan narapidana yang lain. Sehingga, hal ini bisa berpeluang memicu residivis (pengulangan kejahatan) bagi para narapidana (biasa disebut dengan napi), karena ketidakadanya pembatasan satu sama lain secara ketat sehingga terhadap napi dengan kejahatan biasa dan napi dengan kejahatan yang lebih berbahaya dapat terbiasa dengan pembagian informasi satu sama lain sehingga menjadi faktor pemicu residivis.

3. Stigma: Hal ini tentu sudah menjadi hal yang sering dijumpai dalam kehidupan bermasyarakat bagi para mantan narapidana. Ketika pertama kali ia dinyatakan menjadi seorang napi, otomatis stigma atau persepsi yang kurang baik dari masyarakat sekitar dilayangkan kepadanya. Sehingga hal ini menjadi pengaruh negatif bagi para mantan napi dalam menjalani kehidupan selanjutnya seperti dalam mencari sebuah pekerjaan untuk memenuhi kebutuhan hidup maupun bersosialisasi akan lebih sulit oleh karena stigma tersebut.

Namun, pada pidana penjara selalu terdapat kerugian-kerugian yang bersifat filosofis maupun praktis yang sulit untuk diselesaikan. Jika ditinjau dari sudut filosofis maka akan ada hal-hal yang saling ambivalen (keadaan yang bertentangan) antara lain: 1. Pidana penjara memiliki tujuan untuk menjamin pengamanan terhadap para narapidana, serta memberikan kesempatan bagi para narapidana untuk direhabilitasi. 2. Hakikat fungsi dari penjara seringkali mengakibatkan dehumanisasi pelaku tindak pidana dan akhirnya menimbulkan kerugiankerugian

tersendiri bagi narapidana dikarenakan terlalu lama berdiam di dalam lapas, misalnya ketidakmampuan untuk melanjutkan kehidupan dalam bermasyarakat.

Pemidanaan selanjutnya bagi pelaku tindak pidana *cybercrime* berbentuk phising, yaitu pidana denda. Pidana denda juga termasuk salah satu pidana pokok yang tercantum dalam Pasal 10 KUHP, dan merupakan urutan pidana paling terakhir dari jenis-jenis pidana pokok yang berarti pidana denda yaitu jenis pidana pokok yang paling ringan diantara yang lain.

Pidana denda berbeda dengan jenis pidana penjara yang mempunyai tujuan untuk penghilangan kemerdekaan, sedangkan pidana denda tujuannya yaitu harta benda dari pelaku tindak pidana. Karena, denda merupakan aturan dengan menitikberatkan pada keharusan untuk membayar sesuatu dalam bentuk uang karena melanggar suatu aturan yang yang berlaku dalam masyarakat.

Pidana denda sebagaimana menjadi bagian dari pemidanaan atau penghukuman bagi pelaku agar dapat membayar sejumlah uang yang telah ditetapkan dalam peraturan perundang-undangan dan dalam putusan pengadilan, disebutkan bahwa ada langkah lain yang dapat ditempuh jika pelaku tidak mampu untuk membayar denda yang dimaksud. Hal tersebut tercatat pada Pasal dalam KUHP sebagai berikut, yaitu:

1. Pasal 30 ayat (2) KUHP menyebutkan bahwa, “Jika pidana denda tidak dibayar, ia diganti dengan pidana kurungan”.
2. Pasal 30 ayat (3) menyebutkan bahwa, “Lama pidana kurungan pengganti paling sedikit satu hari dan paling lama enam bulan”.
3. Pasal 30 ayat (6) yaitu “Pidana kurungan pengganti sekali-kali tidak boleh lebih dari delapan bulan”

Tindak pidana *cybercrime* berbentuk phising yang menggunakan UU ITE, sebagaimana pemberian pidana menurut UU ITE menggunakan gabungan sistem kumulatif dan alternatif sehingga hakim harus menentukan pemberian hukumannya antara pidana penjara saja, pidana denda saja ataupun keduanya sekaligus. Namun selanjutnya, dalam ketentuan KUHP baru Pasal 80 ayat (1) menyebutkan bahwa, “Dalam menjatuhkan pidana denda, hakim wajib mempertimbangkan kemampuan terdakwa dengan memperhatikan penghasilan dan pengeluaran terdakwa secara nyata.

Karena, terhadap subjek hukum yang wajib memenuhi pidana denda dalam suatu tindak pidana tidak dijelaskan secara tegas dalam peraturan perundang-undangan, maka dapat disimpulkan bahwa pembayaran denda dapat dilakukan oleh orang lain atau pihak ketiga dari pelaku. Ketika pemberian denda yang seharusnya diberikan kepada pelaku agar dapat memunculkan efek jera tidak sepenuhnya dilakukan oleh pelaku itu sendiri, maka dapat membuat tujuan pemidanaan kepada pelaku *cybercrime* berbentuk phising ini menjadi kurang maksimal.

Terdapat berbagai pengaturan dan dasar hukum dari tindak pidana *cybercrime*, Dasar hukum yang mengatur tentang tindak pidana *cybercrime* antara lain :

1. Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi

   Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi telah mengatur perbuatan yang dilarang terkait tindak pidana *cybercrime*. Adapun beberapa pasal tersebut yakni sebagai berikut.

   1) Pasal 22 Pasal ini mengatur larangan untuk melakukan perbuatan tanpa hak, tidak sah, atau memanipulasi, akses ke jaringan telekomunikasi, dan atau akses ke jasa telekomunikasi, dan atau akses ke jaringan telekomunikasi khusus.
   2) Pasal 38 Pasal ini mengatur larangan untuk melakukan perbuatan yang dapat menimbulkan gangguan fisik dan elektromagnetik terhadap penyelenggaraan telekomunikasi.
   3) Pasal 40 Pasal ini mengatur larangan untuk melakukan kegiatan penyadapan atas informasi yang disalurkan melalui jaringan telekomunikasi dalam bentuk apapun.

2. Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas UndangUndang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

   Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas UndangUndang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik telah mengatur perbuatan yang dilarang terkait

tindak pidana *cybercrime*. Adapun beberapa pasal tersebut yakni sebagai berikut:

1) Pasal 27 ayat (1) Pasal ini mengatur larangan bagi seseorang yang dengan sengaja atau tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya informasi elektronik dan/atau dokumen elektronik yang memiliki muatan yang melanggar kesusilaan.
2) Pasal 27 ayat (2) Pasal ini mengatur larangan bagi seseorang yang dengan sengaja tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan perjudian.
3) Pasal 27 ayat (3) Pasal ini mengatur larangan bagi seseorang yang tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atauDokumen Elektronik yang memiliki muatan penghinaan dan/atau pencemaran nama baik.
4) Pasal 27 ayat (4) Pasal ini mengatur larangan bagi seseorang tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan pemerasan dan/atau pengancaman.

5) Pasal 28 ayat (1) Pasal ini mengatur larangan bagi seseorang tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik.
6) Pasal 28 ayat (2) Pasal ini mengatur larangan bagi seseorang tanpa hak menyebarkan yang ditujukan untuk menimbulkan rasa kebencian atau permusuhan individu dan/atau kelompok masyarakat tertentu berdasarkan atas suku, agama, ras, dan antar golongan.
7) Pasal 29 Pasal ini mengatur larangan bagi seseorang yang tanpa hak mengirimkan Informasi Elektronik dan/atau Dokumen Elektronik yang berisi ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi.
8) Pasal 30 ayat (1) Pasal ini mengatur larangan bagi seseorang yang tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apa pun.
9) Pasal 30 ayat (2) Pasal ini mengatur larangan bagi seseorang yang tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik.
10) Pasal 30 ayat (3) Pasal ini mengatur larangan bagi seseorang yang tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan

melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.

11) Pasal 31ayat (1) Pasal ini mengatur larangan bagi seseorang yang tanpa hak atau melawan hukum melakukan intersepsi atau penyadapan atas Informasi Elektronik dan/atau Dokumen Elektronik dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik Orang lain.
12) Pasal 31 ayat (2) Pasal ini mengatur larangan bagi seseorang yang tanpa hak atau melawan hukum melakukan intersepsi atas transmisi Informasi Elektronik dan/atau Dokumen Elektronik yang tidak bersifat publik dari, ke, dan di dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik Orang lain, baik yang tidak menyebabkan perubahan apa pun maupun yang menyebabkan adanya perubahan, penghilangan, dan/atau penghentian Informasi Elektronik dan/atau Dokumen Elektronik yang sedang ditransmisikan.
13) Pasal 31 ayat (3) Pasal ini mengatur larangan bagi seseorang yang melakukan intersepsi yang dilakukan dalam rangka penegakan hukum atas permintaan kepolisian, kejaksaan, dan/atau institusi penegak hukum lainnya yang ditetapkan berdasarkan undang-undang.
14) Pasal 32 ayat (1) Pasal ini mengatur larangan bagi seseorang yang tanpa hak atau melawan hukum dengan cara apa pun

mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik publik.

15) Pasal 32 ayat (2) Pasal ini mengatur larangan bagi seseorang yang tanpa hak atau melawan hukum dengan cara apa pun memindahkan atau mentransfer Informasi Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik Orang lain yang tidak berhak.
16) Pasal 32 ayat (3) Pasal ini mengatur larangan bagi seseorang yang mengakibatkan terbukanya suatu Informasi Elektronik dan/atau Dokumen Elektronik yang bersifat rahasia menjadi dapat diakses oleh publik dengan keutuhan data yang tidak sebagaimana mestinya.
17) Pasal 33 Pasal ini mengatur larangan bagi seseorang yang tanpa hak atau melawan hukum melakukan tindakan apa pun yang berakibat terganggunya Sistem Elektronik dan/atau mengakibatkan Sistem Elektronik menjadi tidak bekerja sebagaimana mestinya. 18) Pasal 34 ayat (1) Pasal ini mengatur larangan bagi seseorang yang tanpa hak atau melawan hukum memproduksi, menjual, mengadakan untuk digunakan, mengimpor, mendistribusikan, menyediakan, atau memiliki:

a) perangkat keras atau perangkat lunak Komputer yang dirancang atau secara khusus dikembangkan untuk memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 33.
b) sandi lewat Komputer, Kode Akses, atau hal yang sejenis dengan itu yang ditujukan agar Sistem Elektronik menjadi dapat diakses dengan tujuan memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 33.

18) Pasal 34 ayat (2) Tindakan sebagaimana dimaksud pada ayat (1) bukan tindak pidana jika ditujukan untuk melakukan kegiatan penelitian, pengujian Sistem Elektronik, untuk perlindungan Sistem Elektronik itu sendiri secara sah dan tidak melawan hukum.
19) Pasal 35 Pasal ini mengatur larangan bagi seseorang yang tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik.
20) Pasal 36 Pasal ini mengatur larangan bagi seseorang yang tanpa hak atau melawan hukum melakukan perbuatan sebagaimana

dimaksud dalam Pasal 27 sampai dengan Pasal 34 yang mengakibatkan kerugian bagi Orang lain.

21) Pasal 37 Pasal ini mengatur larangan bagi seseorang yang 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.