TINDAK PIDANA PENCURIAN DATA PRIBADI DI INTERNET

Difla Nur Maulida,[1] Arfan Kaimuddin,[2] M. Fahrudin Andriyansyah[3]
Fakultas Hukum Universitas Islam Malang
Jalan Mayjen Haryono No 193 Malang 65144, Telepon (0341) 551932, Fax (0341) 552249
E-mail: diflanurm@gmail.com

ABSTRACT

The number of cases of the mode of theft of personal data through the internet is not a cyber crime caused by weaknesses in the security system on the internet and theft is carried out by individuals illegally. From this, the problem is how the crime mode of theft of personal data through the internet and legal protection for victims. With these problems, the research method used is normative juridical research. By using this method, it is found that perpetrators will look for data that can be accessed without permission, usually through social media. In addition, perpetrators also look for weaknesses in the system to be accessed so that they are right on target. For victims, there is legal protection regulated by the Indonesian state, namely preventive protection, namely protection to prevent more harm from occurring from the beginning. In addition, there is repressive protection aimed at perpetrators and regulated in law number 27 of 2022 concerning personal data protection.
Keywords: *Personal data, Internet, Criminal Acts*

ABSTRAK

Banyaknya kasus dari modus pencurian data pribadi melalui internet merupakan tidak kejahatan dunia maya yang disebabkan oleh adanya kelemahan pada sistem keamanan yang ada di internet dan pencuriannya dilakukan oleh individu secara ilegal. Dari hal tersebut maka didapatkan permasalahan yakni bagaimana modus tindak kejahatan pencurian data pribadi melalui internet dan perlindungan hukum bagi korban. Dengan adanya permasalahan tersebut, adapun metode penelitian yang digunakan yakni penelitian yang bersifat yuridis normatif. Dengan menggunakan metode tersebut didapatkan hasil bahwa pelaku akan mencari data yang dapat diakses tanpa izin, biasanya melalui media sosial. Selain itu, pelaku juga mencari kelemahan sistem yang akan diakses sehingga tepat sasaran. Bagi korban terdapat perlindungan hukum yang diatur oleh negara indonesia yakni perlindungan preventif yakni perlindungan untuk mencegah terjadinya bahaya lebih sejak awal. Selain itu, terdapat perlindungan represif yang ditujukan kepada pelaku dan diatur dalam undang-undang nomor 27 tahun 2022 mengenai perlindungan data pribadi.
Kata kunci: Data pribadi, Internet, Tindak Pidana

[1] Mahasiswa Fakultas Hukum Universitas Islam Malang
[2] Dosen Pembimbing 1 Fakultas Hukum Universitas Islam Malang
[3] Dosen Pembimbing 2 Fakultas Hukum Universitas Islam Malang

PENDAHULUAN

Teknologi informasi mengalami perkembangan dan kemajuan yang sangat pesat. Sehingga, memudahkan masyarakat Indonesia untuk mendapatkan informasi yang diinginkan. Hal ini menciptakan warga mengakibatkan teknologi liputan menjadi kebutuhan sehari-hari untuk akses informasi yang lebih cepat.[4] Ilmu Pengetahuan dan Teknologi Hal ini menunjukkan perkembangan yang semakin tak terbendung dalam satu decade terakhir. Diantaranya adalah internet yang dapat medobrak batasan antarnegara dan mampu menyebarkan pengetahuan atau ilmu diantara para ilmuwan serta peneliti dengan cepat.

Hanya saja internet memiliki sisi gelap keamanannya di balik kesederhanaan penggunaannya. Karena sifat publik dari jaringan internet dan perubahan signifikan yang ditimbulkan oleh perkembangannya dalam berbagai bentuk kejahatan dunia maya.

Tindakan kejahatan kini banyak terjadi tidak terbatas tempat baik diruang nyata ataupun virtual. Dewasa ini, kejahatan di dunia maya *(cybercrime)* semakin meningkat dan semakin kompleks modusnya, semakin beragam karateristik pelakunya dan semakin serius akibatnya.[5] *Cybercrime* dibagi berdasarkan dua kategori, antara lain: *cybercrime* yang menargetkan komputer dan *cybercrime* yang kejahatannya menggunakan alat yaitu Dengan bertambahnya pengguna jejaring sosial di Indonesia, tak dipungkiri banyak informasi pribadi pengguna yang bocor. Menurut Polri, terdapat 1.409 perkara terkait penipuan yang terjadi setiap tahun yang diakibatkan bocornya informasi para pengguna *social media* yang bersifat pribadi. Data pribadi adalah hal yang biasa bagi semua orang. Data yang bersifat pribadi sangat sensitif. Data pribadi harus mendapat perlindungan karena hal tersebut merupakan hak atas privasi tiap orang. Hak atas privasi merupakan kewarganegaraan konstitusional yang diabadikan dalam UUD RI 1945. Hak dasar ialah sesuatu yang harus dilakukan negara terhadap tiap warga negaranya. Saat ini, di Indonesia sendiri marak problematika hukum yang berkaitan dengan penyalahgunaan informasi pribadi yang digunakan untuk keuntungan sendiri.[6]

Kini Indonesia telah memiliki Undang-Undang Nomor 27 tahun 2022 Tentang Perlindungan Data Pribadi (UU PDP) tersendiri. Dalam UU PDP tersebut, diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya tersendiri. Dalam UU PDP tersebut, data

[4] Disemadi, H. S. (2021). Urgensi Regulasi Khusus dan Pemanfaatan *Artifical Intelligence* dalam Mewujudkan Perlindungan Data Pribadi di Indonesia. Jurnal Wawasan Yuridika,5(2), hlm. 177-199

[5] Widodo, (2013). Memerangi *Cybercrime* Karateristik, Motivasi, dan Strategi Penanganannya dalam Prespektif Kriminologi, Asswaja Pressindo, Yogyakarta ,hlm. 1

[6] Fitria Dewi Navisa, Perlindungan Hukum Atas Kebocoran Data Dan Informasi Pribadi Pada Penumpang Transportasi Udara, Yurispruden: Jurnal Fakultas Hukum Universitas Islam Malang Vol. 5 No. 1 (2022), Hlm 125-140

ISSN (*Print*) : 0854-7254 | ISSN (*Online*) : 2745-9829
Volume 30 Nomor 1 Bulan Januari Tahun 2024, 9370-9385

pribadi adalah data tentang orang perseorangan yang teridentifikasi atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik atau nonelektronik.[7] Pengendali data pribadi wajib melindungi dan memastikan keamanan data pribadi yang diprosesnya, dengan melakukan: a) penyusunan dan penerapan langkah teknis operasional untuk melindungi data pribadi dari gangguan pemrosesan data pribadi b) penentuaan tingkat keamanan data pribadi dengan memperhatikan sifat dan resiko dari data pribadi yang harus dilindungi dalam pemoresan data pribadi. Salah satu dari beberapa UU yang menjadi dasar PDP ini adalah UU 24 Pasal 79 Tahun 2013 yang berbunyi:[8] 1) Data Perseorangan dan dokumen kependudukan wajib disimpan dan dilindungi kerahasiaannya oleh Negara 2) Menteri sebagai penanggung jawab memberikan hak akses Data Kependudukan kepada petugas provinsi dan petugas Instansi Pelaksana serta pengguna 3) Petugas dan pengguna sebagaimana dimaksud pada ayat (2) dilarang menyebarluaskan Data Kependudukan yang tidak sesuai dengan kewenangannya 4) Ketentuan lebih lanjut mengenai persyaratan, ruang lingkup, dan tata cara mengenai pemberian hak akses sebagaimana dimaksud pada ayat (2) diatur dalam Peraturan Menteri. Namun saat ini, pemerintah dalam menangani problematika hukum tersebut masih belum optimal karena belum adanya standar perlindungan hukum terhadap data pribadi.

Namun saat ini, pemerintah dalam menangani problematika hukum tersebut masih belum optimal karena belum adanya standar perlindungan hukum terhadap data pribadi. Kerahasiaan terkait data data pribadi milik seseorang dianggap penting karena hal tersebut menyangkut martabat dan kebebasan berekspresi tiap orang. Hingga saat ini, Indonesia masih tidak memiliki aturan khusus untuk memberantas tindakan yang menyalahgunakan data pribadi seseorang dimana bisa mengakibatkan masalah hukum terhadap data pribadi pemerintah. Ada beberapa faktor yang mendukung pencurian data criminal.

Indonesia ialah negara berkembang yang dianggap masih ketinggalan dalam hal perkembangan teknologi serta informasi. Hal tersebut disebabkan akibat rencana pengembangan teknolgi yang tidak tepat sasaran dan tidak memperhatikan penelitian ilmiah dan teknologi sehingga Indonesia menjadi negara tanpa teknologi. Selain karena kurangnya kesadaran hukum masyarakat Indonesia untuk menyikapi kejahatan dunia maya, masyarakat yang masih belum faham mengenai berbagai jenis kejahatan yang terjadi di dunia maya menyebabkan maraknya kasus kejahatan duni maya.

[7] Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi
[8] Undang-Undang Nomor 24 Tahun 2013 Tentang Adminduk

Fakta ini menghadirkan tantangan yang seringkali sulit untuk diatasi karena, selain ilegal, dilakukan oleh individu yang tidak diketahui keberadaannya, sehingga sulit untuk mengungkap kebenaran bahkan jika pelakunya ditangkap. Namun, hanya bergantung pada hukum positif tradisional Indonesia akan membuat sangat sulit untuk memberantas kejahatan yang dilakukan secara online.[9]

Dengan adanya permasalahan yang terjadi, pada penelitian ini penulis mengangkat rumusan masalah yakni bagaimana modus tindak pidana pencurian data pribadi melalui internet bisa terjadi dan bagaimana bentuk dari perlindungan hukum bagi korban dari tindak pidana pencurian data pribadi melalui internet tersebut. Permasalahan ini sesuai dengan latar belakang dari adanya pencurian data pribadi melalui internet.

Metode penelitian yang digunakan dalam peneitian ini yakni dengan yuridis normatif melalui pendekatan yang mengacu pada ketentuan hukum dengan norma tertulis atau perundang-undangan yang sah. Pendekatan ini meliputi pendekatan perundang-undangan dengan cara menelaah dan meniliti semua undang-undang dan regulasi. Pendekatan konseptual dengan menggunakan konsep yang bersumber dari pandangan doktrin atau pendapat yang berkembang. Pendekatan kasus dilakukan dengan cara melakukan telaah terhadap kasus-kasus yang berkaitan dengan isu yang dihadapi yang telah menjadi putusan pengadilan.

PEMBAHASAN

A. Modus Tindak Pidana Pencurian Data Pribadi Di Internet

Pesatnya perkembangan teknologi dan informasi menyebabkan perubahan kebutuhan dan gaya hidup masyarakat yang semakin tergantungpada teknologi. Pemanfaatan teknologi dan informasi dapat dirasakan, baik dalam bidang pendidikan,ekenomi maupun hal-hal lain yang berkaitan dengan perkembangan ilmu pengetahuan. Akses terasa begitu mudah, sehingga kita bisa dengan cepat mendapatkan jutaan atau bahkan milyaran informasi. Dalam bidang pekerjaan, pengelolaan volume data yang besar dapat diproses secara akurat, cepat, efisien dan minim kesalahan. Di bidang ekonomi, berpotensi untuk meningkatkan kesejahteraan rakyat terwujud secara cepat, tanpa batasan lokasi, wilayah dan menjangkau seluruh lapisan masyarakat, baik nasional maupun internasional.

[9] Alhakim, A., & Sofia, S. (2021). Kajian Normatif Penanganan *Cyber Crime* Di Sektor Perbankan Di Indonesia. Jurnal Komunitas Yustisia, 4(2), hlm.377-385

Namun, perkembangan teknologi dan informasi ini tidak hanya membawa manfaat, tetapi juga menimbulkan permasalahan yang dapat merugikan masyarakat, seperti penyalahgunaan data, pencurian data pribadi, penjualan data pribadi, phising dan lain sebagainya. Pelaku komersial atau operator sistem elektronik dapat mengumpulkan data pribadi dari pelanggan atau calon pelanggan secara offline atau online, di mana data digital dapat dipertukarkan tanpa diketahui pemiliknya dan data yang tidak sah atau penggunaan yang tidak benar (untuk tujuan selain transmisi, pengiriman dan data pribadi) juga bisa diretas ataupun dicuri *(hack)* oleh pihak ketiga.

Dengan adanya penyalahgunaan data pribadi, terlihat adanya kelemahan pada sistem, kurangnya pengawasan, sehingga data pribadi disalahgunakan serta dapat menimbulkan kerugian bagi pemilik data. Penyalahgunaan, pencurian dan penjualan data pribadi merupakan pelanggaran hukum di bidang teknologi informasi serta dapat dianggap sebagai pelanggaran hak asasi manusia, karena data pribadi merupakan bagian dari hak asasi manusia yang harus dilindungi.

Sehubungan hal tersebut, terdapat beberapa contoh penyalahgunaan data pribadi, antara lain:

1. Menyalin informasi dan data kartu bank nasabah *(skimming)* saat penipu melakukan penarikan uang di tempat lain.
2. Pinjaman online, di mana mekanisme transaksi pengisian data secara online, namun dalam hal keterlambatan pembayaran, tidak jarang menggunakan *cash collector* untuk mengintimidasi nasabah, keluarga nasabah, pengelola tempat nasabah, bahkan dapat mengakses data dari handphone nasabah telepon.
3. Lalu lintas online, di mana konsumen dilecehkan secara seksual melalui nomor WhatsApp.

Adapun modus operandi yang dilakukan para pelaku ini adalah terdapat dalam pasal 30 Undang-undang Informasi dan Transaksi Elektronik yang melakukan akses ke dalam sistem suatu komputer atau sistem elektronik secara tidak sah, tanpa hak serta tanpa izin dari pemiliksistem tersebut.

Pertama, pencurian data : pelaku mencari data yang kira-kira dapat diakses dengan tanpa izin, menentukan ruang lingkup wilayah dimana akan dilakukan serangan, menyeleksi jaringan dan mengintai jaringan. Penulis mencontohkan hal ini adalah suatu

ISSN (*Print*) : 0854-7254 | ISSN (*Online*) : 2745-9829
Volume 30 Nomor 1 Bulan Januari Tahun 2024, 9370-9385

aplikasi bernama *"Instagram"* dimana *Instagram* merupakan salah satu media *social* yang memuat beberapa informasi atau data pribadi seseorang.[10]

Kedua, adalah pemilihan sasaran. Di sini pelaku mulai meraba-raba di mana letak kelemahan sistemnya tersebut. Pelaku mencari sistem mana yang bisa ditembus dan diakses dengan tepat sasaran.

Ketiga, pencarian data mengenai sasaran yang dituju. Hal ini sudah bersifat sangat mengganggu terhadap suatu sistem. Di sini pelaku dapat mencari mengenai nama akun, *password* akun korban, isi percakapan maupun transaksi data-data berupa foto/vide, file dokumen, phonesex antara korban dengan lawan interaksi di sistem tersebut.

Keempat, akses secara illegal telah ditetapkan atau ditentukan. Aksi ini ditunjukan untuk mencoba mendapatkan akses kedalam sistem seolah- olah pelaku adalah user biasa sistem tersebut. Pada tahap ini, biasanya seseorang atau pelaku tersebut sudah memiliki paling tidak akun penggunayang sah, dan tinggal mencari hal lainnya. Apabila sistem tersebut memiliki *password*, hanya dilengkapi dengan *password* yang sederhana dalam melindungi sistemnya.[11]

Yang kelima adalah menaikan atau mengamankan suatu polisi, mengansumsikan bahwa penyerang atau pelaku sudah memiliki *log-on acces* pada sistem tersebut sebagai pengguna biasa. Selanjutnya setelah pelaku mendapatkan akses dan mendapatkan data pribadinya melalui cerita atau *"instastory"* yang bertujuan agar apa yang pelaku sebarkan dilihat oleh lawan interaksi pengguna tersebut di instagram. Selain melalui instastory pelaku juga bisa menyebarkan data pribadi tersebut melalui postingan diberanda atau timeline atau bahkan menyebarkannya melalui chating atau percakapan antar pengguna dengan lainnya dengan maksud tujuan yang sama agar dapat dilihat para khalayak penguna lainnya.[12]

Berdasarkan catatan CNNIndonesia.com, setidaknya ada 10 kasus kebocoran data, dengan jumlah yang sangat memprihatinkan pada tahun ini. Sebagaian besar data yang bocor diyakini berasal dari aplikasi pemerintah atau organisasi Negara, meski belum ada yang mengakuinya secara terbuka.[13] Dari 10 kasus yang terdomentasi, Bjorka berperan dalam

[10] Nur Khalimatus, "Modus Operandi Tindak Pidana Cracker Menurut Undang-undang Informasi Dan Transaksi Elektronik". Jurnal Hukum Wijaya Kusuma Surabaya, Vol 20 20, Maret 2017, hlm. 83

[11] Ibid. hlm. 83
[12] Ibid. hlm. 83
[13] https://www.cnnindonesia.com/teknologi/202211230125430-192-894094/10-kasus-kebocoran-data-2022-bjorka-domain-ramai-ramai-bantah.

ISSN (*Print*) : 0854-7254 | ISSN (*Online*) : 2745-9829
Volume 30 Nomor 1 Bulan Januari Tahun 2024, 9370-9385

sebagian besar kasus tersebut. Kepala Badan Keamanan Siber dan sandi Negara (BSSN) Hina Siburian mengatakan, kebocoran yang dilakukan Bjorka masih dalam intensitas rendah. jika kita melihat kategori atau klarifikasi serangan terkait pencurian data, intensitasnya masih sangat rendah. Namun sejumlah pengamat menilai adanya kebocoran data pribadiberupa nomor ponsel dan nomor induk kependudukan.

Untuk lebih jelasnya, berikut daftar kebocoran data besar di tahun 2022:

1. Lindungi data dengan hati-hati

   Sebanyak 3,2 miliar data pengguna aplikasi PeduliLindungi bocor. Data yang bocor tersebut dijual oleh Bjorka di web gelap. Di antaranya Menteri Informasi dan Komunikasi Johnny G.Plate, Menteri Koordinator Bidang Kemaritiman dan Investasi Luhut Pandjaitan, dan YouTuber Deddy Corbuzier. Data yang bocor tersebut meliputi data terkompresi sebesar 48 GB, data tidak terkompresi sebesar 157 GB, sehingga totalnya ada 3.250.144.777 data. Data dalam format CSV berupa "Nama, Email, NIK (Nomor Kartu Tanda Penduduk), Nomor Telepon, Tanggal Lahir. ID perangkat (Nomor perangkat, Status Covid-19, Riwayat Data Daftar, Riwayat Pelacakan kontak.[14]

2. Data MyPertamina

   Sebanyak 44 juta pengguna aplikasi MyPertamina dibocorkan Bjorka, dan dijual seharga Rp392 juta dalam bentuk BitCoin. MyPertamina merupakan*platform* layanan keuangan digital milik Pertamina yang terintegrasi dalamaplikasi LinkAja. Aplikasi ini dipakai untuk pembayaran BBM non-tunai di SPBU Pertamina.[15]

3. Data SIM Card

   Sebanyak 1,3 miliar data registrasi kartu SIM atau SIM card diduga bocor dan dijual di forum gelap pada September lalu, Bjorka mengatakan data tersebut diperoleh dari informasi dan Komunikasi. Data yang bocor meliputi NIK, nomor telepon, nama penyedia (provider), dan tanggal pendaftaran berkapasitas 87 GB. GB senilai 50.000 USD(Rp 743,5 juta). Bjorka menyertakan sampel data 2 GB. Lembaga penelitian pusat, penelitian keamanan sistem Informasi dan Komunikasi (CISSReC), yang menganalisis sampel data Bjorka, mengatakan data yang bocor di forum gelap itu sah. Kominfo sendiri sejak Oktober 2017 telah mewajibkan seluruh pengguna kartu SIM

[14] Indonesia Covid-19 app Peduli Lindungi 3,2 bilion, demikian judul unggahan Bjorka di situs BreachForums, selasa (15/11) pukul 06.42 waktu unggahan atau pukul 13.43 WIB

[15] MYPERTAMINA INDONESIA 44 MILLION di situs BreachForums, bertanggal kamis (10/11) pukul 02.31 AM

prabayar harus mendaftarkan nomor telepon. Syaratnya, berikan nomor NIK dan nomor Kartu Keluarga (KK). Penyebab kebocoran data ini juga tidak jelas. Kominfo meluncurkannya di Asosiasi Telekomunikasi Seluler Indonesia (ATSI). Organisasi operatorseluler tersebut membantah bocoran informasi dari pihaknya. Begitu pula dengan Departemen Umum Kependudukan dan kependudukan Sipil (Dukcapil) kemendagri yang menyediakan data registrasi.[16]

4. 105 Juta Data KPU Bocor

   Masih menurut Bjorka, tak kurang dari 105 juta data terjual di situs gelap *Breached.to* bertajuk Basis Data Warga Negara Indonesia dari KPU 105M, tak lupa ia menempelkan logo Komisi Pemilihan Umum (KPU). Pada September lalu, konter penjualanya. Bjorka mengklaim memiliki data 105.003.428 juta penduduk Indonesia dengan rincian NIK, KK, namalengkap, lokasi**,** tanggal lahir, jenis kelamin, umur, dan lain-lain. Data pribadi dijualseharga 5.000 USD atau setara dengan Rp 7,4 juta juta (1 USD = Rp 14.898,20). Semua data disimpan dalam file 20 GB (tidak terkompresi). atau 4 GB (terkompresi). Untuk mengatasi permasalahan tersebut, KPU membentuk kelompok kerja dan menyimpulkan bahwa unsur data yang bocor.[17]

5. Dokumen Rahasia untuk jokowi Bocor

   Beberapa judul surat rahasia untuk presiden jokowi, termasuk dari Badan Intelijen negara (BIN), bocor dan diungkap oleh Bjorka di *Breach Forums* pada September 2022. Dalam keterangannya. Dokumen yang dicuri pada September 2022 itu terdiri dari 679.180 data dengan kapasitas 40 MB *(Compressed)* dan 189 MB *(Uncompressed)*. Dalam unggahannya ini, Bjorka tak menyertakan rincian harga jual maupun isi dari surat-surat itu. Kemungkinan sekadar unjuk gigi membuktikan ucapan sebelumnya di Telegram untuk membobol data Presiden. Ia juga menyertakan sejumlah sampel atau contoh dokumen yang dibobol. Isinya, kata Bjorka, "*little of the letter, letters number,sender,receiveremploye id, letter date etc.*

Proxy berguna bagi penyerang dalam banyak hal. Kebanyakan penyerang menggunakan *proxy* untuk menyembuyikan alamat IP mereka dan oleh karena itu, lokasi fisik mereka yang sebenarnya. Dengan cara ini, serangan atau melakukan transaksi keuangan palsu,

[16]https://www.cnnindonesia.com/teknologi/202211230125430-192-894094/10-kasus-kebocoran-data-2022-bjorka-domain-ramai-ramai-bantah.
[17]https://www.cnnindonesia.com/teknologi/202211230125430-192-894094/10-kasus-kebocoran-data-2022-bjorka-domain-ramai-ramai-bantah.

melancarkan serangan,atau melakukan tindakan lain dengan risiko kecil. Sementara alamat IP, penyerang yang menggunakan satu atau beberapa *proxy* melintasi batas negara lebih sulit ditemukan. Titik akhir hanya dapat melihat *proxy* terakhir yang berkomunikasi langsung dengannya dan bukan *proxy* perantara atau lokasi aslinya.

Proxy menyediakan cara bagi untuk menurunkan risiko mereka dalam identifikasi penyelidik atas alamat IP mereka yang sebenarnya. Dalam serangan hipotesis, file log korban hanya berisi satu penyerang. Penyerang mengoperasikan *proxy* gratis atau mengubah pengaturan *proxy* korban karena *proxy* dapat berfungsi sebagai alat pemantauan. *Anonproxy* adalah salah satu contoh *proxy* jahat yang dirangcang oleh pembuatnya untuk memantau pengguna dan mencuri informasi seperti kata sandi jaringan sosial karena *proxy* menyampaikan lalu lintas maka ia juga memiliki kemampuan untuk mencatat dan mengubah halaman atau informasi sensitif. Penyerang harus menyakinkan pengguna atau menginstal kode berbahaya yang mengubah pengaturan *proxy* sendiri.[18]

Proxy sangat umum digunakan oleh user sehingga banyak penyerang melakukan scanning pada internet untuk mendengarkan port *proxy* yang umum. *Proxy* yang paling umum mendengarkan port TCP 80,8000,8081, 443, 1080 (SOCKS *proxy*) dan 3128 yang digunakan *squid proxy,* dan beberapa juga menagani *user* Datagram *Protocol* (UDP). Penyerang yang memasang *proxy* khusus sering kali tidak menggunakan port standar menggunakan port tinggi yang acak. Beberapa *proxy* ringan ditulis dalam bahasa script yang dijalankan dengan server HTTP dan lebih mudah dimodifikasi oleh penyerang. Aplikasi *proxy* memerlukan konfigurasi. Beberapa aplikasi tidak beroperasi dengan benar melalui layanan *proxy* karena server *proxy* menghapus informasi yang diperlukan atau tidak dapat memenuhi permintaan. Beberapa layanan seperti *TheOnion Router* (TOR2) juga memberi pengguna kemampuan untuk mem- *proxy* lalu lintas dan menyembuyikan lokasi asli mereka dari korban.

Aplikasi VPN dapat bertindak sebagai *proxy* yang lebih fleksibel dan mendukung lebih banyak fitur keamanan. Alih-alih mengonfigurasi aplikasi untuk menggunkan *proxy*. Pengguna dapat melakukan *tunnel* semua lalu lintas melalui VPN. layanan VPN biasanya mendukung autentikasi yang *secure* dan cendurung tidak membocorkan informasi yang dapat mengidentifikasi pengguna *proxy*.[19]

[18] Ibid, hlm.31
[19] Ibid, hlm. 31

Mendeteksi *proxy* itu sulit dan kadang tidak selalu dapat diandalkan. Karena banyak pembuat kode berbahaya memasang *proxy* secara khusus sehingga sangat sulit untuk mendeteksi semua *proxy*. Ada teknik untuk mendeteksi *proxy* umum, tetapi teknik seperti itu tidak mungkin efektif melawan penyerang yang menggunakan *proxy* secara agresif. Proxy gratis dan komersial sangat banyak di Internet dan dapat menggunakan protokol dan port standar. Proxy lain lebih sulit untuk diidentifikasi, dan administrator dapat medeteksi penggunaan proxy melalui perubahan konfigurasi, mesin IDS atau alat seperti decloak. Penyerang yang ingin menyembunyikan lokasi mereka memiliki sumber daya yang tersedia untuk mereka. Karena sulit untuk mendeteksi semua pengguna proxy secara akurat, alat dan layanan proxy akan terus berguna bagi penyerang.[20]

Bentuk umum dan sederhana dan sederhana dari *traffic tunneling*di SSH adalah *tunneling* dari *port Transmission Control Protocol* (TCP). Ketika pengguna mengonfigurasi *tunneling* seperti melalui sesi SSH, protokol hanya mem-*proxy* koneksi TCP melalui koneksi SSH dan konten koneksi TCP mengalir langsung dari sumber ke tujuan, melainkan melalui koneksi SSH. Satu sisi koneksi SSH di sisi server klien mendengarkan pada port TCP tertentu sebagai sumber data dan mentransfer semua data ke sisi lain koneksi SSH. Sisi lain kemudian meneruskan data ke tujuan TCP yang ditentukan. Konfigurasi *tunneling* SSH dapat menjadi lebih rumit karena pengguna dapat mengonfigurasinya untuk mendyediakan *tunnel* terbalik atau proxy aplikasi arbiter melalui protokol seperti SOCKS tetapi konsep dasarnya tetap sama. Koneksi SSH dapat menggabungkan koneksi Telnet dengan aman di antara lingkungan terpercaya. Contoh jalurlalu lintas antara dua host yang tidak terkait yang memiliki kemamuan SSH untuk menggambarkan fleksibilitas solusi.[21]

B. Bentuk Perlindungan Hukum Bagi Korban Tindak Pidana Pencurian Data Pribadi Di Internet

Untuk memberi rasa aman kepada korban perlu adanyaperlindungan hukum bagi korban. Yang dimaksud dengan perlindungan hukum adalah upaya untuk melindungi hak asasi manusia yang telah dilanggar ataupun dirampas oleh orang lain. Perlindungan hukum dapat dilakukan dalam beberapa bentuk, antara lain peraturan perundang-undangan, pemberian pertolongan kepada saksi dan/atau korban, dan pemberian jaminan kepastian hukum. Perlindungan hukum juga dapat dipandang sebagai jaminan yang

[20] Ibid, hlm. 33
[21] Ibid, hlm. 35

diberikan oleh negara kepada semuapihak untuk dapat memperjuangkan hak dan kepentingan hukumnya dalam kedudukannya sebagai subjek hukum yang adil dan perlakuan yang sama di depan hukum. Pegawai Negeri Sipil (ASN) juga dapat diberikan perlindungan hukum berdasarkan asumsi tidak bersalah.[22]

Cara untuk memperoleh perlindungan hukum bisa dilakukan juga dengan cara mengajukan gugatannya kepada pengadilan, melaporkan kejadian ke pihak berwajib, atau meminta bantuan dari lembaga perlindungan hukum seperti advokat atau lembaga bantuan hukum. Selain itu, masyarakat juga dapat memperoleh perlindungan hukum melalui kebijakan pemerintah yang memberikan perlindungan terhadap hak-hak warga negaranya. Dalam praktiknya, perlindungan hukum dapat diberikan dalam berbagai bentuk, seperti perlindungan hukum perdata, perlindungan anak, perlindungan konsumen, dan lain sebagainya. Perlindungan hukum juga dapat diberikan dalam bentuk preventif maupun represif. Ada berbagai bentuk perlindungan hukum dalam konteks transaksi dan aktivitas digital di Indonesia.[23] Berikut beberapa contohnya:

1. Perlindungan Preventif: Perlindungan preventif ditujukan untuk mencegah terjadinya bahaya sejak awal. Dalam konteks transaksi digital, perlindungan preventif dapat dilakukan melalui edukasi dansosialisasi, maupun melalui pembentukan badan pengatur seperti Otoritas Jasa Keuangan (OJK) yang memiliki tugas untuk memberi rasaaman terhadap konsumen juga masyarakat.
2. Perlindungan Represif: Perlindungan represif ditujukan untuk menghukum mereka yang telah melakukan kejahatan. Dalam konteks transaksi digital, perlindungan represif dapat diberikan melalui upaya litigasi dan penegakan hukum oleh otoritas seperti kepolisian.
3. Kerangka Hukum: Kerangka hukum seperti UU ITE memberikan dasar perlindungan hukum dalam konteks transaksi digital. UU ITE memuat ketetuan terkait kontrak elektronik, cybercrime, dan perlindungan konsumen.
4. Bukti Elektronik: Penggunaan bukti elektronik dalam proses hukum adalah bidang lain di mana perlindungan hukum penting. UU ITE yaitu memberikan penggunaan alat-alat bukti/proof elektronik dipengadilan, namun masih terdapat tantangan terkait pembuktian dan keabsahan alat bukti tersebut.

[22] M. Nurul Jadid and T. *Michael,* "Perlindingan Hukum Bagi Pelaku Kekerasan Karena Pembelaan Terpaksa". Yustisi, vol,10, no. 1, pp. 175-18, Feb 2023

[23] S.Yuniarti "Perlindungan Hukum Data Pribadi Di Indonesia"*Business Economic, Communication and Social Science* (BECOSS) *Journal,* vol 1, no. pp. 147-154, Sep. 2019, doi :1021512/*becossjournal*.vlil.6030.

ISSN (*Print*) : 0854-7254 | ISSN (*Online*) : 2745-9829
Volume 30 Nomor 1 Bulan Januari Tahun 2024, 9370-9385

5. Kerjasama Internasional: Kerjasama internasional juga merupakan bentuk perlindungan hukum yang penting dalam konteks transaksi digital. Kejahatan dunia maya semakin menjadi perhatian di Indonesia, dan perlindungan hukum terhadap kejahatan dunia maya merupakan aspek penting dari keamanan digital. *Convention on Cybercrime* misalnya, menekankan perlunya kerjasama internasional dalam memerangi cybercrime yang bersifat global dan tanpa batas wilayah.
6. Bitcoin dan Mata Uang Virtual: Dengan uang tesebut maupun lainnya dapat menghadirkan tantangan unik untuk perlindungan hukum. Meskipun ada upaya yang sedang berlangsung untuk mengatur mata uang virtual di Indonesia, masih terdapat ketidakjelasan mengenai status hukumnya dan perlindungan yang diberikan kepada investor.

Secara keseluruhan, perlindungan hukum dalam konteks transaksi digital di Indonesia dapat dilakukan dalam berbagai bentuk, antara lain tindakan preventif dan represif, kerangka hukum, dan kerjasama internasional. Bentuk-bentuk perlindungan ini bertujuan untuk mencegah terjadinya kerugian, menghukum mereka yang telah melakukan kerugian, dan memberikan dasar hukum untuk menangani masalah yang berkaitan dengan transaksi digital.[24]

Adapun terkait dengan perlindungan hukum bagi korban pencurian secara digital, di mana dalam era modern seperti saat ini tentunya sudah memasuki era digital/online, yakni semua hal berbasis online, namun masih kurang adanya perlindungan hukum dan perlu adanya peraturan perundang-undangan yang membahas mengenai ini. Pencurian secara digital dapat memiliki dampak yang merugikan bagi korban. Korban pencurian data pribadi dapat mengalami kerugian finansial, seperti kehilangan uang dari rekening bank atau kartu kredit yang digunakan oleh pelaku. Selain itu, korban juga dapat mengalami kerugian non-finansial, seperti pencemaran nama baik atau identitas palsu yang digunakan oleh pelaku untuk melakukan tindakan kriminal lainnya. Korban juga dapat mengalami kerugian emosional, seperti kehilangan privasi dan rasa aman karena data pribadi mereka telah dicuri. Dalam hal ini, perlindungan hukum bagi ciptaan-ciptaan didalam era digital dan perlindungan data pribadi menjadi penting untuk mencegah terjadinya pencurian secara digital dan melindungi korban dari dampak yang merugikan. Hak asasi manusia digital

[24] M. Minorosa, *"legal Protection of Personal Data Owners as Cybercrime Victims Based on regulation regarding Electronic Information and Transaction" in Proceedings of the first Multidicipline International Conference*, MIC 2021, 30 October 20221, Jakarta, Indonesia, EAI, 2022. Doi:10.4108/eai.30-10-2021.2315833

didefinisikan sebagai seperangkat hak masyarakat untuk mengakses, memanfaatkan, membuat, mentransmisikan, dan memperdagangkan informasi dan teknologi digital serta menyadari hak asasi manusia dalam ranah digital yang terikat pada pengguna tersebut sebagai subjek hukum.[25]

Selain itu, perlindungan hukum di era digital juga mencakup perlindungan hak privasi atas data diri, hak cipta karya, dan hak konsumen dalam transaksi digital. Pemerintah dan regulator perlu memperkuat sistem hukum di era teknologi digital untuk melindungi hak-hak tersebut. Perlindungan hukum Adapun terkait dengan perlindungan hukum bagi korban pencurian secara digital, di mana dalam era modern seperti saat ini tentunya sudah memasuki era digital/online, yakni semua hal berbasis online, namun masih kurang adanya perlindungan hukum dan perlu adanya peraturan perundang- undangan yang membahas mengenai ini. Pencurian secara digital dapat memiliki dampak yang merugikan bagi korban. Korban pencurian data pribadi dapat mengalami kerugian finansial, seperti kehilangan uang dari rekening bank atau kartu kredit yang digunakan oleh pelaku. Selain itu, korban juga dapat mengalami kerugian non-finansial, seperti pencemaran nama baik atau identitas palsu yang digunakan oleh pelaku untuk melakukan tindakan kriminal lainnya. Korban juga dapat mengalami kerugian emosional, seperti kehilangan privasi dan rasa aman karena data pribadi mereka telah dicuri. Dalam hal ini, perlindungan hukum bagi ciptaan-ciptaan didalam era digital dan perlindungan data pribadi menjadi penting untuk mencegah terjadinya pencurian secara digital dan melindungi korban dari dampak yang merugikan. Hak asasi manusia digital didefinisikan sebagai seperangkat hak masyarakat untuk mengakses, memanfaatkan, membuat mentransmisikan, dan memperdagangkan informasi dan teknologi digital serta menyadari hak asasi manusia dalam ranah digital yang terikat pada pengguna tersebut sebagai subjek hukum.[26]

KESIMPULAN

Dari hasil penelitian diatas didapatkan hasil bahwa modus kejahatan yang dilakukan oleh pelaku yakni dengan mencari data korban yang dapat diakses tanpa melalui izin. Dimana pelaku akan menyasar kelemahan dari sistem dan melakukan pencarian data mengenai akun, password dan data-data pribadi korban. Aksi ini dilakukan secara ilegal agar

[25] S. A. Kusnadi, "PERLINDUNGAN HUKUM DATA PRIBADI SEBAGAI HAK PRIVASI"AL WASHTH Jurnal Ilmu Hukum, Vol.2, no. 1, 2021, doi:10.47776/alwashth.v2il. hlm. 1287

[26] S. A. Kusnadi, "PERLINDUNGAN HUKUM DATA PRIBADI SEBAGAI HAK PRIVASI"AL WASHTH Jurnal Ilmu Hukum, Vol.2, no. 1, 2021, doi:10.47776/alwashth.v2il. hlm. 127

pelaku dapat mengakses sistem seolah-oleh sebagai user. Setelah itu, pelaku akan meningkatkan keamaan akun yang telah direntas engan mengganti passwrod dan membajak akun email. Pelaku biasa melakukan kejahatan digital dengan menyerang *proxy*. Dampak dari penggunaan *proxy* ini adalah penyerang dapat menyembunyikan lokasi fisik mereka, sementara alamat IP penyerang menggunakan beberapa *proxy* melintasi batas negara agar sulit untuk ditemukan, *proxy* menyediakan berbagai cara untuk menurunkan resiko dalam identifikasi penyelidik atas alamat IP, penyerang mengoperasikan *proxy* secara gratis dan dapat mengubah pengaturan *proxy* korban dan banyak dampak lainnya.

Maka dari itu, korban mendapatkan mendapatkan 2 perlindungan hukum yakni perlindungan secara preventif dan secara represif. Perlindungan secara preventif ini ditujukan untuk mencegah terjadinya bahaya sejal awal melalui edukasi dan sosialisasi ataupun melalui pembenmtukan badan pengatur. Sedangkan perlindungan represif ditujukan untuk menghukum pelaku kejahatan. Salah satu undang-undang yang mengatur mengenai perlindungan data pribadi yakni dalam Undang-Undang Nomor 27 Tahun 2022. Pada undang-undang tersebut menjelaskan mengenai perlindungan data pribadi yang memberikan hak kepada pemilik data untuk menuntut kerugian yang timbul akibat penggunaan data pribadi yang tidak sah.

DAFTAR PUSTAKA

Alhakim, A., & Sofia, S. (2021). Kajian Normatif Penanganan *Cyber Crime* di Sektor Perbankan di Indonesia. Jurnal Komunitas Yustisia, 4(2), 377-385.

S. A. Kusnadi,"PERLINDUNGAN HUKUM DATA PRIBADI SEBAGAI HAK PRIVASI"*ALWASHTH* Jurnal Ilmu Hukum, Vol.2, no. 1,

Bambang Sunggono, 1998, Metodologi Penelitian Hukum, Jakarta: Raja Grafindo Persada,

Disemadi, H. S. (2021). Urgensi Regulasi Khusus dan Pemanfaatan Artificial *Intelligence* dalam Mewujudkan Perlindungan Data Pribadi di Indonesia. Jurnal Wawasan Yuridika, 5(2),177-199.

Djanggih Hardianto, and Nurul Qamar. "Penerapan Teori-Teori Kriminologi Dalam Penanggulangan Kejahatan Siber (*Implementation Of Criminological Theories In CyberCrime Prevention).*" Pandecta: *ResearchLaw Journal* 13, no. 1 (2018): 10–23. Menurut, Transnasional, and Hukum Internasional. "Jurnal Pencegahan Kejahatan Carding Sebagai Kejahatan Transnasional Menurut Hukum Internasional" (2014).

Daniel Shoesmasker, Anne Konke, Ken Singler, "The cybersecurity Body of Knoowledge" 2020, Taylor & Francia Group, New York, USA

Herlambang, I. T. (2019). Korban Kejahatan Tindak Kejahatan Perbankkan Dalam Presepektif Hukum Dan Viktimologis. Negara dan Keadilan, 8(1). http://riset.unisma.ac.id.id/index.php/nengkea/article/view/4481.

Indonesia Covid-19 app Peduli Lindungi 3,2 bilion, demikian judul unggahan Bjorka di situs *BreachForums*, selasa (15/11) pukul 06.42 waktu unggahan pukul 13.43 WIB

MYPERTAMINA INDONESIA 44 MILLION di situs *BreachForums*, bertanggal kamis (10/11) pukul 02.31 AM

M. Nurul Jadid and T. *Michael*, "Perlindingan Hukum Bagi Pelaku Kekerasan Karena Pembelaan Terpaksa". Yustisi, vol,10, no. 1, pp. 175-18, Feb 2023

M. Minorosa, *"legal Protection of Personal Data Owners as Cybercrime Victims Based on regulation regarding Electronic Information and Transaction" in Proceedings of the first Multidicipline International Conference*, MIC 2021, 30 October 20221, Jakarta, Indonesia, EAI, 2022. Doi:10.4108/eai.30-10-2021.2315833

M.P. Mamang and M. Zakky , "Penegakkan Hukum Terhadap Tindak Pidana Pencurian Data Pribadi Melalui Internet Ditinjau dari Undang-Undang No 19 Tahun 2016 tentang perubahan atas Undang-Undang Nomer 11 tahun 2008 Tentang ITE (Informasi dan Transaksi Elektronik)" Jurnal Hukum Jurisdictie, vol. 3, no.2, 2021, doi: 10.34005/jhj.v3i2.

Muhaimin, 2020, Metode Penelitian Hukum, Mataram: *Universty Press*,

M.R. Herianto. "Sistem Penegakkan Hukum Terhadap Kegagalan Dalam Perlindungan Data Pribadi Di Indonesia" kerthaPatrika, vol.43, no. 1, p.9, April 2021, doi: 10.24843/KP.2021.v43.i01.p07

Nur Khalimatus, "Modus Operandi Tindak Pidana Cracker Menurut Undang-undang Informasi Dan Transaksi Elektronik". Jurnal Hukum Wijaya Kusuma Surabaya, Vol 20 20, Maret 2017

Restri, Fauzi Sekar dan Fery Dona. (2022), Penyidikan Tindak PidanaPencurian di PolresPurworejo, Jurnal Al-Hakim, 4(1), 44

Soerjono Soekanto dan Sri Mamudi, 2010, Penelitian Hukum Normatif Suatu Tinjauan Singkat, Jakarta: Rajawali Press,

Sudikno Mertokusumo, 2014, *discovery of the law an introduction*, Cahya Atma Pustaka, Yogyakarta, p.

Soekanto, S., & Mamudji, S. (2006). Penelitian Hukum Normatif: Suatu Tinjauan Singkat. Jakarta: Raja Grafindo Persada.

Suratman dan Philips Dillah, 2015, Metode Penelitian Hukum, Bandung: Alfabeta.

Sugiyono, 2009, Metode Penelitian Pendidikan: Pendekatan Kuantitatif,Kualitatif dan R & D,Bandung: Alfabeta.

Tomlili, Rahamuddin. (2019). Hukum Pidana. Sleman: Penerbit Deepublish. Puspita, Heni dkk.(2022). Pengantar Teknologi Informasi. Sukabumi: CV Haura Utama.

Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi

Undang-Undang Nomor 24 Tahun 2013 Tentang Adminduk

Widodo. (2013). Memerangi *Cybercrime* Karateristik, Motivasi, dan Strategi Penanganannya dalam Prespektif Kriminologi. Yogyakarta: Asswaja Pressindo

Wahyudi, Dheny. "Perlindungan Hukum Terhadap Korban Kejahatan *CyberCrime* Di Indonesia." Jurnal Ilmu Hukum Jambi 4, no. 1 (2013): 43295.

Yesmil Anwar dan Adang, 2008, Pembaharuan Hukum Pidana: Reformasi Hukum Pidana,Jakarta: Grasindo.

Yoki Firimansyah, Nanda Diaz, Windi irmayani,(2020). Etika Profesi Teknologi Informasi dan Komunikasi. Yogyakarta : Graha Ilmu.

Zainuddin Ali, 2013, Metode Penelitian Hukum, Jakarta: Sinar Grafika.

https://www.cnnindonesia.com/teknologi/202211230125430-192-894094/10-kasus-kebocoran-data-2022-bjorka-domain-ramai-ramai-bantah.

INTERNET

Cindy Mutia Annur, 2022,Rawannya Perlindungan Data Pribadi di Indonesia https://katadata.co.id/ariayudhistira/infografik/6306f43b1e8b9/rawannya-perlindungan- data-pribadi-di-indonesia akses pada 22 Desember 2022

Daniar Supriyadi. 2017. "Data Pribadi dan Dua Dasar legalitas Pemanfaatannya".https://www.hukumonline.com/berita/baca/lt59cb4b3feba88/data-pribadi-dan-dua-dasar-legalitas pemanfaatannya-oleh daniar-supriyadi/. Diakses pada 26 Desember 2022. Pukul 18.04 WIB. 28 Pasal 1 ayat (1). Data Protection Act Inggris tahun 1998

Fitria Dewi Navisa, Perlindungan Hukum Atas Kebocoran Data Dan Informasi Pribadi Pada Penumpang Transportasi Udara, Yurispruden: Jurnal Fakultas Hukum Universitas Islam Malang Vol. 5 No. 1 (2022)

Humas PMK, Jumlah Penduduk Indonesia Terbesar Dunia Setelah China, India,dan Amerika, https://www. Kemenkopmk.go.id/artikel/jumlah- penduduk-indonesia-terbesarke-empat- dunia-setelah-china-india-dan-Amerika .