COMSERVA
JURNAL PENELITIAN DAN PENGABDIAN MASYARAKAT
Volume 2 No. 11, Maret 2023 (2686-2696)
e-ISSN: 2798-5210
p-ISSN: 2798-5652

Optimalisasi Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik dalam Penanganan Perkara Tindak Pidana Phising

Optimization of Law Number 11 of 2008 concerning Information and Electronic Transactions in Handling Phishing Criminal Cases

Septian Arya Budi Mahesa, Hervina Puspitosari
UPN Veteran Jawa Timur, Indonesia

*Email: septianarya77@gmail.com, hervina.ih@upnjatim.ac.id
Correspondence: Septian Arya Budi Mahesa

DOI: 10.59141/comserva.v2i11.670

Histori Artikel
Diajukan : 03-02-2023
Diterima : 18-03-2023
Diterbitkan : 27-03-2023

ABSTRAK

Cybercrime di Indonesia begitu pesat dan mengalami perkembangan yang sangat luar biasa, namun hal itu tidak dibarengi dengan Kepastian Hukum atas Perlindungan Data Pribadi Masyarakat Indonesia yang saat ini sedang mengalami berbagai macam Penyerangan terhadap Data Pribadi salah satunya dengan Tindak Pidana *Phising*. Tindak Pidana *Phising* merupakan Tindak Pidana yang dilakukan dengan cara mengirim *link* secara *random* kepada Korbannya dan jika Korban membuka *link* tersebut maka akan terjadi Pencurian Data Pribadi dan berakibat Penjualan Data Pribadi ke *Dark Web* atau *Deep Web*. Revolusi Industri 4.0 atau yang sering disebut dengan *cyber physical system* merupakan revolusi yang menitikberatkan pada otomatisasi serta kolaborasi antara teknologi siber. Revolusi 4.0 ini sendiri muncul di abad ke-21 dengan ciri utama yang ada adalah penggabungan antara informasi serta teknologi komunikasi ke dalam bidang industri. Metode yang peneliti pergunakan berupa hukum normatif, yakni sebuah penelitian kepustakaan hukum yang berlandaskan terhadap norma hukum pada peraturan dimana khususnya di sini mempergunakan Undang-Undang 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik.

Kata Kunci: *Phising; Cybercrime;* Informasi dan Transaksi Elektronik

ABSTRACT

Cybercrime in Indonesia is growing rapidly and experiencing extraordinary developments, but this is not accompanied by legal certainty for the protection of personal data for Indonesian people who are currently experiencing various types of attacks on personal data, one of which is phishing. Phishing is a crime committed by sending a link randomly to the victim and if the victim opens the link, personal data theft will occur and result in selling personal data to the dark web or deep web. The Industrial Revolution 4.0 or what is often referred to as the cyber physical system is a revolution that focuses on automation and collaboration between cyber technologies. The 4.0 revolution itself emerged in the 21st century with the main characteristic being the incorporation of information and communication technology into the industrial sector. The method that the researcher uses is normative law, namely a legal literature research based on legal norms in regulations where especially here using Law 11 of 2008 concerning Information and Electronic Transactions.

***Keywords**:Phising; Cybercrime; Information and Electronic Transactions*

PENDAHULUAN

Perkembangan teknologi pada beberapa tahun akhir ini mengalami kemajuan yang sangat pesat dan jumlah pengguna teknologi menjadi terus meningkat dari tahun ketahun, hal ini yang membuat kebutuhan atas internet semakin penting bagi manusia abad ke 21 ini. Selain itu, menurut (Andrew, 2021) mengistilahkan Revolusi Industri 4.0 atau yang sering disebut dengan *cyber physical system* merupakan revolusi yang menitikberatkan pada otomatisasi serta kolaborasi antara teknologi siber. Revolusi 4.0 ini sendiri muncul di abad ke-21 dengan ciri utama yang ada adalah penggabungan antara informasi serta teknologi komunikasi ke dalam bidang industri (Fonna, 2019).

Peranan teknologi informasi dan komunikasi di era globalisasi telah menempatkan pada posisi yang amat strategis karena menghadirkan suatu dunia tanpa batas, jarak, ruang, dan waktu, yang berdampak pada peningkatan produktivitas dan efisiensi. Pengaruh globalisasi dengan penggunaan sarana teknologi informasi dan komunikasi telah mengubah pola hidup masyarakat, dan berkembang dalam tatanan kehidupan baru dan mendorong terjadinya perubahan sosial, ekonomi, budaya, pertahanan, keamanan, dan penegakan hukum (Arif, 2019).

Banyak sekali kita jumpai akhir-akhir ini terkait tindak pidana cyber yang merupakan dari bagian pidana khusus. Artinya tindak pidana khusus itu sendiri merupakan sebuah tindak pidana yang diatur diluar KUHP atau Pengaturan Umum dalam Hukum Positif Indonesia. Menurut Sudarto mendefinisikan tindak pidana khusus adalah: "Hukum pidana yang ditetapkan untuk golongan khusus atau yang berhubungan dengan perbuatan-perbuatan khusus. Termasuk di dalamnya hukum pidana militer (golongan orang khusus) dan hukum pidana fiskal (perbuatan-perbuatan khusus). Termasuk hukum pidana khusus adalah hukum pidana ekonomi." (Ruslan Renggong, 2017)

Problem pelanggaran hukum atau dengan nama lain "kejahatan" merupakan tanggungjawab setiap unsur masyarakat. Karena selain kejahatan itu setua usia sejarah kehidupan masyarakat, juga berembrio dari konstruksi masyarakat itu sendiri (Samsir et al., 2020).

Van Bammelen yang dikutip dalam Abdul Wahid dan Mohammad Labib mengatakan bahwa: "Kejahatan adalah tiap perbuatan yang bersifat tidak susila, melanggar norma, mengacaukan, dan menimbulkan begitu banyak ketidaktenangan dalam kehidupan masyarakat, sehingga masyarakat berhak untuk mencela, mereaksi, atau mengatakan penolakannya atas perbuatan itu. Masyarakat berhak membenci segala tindak kejahatan, karena di dalam kejahatan bukan hanya mengandung perbuatan melanggar hukum, tetapi juga melanggar hak-hak sosial, ekonomi dan lain sebagainya." (IfranI, 2012)

Kejahatan terus berkembang seiring dengan perkembangan peradaban manusia, dengan kualitas dan kuantitasnya kompleks dengan variasi modus operandinya (Rahmani Fitra, 2017).

Mengingat kejahatan itu setua usia kehidupan manusia, maka tingkat dan ragam kejahatan juga mengikuti realitas perkembangan kehidupan manusia. Kecenderungannya terbukti, bahwa semakin maju dan modern kehidupan masyarakat, maka semakin maju dan modern pula jenis dan modus operandi kejahatan yang terjadi di tengah masyarakat (Flora, 2022).

Hingga akhirnya memunculkan kejahatan baru di dunia siber yang sering disebut *Cyber Crime*. *Cyber Crime* merupakan salah satu bentuk atau dimensi baru dari kejahatan masa kini yang mendapat perhatian luas di dunia internasional. Volodymyr Golubev menyebutnya sebagai *the new form of anti-social behavior* (Erna Dewi, 2013).

Perbuatan melawan hukum di dunia maya (*cyber crime*) merupakan sebuah fenomena yang sangat mengkhawatirkan, mengingat tindakan carding, hacking, penipuan, terorisme, dan penyebaran informasi destruktif telah menjadi bagian dari aktivitas pelaku kejahatan di dunia maya (Manurung, 2023).

Salah satu tindak pidana tersebut adalah *Phising*. *Phising* dalam ruang lingkup keamanan komputer, *Phising* adalah salah satu kejahatan elektronik dalam bentuk penipuan. Dimana proses phising ini bermaksud untuk menangkap informasi yang sangat sensitif seperti username, password dan detail kartu kredit dalam bentuk meniru sebagai sebuah entitas yang dapat dipercaya/*legitimate organization* dan biasanya berkomunikasi secara elektronik (Rachmawati, 2014).

Cyber Crime dalam bentuk Phising secara normatif pada Peraturan Perundang-Undangan di Indonesia belum ada peraturan perundang-undangan yang secara khusus mengatur mengenai *Phising*. Meski demikian, pelaku dapat dijerat ketentuan dalam Kitab UndangUndang Hukum Pidana (KUHP) serta Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) dan perubahannya, sesuai dengan tindak pidana pelaku.

Ketidakefektifan Penggunaan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) inilah yang membuat Perkara Tindak Pidana *Phising* menjadi dilemma dikarenakan kurangnya Kesadaran Hukum dari Penegak Hukum dalam memaksimalkan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) sebagai garda dan Dasar Utama untuk menjerat Pelaku Tindak Pidana Phising di Indonesia.

Penegak Hukum kita lebih berfokus menggunakan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) sebagai bentuk senjata untuk menjerat Pelaku Pencemaran Nama Baik dan Ujaran Kebencian dibandingkan memaksimalkan dalam memberikan Perlindungan Terhadap Data Pribadi Masyarakat Indonesia, sehingga hal ini memaksa DPR untuk mengeluarkan Undang-Undang Perlindungan Data Pribadi yaitu Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

METODE

Penelitian ini tergolong hukum normatif, yakni sebuah penelitian kepustakaan hukum yang berlandaskan norma hukum pada peraturan undang-undang ataupun peraturan internasional (Agus, 2017). Fokus kajiannya berupa hukum positif (Maulana, 2022). Sebuah hukum yang diberlakukan di sebuah tempat ataupun waktu, yakni sebuah norma ataupun aturan tertulis yang dibentuk dengan resmi serta telah diundangkan pihak yang berkuasa, di samping hukum tertulis ini, adapun norma yang tidak dituliskan pada masyarakat yang mampu mengelola perilaku anggotanya dengan efektif (Rahman Syamsuddin, 2019).

HASIL DAN PEMBAHASAN

Definisi *Cybercrime*

Perkembangan dan kemajuan teknologi kini tak dapat dibendung lagi, dikarenakan semakin pesatnya perubahan yang terjadi di era abad ke-21 ini, tentu akan semakin banyak memunculkan permasalahan siber terus bermunculan hingga muncul sebuah istilah kriminal siber yang bernama *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 misue*". "*computer abuse*", "*computer fraud*", "*computer-related crime*", "computer-assisted crime", atau "*computer crime*". Namun para sarjana waktu itu, pada umumnya lebih menerima penggunaan istilah "*computer crime*" oleh karena dianggap lebih luas dan biasa dipergunakan dalam hubungan internasional (Falah et al., 2017).

The British Law Comission misalnya, mengartikan "*computer fraud*" sebagai manipulasi komputer dengan cara apa pun yang dilakukan dengan itikad buruk untuk memperoleh uang, barang atau keuntungan lainnya atau dimaksudkan untuk menimbulkan kerugian kepada pihak lain. Mandell membagi "*computer crime*" atas dua kegiatan, yaitu:

1. Penggunaan komputer untuk melaksanakan perbuatan penipuan, pencurian atau penyembunyian yang dimaksud untuk memperoleh keuntungan keuangan, keuntungan bisnis, kekayaan atau pelayanan.
2. Ancaman terhadap komputer itu sendiri, seperti pencurian perangkat keras atau lunak, sabotase dan pemerasan (Kwarto & Angsito, 2018).

The US Computer Crime Manual menggunakan "*computer-related crime*" di samping "*computer crime*". Komisi Franken lebih condong menggunakan "*computer misue*" oleh karena "*computer crime*" lebih membatasi pada perbuatan yang dilarang oleh UndangUndang Hukum Pidana, padahal perbuatan pernyalahgunaan komputer dapat dilarang pula oleh ketentuan lainnya. Dalam bahasa Belanda sering digunakan istilah "*computer misbruik*" di samping "*computer criminaliteit*". Dengan berkembangnya jaringan internet14 dan telekomunikasi dikenal juga dengan istilah "*digital crimes*" dan "*cybercrime*".

Sitem teknologi informasi berupa internet telah dapat menggeser paradigm para ahli hukum terhadap para ahli hukum terhadap definisi kejahatan komputer sebagaimana ditegaskan sebelumnya, bahwa pada awalnya para ahli hukum terfokus pada alat/perangkat keras yaitu komputer. Namun dengan adanya perkembangan teknologi informasi berupa jaringan internet, maka terfokus dari identifikasi terhadap definisi *cybercrime* lebih diperluas lagi yaitu seluas aktivitas yang dapat dilakukan di dunia *cyber*/maya melalui sistem informasi yang digunakan. Jadi tidak sekedar pada komponen hardwarenya saja kejahatan tersebut dimaknai sebagai *cybercrime*, tetapi sudah dapat diperluas dalam lingkup dunia yang dijelajah oleh sistem teknologi informasi yang bersangkutan. Sehingga akan lebih tepat jika pemaknaan dari *cybercrime* adalah kejahatan teknologi informasi, juga sebagaimana dikatakan Barda Nawawi Arief sebagai kejahatan mayantara (Suhariyanto, 2013).

Pada dasarnya *cybercrime* meliputi semua tindak pidana yang berkenaan dengan sistem informasi, sistem informasi (*information system*) itu sendiri, serta sistem komunikasi yang merupakan sebuah sarana untuk penyampaian/pertukaran informasi kepada berbagai pihak lainnya (*transmitter*/*originator to reciptient*). Sehingga menyebabkan perkembangan definisi dari cybercrime yang digunakan hingga hari ini oleh para sarjana hukum (Ikhsan, 2015).

Karakteristik *Cybercrime*

Perubahan yang terjadi itu dengan sendirinya terjadi pula pada perubahan hukum karena kebutuhan masyarakat akan berubah secara kuantitatif. Permasalahan yang timbul dalam perubahan hukum itu adalah sejauh mana hukum bisa sesuai dengan perubahan hukum itu adalah sejauh mana hukum bisa sesuai dengan perubahan tersebut dan bagaimana tatanan hukum itu agar tidak tertinggal dengan perubahan masyarakat. Di samping itu, sejauh mana masyarakat dapat mengikatkan diri dalam

perkembangan hukum agar ada keserasian antara masyarakat dan hukum supaya melahirkan ketertiban dan ketenteraman yang diharapkan (Gineng & Natangsa Surbakti, 2017).

Era globalisasi juga menyebabkan makin canggihnya teknologi informasi sehingga telah membawa pengaruh terhadap munculnya berbagai bentuk kejahatan yang sifatnya modern yang berdampak lebih besar daripada kejahatan konvensional. Berbeda dengan kejahatan konvensional, yang bercirikan setidaknya terdiri dari beberapa hal, di antaranya penjahatnya bisa siapa saja (orang umum berpendidikan maupun orang awam berpendidikan) dan alat yang digunakan sederhana serta kejahatannya tidak perlu menggunakan suatu keahlian. Kejahatan dibidang teknologi informasi dapat digolongkan sebagai *white collar crime* karena pelaku *cybercrime* adalah orang yang menguasai penggunaan internet beserta aplikasinya atau ahli di bidangnya. Selain itu, perbuatan tersebut sering kali dilakukan secara *transnasional* atau melintasi batas negara sehingga dua criteria kejahatan melekat sekaligus dalam kejahatan cyber ini, yaitu *white collar crime* dan *transnational crime*. Modern di sini diartikan sebagai kecanggihan dari kejahatan tersebut sehingga pengungkapannya pun melalui sarana yang canggih pula.

Berdasarkan beberapa literature serta praktiknya, cybercrime memiliki beberapa karakteristik, yaitu:

1. Perbuatan yang dilakukan secara illegal, tanpa hak atau tidak etis tersebut terjadi dalam sebuah ruang/wilayah siber/*cyber* (*cyberspace*), maka hal itu tidak dapat dipastikan yurisdiksi negara mana yang berlaku terhadapnya.
2. Perbuatan tersebut dilakukan dengan cara menggunakan peralatan apa pun yang terhubung dengan internet.
3. Perbuatan tersebut tentunya mengakibatkan kerugian materil maupun immateril (waktu, nilai, jasa, uang, barang, harga iri, martabat, kerahasiaan informasi) yang cenderung lebih besar tentunya dibandingkan dengan sebuah kejahatan konvensional.
4. Pelakunya adalah orang yang menguasai penggunaan internet beserta aplikasinya.
5. Perbuatan tersebut sering terjadi dan dilakukan secara transnasional/melintasi batas negara (Bunga, 2019).

Definisi Tindak Pidana Phising

Ruang lingkup keamanan komputer, *phising* adalah salah satu kejahatan elektronik dalam bentuk penipuan. Dimana proses *phising* ini bermaksud untuk menangkap informasi yang sangat sensitif seperti username, password dan detil kartu kredit dalam bentuk meniru sebagai sebuah entitas yang dapat dipercaya/*legitimate organization* dan biasanya berkomunikasi secara elektronik (Rachmawati, 2014).

Phising ini juga biasanya ditujukan kepada pengguna online banking, karena menggunakan isian data (ID) pengguna dan kata sandi, dan tidak menutup kemungkinan untuk ditujukan ke pengguna *online* lainnya. Ketika pengguna memasukkan isian data pengguna miliknya dan kata sandinya ke form login yang merupakan *fake form login* maka akan diketahui oleh pelaku *cybercrime* dalam bentuk phising tersebut (Saputra Gulo et al., 2020).

Pengaturan Tindak Pidana *Phising* di Indonesia

Phising saat ini di Indonesia dimungkinkan dapat dikenakan Pasal 35 jo Pasal 51 ayat (1) karena phising merupakan kejahatan siber yang membuat situs yang menyerupai situs asli yang resmi, padahal situs tersebut adalah situs palsu. *Cybercrime* dalam bentuk *phising* ini juga dapat dikenakan Pasal 28 ayat (1) jo Pasal 45A ayat (1) karena *phising* juga melakukan kebohongan untuk menyesatkan orang

lain dimana mengarahkan orang yang dibohongi untuk mengakses sebuah link yang dimana link tersebut ditujukan ke situs palsu dan memberikan suatu perintah untuk memperbarui informasi pribadinya yang rahasia ke dalam situs palsu yang telah dibuat oleh pelaku phising, sehingga informasi pribadinya yang rahasia tersebut diketahui oleh pelaku phising dan menyebabkan orang tersebut mengalami kerugian (Saputra Gulo et al., 2020).

Perlu digaris bawahi adalah dengan adanya pengaturan tersebut tidak sepenuhnya mampu memberikan kepastian hukum dalam penegakan hukum pada kasus tindak pidana *phising*, karena masih banyak penerapan saat penjatuhan hukuman kepada setiap pelaku tindak pidana *phising* yang begitu beragam. Sehingga hal ini seakan membuat sebuah kekaburan hukum didalamnya karena akan membuat penegak hukum khususnya dari pihak kepolisian dan kejaksaan akan menjatuhkan hukuman yang tidak dapat dipastikan pengaturan secara khusus dan pastinya, dan jalan satu-satunya pada setiap penjatuhan hukum tindak pidana *phising* dapat dilihat dari unsur-unsur dari tindak pidananya serta unsur turut serta tindak pidana lain yang dilakukan oleh pelaku tindak pidana *phising*.

Contoh Kasus Tindak Pidana *Phising* di Indonesia

Contohnya sama seperti kasus phising yang pernah terjadi yang dilakukan oleh seorang laki-laki bernama Steven Haryanto yaitu seorang hacker dan jurnalis. Lelaki asal bandung tersebut dengan sengaja membuat situs asli tapi palsu sebuah layanan internet banking Bank Central Asia (BCA). Steven Haryanto membeli domain-domain dengan nama yang hampir mirip dengan situs asli Internet Banking BCA yaitu "*www.klikbca.com*". Namanama domain yang dibelinya adalah dengan nama domain wwwklik-*bca.com*, *klikbca.com*, *clickbca.com*, klickca.com, dan klikbac.com. Tampilan dan isi situssitus tersebut hampir mirip dengan situs aslinya. Jika nasabah BCA salah mengetik nama domain situs BCA yang asli, maka nasabah tersebut dapat masuk perangkap situs palsu yang telah dibuat oleh Steven Haryanto apalagi nasabah memasukkan informasi pribadinya seperti username dan passwordnya, nomor kartu kredit, Pin, nomor rekening, tanggal lahir, atau nama ibu kandung sehingga Steven Haryanto mengetahui informasi pribadi nasabah tersebut.

Berdasarkan kasus diatas, Steven Haryanto dapat dikenakan dengan Pasal 35 UndangUndang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik karena Steven Haryanto memenuhi unsur-unsur didalam Pasal 35 tersebut dengan membuat situs palsu seolah-olah situs aslinya.

Lalu kasus WNI insial SFR dan MCL yang menipu Warga Negara Amerika Serikat dengan menipu ribuan warga Amerika Serikat dengan menggunakan website palsu sehingga berakibat korban tidak dapat menerima dana bantuan Covid-19 yang diberikan oleh negara Amerika Serikat, dan kasus ini ditanggani oleh Kapolda Jawa Timur serta bekerjasama dengan FBI untuk mencari kedua pelaku yang berasal dari Jawa Timur ini. Tersangka dikenakan pasal 35 Jo Pasal 51 ayat (1) Undang-Undang RI No. 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik Jo Pasal 55 ayat (1) KUHP dan Pasal 32 ayat (2) Jo Pasal 48 ayat (2) UndangUndang RI No. 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik Jo Pasal 55 ayat (1) KUHP.

Kemudian kasus email phising yang mensabotase transaksi 8 miliar Perusahaan Jepang yang Pelakunya adalah tiga orang bernama Reza Hernanda, Syahruddin Noor, dan Denny Anggriawan. Dan Saat ini, RH, SN dan DA tengah dilakukan proses pemeriksaan terkait pasal 31 ayat 1 dan 2 Jo pasal 46 ayat 1 dan 2 atau pasal 35 Jo pasal 51 ayat 1 UU Nomor 19 tahun 2016 tentang perubahan atas UU Nomor 11 tahun 2008 tentang informasi dan transaksi elektronik pasal 55 ayat 1 atau 56 KUHP atau

pasal 5 atau pasal 4 atau pasal 5 UU Nomor 8 Tahun 2010 tentang pencegahan dan pemberantasan tindak pidana pencucian uang (TPPU).

Dari sini dapat terlihat ketidak sama rataan dan kesinambungan pengaturan terhadap tindak pidana *phising* yang beragam dan disesuaikan dengan setiap *modus operandi* serta turut serta tindak pidana lainnya.

Analisa Pengaturan Tindak Pidana Phising di Indonesia

Sebuah peraturan mengenai tindak pidana *phising* tentunya memerlukan sebuah kepastian hukum untuk menjamin penegakan hukum yang dilakukan oleh negara kepada para pelaku tindak pidana *phising*. Pada dasarnya Asas Kepastian Hukum (*het rechtszekerheidsbeginsel*), Asas kepastian hukum merupakan konsekuensi sendi negara berdasarkan atas hukum. Oleh karena itu setiap peraturan yang dibentuk harus jelas. Kepastian hukum menunjuk kepada pemberlakuan hukum yang jelas, tetap dan konsisten dimana pelaksanaannya tidak dapat dipengaruhi oleh keadaan-keadaan yang sifatnya subjektif (Julyano & Sulistyawan, 2019).

Indonesia mengenal Asas "*Lex Specialis Derogat Legi Generali*". Berdasarkan asas *lex specialis derogat legi generali*, berarti aturan-aturan hukum yang bersifat khusus dianggap berlaku meskipun bertentangan dengan aturan-aturan hukum yang umum. Dapat disimpulkan bahwa yang berlaku saat ini untuk mengatur tentang bagaimana pengaturan hukum *cybercrime* dalam bentuk phising tersebut saat ini diatur oleh Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik karena Undang-Undang ini bersifat khusus. Pada saat ini perbuatan *phising* tersebut diatur pada Pasal 35 jo Pasal 51 Ayat (1), yang dirumuskan sebagai berikut:

1. 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 yang otentik.
2. Pasal 51: "Setiap Orang yang memenuhi unsur sebagaimana dimaksud di dalam Pasal 35 dipidana dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp 12.000.000.000,00 (dua belas miliar rupiah)." Unsur-unsur yang terdapat di dalam Pasal 35, yaitu:
    a. Setiap Orang;
    b. Dengan sengaja dan tanpa hak atau melawan hukum;
    c. Melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi Elektronik dan/atau Dokumen Elektronik;
    d. Dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik.

Phising juga memuat sebuah kebohongan yang membuat orang lain mengakses website palsu yang diberikan oleh pelaku kepada korban sehingga Pasal selanjutnya yang dapat dikenakan adalah Pasal 45A ayat (1) Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik karena telah melakukan tindakan kebohongan. Pasal 28 Ayat (1) Jo Pasal 45A Ayat (1) dirumuskan sebagai berikut:

1. Pasal 28 Ayat (1): "Setiap Orang dengan sengaja, dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik."
2. Pasal 45A Ayat (1): "Setiap Orang yang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik

sebagaimana dimaksud dalam Pasal 28 Ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp 1.000.000.000,00 (satu miliar rupiah) (Choiroh, 2017).

Pada prakteknya tindak pidana phising begitu beragam penjatuhan pidananya, sehingga hal ini menjadikan Penulis menganalisa ketimpangan dan ketidakselarasan yang membuat asas kepastian hukum menjadi kabur, beragamnya pengaturan seperti yang dijelaskan pada sub bab sebelumnya mengindikasikan kebingungan penegak hukum kita dalam memproses pelaku tindak pidana phising. Alasan kedua yang menyebabkan kebijakan dan pengaturan *phising* sendiri mengalami kekaburan hukum dikarenakan tidak ada definisi pasti yang terdapat di dalam peraturan perundang-undangan yang menjelaskan tentang phising itu sendiri. Tidak terdapat konsep pasti oleh ahli hukum mengenai *phising* dan penekanan secara regulasi oleh undang-undang mengenai *phising*.

Optimalisasi Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) dalam Penanganan Perkara Tindak Pidana *Phising*

Salah satu upaya agar dapat membuat tindak pidana *phising* dapat segera memberikan kepastian hukum dan selaras dengan asas-asas hukum serta dapat mengoptimalkan keberadaan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), salah satunya mengenai asas kepastian hukum (*het rechtszekerheidsbeginsel*) adalah berada pada Kebijakan Hukum terhadap *cybercrime* dalam bentuk *phising* berdasarkan Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik adalah dilakukannya perubahan terhadap Undang-Undang tentang ITE tersebut dengan merumuskan konsep *phising* dengan jelas dan tegas serta merubah isi dan unsur pada Pasal 35 agar kemudian Pasal 35 tersebut dapat diterapkan dan/atau dikenakan terhadap pelaku *cybercrime* dalam bentuk phising. Selain itu dapat disimpulkan karena ketidakpastiaan konsep *phising* tindak pidana ini menjadi tindak pidana yang memiliki multi regulasi/regulasi yang beragam.

Langkah selanjutnya adalah dengan mengembalikan esensi dan fungsi utama Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) sebagai *Protector* dari Kejahatan Siber yang ada di Indonesia baik yang dilakukan dari dalam maupun luar negeri hal ini tentunya dapat memberikan sebuah keamanan terbaik dan Kepastian Hukum terhadap Masyarakat Indonesia dimana sifat dari Pasal Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) adalah fleksibel maka dapat dioptimalkan dalam menjerat setiap Delik dan Unsur Tindak Pidana *Phising* yang dapat dikaitkan dengan Tindak Pidana Umum lainnya seperti Penipuan, Pencurian Data Pribadi, Penyebaran Berita Bohong, Penggelapan, Tindak Pidana Pencucian Uang (TPPU) dan lain sebagainya.

Analisa ini jauh lebih efektif dibandingkan Penegak Hukum yang lebih banyak menyelesaikan Perkara Pencemaran Nama Baik dan Ujaran Kebencian menggunakan Pasal 27 Ayat (3) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), yang justru sifatnya adalah Privat dan Individu.

Tujuan hukum pidana bukan hanya sebagai upaya pembalasan, akan tetapi bagaimana hukum mampu memberikan keadilan bagi korban maupun pelaku. Asas keseimbangan dalam konsep pembaharuan hukum pidana tidak hanya melihat persyaratan pidana hanya sebatas pada adanya "tindak pidana" (TP) dan "kesalahan" atau "pertanggungjawaban pidana", tetapi juga didasarkan pada tujuan pemidanaan, maka dapat disimpulkan dengan pembaharuan hukum pidana serta berkembangnya peraturan perundang-undangan dan berkembangnya tindak pidana salah satunya *cybercrime* maka

diperlukan juga penanganan secara seimbang agar dapat menciptakan hukum yang konkrit terhadap tindak pidana *phising.* Sekaligus dengan lagi mengembalikan fungsi Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) sebagai esensi Perlindungan Data Pribadi dan Digitalisasi yang berfokus pada duni *Cyber* tentunya perkara Tindak Pidana *Phising* yang lainnya dengan ragam *Modus Operandi* yang ada dapat diantisipasi baik secara Preventif maupun Represif. Amerika Serikat sebagai salah satu negara yang sering mengalami Penyerangan Digital dan *Hack* setiap tahunnya tetap mampu mengembalikan fungsi dan *Security Defence* dan *Security Access* kembali sehingga tidak terjadi Pembobolan Data Pribadi dari Warga Negaranya sekitar 75% jauh lebih aman dibandingkan di Indonesia, ditambah lagi dengan dimaksimalkannya *Stop Online Piracy Act* (SOPA) dan *Protect Intelectual Property Act* (PIPA) sebagai salah satu regulasi dalam menyelesaikan Permasalahan *Cybercrime* khususnya Tindak Pidana *Phising*.

SIMPULAN

Berdasarkan hasil dan pembahasan penelitian, maka dapat ditarik kesimpulan bahwa optimalisasi Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) dalam Perkara Tindak Pidana *Phising* dapat dioptimalkan fungsi dan fleksibilitas yang dimiliki dalam menjerat dengan beragam Delik Pidana dan Unsur yang nantinya akan dimasukkan ke dalam Surat Dakwaan (P-29) dan Surat Tuntutan (P-42) dari Kejaksaan Republik Indonesia. Pada dasarnya Tindak Pidana *Phising* memiliki beragam Unsur yaitu Penipuan, Pencurian Data Pribadi, Penyebaran Berita Bohong, Penggelapan, Tindak Pidana Pencucian Uang (TPPU) dan lain sebagainya. Pengaturan *Phising* lebih sering diatur dan penegakkannya menggunakan Pasal 35 Jo Pasal 51 Ayat (1) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE).

DAFTAR PUSTAKA

Agus, P. A. (2017). Kedudukan sertifikasi halal dalam sistem hukum nasional sebagai upaya perlindungan konsumen dalam hukum Islam. *Amwaluna: Jurnal Ekonomi Dan Keuangan Syariah*, *1*(1), 149–165.

Arif, A. N. (2019). *Transaksi Uang Elektronik Ditinjau dari Hukum Bisnis Syariah*. Universitas Andalas.

Bunga, D. (2019). Kebijakan Formulasi Judi Online dalam Hukum Indonesia. *Vyavahara Duta*, *14*(1), 21–34.

Choiroh, L. U. (2017). Pemberitaan Hoax Perspektif Hukum Pidana Islam. *Al-Jinayah: Jurnal Hukum Pidana Islam*, *3*(2), 325–348.

Erna Dewi, E. (2013). *Pengaruh Perkembangan Cyber Crime Terhadap Penegakan Hukum Pidana*.

Falah, M. F., Tanuwijaya, F., & Samosir, S. S. M. (2017). Perjudian Online: Kajian Pidana atas Putusan Nomor 1033/PID. B/2014/PN. BDG. *E-Journal Lentera Hukum*, *2*(1), 28–41.

Flora, H. S. (2022). Modus Operandi Tindak Pidana Prostitusi Melalui Media Sosial Online. *Journal Justiciabelen (JJ)*, *2*(2), 120–138.

Fonna, N. (2019). *Pengembangan Revolusi Industri 4.0 dalam Berbagai Bidang*. Guepedia.

Gineng, P., & Natangsa Surbakti, S. H. (2017). *Upaya Pembuktian oleh Aparat Penegak Hukum dalam Rangka Mencari Kebenaran Materiil Dalam Perkara Pidana Cyber crime*. Fakultas Hukum.

IfranI, I. (2012). *Hukum Perlindungan Nasabah Bank.* Nusa Media.

Ikhsan, M. (2015). Faktor-Faktor Penyebab Terjadinya Perjudian Online Melalui Mediainternet Yang Dilakukan Oleh Mahasiswa Di Kota Pontianak Ditinjau Dari Sudut Kriminologi. *Jurnal Hukum Prodi Ilmu Hukum Fakultas Hukum Untan (Jurnal Mahasiswa S1 Fakultas Hukum) Universitas Tanjungpura*, *3*(3).

Julyano, M., & Sulistyawan, A. Y. (2019). Pemahaman terhadap asas kepastian hukum melalui konstruksi penalaran positivisme hukum. *Crepido*, *1*(1), 13–22.

Kwarto, F., & Angsito, M. (2018). Pengaruh Cyber Crime Terhadap Cyber Security Compliance Di Sektor Keuangan. *Jurnal Akuntansi Bisnis*, *11*(2).

Manurung, R. E. (2023). *Tinjauan Yuridis Cyber Crime Phising dan Carding pada Kartu Kredit (Studi Kasus Putusan No. 958/Pid. Sus/2020/PN. PBR dan Putusan No. 2322/Pid. B/2019/PN. SBY)*. Universitas Kristen Indonesia.

Maulana, A. B. (2022). *Tinjauan Hukum Islam dan Hukum Positif terhadap Perkawinan Beda Agama (An Overview of Islamic Law and Positive Law on Interfaith Marriages)*. Universitas 17 Agustus 1945 Surabaya.

Rachmawati, D. (2014). Phising Sebagai Salah Satu Bentuk Ancaman Dalam Dunia Cyber. *Jurnal Saintikom Vol*, *13*(3), 210.

Rahman Syamsuddin, S. H. (2019). *Pengantar Hukum Indonesia*. Prenada Media.

Rahmani Fitra, S. E. (2017). Meningkatkan Pemasaran Melalui Media On Line Dan Mengenali Modus Penipuan Dalam Transaksi On Line. *Entrepreneurship at Global Crossroad: Challenges and Solutions*, 484.

Ruslan Renggong, S. H. (2017). *Hukum Pidana Khusus: Memahami delik-delik diluaR KUHP*. Prenada Media.

Samsir, S., Bahmid, B., & Siregar, E. S. (2020). Strategi dan Kebijakan Penanganan PSK di Polsek Datuk Bandar Kota Tanjungbalai. *JURNAL PIONIR*, *6*(1).

Saputra Gulo, A., Lasmadi, S., & Nabawi, K. (2020). Cyber Crime dalam Bentuk Phising Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik. *PAMPAS: Journal Of Criminal*, *1*(2), 68–81.

Suhariyanto, B. (2013). *Tindak Pidana Teknologi Informasi (Cybercrime)*. PT. Raja Grafindo Persada.