Perlindungan Hukum Korban Pencurian Data Pribadi (*Phishing Cybercrime*) dalam Perspektif Kriminologi

Akbar Galih Hariyono[1*], Frans Simangunsong[2]

[1]Fakultas Hukum Universitas 17 Agustus 1945 Surabaya, Indonesia
[2]Fakultas Hukum Universitas 17 Agustus 1945 Surabaya, Indonesia

*Corresponding Author
E-mail : akbargalih84@gmail.com

Abstract
Phishing Cybercrime is a crime of criminal acts committed on internet technology (cyber space), both attacking public facilities and private facilities. crime Phishing cyber is an unlawful act committed using the internet based on the sophistication of computer and telecommunications technology. Activities Phishing cybercrime can be carried out at any location or even between countries. crimes Phishing cybercrimes such as hacking, sharing personal information and counterfeiting credit cards. Actors Phishing themselves are called hackers. Hackers have the knowledge and ability to master and apply programming languages. This ability is obtained hackers in various ways, including by learning from experts or self-taught. In a criminological perspective, phishing cybercrime occur because of 2 (two) important factors, namely Technical Factors and Economic Factors which can cause phishing cybercrime to occur. Legal protection regarding cybercrime phishing has been regulated in the ITE Law and the Personal Data Protection Law. Phishing cybercrime still cannot be completely eliminated. The existence of this law can at least reduce the amount of cybercrime in Indonesia.
KeyWords : *Phishing, Cybercrime, Criminology, Internet*

Abstrak
Phishing Cybercrime adalah kejahatan tindak kriminal yang dilaksanakan di teknologi internet, baik melakukan penyerangan fasilitas umum / pribadi. Kejahatan phishing *cybercrime* ialah aksi melawan hukum yang dilaksanakan memakai internet dengan basis canggihnya teknologi komputer serta telekomunikasi. Kegiatan *Phishing cybercrime* bisa dilaksanakan di manapun / bahkan bisa dilaksanakan antar negara. Kejahatan *phishing cybercrime* termasuk kejahatan seperti peretasan penyebaran informasi pribadi dan pemalsuan kartu kredit. Pelaku Phishing sendiri disebut *hacker. Hacker* memiliki pengetahuan serta kompetensi menguasai dan mengaplikasi Bahasa pemrograman. Kompetensi itu didapat *hacker* dengan beragam metode meliputi belajar dengan pakarnya / otodidak. Dalam perspektif *kriminologi* kegiatan *phishing cybercrime* terjadi karena adanya 2 aspek utama yakni Teknis serta Ekonomi yang dapat mengakibatkan kejahatan *phishing cybercrime* ini dapat terjadi. Perlindungan hukum mengenai kejahatan *phishing cybercrime* sudah diatur pada UU ITE dan UU Perlindungan Data Pribadi. Kejahatan *Phishing cybercrime* tetap tidak bisa dihilangkan secara total. Adanya undang-undang tersebut setidaknya dapat mengurangi jumlah *cybercrime* di Indonesia.
Kata Kunci : *Phishing, Cybercrime, Kriminologi, Internet*

Pendahuluan

Majunya teknologi informasi telah dianggap sebagai power yang mampu menentukan nasib manusia. Hampir emua kegiatan sehari-hari di lakukan ke internet, hubungan dengan internet yang memberi data pribadi ketika mempunyai akun tertentu yang tersambung ke data global. Serta problematika keamanan serta privasi data menjadi sebuah elemen utama dari sebuah sistem informasi[1]. Sehingga bisa menimbulkan warga Indonesia begitu ketergantungan dengan teknologi informasi yang menimbulkan semakin banyak juga potensi yang bisa memicu adanya tindak kriminal.

Teknologi informasi bisa memacu kemajuan di perspektif kehidupan, tetapi bisa pula menjadi sarana melaksanakan aksi kejahatan melawan hukum *(cybercrime)*.

Aksi melawan hukum di internet ataupun dunia maya (*cybercrime*) menjadi fenomena yang begitu mengkhawatirkan melihat jika aksi *carding, hacking*, penipuan, terorisme, serta distribusi *destruktif* mengenai informasi sudah seperti elemen dari kegiatan pelaku kriminal di dunia online. Aksi yang mengenai melawan hukum yang terjadi di dunia *online* bisa dimaknai pasti mempunyai sesuatu mengapa seseorang melaksanakan aksi siber. Sebab perlu dipahami jika kejahatan ciber yang dilaksanakan itu pasti bisa memicu kerugian pihak lainnya. *Cybercrime* ialah sebutan yang arahnya kepada kegiatan criminal menggunakan komputer / jaringan komputer sebagai media, sasaran / lokasi tindak criminal. Termasuk dalam kejahatan dunia online diantaranya penipuan lelang dengan online, memalsukan cek, penipuan kartu kredit/carding, confidence fraud, penipuan identitas, pornografi anak, serta sebagainya. [2]

Ada 2 hal yang bisa memicu munculnya *cybercrime* yakni teknis serta sosio ekonomi (kemasyarakatan). Pertama, pada hal teknis, Tak bisa dipungkiri jika dampak majunya teknologi (teknologi informasi) bisa memicu dampak buruk untuk kemajuan di masyarakat. Suksesnya teknologi itu pula bisa menghilangkan batas wilayah negara yang membuat dunia sangat sempit. Korelasi antar jaringan bisa mempermudah pelaku kriminal melancarkan kegiatannya. Lalu, tak meratanya distribusi teknologi membuat yang satu lebih kuat dari lainnya.

Sebuah metode yang dilaksanakan oleh pelaku *phishing* yakni dengan metode meletakkan *fake* link di akunmedia social dengan seruan iklan sederhana serta menggiurkan. Dengan metode itu pelaku bisa mencuri data informasi dari orang itu guna menghasilkan laba diantaranya mengambil uang dari rekening pemakai / memakai rekening sebagai media payment online.

Kasus seperti *phishing (cybercrime)* bisa menimbulkan kerugian korban baik material serta immaterial. Di kasus pencurian informasi / data pribadi bisa pula memicu korban berkesinambungan, tak cuma pengunjung situs web serta sistem elektronik, melainkan perusahaan yang mempunyai sistem elektronik serta bank sebagai mitra pembayaran. Sehingga aksi *phishing* bisa dijatuhi UU No. 11 Tahun 2008 seputar informasi transaksi elektronik serta UU No. 27 Tahun 2022 seputar Perlindungan Data Pribadi.

Metode Penelitian

Di riset ini, peneliti memakai jenis riset hukum normatif. Riset hukum normatif ialah riset hukum yang dilaksanakan dengan metode melakukan penelitian bahan pustaka. Riset hukum normatif yang dipakai peneliti yakni riset kepada -asas hukum. Riset kepada asas-asas hukum ialah riset yang dilaksanakan kepada aturan-aturan hukum, yang menjadi pegangan berperilaku / bersikap tak layak. Riset itu bisa dilaksanakan (terkhususnya) kepada bahan hukum primer serta sekunder, selama beberapabahan itu memiliki aturan-aturan hukum.[3]

Hasil Penelitian Dan Pembahasan

Bagaimana Perlindungan Hukum Bagi Korban *Phishing Cybercrime* dalam Perspektif Kriminologi ?

Berdasarkan pengertian *phising* bisa dipahami metode dari *phising* itu dilaksanakan guna menjebak korban . Phising yakni kegiatan guna memperoleh informasi privasi pemakai dengan metode memakai email serta situs palsu dengan tampilan seperti asli.[4]

Phishing ialah wujud kejahatan ciber, yang kini marak ada di platform jaringan komputer. Di ruang lingkup keamanan komputer, *phising* ialah sebuah tindak kriminal elektronik di wujud penipuan. Yang mana ekanisme *phising* ini bertujuan[5]. Sejalan dengan majunya zaman, tindak kriminal menjadi berkembang serta tersebar di seluruh penjuru. Sehingga ancaman tindak kriminal yang kini terjadi, bisa pula menyerang lewat jaringan komputer. Untuk *hacker* metode *phishing* ini menjadi metode paling

mudah sebagai ajang mencuri data. Walaupun *phishing* di anggap simple serta jarang terjadi namun tetap ada pemakai internet yang masuk ke jebakan *hacker*.

Ketika banyak pemakai sosmed di seluruh penjuru dunia, kini juga penjahat-penjahat dunia ciber mulai menjalankan kegiatannya guna menghasilkan laba dari pemakai sosmed. Diantaranya phishing. Phishing menjadi sebuah wujud Tindakan yang sifatnya memberi ancaman serta perangkap menggunakan konsep memancing orang itu. Yakni dengan melakukan penipuan yang menjadikan orang itu dengan tak sadar bisa tertipu[6].

Mayoritas pemakai sosmed tak memikirkan beberapa ancaman itu. Mereka mengangap hal itu sepele serta tak perlu di besar-besarkan. Hingga kini, beragam akun sosmed terperangkap *phishing*. Diantara serangan yang di luncurkan penjahat siber ialah menyisipkan *fake* link di akun sosmed dengan seruan sederhana yang menggiurkan. Dengan hal itu penyerang bisa memperoleh informasi pemakai serta memakainya dalam menghasilkan laba seperti mengutip uang dari rekening pemakai / memakai rekening sebagai payment online.[7]

Dalam ruang lingkup keamanan pada bidang teknologi komputer, dapat diartikan *phising* yaitu salah satu bentuk tindak kejahatan yang menyasar pada ranah elektronik yang dapat berupa di wujud penipuan. Pada mekanisme tindak kejahatan *phising* pelaku bermaksud mendapatkan atau mencuri informasi yang begitu sensitif pada korban seperti username, password serta detail mengenai kartu kredit. *Phising* mulai terkenal di tahun 1995. James (2005) menjelaskan metode awal yang dilaksanakan ialah memakai algoritma yang menjadikan nomor kartu kredit dengan acak. *Phising* / "*Brandspoofing*" / "*Carding*" ialah wujud layanan penipuan yang menjanjikan keabsahan serta keamanan transfer data yang anda laksanakan. Di sistem operasi itu, bisa dibilang jika internet sudah memberi perubahana jarak serta masa tak terbatas. Internet diilustrasikan menjadi sekumpulan jaringan komputer meliputi beragam jaringan mikro menggunakan sistem jaringan yang tidak sama.[8]

Cyber crime dimaknai yang merpakan aksi pelanggaran hukum yang mendayagunakan teknologi komputer dengan basis anggihnya perkembangan teknologi internet. Jenis serta pelanggaran cybercrime begitu variatif sebagai dampak pengaplikasian teknologi. Cybercrime bisa berwujud penyadapan serta penyalahgunaan informasi/data berwujud elektronik/yang ditransfer dengan elektronik, mencuri data elektronik, pornografi, menyalahgunakan menjadi sembagai objek melawan hukum, penipuan lewat internet, perjudian online, perusakan website, perusakan sistem komputer/handphone lewat serta lainnya.[9]

Cyber crime ialah aksi pidana yang dilaksanakan di teknologi internet (*cyber space*), baik yang melakukan penyerangan fasilitas umum / pribadi. Dengan Teknik bisa diklasifikasikan kedalam offline crime, semi online crime, serta *cyber crime.* Salah satu Tindakan dari offline crime ialah dengan metode sederhana seperti melakukan pencurian dompet yang selanjutnya dikutip kartu kreditnya, / melakukan Kerjasama dengan dengan kasir dalam melakukan pencatatan nomor kartu kredit seseorang lalu menduplikatnya. Misal Teknik semi online crime ialah melakukan pemasangan skimming di mesin ATM guna melakukan pencurian informasi kartu kredit korban. Sementara bagi *cybercrime* pelaku serta korban tak perlu bertatap muka, serta bersentuhan, yakni memakai kecanggihan teknologi, misal pemakaian situs web. Masing-masing di Teknik itu mempunyai karakter tersendiri, tetapi perbedaan pokok dari ketiganya ialah keterkaitan dengan jaringan internet.

Cybercrime bisa diartikan menjadi aksi melawan hukum yang dilaksanakan memakai internet pada canggihnya teknologi computer serta telekomunikasi. *The prevention of crime and the treatment of offlenderes* di Havana, Cuba di tahun 1999 dan di Wina, Austria tahun 2000, menjelaskan terdapat 2 sebutan yang dikenal:

1. *Cybercrime* di makna dikenal *computer crime,* yakni aksi illegal dengan eksklusif melakukan penyerangan sistem computer serta data yang di proses.

2. *Cybercrime* di makna luas dikenal computer related crime, yakni aksi illegal yang berkenaan dengan sistem komputer / jaringan. Dari banyak definisi diatas, cybercrime diartikan menjadi aksi melawan hukum yang dilaksanakan dengan jaringan komputer untuk sarana/ komputer menjadi objek, baik guna mendapat laba / tidak, yang menimbulkan kerugian lain pihak.

Sebetulnya tujuan jurnal ini dibuat yakni pertama agar orang-orang mulai dapat mengubah mengenai pola pemikirannya kepada serangan *phishing*. Sehingga beberapa orang ajib memahami beberapa sesuatu yang mencurigakan mengenai akun jejaring sosial yang mereka buka dan tidak menganggap itu merupakan hal yang biasa dan sepele. Bila sekiranya benar apabila terdapat serangan phishing, maka pertama yang wajib dilakukan yakni meninggalkan laman palsu pada web tersebut itu sedini mungkin. Tidak cuma pergi saja, kita wajib pula menemukan pemecahan dalam menyelamatkan akun kita. Sebab jika sekali kita terjebak serangan dari phishing itu, maka bisa sangat berbahaya untuk akun pribadi yang kita miliki. Serangan *phishing* tersebut akan terus menyebar dan meretas akun kita yang lain.

Kemajuan teknologi informasi sudah memberi perubahan hamper seluruh elemen kehidupan. Di satu sisi teknologi komputer mencurahkan banyak keuntungan dalam wujud peluang dalam memperoleh informasi, pekerjaan, berpartisipasi di politik serta kehidupan berdemokrasi dan beberapa keuntungan lainnya. Namun, di lain sisi ia akan begitu menggerogoti celah yang sudah lama, kemudian melakukan peretasan dengan semua situs yang wajib dipecahkan sebelum ia masuk lebih jauh menelusuri jalan serta celah-celah *cyberspace.* Untuk mereka yang mendayagunakan teknologi informasi ini sebagai aktivitas bisnis, pelayanan public, serta sarana hiburan dengan membangun beberapa situs yang bisa dikunjungi masyarakat.

Hacking merupakan sebuah aktivitas yang sifatnya buruk, walaupun mulanya hacking mempunyai maksud baik yakni dalam merestorasi sistem keamanan yang sudah dibangun serta memperkuatnya. Namun di pertumbuhannya hacking dipakai sebagai kebutuhan lain yang sifatnya merugikan. Hal tersebut tak lepas dari pemakai internet yang kian merebak menjadikan penyalahgunaan kompetensi hacking menjadi luas pula. Setiap sistem operasi memiliki titik lemah. Kelemahan itu perlahan akan dipahami oleh para hacker lewat beragam metode, meliputi ialah mempelajari sistem operasi itu, diskusi dengan sesama *hacker* lewat *mailing list*, *newsgroup* / mengutip informasi dari sebuah situs di internet yang memberikan informasi tentang sisi lemah sistem operasi komputer. Kemudahan mendapat informasi memudahkan *hacker* bisa memahami kelemahan sistem operasi itu.

Cara *hacker* untuk memahami bagaimana sistem serta apa yang digunakan di suatu sasaran ialah menyusup / mengakses jaringan pada komputer yang menjadi incaran. Menyusup / mengakses jaringan komputer target sasaran ini dilaksanakan dengan cara menyerang dari kelemahan yang terdapat di sistem komputer tersebut. Dengan istilah lain hacker masuk ke situs orang secara illegal tanpa izin. Hacker dengan kompetensinya bisa masuk serta mengakses di situs korban walaupun situs itu sudah lengkap dengan sistem keamanan. Misi untuk para hacker ialah melakukan pembongkaran sistem yang dipakai pemilik web itu. Hacker yang telah mampu memasuki sistem orang lain ialah kejahatan cybercrime sebab situs menjadi bilik privat orang yang menciptakan situs itu. Dengan merubah tampilan web tidak sesuai dari orisinalnya serta melakukan penghapusan beberapa file yang terdapat di situs itu telah bukan rasa keingintahuan biasa yang dimiliki orang, hal tersebut telah termasuk di tindak pidana. Sebab telah menjadikan kerugian tersendiri untuk pemilik akun.

Mengamati fakta hukum seperti yang terjadi kini, dampak pesatnya dan perkembangan IPTEK yang disalah gunakan menjadi sarana kriminal ini menjadi begitu penting untuk diantisipasi bagaimana kebijakan hukumnya, sehingga *cybercrime* yang ada bisa dilaksanakan usaha mengatasinya dengan hukum pidana, termasuk dalam situasi ini ialah seputar mengenai pembuktiannya. Kenapa sangat

penting sebab mengenai penegakan dalam hukum pidana dasar pembenaran terhadap seseorang bisa di vonis bersalah / tak melaksanakan tindak pidana, dimana aksinya bisa dipersalahkan atas power UU yang sudah muncul sebelumnya yaitu asas legalitas, juga mengenai perbuatan mana yang didukung oleh power adalah bukti yang sah serta kepadanya bisa dipertanggung jawabkan mengenai unsur kesalahannya. Pemikiran demikian sudah selaras dengan pengaplikasian asas legalitas di KUHP, yaitu seperti dirumuskan dengan tegas di Pasal 1 ayat (1) KUHP "*Nullum delictum nulla poena sine praevia lege poenali*" / di istilah lain bisa disebut, "tiada tindak pidana, tidak ada pidana, tanpa adanya aturan hukum pidana terlebih dahulu".[10]

Tindak pidana kriminal teknologi informasi bisa dibagi sebagai *white crime* disebabkan beberapa pelaku kriminal di dunia online ialah seseorang yang mengerti penggunaan aplikasi internet, / mahir di bagian itu. Sebab tindak kriminal ini kerap dilaksanakan dengan metode transnasional / melewati pemisah antar negara, tindak kriminal dunia online ini disertai dengan 2 kriteria kriminal, meliputi whitecrime serta transnational crime. Ada banyak kasus tindak kriminal di internet *(cyber crime)* yang sering beraksi di kalangan masyarakat di Indonesia yaitu penipuan, judi online, distribusi berita *hoax, cracking*, sampai pencurian data pribadi lewat internet.[11]

Kriminologi berakar dari istilah *crimen* serta *logos* yang memiliki arti menjadi ilmu pengetahuan seputar kejahatan. Istilah kriminologi pertama kali muncul setelah seorang antropolog Prancis pada tahun 1879 yang bernama P. Topinard. Kriminologi juga digambarkan selaras dengan Namanya, yakni ilmu pengetahuan yang belajar kriminal. Kriminal yang dimaksud ialah sebuah aksi yang dilaksanakan orang-orang serta instansi yang dilarang oleh sebuah UU. Pemahaman itu diatas tentu tak dapat disalahkan untuk memandang kriminologi yang menjadi elemen dari ilmu yang belajar sebuah kriminal[12]. Kriminologi diklasifikasikan menjadi 3 cabang ilmu utama, yakni :

1. Sosiologi hukum yaitu belajar kejahatan menjadi aksi yang oleh hukum dilarang serta diancam dengan sanksi. Sehingga yang menetapkan jika sebuah aksi tersebut criminal ialah kaidah hukum.
2. Etiologi Kriminal yang menjadi cabang kriminologi yang berupaya melaksanakan analisa ilmiah tentang asal mula kriminal.
3. Penologi hakikatnya ialah ilmu mengenai hukuman, yaitu memasukkan hak-hak yang berkenaan dengan upaya pengendalian kriminal, baik represif / preventif.

Kriminologi mempunyai tujuan yakni mencurahkan petunjuk bagaimana masyarakat bisa memberantas kriminal dengan hasil yang baik serta lebih-lebih agar bisa menghindarinya. Kriminologi mempunyai 2 tujuan yakni :

1. Apa yang dirumuskan oleh criminal serta fenomenanya yang ada di kehidupan masyarakat, kriminal hal serta siapa penjahatnya ialah bahan riset para kriminolog.
2. Apa faktor-faktor yang memicu munculnya / dilaksanakan kriminal.

Kriminologi dengan hukum pidana atas banyak pertimbangan menjadi instrument serta sekaligus media kekuasaan oleh negara untuk menjalankan sebuah tugas serta wewenang mempunyai kolerasi positif. Banyak pertimbangan itu diantaranya jika hukum pidana serta kriminologi bertumpu di premis serupa :

1. Negara menjadi sumber kekuasaan serta semua media perlengkapan negara enjadi penyelenggaraan dari kekuasaan negara.
2. Hukum pidana serta kriminologi mempunyai persamaan mengenai persepsi jika masyarakat luas ialah elemen dari obyek pengaturan oleh kekuasaan negara bukan subyek (hukum) yang mempunyai posisi serupa dengan suatu negara.

3. Hukum Pidana serta kriminologi masih memposisikan kontribusi negara lebih dominan dari peranan individu untuk menghadirkan ketertiban serta keamanan serta menjadi perusak ketertiban serta keamanan itu.

Membedakan Kriminologi dalam makna sempit serta luas. Kriminologi di makna sempit belajar kriminal. Kriminologi di makna luas, mempelajari penologi serta beberapa metode yang berkenaan dengan criminal serta problematika prevensi kriminal dengan ksi yang sifatnya non penal. Sebab belajar kriminal ialah belajar perilaku manusia, sehingga paradigma yang dipakai ialah *descriptive, causality* serta *normative*.

Kriminologi mempelajari pertumbuhan perilaku yang mengarah ke kesejahteraan / pertumbuhan perilaku mereka yang sudah melaksanakan kriminal. Kriminologi belajar pula kegiatan kriminal di wujud individual / terorganisasi termasuk beberapa metode dipakai penjahat. Bagaimana beberapa penjahat bersikap kepada aparat hukum, yakni ketika ditangkap, diadili / dihukum.

Selaras dengan penjelasan sebelumnya bisa dipahami jika riset terdahulu seputar asal-usul kejahatan senantiasa di konteks antara hukum serta organisasi sosial. Hal ini terbukti jika ketika masa aliran klasik, perhatian senantiasa tertuju pada kaidah-kaidah social yang bisa menjabarkan eksistensi hukum serta dampaknya di setiap anggota masyarakat. Pertumbuhan kriminologi sejak 1970-an ialah kelahiran *new criminology* yang sudah memacu perhatian di struktur pemikiran kriminologi yang berlandaskan pada pendekatan-pendekatan: apa sifatnya dikotomi, trikotomi, / 4 klasifikasi.

Pengaturan terkait penanganan atisipasi cybercrime dengan hukum pidana masuk sektor penal policy yang menjadi elemen criminal policy (kebijakan penanggulangan kejahatan). Diamati dari kacamata criminal policy, usaha penanggulangan kriminal (termasuk dalam penanganan penanggulangan cybercrime) tak bisa dilaksanakan hanya dengan parsial dengan hukum pidana (sarana penal), namun wajib juga ditempuh dengan paradigma integral/ sistemik.[13]

Cybercrime ialah problematika di dunia maya kini yang wajib diatasi dengan serius. Sebagai kejahatan, mengatasi*cybercrime* bisa dianalogikan serupa pada dunia nyata, wajib hukum yang mengatur. Terdapat 2 usaha metode penanganan cybercrime yakni

1. Dengan Usaha non Hukum
   Semua usaha yang sifatnya preventif serta persuasive kepada para pelaku, korban serta seluruh pihak yang memiliki peluang berkenaan dengan kejahatan dunia online.
2. Dengan Usaha Hukum
   Semua usaha yang sifatnya mengikat, lebih banyak mencurahkan informasi tentang hukuman serta jenis pelanggaran/kejahatan dunia online dengan spesifik.

Dalam perspektif kriminologi ada beberapa faktor dan motif yang mengakibatkan terjadinya kasus *phishing cybercrime*. Dari segi motif terjadinya Tindakan *phishing cybercrime* biasanya bisa diklasifikasi ke dalam 2 klasifikasi, yakni:

1. Motif Intelektual
   Kriminal yang ilaksanakan hanya sebagai kepuasan pribadi serta memperlihatkan jika ia sudah bisa melakukan rekayasa serta implementasi sektor teknologi informasi. Kejahatan dengan motif ini biasanya dilaksanakan oleh seseorang dengan individual.
2. Motif Ekonomi, Politik, serta Kriminal
   Kriminal yang dilaksanakan sebagai laba pribadi / golongan tertentu yang dampaknya ke ruginya ekonomi serta politik pihak lain. Sebab mempunyai maksud yang memberi efek besar, kriminal dengan motif ini biasanya dilaksanakan oleh suatu korporasi.

Beberapa aspek utama yang dapat menyebabkan timbulnya *phishing cybercrime* yaitu:

1. Semakin maju suatu negara, namun tak diimbangi kesejahteraan masyarakatnya, makin besar potensi kesenjangan social muncul.
2. *Lifestyle*.
3. Minimnya sosialisasi / arahan baik dari akademi umum misal sekolah / edukasi dari orang tua tentang kegunaan internet, sehingga beragam penyalahgunaan muncul.
4. Makin banyak sosmed, media elektronik, serta media penyimpanan *virtual (cloud)*, menjadikan manusia makin tergandrungi dengan akses internet di kehidupanya.
5. Lalai.
6. Muncul hasrat pengakuan dari manusia lain.
7. Semakin maju teknologi serta mudahnya melakukan akses jaringan internet *anytime anywhere* tanpa terbatas masa.

Apabila ilihat dari sisi yang tidak sempit ada 2 (dua) aspek penting terjadinya *phishing cybercrime* yakni:

1. Aspek Teknis
   Dengan munculnya teknologi internet meraibkan batas wilayah negara yang membuat dunia ini semakin dekat serta tak luas. Saling berhubungnya antar jaringan mempermudah pelaku kriminal elancarkan aksinya. Lalu tak ratanya distribusi teknologi membuat pihak yang satu lebih kuat dari lainnya.
2. Aspek Ekonomi
   Cybercrime bisa dilihat menjadi produk ekonomi. Isu global yang selanjutnya dikorelasikan dengan kriminal itu ialah keamanan jaringan. Keamanan jaringan ialah isu global yang hadir dengan internet. Menjadi komoditi ekonomi, beberapa negara yang tentu begitu memerlukan perangkat keamanan jaringan. Dilihat dari realita itu *cybercrime* ada di scenario besar dari aksi ekonomi dunia.

Penanganan hukum mengenai tindak kejahatan *phising cybercrime* di negara Indonesia dapat dipengaruhi oleh beberapa faktor diantaranya yakni hukum, mentalitas, perilaku social, sarana, serta budaya. Hukum yang dapat ditegakkan sangat harus mengikutsertakan manusia serta juga mengikutsertakan perilaku manusia. Hukum juga tak dapat dilaksanakan mandiri tanpa terdapat penegak hukum. Karena sesuai dengan negara Indonesia bahwa "Indonesia dikenal sebagai rechtstaat atau negara hukum. Salah satu ciri yang menunjukan Indonesia adalah negara hukum adalah setiap sendi kehidupan di Indonesia diatur oleh suatu aturan yang jelas, atau hukum yang jelas."[14]

Penegak hukum diwajibkan bekerja keras sebab penegakan hukum ialah subyek pokok perang melawan cyber. Seperti, Resolusi PBB No. 5 tahun 1963 eputar usaha pemberantasan kejahatan penyalahgunaan Teknologi Informasi pada 4 Desember 2001, menjadi indikator jika terdapat problematika internasional yang parah, serius serta segera terjadi. KUHP masih dipakai sebagai dasar hukum meliput cybercrime, terkhusus cybercrime yang melengkapi beberapa unsur di beberapa pasal KUHP.[15]

Di kasus pencurian informasi / data pribadi bisa pula memicu korban berkesinambungan, tak hanya pengunjung situs web serta elektronik, melainkan perusahaan yang mempunyai sistem elektronik serta bank yang merupakan mitra payment. ehingga tindak kriminal *phishing* bisa dikenai UU No. 11 Tahun 2008 seputar informasi serta transaksi elektronik serta UU No. 27 Tahun 2022 seputar Perlindungan Data Pribadi.

Kaidah tindak pidana yang dilaksanakan terbukti memberi ancaman pemakai internet. Dari berlakunya UU No. 11 Tahun 2008 seputar Informasi dan Transaksi Elektronik yang telah dirubah oleh UU No. 19 Tahun 2016 seputar Perubahan atas UU No. 11 Tahun 2008 seputar Informasi serta Transaksi Elektronik serta terdapat UU baru seputar perlindungan data pribadi yakni UU No. 27 Tahun 2022.

Pelaku dari tindak kejahatan phising cybercrime adalah pengguna internet aktif yang secara sengaja mengambil data informasi dari para korban. Mereka yang dituduh berdasarkan Undang-Undang Hukum ITE mengenai pencurian data pribadi cenderung tunduk pada Pasal 32 ayat (2) *jo*. Pasal 48 ayat (2) UU ITE *jis.* Pasal 67 ayat 1 UU No. 27 Tahun 2022 seputar Perlindungan Data Pribadi

Hukum Undang-Undang ITE pada pasal tersebut bisa digunakan untuk menjerat semua aktivitas cybercrime mengenai pencurian data pribadi / *phishing* yang terjadi di internet tanpa terkecuali.

Kesimpulan

Phishing cybercrime merupakan kriminal yang muncul dari efek buruk teknologi yang kini tumbuh begitu pesat. Kejahatan *phishing cybercrime* bersifat virtual dikarenakan pelaku tidak tampil atau menyerang secara fisik. Dari segi perspektif kriminologi phishing *cybercrime,* ada 2 (dua) faktor penting yang mempengaruhi terjadinya tindak kejahatan komputer *(cybercrime)* yakni Faktor Teknis dan Faktor Ekonomi. Dalam penegakan hukumya berkaitan dengan *cybercrime* sanksi yang dikenakan dari KUHP dan UU ITE masih cukup ringan. Padahal apabila dilihat dari kasus yang terjadi*, Cybercrime* sangat menimbulkan kerugian besar bagi korban sehingga tidak adanya kata sepadan dengan akibat yang ditimbulkan oleh pelaku.

Daftar Pustaka

[1] Suhardi Rustam, "ANALISA CLUSTERINGPHISING DENGAN K-MEANSDALAM MENINGKATKAN KEAMANAN KOMPUTER," 2018.

[2] B. Suharto and A. B. Kurniawan, "JHP 17 (Jurnal Hasil Penelitian) TINDAK PIDANA CYBERCRIME BAGI PELAKU PEMALSUAN DATA PADA SITUS E-COMMERCE (PHISING)," vol. 5, no. 2, pp. 2579–7980, 2020, [Online]. Available: http://jurnal.untag-sby.ac.id/index.php/jhp17

[3] E. Fernando Siregar, H. Helvis, and M. Markoni, "Analisa Yuridis Eksekusi Sita Jaminan Terhadap Tindak Pidana Pencucian Uang (TPPU) First Travel," *Jurnal Syntax Transformation*, vol. 2, no. 11, pp. 1560–1573, Nov. 2021, doi: 10.46799/jst.v2i11.454.

[4] D. Rachmawati, "PHISING SEBAGAI SALAH SATU BENTUK ANCAMAN DALAM DUNIA CYBER," 2020. [Online]. Available: http://www.it-artikel.com/

[5] A. Saputra Gulo, S. Lasmadi, and K. Nawawi, "Cyber Crime dalam Bentuk Phising Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik," *PAMPAS: Journal Of Criminal*, vol. 1, p. 2020.

[6] M. H. Wibowo and N. Fatimah, "ANCAMAN PHISHING TERHADAP PENGGUNA SOSIAL MEDIA DALAM DUNIA CYBER CRIME," 2017.

[7] M. H. Wibowo and N. Fatimah, "ANCAMAN PHISHING TERHADAP PENGGUNA SOSIAL MEDIA DALAM DUNIA CYBER CRIME," 2017.

[8] M. A. Ferdiansyah and F. Simangunsong, "PERTANGGUNG JAWABAN PELAKU BINARY OPTION TERHADAP HUKUM POSITIF DI INDONESIA," *Bureaucracy Journal: Indonesia Journal of Law and Social-Political Governance*, vol. 2, no. 2, p. 2022, 2022, doi: 10.53363/bureau.v2i2.93.

[9] A. Wahid and A. Shodikin Mahkamah, "ALAT BUKTI TINDAK PIDANA CYBERCRIME DALAM SISTEM PERADILAN DI INDONESIA," *Jurnal Kajian Hukum Islam*, vol. 87, no. 1, 2022.

[10] M. A. Aldriano and M. A. Priyambodo, "CYBER CRIME DALAM SUDUT PANDANG HUKUM PIDANA," *Jurnal Kewarganegaraan*, vol. 6, no. 1, 2022.

[11] F. Anugerah, "PENCURIAN DATA PRIBADI DI INTERNET DALAM PERSPEKTIF KRIMINOLOGI," 2021, [Online]. Available: https://ejournal.undiksha.ac.id/index.php/jkh

[12] Ni Putu Rai Yuliartini, "KENAKALAN ANAKDALAM FENOMENA BALAPAN LIARDI KOTA SINGARAJA DALAM KAJIAN KRIMINOLOGI," 2019.

[13] Y. Mahasaraswati *et al.*, “FAKTOR PENYEBAB TERJADINYA KEJAHATAN CYBER CRIME YANG DILAKUKAN OLEH ORANG ASING DI BALI DITINJAU DARI PERSPEKTIF KRIMINOLOGI,” 2021.
[14] Deawit Sutriadi1) and Frans Simangunsong2), “DINAMIKA PERSINGGUNGAN HUKUM ADMINISTRASI DAN HUKUM PIDANA DI INDONESIA,” 2022.
[15] A. Putera, U. Siahaan, and K. Kunci -Cybercrime, “PELANGGARAN CYBERCRIME DAN KEKUATAN YURISDIKSI DI INDONESIA”.