



Pencurian Data Berbentuk Digital Melalui Sistem Elektronik di Indonesia

Seila Ratunguri¹, Yoan B. Runtunuwu², Henry L. Lumenta³

^{1,2,3} Program Studi Ilmu Hukum, Universitas Negeri Manado

E-mail: seilaratunguri12@gmail.com¹, yoanruntunuwu@unima.ac.id²,
henrynochlumenta@unima.ac.id³

Abstract This study aims to analyze the legal regulations and law enforcement regarding digital data theft in Indonesia, as well as to examine the effectiveness of legal protection for personal data owners in the digital age. The research uses a normative legal method or library research, with a normative juridical approach that examines primary, secondary, and tertiary legal materials such as legislation, legal literature, and other supporting documents. The analysis is conducted qualitatively, by describing and interpreting the data logically and systematically. The results of the study show that legal regulations regarding personal data protection in Indonesia are stipulated in Law Number 27 of 2022 concerning Personal Data Protection and Law Number 1 of 2024 concerning the Second Amendment to the ITE Law. However, its implementation still faces various obstacles, such as weak law enforcement, limited law enforcement resources, and low public awareness of the importance of personal data security. In cases of electronic data theft (phishing), even though a legal basis is available, the process of tracking perpetrators and taking legal action is still not optimal due to the cross-border nature of cybercrime. This research discussion emphasizes that the protection of personal data requires regulatory strengthening, increased capacity of law enforcement agencies, and collaboration between the government, digital industry players, and the public to create comprehensive cyber security.

Keywords: personal data protection, digital data theft, cyber law, ITE Law.

Abstrak: Penelitian ini bertujuan untuk menganalisis pengaturan hukum dan penegakan hukum terhadap tindak pidana pencurian data digital di Indonesia, serta menelaah efektivitas perlindungan hukum bagi pemilik data pribadi dalam era digital. Penelitian menggunakan metode hukum normatif atau penelitian kepustakaan (library research), dengan pendekatan yuridis normatif yang menelaah bahan hukum primer, sekunder, dan tersier seperti peraturan perundang-undangan, literatur hukum, serta dokumen pendukung lainnya. Analisis dilakukan secara kualitatif, dengan menguraikan dan menafsirkan data secara logis dan sistematis. Hasil penelitian menunjukkan bahwa pengaturan hukum mengenai perlindungan data pribadi di Indonesia telah diatur dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi dan Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas UU ITE. Namun, implementasinya masih menghadapi berbagai kendala, seperti lemahnya penegakan hukum, keterbatasan sumber daya penegak hukum, serta rendahnya kesadaran masyarakat terhadap pentingnya keamanan data pribadi. Dalam kasus pencurian data elektronik (phishing), meskipun telah tersedia landasan hukum, proses pelacakan pelaku dan penindakan hukum masih belum optimal karena sifat kejahatan siber yang lintas batas. Pembahasan penelitian ini menegaskan bahwa perlindungan terhadap data pribadi membutuhkan penguatan regulasi, peningkatan kapasitas lembaga penegak hukum, serta kolaborasi antara pemerintah, pelaku industri digital, dan masyarakat untuk menciptakan keamanan siber yang komprehensif.

Kata Kunci: perlindungan data pribadi, pencurian data digital, hukum siber, Undang-Undang ITE.

PENDAHULUAN

Hukum pidana memiliki tujuan utama untuk menegakkan keadilan dengan menjatuhkan hukuman yang sesuai kepada individu atau kelompok yang berusaha merusak tatanan sosial dan otoritas negara. Sanksi yang ditegakkan oleh hukum pidana dirancang untuk membatasi kebebasan individu sebagai sarana pencegahan dan pembalasan. Tindakan ini dapat mengambil berbagai bentuk, termasuk denda uang, pemenjaraan, atau, dalam kasus yang paling berat, hukuman mati. Dengan menerapkan hukuman ini, hukum pidana tidak hanya bertujuan untuk menghukum pelanggaran tetapi juga untuk melindungi masyarakat dan menjaga keselamatan publik, dengan demikian memperkuat supremasi hukum dan prinsip-prinsip keadilan dalam masyarakat.

Leden Marpaung menyatakan bahwa tujuan penjatuhan pidana dalam hukum pidana ialah:

Untuk melindungi dan memelihara ketertiban hukum guna mempertahankan keamanan dan ketertiban masyarakat sebagai satu kesatuan (*for the public as a whole*). Hukum pidana tidak hanya melihat penderitaan korban atau penderitaan terpidana (*not only for the person injured*), tetapi melihat ketentraman masyarakat sebagai suatu kesatuan yang utuh.

Penjatuhan pidana oleh hakim harus didasarkan pada faktor kesalahan yang dilakukan seseorang, dan hakim tidak bisa menjatuhkan pidana tanpa adanya aturan pidana yang berlaku sebagaimana yang dirumuskan dalam Pasal 1 ayat (1) KUHP sebagai berikut: “Tiada satu perbuatan yang dapat dipidana dalam perundang-undangan yang telah ada, sebelum perbuatan dilakukan”.

Ketentuan dalam Pasal 1 ayat (1) tersebut diatas *ialah* asas umum dalam hukum pidana yang dikenal dengan asas legalitas atau asas ‘*Nullum Delictum Sine Praevia Lege Poenali*’ yang artinya: “peristiwa pidana tidak akan ada, jika ketentuan pidana dalam undang-undang tidak ada terlebih dahulu”. Dengan adanya ketentuan dalam Pasal 1 ayat (1) KUHP ini, maka dalam menjatuhkan pidana kepada seseorang yang terbukti melakukan tindak pidana hakim terikat oleh undang-undang sehingga terjaminlah hak kemerdekaan diri pribadi seseorang.

Dalam kerangka hukum yang berlandaskan pada asas legalitas, khususnya dalam hukum pidana, terdapat mekanisme untuk mengurangi potensi tindakan sewenang-wenang oleh lembaga penegak hukum. Asas ini memastikan bahwa individu hanya dapat dituntut atas tindakan yang secara eksplisit didefinisikan sebagai kejahatan dalam undang-undang tertulis, sehingga memberikan perlindungan terhadap penegakan hukum yang tidak menentu. Namun, kepatuhan terhadap hukum yang dikodifikasi ini menimbulkan tantangan yang signifikan: undang-undang tertulis sering kali gagal mengimbangi kemajuan pesat dalam ilmu pengetahuan dan teknologi. Akibatnya, perilaku atau tindakan yang dapat dianggap bersifat kriminal mungkin tidak dikenakan sanksi hukum jika belum diakui secara resmi dan dimasukkan ke dalam kode hukum yang ada.

Kesenjangan antara norma masyarakat yang berkembang dan sifat statis hukum tertulis ini dapat menyebabkan situasi di mana individu terlibat dalam perilaku yang, meskipun berpotensi merugikan atau tidak etis, tetap tidak dapat dihukum karena tidak adanya ketentuan hukum yang relevan. Terlepas dari keterbatasan ini, komitmen terhadap asas legalitas memainkan peran penting dalam memastikan kepastian hukum. Prinsip legalitas berfungsi sebagai benteng terhadap potensi penindasan dan tindakan sewenang-wenang oleh penguasa, dengan demikian menegakkan perlindungan hak asasi manusia. Dengan mensyaratkan agar hukum didefinisikan dengan jelas dan dapat diakses publik, asas legalitas mendorong terciptanya lingkungan tempat individu dapat memahami hak dan kewajiban mereka, yang pada akhirnya berkontribusi pada sistem hukum yang lebih adil dan setara.

Pengamanan hak asasi manusia dan penyediaan perlindungan yang memadai bagi hak-hak ini harus menjadi hal yang sangat penting ketika mempertimbangkan praktik penegakan hukum dalam kerangka hukum yang didasarkan pada prinsip-prinsip Pancasila. Filsafat dasar ini menekankan keadilan, kemanusiaan, dan supremasi hukum, yang penting untuk memastikan bahwa semua individu diperlakukan secara adil dan bermartabat. Oleh karena itu, sangat penting bagi seorang hakim untuk menahan diri dari menjatuhkan segala bentuk hukuman kepada terdakwa sampai proses peradilan telah dilakukan dengan tingkat ketelitian dan ketepatan tertinggi. Hanya setelah pengadilan dengan cermat memeriksa semua bukti dan menetapkan tanpa keraguan yang wajar bahwa terdakwa memang telah melakukan tindak pidana yang dituduhkan, hukuman baru dapat dijatuhkan. Pendekatan ini tidak hanya menegakkan integritas sistem hukum tetapi juga memperkuat komitmen terhadap hak asasi manusia yang *ialah* inti dari Pancasila.

Tindakan pencurian *ialah* salah satu pelanggaran paling umum terhadap harta benda dalam masyarakat kita, dan tren terkini menunjukkan peningkatan yang mengkhawatirkan dalam kejadiannya. Peningkatan pencurian ini sebagian besar dapat dikaitkan dengan krisis ekonomi yang sedang berlangsung yang telah berdampak pada negara kita untuk waktu yang lama. Kemerosotan ekonomi telah mengakibatkan peningkatan yang signifikan dalam angka pengangguran, terutama karena kelangkaan kesempatan kerja yang tersedia. Ketika orang-orang berjuang untuk mendapatkan pekerjaan, kombinasi dari berkurangnya pendapatan masyarakat dan meningkatnya harga—terutama untuk komoditas penting—menciptakan lingkungan yang menantang. Dalam keadaan seperti itu, mereka yang memiliki keyakinan moral yang kurang kuat mungkin merasa terpaksa untuk melakukan tindakan kriminal, dengan pencurian menjadi pilihan yang umum di antara mereka.

Dalam catatan kriminal di Indonesia sebagaimana dikemukakan oleh Badan Pusat Statistik, tindak pidana pencurian tanpa kekerasan memiliki porsi yang paling besar di tahun 2023 yaitu sebanyak 140.076 kasus, meningkat sebesar 52% dari tahun sebelumnya 2022 yaitu sebesar 91.631 kasus,...

Integrasi teknologi informasi telah menjadi aspek standar kehidupan modern. Akses terhadap informasi—baik yang bersumber dari internet, komputer, atau platform lain—kini tidak dibatasi.

Individu dapat dengan bebas memperoleh dan menggunakan informasi ini tanpa mempertimbangkan kepemilikannya. Ini mencakup tidak hanya data dari pemilik yang tidak dikenal tetapi juga informasi yang sengaja dirahasiakan oleh pemiliknya. Perilaku seperti itu sering terwujud dalam persaingan bisnis, dengan tujuan untuk melemahkan pesaing. Lanskap digital secara progresif mengubah kejahatan tradisional, seperti ancaman, pencurian, dan penipuan, menjadi aktivitas yang dapat dilakukan melalui komputer dengan kemungkinan deteksi yang lebih rendah. Tindakan ini, yang dilakukan oleh individu atau kelompok, menyebabkan kerugian besar bagi masyarakat dan negara.

Kemajuan teknologi telah membawa kita ke ranah dunia maya, sebuah ranah yang masih sulit dipahami oleh manusia. Dunia maya hanya ada dalam imajinasi manusia dan tidak memiliki kehadiran yang nyata dalam dunia nyata. Hukum positif saat ini belum memberikan bukti yang memadai untuk masalah yang terkait dengan dunia maya, sehingga proses pembuktian kasus-kasus tersebut menjadi sangat sulit. Meskipun Indonesia memiliki kerangka hukum seperti Kitab Undang-Undang Hukum Pidana (KUHP), peraturan-peraturan ini tidak cukup untuk secara efektif memerangi kejahatan dunia maya. Oleh karena itu, pemerintah Indonesia memberlakukan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE), yang bertujuan untuk mengatur penggunaan teknologi informasi secara komprehensif dan terarah, serta mendorong terciptanya masyarakat elektronik yang mematuhi standar moral dan etika dalam semua bidang kehidupan.

Tindak pidana pencurian diatur dalam Pasal 362 Kitab Undang-Undang Hukum Pidana (KUHP). Adapun isi dari pasal tersebut *ialah* :

“Barang siapa mengambil barang sesuatu, yang seluruhnya atau sebagian kepunyaan orang lain, dengan maksud untuk dimiliki secara melawan hukum, diancam karena pencurian, dengan pidana penjara paling lama lima tahun atau pidana denda paling banyak sembilan ratus rupiah”

Menurut Pasal 362 KUHP, pencurian diartikan sebagai perampasan secara melawan hukum atas harta orang lain, baik seluruhnya maupun sebagian, dengan maksud untuk mengklaimnya sebagai miliknya sendiri. Perampasan berarti pengalihan suatu barang yang diakui oleh orang tersebut sebagai milik orang lain. Istilah "harta" mencakup barang apa pun yang memiliki nilai ekonomi. Data yang ditemukan dalam jaringan komputer, seperti Internet, *ialah* salah satu contoh harta yang berharga tersebut. Meskipun tidak berwujud, data dapat mewakili nilai ekonomi yang substansial bagi pemiliknya dan dianggap sebagai harta dalam jaringan komputer. Pelaku yang melakukan pencurian yang melibatkan barang fisik dapat dituntut berdasarkan Pasal 362 KUHP, karena penegak hukum dapat dengan mudah mengumpulkan bukti nyata. Sebaliknya, menetapkan pencurian dalam konteks digital jauh lebih sulit karena tantangan dalam mengumpulkan bukti, yang memungkinkan pelaku untuk melanjutkan aktivitas mereka tanpa menghadapi akibat hukum. Selain itu, korban pencurian data daring sering kali tidak menyadari kejahatan tersebut hingga data mereka dipublikasikan di internet atau dieksploitasi oleh pesaing.

Banyak sekali kejadian pencurian yang terjadi, terutama yang melibatkan barang-barang yang memiliki faktor-faktor yang memberatkan. Termasuk pencurian dokumen berharga atau surat-surat perusahaan, yang dapat berdampak signifikan terhadap masyarakat. Perkembangan teknologi telah menyebabkan meningkatnya kejahatan yang terkait dengan pencurian informasi pribadi yang tersedia secara daring. Selain itu, telah terjadi banyak pelanggaran yang melibatkan akses tidak sah ke jaringan internal. Data yang diakses dan dikumpulkan sangat penting bagi perusahaan dan individu, terutama jika data tersebut terekspos atau dijual di pasar gelap. Selain itu, ketentuan-ketentuan Kitab Undang-Undang Hukum Pidana yang sudah ketinggalan zaman dapat mengakibatkan kejahatan berat dikategorikan sebagai pelanggaran biasa karena kurangnya definisi yang jelas. Kesalahan klasifikasi ini dapat mengakibatkan kerugian yang cukup besar bagi korban dan masyarakat secara keseluruhan.

METODE PENELITIAN

Jenis penelitian yang digunakan dalam penelitian ini *ialah* penelitian hukum normatif atau penelitian hukum kepustakaan (*library research*). Penelitian ini mengkaji hukum sebagai norma atau kaidah yang berlaku, terutama yang bersumber dari norma hukum positif tertulis seperti Undang-Undang Dasar, kodifikasi, undang-undang, dan peraturan pemerintah. Penelitian hukum normatif juga dikenal sebagai *doctrinal research* atau studi dogmatik yang bersifat teoritis-rasional dan menggunakan metode logika deduktif untuk memperoleh ketepatan dan kejelasan analisis hukum. Dalam penelitian ini, bahan hukum yang digunakan terdiri dari bahan hukum primer (seperti UUD 1945, KUHP, dan peraturan terkait teknologi informasi), bahan hukum sekunder (hasil karya ilmiah dan penjelasan

undang-undang), serta bahan hukum tersier (bahan penunjang seperti kamus hukum dan referensi tambahan).

Pengumpulan data dilakukan melalui studi kepustakaan dan studi dokumen, dengan menelaah berbagai sumber hukum yang relevan, baik dalam bentuk media cetak maupun media elektronik. Data yang digunakan mencakup kaidah-kaidah hukum primer seperti KUHP, bahan hukum sekunder berupa pendapat para ahli dan karya tulis ilmiah, serta bahan hukum tersier yang berfungsi sebagai pendukung. Semua sumber data dipilih secara selektif untuk mendukung pembahasan mengenai permasalahan hukum yang dikaji.

Data yang diperoleh kemudian diolah secara kualitatif dengan metode yuridis normatif, yaitu menganalisis hukum tertulis dari berbagai aspek, seperti teori, sejarah, filosofi, dan struktur peraturan perundang-undangan. Analisis dilakukan dengan cara menguraikan, mengelompokkan, dan menafsirkan data secara logis dan sistematis. Karena penelitian ini berbasis studi kepustakaan, hasilnya disajikan dalam bentuk uraian deskriptif yang menjelaskan pola, hubungan, dan makna dari data hukum yang dikaji. Pendekatan analisis dilakukan melalui tiga tingkatan, yaitu legal exploration, legal review, dan legal analysis, untuk memperoleh pemahaman menyeluruh mengenai permasalahan hukum yang dibahas.

HASIL PENELITIAN DAN PEMBAHASAN

A. Pengaturan Tentang Data Yang Berbentuk Digital Di Indonesia Serta Perlindungannya

Pada era saat ini, data ialah perihal yang berarti serta memastikan kemajuan ekonomi sesuatu negeri bagus negeri bertumbuh ataupun negeri maju. Data hal orang senantiasa diatur oleh penguasa serta swasta, namun timbulnya masa pc menghasilkan bahaya yang lebih besar untuk pribadi orang itu, dan mungkin orang mengidap kehilangan selaku dampak dari ketidaktelitian ataupun pembocoran data jauh lebih besar. Masa digital sudah mengakibatkan dentuman perkembangan informasi individu yang terbuat, ditaruh serta dikirimkan pada pc serta fitur mobile, broadband serta web internet serta media

Perkembangan teknologi pula memunculkan bahaya sungguh- sungguh untuk pribadi individu serta keamanan data. Rancangan hukum telematika, mengemukakan kalau informasi ialah representasi resmi sesuatu rancangan, kenyataan, ataupun instruksi. Pada pemakaian tiap hari informasi berarti sesuatu statment yang diperoleh dengan cara apa terdapatnya. Pada Informasi Protection Act Artikel 1 bagian 1, informasi yakni tiap data yang diproses lewat perlengkapan yang berperan dengan cara otomatis menjawab perintah- perintah yang diserahkan untuk tujuannya serta ditaruh dengan arti buat bisa diproses. Informasi pula tercantum data yang ialah bagian khusus dari catatan- catatan kesehatan, kegiatan sosial, pembelajaran, ataupun yang ditaruh selaku bagian dari sesuatu sistem yang relevan.

Bagi Purwanto informasi ialah materi dasar data, yang didefinisikan selaku golongan tertib simbol- simbol yang menggantikan jumlah, aksi, barang, serta serupanya. Informasi tercipta dari kepribadian yang bisa berbentuk alphabet, nilai, ataupun ikon spesial. Informasi disusun buat diolah dalam wujud bentuk informasi, bentuk file, serta informasi base. Informasi serta pula data ialah pangkal energi yang amat berarti untuk jalannya sesuatu badan. Pada era saat ini ini badan yang sanggup memakai informasi serta data dengan cara kilat, betul, pas serta komplit yang sanggup bersaing dengan rivalnya. Pengumpulan ketetapan selaku bagian dari aktivitas orang tidak bebas dari terdapatnya informasi serta data ini. Pengumpulan ketetapan tidak terjalin apabila mana tidak terdapat informasi serta data.

Pada tahun 1970 Swedia serta Jerman sudah menghasilkan UndangUndang hal proteksi informasi. Hukum ini dikeluarkan disebabkan banyaknya sudah di temui pemakaian pc dalam pemrosesan serta penyimpanan informasi, alhasil di perlukannya UndangUndang buat mencegah informasi itu. Tiap Negeri memakai sebutan yang berlainan antara data individu serta informasi individu, namun dengan cara substansif kedua sebutan itu memiliki penafsiran yang nyaris serupa alhasil kedua sebutan itu kerap kali dipakai bergantian. Informasi individu terdiri dari fakta- fakta, opini ataupun komunikasi yang berhubungan dengan orang yang ialah data amat individu ataupun sensitif alhasil orang yang berhubungan

mau menaruh ataupun membatasi orang lain buat mengoleksi, memakai, ataupun menyebarkan pada pihak orang lain. Bagi Jerry Kang, informasi individu melukiskan sesuatu data yang akrab kaitannya dengan seorang yang melainkan karakter tiap- tiap orang. Pada dasarnya proteksi informasi di atas 2(2) tipe ialah wujud proteksi informasi yang berbentuk proteksi raga informasi, bagus informasi yang nampak ataupun tidak nampak. Wujud proteksi informasi yang selanjutnya ialah bagian regulasi yang menata hal pemakaian informasi oleh orang lain yang tidak berkuasa, penyalahgunaan informasi buat kebutuhan khusus, serta peluhlantahkan kepada informasi itu sendiri.

Pada Hukum No 27 Tahun 2022 mengenai Proteksi Informasi Individu, pada Artikel 1 dituturkan kalau Informasi Individu ialah informasi tentang orang perseorangan yang teridentifikasi ataupun bisa diidentifikasi dengan cara tertentu ataupun dikombinasi dengan data yang lain bagus dengan cara langsung ataupun tidak langsung lewat sistem elektronik ataupun nonelektronik. Sedang pada Artikel itu dituturkan di biji 3 kalau Data ialah penjelasan, statment, buah pikiran, serta isyarat yang memiliki angka, arti, serta catatan, bagus informasi, kenyataan, ataupun uraiannya yang bisa diamati, didengar, serta dibaca yang dihidangkan dalam bermacam bungkus serta bentuk cocok dengan kemajuan teknologi data serta komunikasi dengan cara elektronik atau nonelektronik.

Dari 2 biji di atas, terlihat nyata kalau hal data serta informasi individu telah diserahkan batas dalam UU PDP ini, walaupun cakupannya lumayan besar. Tetapi pula butuh dicermati kalau data ataupun informasi individu ini tidak terbatas pada alat elektronik tetapi pula non elektronik, dimana data ataupun informasi individu yang dipunyai tidak wajib dalam wujud elektronik. Pada bermacam Negeri maju, dipakai sebutan *privacy* atau pribadi selaku hak yang wajib dilindungi, ialah hak seorang buat tidak di goda kehidupan pribadinya. Rancangan pribadi buat awal kalinya dibesarkan oleh Warren serta Brandeis yang menulis suatu postingan dalam harian objektif sekolah hukum Universitas Harvard yang bertajuk “The Right to Privacy” ataupun hak buat tidak diusik. Dalam harian itu bagi Warren serta Brandeis dengan terdapatnya kemajuan serta perkembangan teknologi hingga mencuat sesuatu pemahaman warga kalau terdapat hak seorang buat menikmati hidup. Hak buat menikmati hidup itu dimaksud selaku hak buat seorang tidak diusik kehidupan pribadinya bagus oleh orang lain ataupun oleh Negeri, oleh sebab itu hukum wajib membenarkan serta mencegah hak pribadi itu.

Alibi pribadi wajib dilindungi ialah): Awal, dalam membina ikatan dengan orang lain, seseorang wajib menutup beberapa kehidupan pribadinya alhasil ia bisa menjaga letaknya pada tingkatan khusus. Kedua, seorang di dalam kehidupannya membutuhkan durasi buat bisa berasing(*solitude*) alhasil pribadi amat diperlukan oleh seorang. Ketiga, pribadi ialah hak yang berdiri sendiri serta tidak tergantung pada perihal lain namun hak ini lenyap bila orang itu mempublikasikan keadaan yang bertabiat individu pada biasa. Keempat, pribadi pula tercantum hak seorang buat melaksanakan ikatan dalam negeri tercantum gimana seorang membina pernikahan, membina keluarganya serta orang lain tidak bisa mengenali ikatan individu itu alhasil setelah itu Warren menyebutnya selaku *the right against the word*. Kelima, alibi lain kenapa pribadi pantas menemukan proteksi hukum sebab kehilangan yang diderita susah buat ditaksir dimana kerugiannya dialami jauh lebih besar dibanding dengan kehilangan raga, sebab sudah mengusik kehidupan pribadinya alhasil apabila terdapat kehilangan yang dialami hingga pihak korban harus menemukan ganti rugi.

Pribadi ialah sesuatu rancangan yang amat susah didefinisikan sebab tiap orang berikan batas yang berlainan terkait dari bagian mana orang menilainya. Bersamaan dengan pesatnya kemajuan di aspek teknologi serta data, informasi jadi sesuatu komoditi yang eksklusif. Proteksi informasi dikala ini jadi kejadian yang menarik sebab itu tindakan- tindakan melindungi atas perampokan, pembobolan serta kehancuran informasi serta data butuh buat memperoleh pandangan hal perlindungannya. Keamanan serta kerahasiaan informasi pada jaringan pc dikala ini jadi rumor yang amat berarti serta lalu bertumbuh.

Dalam UU PDP dituturkan kalau Proteksi Informasi Individu ialah totalitas usaha buat mencegah Informasi Individu dalam susunan pemrosesan Informasi Individu untuk menjamin hak konstitusional poin Informasi Individu. Sebagian permasalahan menyangkut sistem keamanan dikala ini jadi sesuatu garapan yang menginginkan bayaran penindakan serta

penjagaan yang sedemikian besar. Sistem- sistem vital semacam sistem pertahanan, sistem perbankan, sistem e- commerce serta sistem- sistem ekuivalen itu menginginkan tingkatan keamanan yang sedemikian besar. Perihal ini lebih diakibatkan oleh perkembangan aspek jaringan pc dengan rancangan open system- nya alhasil siapapun, dimanapun, serta kapanpun mempunyai peluang buat mengakses kawasan- kawasan vital itu.

Tidak hanya keamanan serta kerahasiaan informasi dalam jaringan pc, rancangan ini pula legal buat keamanan serta kerahasiaan informasi pada internet. Perihal ini mengengang kalau perkembangan yang digapai dalam aspek pengembangan sistem pembedahan pc sendiri serta utilitasnya telah sedemikian jauh dimana tingkatan performasi, kehandalan, serta elastisitas aplikasi jadi patokan penting serta berharganya data itu serta ditopang oleh keahlian pengembangan aplikasi pastinya menarik atensi para pembobol(hacker) serta penyelinap(intruder).

Permasalahan keamanan serta kerahasiaan informasi ialah salah satu pandangan sangat berarti dari sesuatu sistem data. Perihal ini terpaut dengan sedemikian itu berartinya data itu dikirim serta diperoleh oleh orang yang bersangkutan. Data tidak bermanfaat lagi bila di tengah jalur data itu disadap ataupun dibajak oleh orang tidak berkuasa. Oleh sebab itu, penjagaan dalam sistem data sudah jadi rumor hangat kala bisnis elektronik mulai dipublikasikan. Tanpa penjagaan yang kencang serta mutahir, kemajuan teknologi data tidak membagikan khasiat yang maksimum pada warga.

Terhubungnya suatu sistem data dengan Internet membuka kesempatan terdapatnya kesalahan lewat jaringan pc. Perihal ini memunculkan tantangan untuk penegak hukum. Hukum dari beberapa besar negeri di bumi belum menjangkau wilayah cyberspace. Dikala ini nyaris seluruh negeri di bumi bersaing buat mempersiapkan alas hukum untuk internet. Terpaut dengan permasalahan yang terjalin serta perlunya penjagaan kepada informasi yang terdapat dalam pc, lingkup keamanan informasi dari sesuatu sistem pc melingkupi keadaan yang tidak saja berhubungan dengan keamanan raga, keamanan akses, keamanan file serta informasi, keamanan jaringan, namun ada keadaan yang lain Bahaya sangat signifikan kepada keamanan dari sistem pc pada dikala ini bukan berbentuk bahaya kepada keamanan raga, namun pula bahaya kepada keamanan non- fisik yang bisa dipecah dalam 2(2) jenis ialah: Intruders serta Malicious Program.

Proteksi informasi dalam sistem keamanan pc diketahui selaku metodologi keamanan pc. Keamanan pc mempunyai banyak agen. Dalam perihal keamanan, estimasi buat mengamankan sistem wajib dicermati, semacam keamanan database, keamanan informasi, keamanan pc, keamanan pc, keamanan aplikasi, keamanan jaringan serta keamanan data. Metodologi keamanan pc ialah suatu yang amat berarti dalam permasalahan keamanan pc sebab seluruh bagian silih terpaut.

B. Penegakan Hukum terhadap Pencurian Data Elektronik di Indonesia

Undang- Undang No 1 Tahun 2024 ialah pergantian kedua atas Hukum No 11 Tahun 2008 mengenai Data serta Bisnis Elektronik(ITE). Pergantian ini bermaksud buat menguatkan regulasi terpaut kesalahan siber, tercantum perampokan informasi Elektronik lewat phishing. Hukum Nomor. 1 Tahun 2024 mengenai Pergantian Kedua atas Hukum Nomor. 11 Tahun 2008 Mengenai Informasi serta Bisnis Elektronik Artikel 28 bagian 1“ Tiap Orang dengan terencana serta atau ataupun mentransmisikan Data Elektronik serta atau ataupun Akta Elektronik yang bermuatan pemberitahuan dusta ataupun data menyesatkan yang menyebabkan kehilangan materiel untuk pelanggan dalam Transaksi Elektronik”.

Artikel 45 bagian 1 “Tiap Orang yang dengan terencana serta tanpa hak megedarkan serta atau ataupun mentransmisikan serta atau ataupun membuat bisa diaksesnya Data Elektronik serta atau ataupun Akta Elektronik yang mempunyai bagasi yang melanggar kesusilaan begitu juga diartikan dalam Artikel 27 bagian (1) dipidana dengan kejahatan bui sangat lama 6(6) tahun serta atau ataupun kompensasi sangat banyak Rp 1. 000. 000. 000, 00(satu miliar rupiah)”. Dalam Hukum Nomor. 27 Tahun 2022 mengenai Proteksi Informasi Individu membagikan proteksi lebih khusus kepada informasi

individu serta memutuskan ganjaran untuk pelakon kesalahan siber, tercantum phishing. Dalam Artikel 67 bagian(1) serta(3).

Phising berawal dari tutur fishing yang berarti memancing, yang ialah salah satu usaha buat memperoleh data informasi seorang dalam wujud menjiplak selaku suatu entitas yang bisa diyakini atau legitimate organization serta umumnya berbicara dengan cara elektronik. Informasi yang jadi target umumnya berbentuk informasi diri semacam julukan, umur, tujuan, setelah itu informasi akun semacam username serta password, serta informasi keuangan yang berhubungan dengan data kartu angsuran ataupun no rekening. Aktivitas phishing bermaksud buat membodohi korban supaya tanpa siuman membagikan data individu mereka, yang setelah itu hendak dipakai buat tujuan kesalahan. Umumnya, modus operandi kesalahan ini diawali dengan berbohong jadi lembaga sah lewat pemakaian web ataupun email yang ilegal buat membodohi korban.

Indonesia sendiri sempat hadapi permasalahan mengenai phishing yang sangat populer *ialah* permasalahan dari Internet banking kepunyaan bank BCA terjalin pada tahun 2001, dikala itu ada seorang bernama samaran Steven Haryanto yang membeli sebagian daerah yang mendekati dengan daerah kepunyaan bca ialah klikbca. com, Steven Haryanto sendiri melaksanakan aksinya dengan membuat daerah seragam dengan mengganti pelafalan dari web asli semacam clickbca. com, klikbca. com, klikbac. com. Steven Haryanto pula merancang web itu sedemikian muka alhasil mendekati dengan web asli kepunyaan bca alhasil banyak orang yang tertipu³³. Tetapi Steven Haryanto melaksanakan perihal itu bukan buat mencuri informasi dari pelanggan, melainkan Steven Haryanto bermaksud buat mencoba tingkatan keamanan dari web kepunyaan bank BCA itu, hendak namun aksi Steven Haryanto yang mengusik suatu sistem kepunyaan orang lain yang dilindungi privasinya serta manipulasi web internet banking kepunyaan BCA alhasil masalah ini dikategorikan selaku masalah awas.

Indonesia sudah mengesahkan UndangUndang No 27 Tahun 2022 mengenai Proteksi Informasi Individu (UU PDP), yang bermaksud buat menata proteksi informasi individu dengan cara global. UU ini melingkupi data yang bisa mengenali orang bagus dengan cara langsung ataupun tidak langsung, bagus lewat sistem elektronik ataupun non- elektronik. Tujuan penting dari UU PDP *ialah* sediakan kerangka hukum yang mencukupi buat mencegah warga serta penguasa dari kesalahan digital, tercantum perampokan informasi individu Departemen Komunikasi serta Informatika melaporkan kalau UU PDP hendak men catat tahap berarti dalam pengurusan informasi individu di Indonesia. Undang-undang ini terdiri dari 18 ayat serta 78 artikel, yang menata bermacam pandangan semacam memindahkan informasi individu, ganjaran administratif, kelembagaan, kerjasama global, kesertaan warga, penanganan bentrokan serta hukum kegiatan, pantangan dalam pemakaian informasi individu, dan determinasi kejahatan serta pancaroba. Hukum PDP membagikan kerangka hukum yang lebih menyeluruh buat proteksi informasi individu, sedang ada gap dalam penguatan hukum kepada kesalahan siber, khususnya dalam perihal adaptasi dengan praktikpraktik kesalahan terkini semacam phishing yang lalu bertumbuh. Terdapat keinginan menekan buat lalu menginovasi serta melengkapi regulasi serta aplikasi hukum untuk mengalami tantangan terkini di ranah kesalahan siber.

Cyber Crime ialah salah satu wujud ataupun format terkini dari kesalahan era saat ini yang menemukan atensi besar dari bumi international. Volodymyr Golubev menyebutnya selaku the new form of anti- social behavior. Sebagian gelar lain yang lumayan populer diserahkan pada tipe kesalahan terkini ini di dalam bermacam catatan, antara lain selaku kesalahan bumi maya(cyber ruang atau virtual ruang offence), format terkini dari high tech crime, format terkini dari transnational crime, serta format terkini dari white collar crime(WCC). Dalam 2 akta Kongres PBB yang diambil oleh Barda Nawawi Arief, hal The Prevention of Crime and the Pengobatan of Offenders di Havana Cuba pada tahun 1990 serta di Wina Austria pada tahun 2000, menarangkan terdapatnya 2 sebutan yang terpaut dengan penafsiran cyber crime, ialah *Cyber Crime* serta computer related crime. Dalam back ground paper buat sanggar kerja Kongres PBB X atau 2000 di Wina Austria, sebutan *Cyber Crime* dipecah dalam 2 jenis. Awal, *Cyber Crime* dalam maksud kecil(in a narrow sense) diucap computer crime. Kedua, *Cyber Crime* dalam maksud besar(in a broader sense) diucap computer related crime.

Dalam UU Nomor. 19 Tahun 2016 diklaim, Artikel 31(1) Tiap Orang dengan terencana serta tanpa hak ataupun melawan hukum melaksanakan intersepsi ataupun penyadapan atas Data Elektronik serta atau ataupun Akta Elektronik dalam sesuatu Pc serta atau ataupun Sistem Elektronik khusus kepunyaan Orang lain.(2) Tiap Orang dengan terencana serta tanpa hak ataupun melawan hukum melaksanakan

intersepsi atas transmisi Data Elektronik serta atau ataupun Akta Elektronik yang tidak bertabat khalayak dari, ke, serta di dalam sesuatu Pc serta atau ataupun Sistem Elektronik khusus kepunyaan Orang lain, bagus yang tidak menimbulkan pergantian apa juga ataupun yang menimbulkan terdapatnya pergantian, penghilangan, serta atau ataupun penghentian Data Elektronik serta atau ataupun Akta Elektronik yang lagi dikirimkan.(3) Determinasi begitu juga diartikan pada bagian(1) serta bagian(2) tidak legal kepada intersepsi ataupun penyadapan yang dicoba dalam bagan penguatan hukum atas permohonan kepolisian, kejaksaan, ataupun institusi yang lain yang kewenangannya diresmikan bersumber pada undangundang.(4) Determinasi lebih lanjut hal aturan metode intersepsi begitu juga diartikan pada bagian(3) diatur dengan Undang- Undang. Terdapatnya pergantian, penghilangan, serta atau ataupun penghentian Data Elektronik serta atau ataupun Akta Elektronik yang lagi dikirimkan.(3) Determinasi begitu juga diartikan pada bagian(1) serta bagian(2) tidak legal kepada intersepsi ataupun penyadapan yang dicoba dalam bagan penguatan hukum atas permohonan kepolisian, kejaksaan, ataupun institusi yang lain yang kewenangannya diresmikan bersumber pada undangundang.(4) Determinasi lebih lanjut hal aturan metode intersepsi begitu juga diartikan pada bagian(3) diatur dengan Undang- Undang. Meski Hukum No 11 Tahun 2008 yang setelah itu dirubah dengan UU Nomor. 19 mengenai Pergantian atas UU Nomor. 11 Tahun 2008, tetapi belum lumayan melingkupi seluruh pandangan dari kesalahan bumi maya. Tidak hanya itu, kita tidak dapat lalu merujuk pada Hukum Data serta Bisnis Elektronik saja, mealainkan kita wajib menata rancangan Buku Hukum Hukum Kejahatan yang terkini. Sebab KUHP lama telah tidak bisa lagi menjangkau tindak- tindak kejahatan terkini yang terwujud oleh kemajuan zaman, buat itu diperlukan konsep- rancangan terkini mengenai KUHP kita. Pengaturan buat menanggulangi kesalahan pc hendaknya diintegrasikan ke dalam KUHP serta bukan ke dalam hukum tertentu. Terdapat beberapa hukum positif lain yang berlaku umum dan dapat dikenakan bagi para pelaku *Cyber Crime* terutama untuk kasuskasus yang menggunakan komputer sebagai sarana, antara lain:

- a. KUHP.
- b. Undang-Undang No. 1 Tahun 2024 tentang Perubahan Kedua atas Undang -Undang No.11 Tahun 2008 Tentang Infomasi dan Transaksi Elektronik
- c. Undang-Undang Nomor 11 tahun 2008 tentang ITE.
- d. Undang-Undang Nomor 44 tahun 2008 tentang Pornografi.
- e. Undang-Undang Nomor 36 tahun 1999 tentang Telekomunikasi.
- f. Undang-Undang Nomor 5 tahun 1999 tentang Larangan Praktek Monopoli dan Persaingan Usaha Tidak Sehat.
- g. Undang-Undang Nomor 8 tahun 1999 tentang Perlindungan Konsumen.
- h. Undang-Undang Nomor 19 tahun 2002 tentang Hak Cipta.
- i. Undang-Undang Nomor 8 Tahun 1997 tentang Dokumen Perusahaan.
- j. Undang-Undang Nomor 25 Tahun 2003 tentang Perubahan atas UndangUndang. Nomor 15 Tahun 2002 tentang Tindak Pidana Pencucian Uang.
- k. Undang-Undang Nomor 15 Tahun 2003 tentang Pemberantasan Terorisme.

Walaupun Indonesia mendiami tingkatan awal dalam Cyber Crime pada tahun 2004, hendak namun jumlah permasalahan yang diputuskan oleh majelis hukum bukanlah banyak. Dalam perihal ini nilai dark number lumayan besar serta informasi yang dikumpulkan oleh Polri pula bukan informasi yang berawal dari analitis Polri, beberapa besar informasi itu

PENUTUP

A. KESIMPULAN

1. Perlindungan terhadap data pribadi sudah cukup diatur dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, namun meskipun ada pengaturan tersebut, perlindungan terhadap data pribadi sendiri belum maksimal karena sangat umum. Hanya lebih ke pemalsuan data dan pengumpulan data secara tidak sah. Masih banyak kejahatan yang berhubungan dengan data pribadi baik elektronik maupun nonelektronik yang belum diatur, tapi hanya diatur dalam UU ITE.
2. Penegakan hukum pidana dalam memberantas kejahatan pencurian data elektronik (phishing) menjadi hal yang sangat penting untuk melindungi hak masyarakat dalam era digital. Phishing,

sebagai salah satu bentuk kejahatan siber, dilakukan dengan cara mengelabui korban untuk memberikan data pribadi, yang kemudian digunakan oleh pelaku untuk tujuan ilegal, seperti penipuan finansial atau penyalahgunaan identitas. Penegakan hukum melibatkan berbagai pihak, termasuk kepolisian, Kementerian Kominfo, dan otoritas terkait lainnya, yang bekerja sama untuk mengidentifikasi, menangkap, dan memberikan sanksi kepada pelaku phishing. Namun, keberhasilan pemberantasan kejahatan phishing juga memerlukan edukasi kepada masyarakat tentang pentingnya menjaga kerahasiaan data pribadi dan mengenali modus-modus phishing. Penegakan hukum terhadap pelaku phishing masih menghadapi kendala dalam hal pelacakan pelaku, koordinasi antar lembaga penegak hukum, serta kurangnya kesadaran masyarakat mengenai metode dan bahaya phishing. Selain itu, perbedaan regulasi hukum siber antar negara juga menyulitkan ekstradisi dan penindakan terhadap pelaku yang beroperasi di luar yurisdiksi nasional.

B. SARAN

- a. Perlu adanya pengaturan yang lebih mendalam tentang perlindungan data pribadi dalam hal ini mengenai kebocoran data, maupun penggunaan kelemahan infrastruktur teknologi informasi perusahaan.
- b. Perusahaan yang menjadi pengendali data pribadi perlu diatur dalam hal kebocoran data maupun pencurian data apabila hal tersebut terjadi karena kelalaian dan ketidakmampuan pengendali data pribadi untuk melindungi data yang dipercayakan oleh masyarakat/konsumen terhadap perusahaan tersebut.

DAFTAR PUSTAKA

- Badan Pusat Statistik, *Statistik Kriminal 2023*, Badan Pusat Statistik, Jakarta, 2024
- Effendi Maruf, “*Fenomena Kejahatan Dunia Maya (Cyber Crime) dan Aplikasi Hukumannya Menuju Ketertiban Masyarakat Online*”. Tersedia di <http://teknologi.kompasiana.com/internet>, diakses pada Hari Rabu, Tanggal 27 Agustus 2018.
- Hadikusuma, Hilman, *Metode Pembuatan Kertas Kerja atau Skripsi Hukum*. Cet 1 ,Bandung : Mandar Maju 1995.
- Hamzah, Andi, *Azas-Azas Hukum Pidana*, Rineka Cipta, Jakarta, 1994.
- Kartanegara, Satochid, *Hukum Pidana I Kumpulan Kuliah*, Balai Lektur Mahasiswa, Jakarta, Tanpa Tahun, hal. 74.
- Marpaung,Laden, *Asas-Teori-Praktek Hukum Pidana*, Sinar Grafika, Jakarta, 2005
- Moeljatno, (*KUHP*) *Kitab Undang-Undang Hukum Pidana*, Bumi Aksara, Jakarta, 1996
- Muhammad, Abdulkadir, *Hukum dan Penelitian Hukum*, cet 1. Bandung : Citra Aditya Bakti, 2004.
- P.A.F. Lamintang, *Dasar-Dasar Hukum Pidana Indonesia*, Penerbit Sinar Baru, Bandung, .
- Poernomo, Bambang, *Asas-Asas Hukum Pidana*, Ghalia Indonesia, Jakarta-Surabaya-Semarang-Yogya-Bandung, 1978
- Prakoso, Djoko,, *Tindak Pidana Penerbangan di Indonesia*, Ghalia Indonesia, Jakarta, 1983.
- Prodjodikoro,Wiryono, *Asas-Asas Hukum Pidana Di Indonesia*, PT. Eresco, Jakarta-Bandung, 1981,
- R. Soesilo, *Kitab Undang-Undang Hukum Pidana (KUHP) Serta Komenta-Komentarnya Lengkap Pasal Demi Pasal*, Politeia, Bogor, 1988
- R. Tresna., *Azas-Azas Hukum Pidana*, PT. Tiara Jakarta, 1959, .
- Rahardjo, Agus, *Cybercrime: Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*. PT. Citra Aditya Bakit, Bandung, 2002.
- Rahardjo, Satjipto,*Hukum Progresif: Sebuah Sintesa Hukum* Indonesia (Yogyakarta: Genta Publishing, 2009)
- Salman,Otje, dan Anton F. Susanto, *Teori Hukum: Mengingat, Mengumpulkan dan Membuka Kembali*, PT Refika Aditama, Bandung, 2004
- Soekanto dan Mamuji, *Penelitian Hukum Normatif Suatu Tinjauan Singkat*, cet 4 ,Jakarta: Raja Grafindo Persada, 1995.