JICN: Jurnal Intelek dan Cendikiawan Nusantara
https://jicnusantara.com/index.php/jicn
Vol : 1 No: 2, April - Mei 2024
E-ISSN : 3046-4560

Pencurian Data Pribadi Di Internet Dari Sudut Pandang Kriminologi

Theft of Personal Data on the Internet from a Criminological Point of View

Regita Citrazalzabilla[1], Hudi Yusuf[2]
[1]Fakultas Hukum, Universitas Bung Karno, *Email: regitacitra5@gmail.com*
[2]Fakultas Hukum, Universitas Bung Karno, *Email: hoedydjoesoef@gmail.com*

Article Info

Article history :
Received : 04-05-2024
Revised : 06-05-2024
Accepted : 08-05-2024
Published : 10-05-2024

Abstract

Advances in information technology are thought to be a force that can determine human destiny. With the existence of the internet, people's activities not only apply in the real world but also spread to cyberspace, as well as criminal acts. There has been a major transformation in the living space made possible through smartphones and connected via systems to the internet. Cases such as fraud can cause material and non-material losses for the victims. In the event that private information/data is stolen, this can also result in ongoing victimization, not only of users of websites and electronic centers but also of companies with electronic systems and banks. The author uses a normative legal method, namely an approach to basic legal literature by examining legal theories, concepts, principles and legal provisions that are relevant to this article. This phishing process aims to be a medium for collecting risky information such as usernames, passwords and card details by disguising themselves as trusted legitimate entities/organizations and generally speaking electronically. Cyber Crime is a term that is widely used to describe criminals via the Internet. Cyber Crime consists of DoS Attack, Hacking, Trojans, Cyber Terrorism, Information Warefare, Cyber Stalking etc. Judging from the elements of fraud and court decisions, regulations related to cyber crime in the form of fraud are regulated in Law Number 11 of 2008 of the Republic of Indonesia concerning Amendments to Law Number 1 of Law Number 19 of 2016 concerning Information and electronic transactions on several items that can be taxed..

Keywords* : *Cybercrime, Internet, Phishing

Abstrak

Kemajuan teknologi informasi diduga menjadi kekuatan yang dapat memastian nasib manusia. Dengan adanya internet, aktivitas masyarakat bukan hanya berlaku di dunia nyata namun menjalar ke cyberspace, sama halnya atas tindakan kriminal. Telah terjadi transformasi besar dalam ruang hidup yang dimungkinkan melalui ponsel pintar dan terhubung melalui sistem ke internet. Kasus-kasus seperti penipuan dapat menimbulkan kerugian materil dan nonmateriil bagi korbannya. Dalam kejadian dimana informasi/data privasi dicuri, hal ini juga dapat mengakibatkan viktimisasi yang berkelanjutan, tidak hanya terhadap pengguna situs web dan pusat elektronik tetapi juga terhadap perusahaan dengan sistem elektronik dan bank. Penulis memakai metode hukum normatif, yaitu pendekatan dengan literatur dasar hukum dengan mengkaji teori-teori hukum, konsep-konsep, asas-asas dan ketentuan-ketentuan hukum yang relevan dengan artikel

ini. Proses phishing ini bertujuan sebagai media pengumpulan info riskan misalnya nama pengguna, kata sandi, dan detail card dengan menyamar sebagai entitas/organisasi sah yang tepercaya dan umumnya berbicara secara elektronik. Cyber Crime merupakan sebutan yang banyak dipakai dalam menjelaskan pelaku kriminal melalui Internet. Cyber Crime terdiri dari DoS Attack, Hacking, Trojan, Cyber Terorisme, Information Warefare, Cyber Stalking dll. Dilihat dari unsur penipuan dan putusan pengadilan, pengaturan terkait kejahatan siber berupa penipuan diatur dalam Undang-Undang Nomor 11 Tahun 2008 Republik Indonesia tentang Perubahan Atas Undang-Undang Nomor 1 Undang-undang Nomor 19 Tahun 2016 tentang Informasi dan transaksi elektronik pada beberapa barang yang dapat dikenakan pajak..

Kata Kunci : Cybercrime, Internet, Phishing

PENDAHULUAN

Kemajuan teknologi informasi diduga menjadi kekuatan yang dapat memastian nasib manusia. Hampir seluruh aktivitas sehari-hari terjadi melalui Internet, koneksi ke Internet menyediakan data pribadi saat Anda memiliki akun yang terhubung ke data agregat. Masalah keselamatan data dan individu menjadi elemen kunci dalam sistem informasi . Akibatnya, masyarakat Indonesia dapat menjadi terlalu bergantung pada teknologi informasi sehingga semakin memicu bahaya. Teknologi informasi dapat mendorong kemajuan dalam kehidupan namun juga dapat menjadi sarana untuk melakukan kejahatan terhadap manusia(Hariyono, dkk, 2023) .

Dengan adanya internet, aktivitas masyarakat bukan hanya berlaku di dunia nyata namun menjalar ke cyberspace, sama halnya atas tindakan kriminal. Telah terjadi transformasi besar dalam ruang hidup yang dimungkinkan melalui ponsel pintar dan terhubung melalui sistem ke internet. Berdasarkan survei APJII 2018, total pemakai internet di Indonesia mencapai 171,17 jt yang menembus 64,8%. Jumlah ini akan naik jika mengingat survei APJII tahun 2017 mendata pemakai Internet di Indonesia berjumlah 143,26 jt yang menembus 54,68%. Pengguna internet di tanah air sebagian besar menggunakan Handphone, pemakai telepon seluler menggapai angka 59,59%, artinya, Masyarakat Indonesia berisiko menjadi korban tindakan kriminal cyberspace lebih dari separuh (Ciptohartono, dkk, 2019) .

Penculikan data di dunia maya dapat dikatakan dengan phishing, yaitu tindak pidana pencurian informasi privasi atau rahasia secara tidak sah. Melalui perlakuan ini dibutuhkan nomor kartu kredit, kode PIN, ID pengguna, nomor HP, nomor rekening dan info data privasi lain. melalui perlakuan ini, pelaku akan mendapatkan keuntungan dari kejahatannya dimana akan memberatkan korban yang datanya dicuri. Ancaman penggalian informasi pribadi di Indonesia lebih riskan karena pemerintah memberlakukan peraturan e-KTP, yaitu cara pengumpulan informasi pribadi dari lembaga swadaya masyarakat publisitas pemerintah, Aturan ini pertama kali diterapkan pada tahun 2011, khususnya penerapan metode NIK. Melalui peraturan tersebut, data tiap masyarakat berjalan selamanya dan setiap masyarakat memiliki kartu yang berisi NIK. Semua data privasi masyarakat dicatat, termasuk ciri fisik dan identitasnya. Dengan demikian, data-data yang terdapat dalam e-KTP dapat dimanfaatkan oleh para penjahat, apalagi bila keamanan yang melindungi data tersebut tidak ketat (Anugerah, dkk, 2023) .

Cybercrime sebagai tindak pidana adalah tindakan kejahatan yang diperbuat dengan corak kriminal, menggunakan internet sebagai media untuk melakukan kejahatan, contohnya pembobolan automatic teller machine (ATM) dan nomor identifikasi pribadi kartu, mencuri nomor kartu kredit orang lain untuk dipakai pada transaksi komersial di Internet; dan menggunakan fasilitas Internet (server web, milis) untuk mendistribusikan materi bajakan. Pengiriman email anonim yang berisi iklan bisa dijadikan sebagai ilustrasi tindakan kriminal menggunakan media internet. Di negara maju, pelaku spam bisa ditangkap karena pelanggaran privasi. Jenis kriminal internet ini termasuk pada area "abu-abu". Sehingga, susah untuk mengetahui apakah perbuatan tersebut adalah tindakan pidana atau tidak, karena corak perbuatan tersebut kadang bukan pidana. Contohnya yaitu scanning, merupakan istilah yang mengacu pada perbuatan memata-matai titik orang melalui pengumpulan informasi sebanyak mungkin untuk disalahgunakan (Mathilda, 2012) .

Kasus-kasus seperti penipuan dapat menimbulkan kerugian materil dan nonmateriil bagi korbannya. Dalam kejadian dimana informasi/data privasi dicuri, hal ini juga dapat mengakibatkan viktimisasi yang berkelanjutan, tidak hanya terhadap pengguna situs web dan pusat elektronik tetapi juga terhadap perusahaan dengan sistem elektronik dan bank. Oleh karena itu, tindakan penipuan diancam dengan pidana berdasarkan UU No. 11 Tahun 2008 tentang Informasi Transaksi Elektronik dan Undang-Undang Nomor 11 Tahun 2008 Tanggal 27 Tahun 2022 tentang Perlindungan Data Pribadi1.

Menurut penjelasan diatas, artikel ini akan membicarakan tentang gunanya perlindungan hukum terhadap tindakan pengambilan data privasi dan faktor-faktor yang dapat menyebabkan terjadinya tindakkan pengambilan data pribadi. Karena dengan adanya peraturan data pribadi di Indonesia kedepannya menjelang adanya undang-undang perlindungan data pribadi yang baru.

METODE PENELITIAN

Penulis memakai metode hukum normatif, yaitu pendekatan dengan literatur dasar hukum dengan mengkaji teori-teori hukum, konsep-konsep, asas-asas dan ketentuan-ketentuan hukum yang relevan dengan artikel ini (Alfiyan, dkk, 2022) . Pendekatan yang dipakai adalah studi pustaka terdiri dari teori hukum primer, sekunder dan tersier. Teknik pengambilan data yang dipakai dalam artikel ini yaitu observasi dan telaah pustaka. Teknik analisis data yang dipakai dalam artikel ini yaitu teknik normatif kualitatif, yaitu mendeskripsikan data yang didapatkan melalui norma hukum, teori serta doktrin dan aturan yang relevan dengan pokok permasalahan untuk melakukan pembahasan secara komprehensif.

HASIL DAN PEMBAHASAN

Berdasarkan bidang keamanan komputer, phishing merupakan jenis tindakan kriminal elektronik yang berbentuk pengelabuan. Proses phishing ini bertujuan sebagai media pengumpulan info riskan misalnya nama pengguna, kata sandi, dan detail card dengan menyamar sebagai entitas/organisasi sah yang tepercaya dan umumnya berbicara secara elektronik. Penipuan ini umumnya menargetkan pemakai perbankan on-line karena memakai data pengguna (ID) dan entri

kata sandi, serta tidak menghilangkan kemampuan memproses alamat pemakai yang berbeda. Bila Seseorang menginput data pribadi serta pasword ke dalam formulir login, yang merupakan formulir login palsu, penjahat dunia maya akan mengetahui bahwa ini adalah penipuan (Gulo, dkk, 2021) .

Dengan meningkatnya total pengguna gadget serta internet, penting mengamankan info atau data privasi juga meningkat secara signifikan. Hal ini selalu terjadi berhubungan pada pencurian data privasi dan tindakan kriminal, misalnya penjualan data privasi, penyalahgunaan rekening bank, pembagian informasi pribadi, penipuan dan kejahatan. Dengan maraknya pengambilan info atau data privasi, pembahasan mengenai pentingnya undang-undang dan peraturan sebagai perlindungan info pribadi harus lebih meningkat. Perlindungan data privasi erat kaitannya pada dasar privasi . Dasar ini merupakan ide untuk melindungi integritas dan martabat masyarakat. Pribadi pun melingkupi usaha individu dalam mengatur siapa saja yand mendapat info tersebut serta bagaimana infotersebut dipakai. Indonesia mempunyai pemakai teknologi dan sistem teknologi dengan tingkatan yang tinggi. Namun hingga saat ini, Indonesia belum memiliki peraturan khas yang mengatur privasi dan perlindungan data. Seiring meningkatnya penggunaan teknologi, peraturan mengenai penanganan masalah hukum terkait privasi dan perlindungan data pun ikut berkembang. Peraturan saat ini sering belum bisa mengikuti perkembangan teknologi. Di Indonesia, peraturan seringkali mendahului perkembangan sosial, termasuk perkembangan teknologi. Tentu saja peluang hukum berdampak pada pribadi dan perlindungan data privasi. Indonesia memerlukan peraturan mengenai privasi dan perlindungan data pribadi dan berharap peraturan tersebut dapat mengatasi permasalahan yang disebabkan oleh penyalahgunaan pengelolaan informasi atau data pribadi 9 murti, 2005).

Cyber Crime merupakan sebutan yang banyak dipakai dalam menjelaskan pelaku kriminal melalui Internet. Dan di beberapa negara di dunia, kejahatan-kejahatan ini dapat dihukum, sementara di negara-negara lain, perdebatan terus berlanjut mengenai bentuk dan status hukumnya. Melalui penjelasan tersebut bisa disimpulkan bahwa cyber crime merupakan perlakuan menggunakan internet untuk alat atau target kriminal . Berikut merupaka tindakan yang tergolong kedalam cyber crime.

DoS Attack

Merupakan serbuan terhadap jaringan komputer yang mencegah jaringan atau sistem menyediakan layanan (e-mail, webb, File Transfer Protocol, Domain Name System, dll.) kepada pengguna. Biasanya, DoS digunakan melalui bandwidth yang terdapat pada jaringan atau dengan mengirimkan permohonan yang salah ke system beberapa kali, yang mengakibatkan system kelebihan beban7.

Hacking

Hackerr merupakan sebutan yang dipakai dalam menjelaskan jenis kecerdasan komputer tertentu. Di perangkat dan pendapat banyak orang melalui artikel media, istilah hackerr selalu didefinisikan pada kejahatan komputer. Namun sebenarnya yang berlaku yaitu hackerr artinya programmer cerdas di bagian pemrograman yang tidak ada hubungannya pada bidang keamanan komputer. Hacking bisa menjadi reward bagi orang yang mempuyai bakat serta pemahaman lebih

dari orang biasanya. Hacking bisa dipahami untuk perlakuan hacker yang menggali sisi lemah pada suatu sistem komputer. Hasilnya bisa suatu program mini yang bisa dipakai dalam mengakses sistem komputer atau menggunakan sistem untuk tujuan tanpa memerlukan akun pengguna. Hackerr yang baik, bila mendapatkan hal seperti itu, akan memberitahukan kepada administrator sistem kalau sistem komputer yang ditembusnya mempunyai sisi lemah yang dapat membahayakan sistem komputer. Jika hasil peretasan ini digunakan oleh pelaku jahat maka perlakuan itu akan tergolong kejahatan dunia maya7.

Trojan

Virus komputer merupakan program komputer yang bisa mereplikasi dirinya sendiri serta menyebar melalui file program biner atau file dokumen yang ditularkan. Bila file program biner atau file dokumen yang telah berisi virus dijalankan, lalu secara langsung virus tersebut hidup pada komputer yang memasuki program itu. Membuat virus kini menjadi mudah karena ada program yang diproduksi yang bertujuan untuk membuat virus. Salah satu contohnya adalah Visual Basic Scripting worm generator yang artinya kita tidak perlu lagi bersusah payah mempelajari pemrograman dalam memproduksi virus, cukup memakai sistem virus generator tersebut.

Trojan berhubungan dengan perangkat lunak berbahaya (malicious software) yang menularkan korbannya dengan mendapatkan akses administrator pada sistem operasi Windows. Membuka port akses melalui komputer memungkinkan pelaku mengakses komputer dari jangkauan yang jauh. Konsep asli pada Trojan ini yaitu pemakaian RAT yang selalu dipakai dari komputer jarak jauh dengan persetujuan hak akses yang diberi. Contoh Trojan yang diberikan yaitu salah satu yang mampu beroperasi dari jangkauan yang jauh dan biasanya dikenal sebagai Trojan akses jarak jauh (Hutauruk, dkk, 2016) .

Cyberterrorism

Cyber terorisme merupakan sebuah perlakuan ilegal yang dirancang oleh seseorang atau sekelompok yang bermotif politik demi mencapai ideologinya, secara langsung ataupun tidak langsung, melakukan gempuran, menyusup, mencuri atau menghancurkan info, pusat komputer, programan komputer, yang bisa menyebabkan kerusakan serius pada korban. Terorisme siber mempunyai dua ciri, yaitu terorisme siber yang merupakan perlakuan terorisme kepada pusat komputer, jaringan dan/atau pangkalan serta info yang disimpan di dalam komputer, dan terorisme siber yang merupakan pemakaian internet dari teroris demi tujuan organisasi dan komunikasi, ditujukan untuk terorisme terhadap pemerintah dan Masyarakat (Jondong, 2020) .

Information warefare

Merupakan perang yang memakai informasi untuk sasara dan alat dalam melakukan serangan. Dalam peperangan informasi, informasi/propaganda bisa disampaikan oleh musuh ketika informasi tersebut tampak benar, dampaknyaa menyebabkan musuh mempercayainya hingga akhirnya bertekuk lutut. Informasi ini bisa berupa penyangkalan terhadap keadaan yang sebenarnya, membingungkan pendukung musuh mengenai informasi yang sebenarnya, sehingga memudahkan mereka untuk menyerang

Cyberstalking

Cyber stalking merupakan tindakan terbaru dari pelaku kejahatan yang terdiri dari ancaman atau perhatian yang tidak diharapkan pada pemakaian Internet serta suatu komunikasi komputer lainnya yang menyinggung korban. Cyber stalking merupakan salah satu tindak kriminal yang tidak jauh berbeda, yang membedakan hanyalah media dan penggunaannya dalam tindakan bisa sangat riskan dan menakutkan khususnya untuk anak-anak dan remaja, karena informasi privasi seseorang tidak diketahui. Internet memberi para pelaku pelecehan kemampuan untuk bergerak bebas dalam melakukan tindakannya. Dalam banyak kasus, kami menemukan bahwa orang yang baru kami temui di jejaring sosial sering kali melakukan pelecehan terhadap korban yang baru mereka temui.

Tabel 1. Penelitian Terdahulu Mengenai Pencurian Data Internet dalam Sudut Pandang Kriminologi

Author/Peneliti	Judul dan Tempat Penelitian	Metode	Kesimpulan
Fiqqih Anugerah dan Tantimin	Pencurian Data Pribadi Di Internet Dalam Perspektif Kriminologi	Metode hukum normatif	Pentingnya membuat evaluasi mengenai perlindungan hukum mengenai masalah pencurian data di internet
Akbar Galih Hariyono dan Frans Simangunsong	Perlindungan Hukum Korban Pencurian Data Pribadi (Phishing Cybercrime) dalam Perspektif Kriminologi	Metode hukum normatif	Ketika menerapkan undang-undang terkait kejahatan siber, hukuman KUHP dan UU ITE masih cukup ringan. Padahal, jika melihat kasus-kasus yang

terjadi, pelaku kejahatan siber menimbulkan kerugian yang sangat besar bagi korbannya, sehingga tidak ada kata yang bisa menandingi akibat yang ditimbulkan oleh pelakunya.

Sebelum UU ITE berlaku, kejadian cybercrime di Indonesia dieksekusi dengan membandingkan ketentuan yang mengandung unsur relevan dalam KUHP, sehingga menghukum pelaku cybercrime. Dalam KUHP, peraturan pidana dalam perkara kejahatan dunia maya berupa penipuan dapat dipakai merujuk Pasal 378 KUHP sebagai berikut: "Barangsiapa bertujuan untuk memperoleh keuntungan secara melawan hukum untuk diri sendiri atau orang lain, dengan menggunakan nama palsu atau perbuatan palsu, dengan menipu atau berbohong secara massal, membujuk orang lain untuk memberikan sesuatu kepada diri sendiri, untuk menyerahkan utang atau menghapuskan utang, diancam dengan pidana penjara paling lama empat tahun karena penipuan. Dilihat dari unsur penipuan dan putusan pengadilan, pengaturan terkait kejahatan siber berupa penipuan diatur dalam Undang-Undang Nomor 11 Tahun 2008 Republik Indonesia tentang Perubahan Atas Undang-Undang Nomor 1 Undang-undang Nomor 19 Tahun 2016 tentang Informasi dan transaksi elektronik pada beberapa barang yang dapat dikenakan pajak, antara lain (Malunsenge, dkk, 2020) :

1. Pasal 28 ayat (1) mengatur "Setiap Orang dengan sengaja dan tanpa hak menyebarkan informasi palsu dan menyesatkan sehingga menimbulkan kerugian bagi konsumen dalam transaksi elektronik". Pasal 45 ayat (2) sebagai ketentuan pidana menyatakan bahwa "Setiap orang yang memenuhi unsur-unsur sebagaimana dimaksud dalam Pasal 28 ayat (1) atau ayat (2) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau atau denda paling banyak satu miliar rupiah
2. " Pasal 35 berbunyi "Setiap orang dengan sengaja dan tanpa hak atau melawan hukum memanipulasi, membuat, mengubah, menghapus, memusnahkan informasi elektronik dan/atau dokumen elektronik dengan tujuan untuk memperlakukan informasi elektronik dan/atau dokumen elektronik tersebut seolah-olah merupakan informasi yang sah." data otentik" Pasal

51 sebagai ketentuan pidana menyatakan bahwa "Setiap orang yang memenuhi syarat-syarat sebagaimana dimaksud dalam Pasal 35 dipidana dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak dua belas miliar rupiah"

KESIMPULAN

Cybercrime sebagai tindak pidana adalah tindakan kejahatan yang diperbuat dengan corak kriminal, menggunakan internet sebagai media untuk melakukan kejahatan. Sebelum UU ITE berlaku, kejadian cybercrime di Indonesia dieksekusi dengan membandingkan ketentuan yang mengandung unsur relevan dalam KUHP, Dilihat dari unsur penipuan dan putusan pengadilan, pengaturan terkait kejahatan siber berupa penipuan diatur dalam Undang-Undang Nomor 11 Tahun 2008 Republik Indonesia tentang Perubahan Atas Undang-Undang Nomor 1 Undang-undang Nomor 19 Tahun 2016 tentang Informasi dan transaksi elektronik pada beberapa barang yang dapat dikenakan pajak

DAFTAR PUSTAKA

Anugerah F, Tantimin T. Pencurian Data Pribadi Di Internet Dalam Perspektif Kriminologi. J Komun Huk. 2022;8(1):419-435.

Chandra SCY, Yulianto FA, Satrya GB. Malware Analysis On Windows Operating System To Detect Trojan. e-Proceeding Eng. 2016;3(2):3590-3595.

Ciptohartono CC, Dermawan MK. Pencegahan Viktimisasi Pencurian Data Pribadi. Deviance J Kriminologi. 2019;3(2):157-169.

Gulo AS, Lasmadi S, Nawawi K. Cyber Crime dalam Bentuk Phising Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik. PAMPAS J Crim Law. 2021;1(2):68-81.

Hariyono AG, Simangunsong F. Perlindungan Hukum Korban Pencurian Data Pribadi (Phislring Cybercrime) dalam Perspektif Kriminologi. Univ 17 Agustus 1945 Surabaya. 2023;27(2):58-66.

Jondong Z. Kebijakan Hukum Pidana bagi Tindak Pidana Cyber Terrorism dalam Rangka Pembentukan Hukum Positif di Indonesia. J Prefer Huk. 2020;1(2):21-27.

Malunsenge LM, Massie CD, Rorie RE. Penegakan Hukum Terhadap Pelaku Dan Korban Tindak Pidana Cyber Crime Berbentuk Phising Di Indonesia. Lex Crim. 2022;11(3):1-10.

Mathilda F. Cyber Crime Dalam Sistem Hukum Indonesia. Sigma-Mu. 2012;4(2):34-45.

Murti H. Cybercrime. J Teknol Inf Din. 2005;1(1):37-40.

Umbara A, Setiawan DA. Analisis Kriminologis Terhadap Peningkatan Kejahatan Siber di Masa Pandemi Covid-19. J Ris Ilmu Huk. 2022;2(2):81-88.