PUSKAPSI Law Review (2023)
Diterbitkan oleh PUSKAPSI FH UNEJ
Tersedia secara online, Desember 2023

Perlindungan Hukum Pengguna Nomor Telepon Seluler dari Penyebaran tanpa Hak atas Data Pribadinya

Belgis Octa Fajrin, Fakultas Hukum, belgisof@gmail.com

ABSTRAK

Permasalahan terkait banyaknya kebocoran terkait nomor telepon seluler yang dilakukan tanpa sepengetahuan pemilik yang ada di Indonesa merupakan bentuk pelanggaran hak asasi dan hak privasi pemilik pengguna telepon seluler yang tidak memiliki perlindunngan hukum yang tepat. Pemilik nomor telepon seluler merupakan seorang yang secara mutlak yang dapat memiliki akses terhadap apa yang dimilikinya atas nomor telepon seluler. Nomor telepon seluler saat ini banyak digunakan sebagai akses penting pada layanan yang ada di telepon seluler. Atas banyaknya percobaan pegambila hak yang dilakukan secara illegal membuat nomor telepon seluler banyak mendapati kerugian yang didapatkan secara materiil ataupun immateriil.

ABSTRACT

The problem is related to the large number of leaks related to cell phone numbers that are carried out without the knowledge of owners in Indonesia, which is a form of violation of the human rights and privacy rights of owners of cell phone users who do not have proper legal protection. The owner of a cell phone number is someone who absolutely can have access to what he has on a cell phone number. Cell phone numbers are currently widely used as important access to services on cell phones. Due to the many attempts to take rights illegally, cell phone numbers have suffered material or immaterial losses.

I. PENDAHULUAN

Hingga saat ini telepon seluler atau Handphone masih menjadi primadona sebagai alat komunikasi di berbagai belahan dunia, termasuk di Indonesia sendiri. Meskipun di Indonesia sendiri pengguna telepon masih sering dijumpai, jumlah pengguna telepon seluler tidak bisa dikatakan sedikit. Hal ini terlihat dari Total populasi masyarakat Indonesia pada Januari 2019 diketahui sebanyak 268,2 juta jiwa. Akan tetapi, angka pengguna layanan operator ponsel diketahui ada sebanyak 355,5 juta pengguna.[1] Salah satu fitur bawaan yang

[1] "Data penggua Telepon seluler menurut Tomato Digital Indonesia", online: <https://www.tomato.co.id/data-digital-indonesia-2019/>.

diberikan oleh telepon seluler adalah Short Masseges Sevice (SMS). Namun, saat ini banyak oknum yang tidak bertanggung jawab yang menggunakan fitur SMS seperti ini sebagai bentuk broadcast spam yang diisi dengan promosi palsu atau penipuan. SMS seperti ini sangat sering diterima oleh para pengguna telepon seluler setiap harinya. Akhir-akhir ini banyak sekali SMS promosi yang menghubungkan dengan suatu tautan yang terhubung ke internet. Tujuan dari hal tersebut adalah melakukan pishing atau sebuah pancingan untuk seseorang memberikan data-data pribadi yang bersifat vital untuk diberikan dalam tautan tersebut.[2]

Badan Regulasi Telekomunikasi Indonesia (BRTI) dan Yayasan Lembaga Konsumen Indonesia (YLKI) menemukan fakta bahwa sedikitnya 25 juta data pelanggan telekomunikasi di Indonesia sudah bocor.[3] Hal ini berarti keamanan privasi data pengguna telepon seluler tidak terjamin aman. Dalam menangani langkah ini Pemerintah mengeluarkan kebijakan berupa Peraturan Mentri Komunikasi dan Informatika Nomor 23/M.KOMINFO/10/2005 tentang Registrasi Terhadap Pelanggan Jasa Telekomunikasi. Dengan adanya peraturan ini diharapkan setiap pelanggan dapat dikenali identitasnya, jadi ketika terjadi kejadian seperti kejahatan cyber dapat dikenali pelakunya. Kendati demikian, masih banyak terjadi SMS palsu yang dapat merugikan penggunanya. Oleh karena itu Kementerian Komunikasi dan Informatika mencabut aturan tersebut sekaligus mengeluarkan aturan baru Peraturan Menteri Komunikasi dan Informatika Nomor 12 Tahun 2016 tentang Registrasi Pelanggan Jasa Telekomunikasi.[4]

Pada aturan ini Pemerintah mengharuskan setiap pengguna telepon seluler yang menggunakan kartu SIM prabayar ataupun pascabayar dapat melakukan registrasi dan validasi dengan cara menginput data pribadi berupa Nomor Induk Kependudukan (NIK), Nomor Kartu Keluarga (KK), dan atau Nama Ibu Kandung. Dan pada setiap NIK yang terdaftar diberlakuan pembatasan registrasi. Nyatanya upaya Pemerintah tidak berjalan seperti semestinya.

---

[2] Gaston L'Huillier et al, "Topic-Based Social Network Analysis for Virtual Communities of Interests in the Dark Web",.

[3] Helmi, "PERLINDUNGAN HUKUM BAGI PENGGUNA JASA OPERATOR SELULER ATAS ADANYA SHORT MESSAGE SERVICE (SMS) SPAM",.

[4] Muttaqin, "KESADARAN PENGGUNA JASA TELEKOMUNIKASI SELULER DALAM MELINDUNGI DATA KEPENDUDUKAN SETELAH PEMBERLAKUAN REGISTRASI NOMOR MSISDN",.

Hingga saat ini masih sering kali pengguna telepon seluler menerima SMS percobaan penipuan dan sebagainya yang dapat merugikan penggunanya.
Pada pemberlakuan Peraturan Mentri Komunikasi dan Informatika Nomor 12 Tahun 2016 tentang Registrasi Pelanggan Jasa Telekomunikasi ini, tidak lepas dari sinergi bersama dengan Pemerintah dibidang Administrasi Kependudukan. Karena registrasi yang dilakukan dalam validasi data untuk aktivasi kartu SIM telepon seluler perlu menyertakan Nomor Induk Kependudukan (NIK), Nomor Kartu Keluarga (KK), dan atau nama ibu kandung. Ketiga data tersebut merupakan data pribadi yang diolah dan dijamin dalam Undang-Undang Nomor 24 Tahun 2013 tentang Administrasi Kependudukan. Dalam Undang-Undang Nomor 24 Tahun 2013 tentang Administrasi Kependudukan telah disebutkan beberapa data yang dikategorikan sebagai data Pribadi. Beberapa diantaranya adalah Nomor Induk Kependudukan dan Nomor Kartu Keluarga (KK). Kemudian hal ini menjadi serius apabila terjadi kebocoran data.
Terdapat beberapa akun vital yang menggunakan data ini sebagai salah satu syarat dalam melakukan suatu pendaftaran atau registrasi akun yang penting. Rekening Bank contohnya, dalam pembuatan rekening bank dibutuhkan tanda pengenal yaitu KTP yang didalamnya tercantum Nomor Induk Kependudukan (NIK). Mengingat bahwasanya saat ini untuk melakukan aktivasi kartu SIM pada telepon seluler adalah menggunakan Nomor Induk Kependudukan, hal ini menjadi masalah yang serius apabila terjadi pembobolan data terhadap nomor telepon seluler penggunanya. Nomor telepon seluler juga dapat digunakan sebagai verifikasi dan autentikasi pada konfirmasi suatu data. Dengan demikian, nomor telepon seluler merupakan data yang penting yang seharusya dilindungi karena pada keadaan yang modern ini banyak kegiatan elektronik yang dihubungkan dengan nomor telepon.
Sesuai dengan Pasal 1 Angka 22 Undang-Undang Nomor 24 Tahun 2013 tentang Adminstrasi Kependudukan bahwasanya data pribadi merupakan data perseorangan

tertentu yang disimpan, dirawat, dan dijaga kebenaran serta dilindungi kerahasiaannya. Namun, sampai saat ini belum ada aturan dalam undang-undang yang menyebutkan secara pasti terhadap perlindungan nomor telepon seluler. Terlebih saat ini marak sekali terjadi penjualan data pribadi milik warga Indonesia pada situr darkweb. Penjualan data pribadi tersebut dapat menjadi

ancaman besar yang mengakibatkan kerugian bagipara pemilik data pribadi yang dijual oleh orang yang tidak bertanggungjawab. Disini peran Pemerintah Indonesia dibutuhkan untuk melindungi kenyamanan dan ketentraman bagi pemilik data pribadi, salah satunya adalah pengguna telepon seluler.

II. METODE PENELITIAN

Penelitian ini merupakan penilitian yang bersifat yuridis normative. Pendekatan masalah dilakuka n dengan Pendekatan Undang-Undang dan pendekatan kasus. Jenis data yang digunakan adalah bahan hukum primer yaitu peraturan perundang-undangan. Bahan hukum sekunder yaitu buku hukum dan jurnal hukum. Juga bahan non hukum yang bersumber dari internet dan media sosial. Dilakukan dengan teknik analisis deskriptif normative dengan menggunakan norma dan kaidah hukum yang relevan untuk mengevaluasi masalah.

III. KEBOCORAN NOMOR TELEPON SELULER DI INDONESIA

Salah satu kodrat manusia adalah bersosialisasi, dan dalam era digital saat ini terdapat beragam bentuk sosialisasi. Namun, kelemahan dari perkembangan digital adalah mudahnya akses terhadap informasi rahasia melalui pencurian dan pembobolan data. Kejadian kebocoran data pribadi pengguna telepon seluler semakin meningkat, dan hal ini disebabkan oleh lemahnya sistem keamanan digital di Indonesia. Kurangnya kesadaran pengguna terhadap keamanan digital juga menjadi faktor penyebab. Penyedia layanan telekomunikasi juga memiliki peran penting dalam menerapkan praktik bisnis yang berfokus pada keamanan data. Kurangnya regulasi yang rinci mengenai perlindungan data pribadi memungkinkan penyebaran data tanpa izin. Meskipun sudah ada undang-undang tentang perlindungan data pribadi di Indonesia, peraturan yang ada bersifat sektoral.

Banyak instansi, termasuk pemerintah, mengumpulkan data pribadi melalui pengisian form fisik atau online. Pengelolaan data pribadi yang baik harus

menjadi perhatian utama instansi tersebut. Kerugian materiil dan immateriil dapat terjadi jika pengelolaan data tidak dilakukan dengan baik. Provider juga memiliki peran penting dalam mengelola data pribadi pengguna layanannya untuk memenuhi hak atas kenyamanan konsumen. Banyak instansi masih menggunakan pengumpulan data secara offline dengan melampirkan fotokopi dokumen pribadi. Praktik pengumpulan data offline ini tidak diatur dengan baik dalam pengumpulan, pemusnahan, dan pemulihan data pribadi.

Setiap individu memiliki hak untuk perlindungan privasi sesuai dengan Undang- Undang Dasar Negara Republik Indonesia Tahun 1945. Pasal 28G ayat (1) menyatakan bahwa setiap orang berhak mendapatkan perlindungan terhadap diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang dimilikinya, serta berhak merasa aman dan terhindar dari ancaman dan ketakutan dalam melaksanakan hak-hak asasinya. Perlindungan terhadap hak-hak pribadi ini memiliki dampak positif, termasuk meningkatkan nilai-nilai kemanusiaan, memperkuat hubungan individu dengan masyarakat, meningkatkan kemandirian dan otonomi, serta mencegah diskriminasi dan membatasi kekuasaan pemerintah. Dalam era ekonomi digital saat ini, pengguna digital, terutama pengguna telepon seluler, harus merasakan keamanan saat mengakses informasi digital untuk melindungi data-data penting. Kerugian materiil dan immateriil dapat timbul jika keamanan tidak terjamin.

IV. REGISTRASI NOMOR TELEPON SEBAGAI BENTUK PERLINDUNGAN HUKUM

Untuk menyikapi peristiwa ini, Pemerintah mengambil tindakan untuk mewajibkan pemilik nomor telepon seluler (Kartu SIM) melakukan registrasi pada Kartu SIM baru maupun yang lama sesuai dengan perintah Peratura Menteri Komunikasi dan Informatika Nomor 14 Tahun 2017 Perubahan atas Peraturan Menteri Komunikasi dan Informatika Nomor 12 Tahun 2016. [5] Sebelum adanya peraturan registrasi kartu SIM, pengguna dapat mengisi data secara sembarangan dan dapat memalsukannya, menyulitkan pelacakan pemilik kartu SIM oleh pihak berwenang. Namun, setelah diberlakukan

[5] Selvi Marlina, "Kajian Hukum Perlindungan Hak Privasi Pengguna SIM Card Terkait Registrasi SIM Card berdasarkan Permen Kominfo Nomor 14 Tahun 2017 Tentang Registrasi Pelanggan Jasa Elektronik",.

peraturan registrasi yang lebih baik, terdapat fitur pendeteksi untuk memastikan kecocokan data pribadi yang diberikan. Fitur ini diharapkan memudahkan pihak berwenang dalam melakukan pelacakan yang efektif saat diperlukan, dengan tujuan memberikan kemudahan dalam melacak pemilik kartu SIM yang digunakan untuk tindakan merugikan.

Dan juga merupakan bentuk pembatasan terhadap kepemilikan SIM card. Pemberlakuan Registrasi sim card tersebut dilakukan dengan menyertakan Nomor Induk Kependudukan (NIK) dan Nomor Karu Keluarga (KK) pada saat melakukan aktivasi pertama kali pada SIM Card.[6] Dalam hal ini, Pemerintah memberikan batasan terhadap pendaftaran NIK pada sim card sebanyak tiga kali. Apabila satu NIK sudah melakukan pendaftaran sim card sebanyak tiga kali maka NIK tersebut sudah tidak bisa digunakan untuk meregistrasi sim card.

Pemerintah memiliki kewenangan untuk mengumpulkan data warga negara demi kepentingan umum, namun pengumpulan data pribadi harus memiliki pengelolaan dan penyimpanan yang jelas. Mekanisme registrasi SIM Card di Indonesia masih rentan disiasati, menyebabkan kebocoran data pribadi. Lemahnya penegakan hukum terhadap kasus kebocoran data pribadi menjadi faktor pendukung bahwa mekanisme yang diterapkan belum efektif. Data pribadi merupakan informasi penting yang harus dilindungi oleh pemerintah untuk mencegah penyalahgunaan dan kerugian individu maupun negara. Nomor Induk Kependudukan (NIK) juga merupakan data penting yang sering digunakan dalam berbagai registrasi. Karena NIK adalah satu-satunya nomor resmi yang diberikan oleh pemerintah untuk mengidentifikasi perorangan.[7]

Dalam bidang yang berhubungan dengan keuangan contohnya yaitu pembuatan rekening bank dan e-Wallet. Penggunaan KTP dan atau KK sebagai syarat registrasi pembukaan rekening bank bertujuan untuk identifikasi terhadap satu rekeking yang akan digunakannya, dalam kemudian hari berguna apabila adanya transaaksi yang merugikan diri sendiri atau pihak lain dapat dimintai pertanggung jawaban sesuai dengan data yang diberikan diawal

---

[6] *Peraturan Mentri Komunikasi dan Informatika Nomor 23/M.KOMINFO/10/2005 Tentang Registrasi Terhadap Pelanggan Jasa Telekomunikasi*.

[7] Moh Muttaqin, "Kesadaran Pengguna Jasa Telekomunikasi Seluler dalam Melindungi Data Kependudukan Setelah Pemberlakuan Registrasi Nomor MSISDN",.

secara sadar oleh nasabah bank. Transaksi keuangan digital yang ada di Indonesia bukan hanya dibawah naungan bank. Terdapat pihak swasta yang meluncurkan banyak pilihan transaksi keuangan digital yang sudah disetujui oleh otoritas Jasa Keuangan (OJK).[8] Aplikasi yang biasa disebut dengan dompet digital atau E-Wallet merupakan aplikasi yang dapat dinikmati oleh pengguna telepon seluler yang berbasis android untuk melakukan transaksi uang elektronik.

Pengumpulan nomor ponsel yang telah didaftarkan seharusnya memberikan manfaat lebih daripada sekedar perlindungan. Pemerintah dapat menggunakannya untuk penyebaran berita penting dan urgensi kepada pemilik nomor telepon seluler, seperti peringatan cuaca buruk, tsunami, kebakaran, orang hilang, dan informasi lainnya. Kurangnya edukasi tentang perlindungan data pribadi di Indonesia menjadi perhatian. Banyak orang tidak memperhatikan perlindungan data pribadi mereka, membuatnya rentan terhadap pencurian data. Diperlukan upaya edukasi yang meningkatkan kesadaran tentang pentingnya melindungi data pribadi, terutama bagi pengguna media sosial, untuk lebih berhati-hati dalam menyimpan dan memberikan data pribadi. Perkembangan teknonologi informasi saat ini sangat kompetan untuk melakukan pencarian terhadap data apapun yang ingin didapatkan. Mulai dari pencarian atau riset, pengumpulan, penyimpanan dan pembagiannya pun dapat dilakukan secara praktis yang kemudian dapat membantu dalam pengimplementasian di kehidupan bermasyarakat.[9] Hampir seluruh lapisan masyarakat menggunakan momen ini untuk segala kepentingannya. Oleh karena itu, perlu ditelaah peraturan- peraturan yang ada di Indonesia mengenai privasi dan data pribadi yang dapat mendorong perkembangan ekonomi digital. [10] Selain itu perlu diketahui bagaimana seharusnya perlindungan privasi dan data pribadi di Indonesia dapat responsif terhadap era digital.

---

[8] Asa Intan Primanta, "Pertanggungjawaban Pidana pada Penyalahgunaan Data Pribadi" (2020) 3:4 Jurist-Diction.

[9] Glen Wijaya, "Perlindungan Data Pribadi Indonesia: Ius Constitutum dan Ius Constituendum" (2020) 19:3 Law Review.

[10] Dararida F M, Emilia Y & Lisa N A, "Consumer Protection System (CPS): Sistem Perlindungan Data Pribadi Konsumen Melalu Collaboration Concept" (2020) 3:3 Legislatif.

V. TANGGUNG JAWAB PELAKU PENYEBARAN DATA PRIBADI PENGGUNA NOMOR TELEPON SELULER

Data pribadi dapat dicuri dengan teknik pembobolan, namun tidak semua orang dapat melakukannya dengan mudah. Kebocoran nomor telepon memungkinkan penipuan dan verifikasi palsu. Pemerintah perlu mengelola nomor telepon dengan sistem yang jelas untuk mencegah kebocoran. Contoh kasus Tokopedia menunjukkan perlunya perlindungan data. Pemerintah dapat menggunakan nomor telepon untuk mengirim pesan siaran saat bencana atau pencarian orang hilang. Pentingnya pengelolaan yang baik dan keamanan yang kuat untuk mencegah kebocoran dan penyalahgunaan data pribadi. Nomor telepon memiliki manfaat positif jika digunakan dengan baik.

Tanpa disadari, penggunaan internet juga memberikan dampak negative yang membuka kesempatan sebagai sarana kejahatan (cyber crime). Cyber Crime merupakan salah satu sisi gelap dari kemajuan teknologi yang mempunyai dampak negatif sangat luas bagi seluruh bidang kehidupan modern saat ini.[11] Perbuatan melawan hukum di dunia maya (cyber crime) merupakan fenomena yang sangat mengkhawatirkan, mengingat tindakan carding, hacking, penipuan, terorisme, dan penyebaran informasi destruktif telah menjadi bagian dari aktivitas pelaku kejahatan di dunia maya.[12]

Berkaitan dengan besarnya penggunaan internet di dunia, cyber crime telah banyak terjadi dari tahun ke tahun. Khususnya di Indonesia, kejahatan cyber yang samapi saat ini menjadi problematika adalah pencurian data yang umum dilakukan dengan hacking (peretasan) dan phising. Phising yaitu aktivitas seseorang untuk mendapatkan informasi rahasia user dengan cara menggunakan situs website palsu yang menyerupai website resminya.[13]Tujuannya adalah mendapatkan identitas yang dapat digunakan secara illegal untuk mendaptkan keuntungan bagi sendirinya tanpa menggunakan identitas asli. Tercatat secara global, jumlah penipuan bermodus phising 42% dari modus selain phising yang dinyatakan dalam website Anti-Phising Working Group (APWG) dalam laporan bulannya, mencatat ada 12.845

[11] Christian Judita, *Pola Komunikasi dalam Cybercrime* (2015).
[12] Ardi Saputra G, Sahuri L & Kabib Nawawi, "Cyber Crime dalam Bentuk Pishing Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik",.
[13] *Ibid*.

e-mail baru dan unik serta 2.560 situs palsu yang digunakan sebagai sarana phising.[14]

Phising biasanya menggunakan media SMS, WhatsApp dan atau aplikasi sejenis lainnya yang terhubung dengan jaringan internet. Motifnya adalah pesan singkat yang mengarah kepada penipuan, seperti memenangkan hadiah lotre, giveaway suatu acara, ataupun sejumlah perayaan ulangtahun organisasi yang harus diklaim terlebih dahulu di sebuah link website tertera yang didalamnya ada ketentuan mengisi beberapa data pribadi yang sensitif. Link yang akan dikunjungi biasanya merupakan link yang bersifat pengisian data. Data yang diminta untuk diisi berupa nama lengkap, alamat, tanggal lahir, nomor telepon, e-mail, nomor kartu ATM, bahkan PIN ATM.[15]

Per tahun 2023 ini, bentuk phising sudah berevolusi mengikuti perkembangan zaman. Motif phising yang dilakukan belakangan ini adalah satu nomor yang mengirim dokumen dalam bentuk .apk (aplikasi) yang dikatakannya isinya adalah gambar paket bagi pemilik nomor pribadi dan atau undangan online.[16] Apabila dokumen tersebut dibuka, otomatis dapat mendownload aplikasi yang dapat berjalan dilatar belakang telepon seluler ataupun aplikasi yang dapat mendeteksi gerak teriknya telepon seluler dalam mengaksesnya. Tentunya ini dapat menyalin segala informasi yang telah diakses setelah pemasangan aplikasi tersebut. Dari sini dapat diketahui bahwasanya phising dapat menimbulkan dampak buruk yang besar, mulai dari dampak finansial hingga ancaman keamanan. Apabila pelaku phising menyerang perseorangan yang mendapatkan akses pada kartu bank, kartu kredit dan e-Wallet nya maka secara pasti akan melakukan transaksi keuangan yang tidak diinginkan. Apabila pelaku phising menyerang perusahaan, organisasi masyarakat, atau pemerintahan yang tujuannya adalah pencurian data sensitif dan bersifat

[14] Suhardi R, "Analisa Clustering Phising dengan K-Means dalam Meningkatkan Keamanan Komputer",.

[15] Michael E, "Pembobolan ATM Menggunakan Teknik Skimming Kaitannya dengan Pengajuan Restitusi", (2019).

[16] "Kasus Yang Banyak Dikeluhkan Di Twitter", online: <https://twitter.com/askDita/status/1618830855639818241?t=uTLe7B7_F4_oopBysie_IQ&s=19>.

pribadi akan berdampak pada ancaman yang mengakibatkan kerugian non materiil yang serius, seperti reputasi dan kepercayaan publik.[17]

Lemahnya sistem keamanan sistem internet sangat menentukan terhadap terjaganya data-data yang pengguna berikan dalam internet. Kejahatan lain di internet yang berkaitan dengan kebocoran data nomor telepon di Indonesia adalah pesan yang berisikan OTP (One Time Password). OTP biasanya berlaku apabila melakukan transaksi digital di internet, dan atau pada saat memasang suatu aplikasi pada ponsel dan perlu mendaftarkan akun untuk menggunakannya, aplikasi akan meminta autentifikasi sebagai bentuk keabsahan atau kebenaran bahwa perangkat yang digunakan adalah miliknya. Salah satu cara umum untuk autentifikasi adalah mengirimkan pesan lewat SMS, WhatsApp, atau e-mail pada nomor telepon yang sudah didaftarkan yang berisi kode unik atau link tertentu untuk menghubungkan ke aplikasi yang dituju yang dikirim hanya satu kali saat menyetujui untuk mengirim OTP yang bersifat rahasia.[18]

Dari berbagai bentuk penyebaran data data pribadi pengguna telepon seluler di Indonesia, pemerintah memberikan ketegasan terhadap pelaku melalui beberapa peraturan perundang-undangan. Beberapa peraturan perundang-undangan yang menyebutkan pertanggung jawaban pelaku terhadap penyebaran data pribadi pengguna telepon seluler diantaranya adalah UU Telekomunikasi, UU ITE, dan UU Perlindungan Data Pribadi. Dalam UU Telekomunikasi disebutkan jika operator telekomunikasi terbukti membuat kontrak yang mengijinkan pengaksesan data pelanggan kepada pihak lain maka dapat diberikan ancaman pidana penjara paling lama 2 tahun dan atau denda paling banyak dua ratus juta rupiah.[19]

Walau dalam UU ITE telah disebutkan bahwasanya penyelenggara sistem elektronik wajib memiliki kebijakan tata kelola, prosedur kerja pengoperasian, dan mekanisme audit yang dilakukan berkala terhadap sistem elektronik, masih dapat ditemukan sistem elektronik yang tidak memenuhi kriteria

---

[17] Lia S, "Urgensi Undang-Undang Pelindungan Data Pribadi di Indonesia: Studi Perlindungan Hukum Inggris dan Malaysia" (2019) 20:2 Kanun Jurnal Hukum.

[18] Dian Rachmawati, "Phising Sebagai Salah Satu Bentuk Ancaman Dalam Dunia Cyber" Jurnal Ilmiah Saintikom.

[19] *Pasal 57 Undang-Undang Nomor 36 Tahun 1999 Tentang Telekomunikasi*.

tersebut. Pelanggaran ini dapat dikenai sanksi berupa sanksi administratif yang diatur dalam Pasal 100 Peraturan Pemerintah PSTE yaitu teguran tertulis, denda administrative, penghentian sementara, pemutusan akses, dan atau dikeluarkan dari daftar. Adapun sanksi pidana yang diberikan terdapat di dalam Pasal 95A Undang-Undang Nomor 24 Tahun 2013 tentang Administrasi Kependudukan menyatakan bahwa "Setiap orang yang tanpa hak menyebarluaskan data kependudukan sebagaimana dimaksud dalam Pasal 79 ayat (3) dan data pribadi sebagaimana dimaksud dalam Pasal 86 ayat (1a) dipidana dengan pidana penjara paling lama 2 (dua) tahun dan/atau denda paling banyak Rp. 25.000.000,00 (dua puluh lima juta rupiah).

Pada UU Perlindungan Data Pribadi itu sendiri, disebutkan bahwasanya kartu seluler merupakan data pribadi yang dikombinasikan, yang juga merupakan salah satu data pribadi yang bersifat umum yang dilindungi.[20] Transaksi yang dilakukan melalui kartu seluler tersebut adalah data pribadi yang dilindungi, maka operator telekomunikasi yang dengan sengaja dan melawan hukum mengungkapkan data pribadi yang bukan miliknya kepada orang lain tanpa dikehendaki oleh pemiliknya dapat dipidana penjara paling lama empat tahun dan/atau pidana denda paling banyak empat miliar rupiah.[21] Dalam hal tindak pidana ini dilakukan oleh korporasi, ancaman pidana yang disebutkan di atas dapat dijatuhkan ke pengurus, pemegang kendali, pemberi perintah, dan pemilik manfaat. Khusus pidana yang dijatuhkan pada korporasi hanya pidana denda paling banyak 10 kali dari maksimal pidana denda yang diancamkan.[22]

Di sisi lain, sebenarnya pengendali data pribadi wajib memiliki dasar pemrosesan data pribadi, salah satunya adalah persetujuan yang sah secara eksplisit dari subjek data pribadi untuk sau atau beberapa tujuan tertentu yang telah disampaikan oleh pengendali data pribadi kepada subjek data pribadi Mengingat operator telekomunikasi juga merupakan pengendali data pribadi, apabila ia melakukan melakukan pemrosesan data pribadi tanpa ada dasar, ia bisa dikenakan sanksi administratif dalam Pasal 57 ayat (1) dan (2) UU PDP berupa peringatan tertulis, penghentian sementara kegiatan pemrosesan data

---

[20] *Penjelasan Pasal 4 ayat (3) huruf f pada Undang-Undang Nomor 27 Tahun 2022 Tentang Data Pribadi*.

[21] *Pasal 65 ayat (2) jo. Pasal 67 ayat (2) Undang-Undang Nomor 27 Tahun 2022 Tentang Data Pribadi*.

[22] *Pasal 20 ayat (2) Undang-Undang Nomor 27 Taun 2022 Tentang Perlindungan Data Pribadi*.

pribadi, penghapusan atau pemusnahan Data Pribadi, dan atau denda administratif. Khusus untuk denda administratif paling tinggi adalah 2 persen dari pendapatan tahunan atau penerimaan tahunan terhadap variabel pelanggaran.[23]

Kebocoran data di Indonesia mengakibatkan konsumen provider sering menerima SMS penawaran palsu dan hoaks. Pemerintah belum mengambil tindakan hukum yang tegas untuk mengatasi kebocoran ini, menyebabkan kerugian bagi pengguna seluler dan perusahaan terkait. Pelaku penyebaran data pribadi yang tidak sah juga belum mendapatkan tindakan yang memadai. Meskipun pengguna dapat memblokir nomor yang mengganggu, tetapi hal tersebut tidak efektif karena setiap hari muncul SMS serupa dengan nomor yang berbeda. Kekosongan hukum menjadi celah bagi kejahatan siber, sehingga diperlukan solusi yang lebih efektif dalam mengatasi masalah ini.

VI. KESIMPULAN

Perlindungan hukum bagi pengguna nomor telepon seluler atas penyebaran tanpa hak telah diatur sebagaimana mestinya dalam Peraturan Perundang-Undangan. Perlindungan hukum preventif yang dilakukan oleh Pemerintah berupa Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 14 Tahun 2017 Tentang Registrasi Pelanggan Jasa Telekomunikasi. Dalam peraturan ini pemerintah mengharapkan pemberlakuan registrasi pada nomor seluler dapat memberikan kemudahan dalam melakukan tracking apabila dibutuhkan. Namun, indikasi keberhasilan dari pemberlakuan registrasi nomor telepon seluler kecil. Melihat masih banyak terjadinya pencurian data yang tidak dapat dikendalikan dengan metode ini, terlebih pencurian data yang dilakukan dengan kejahatan siber.

Tanggung jawab hukum pelaku penyebaran tanpa hak atas data pribadi pengguna nomor telepon seluler diatur dalam beberapa peraturan perundang-undangan. Mulai dari sanksi bagi pelaku perorangan hingga penyedia jasa layanan komunikasi, beberapa diantaranya diatur dalam UU Telekomunikasi, UU Administrasi Kependudukan, UU Informasi dan Transaksi Elektronik, dan UU Perlindungan Data Pribadi. Meskipun demikian, penyelenggara sistem

[23] *Pasal 57 ayat (3) Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi*.

elektronik dalam hal ini Pemerintah dan penyedia jasa telekomunikasi belum mengoptimalkan penerapan regulasi yang dimaksud. Terbukti dari masih maraknya ketajahan siber seperti hacking dan phising yang dapat terjadi pada nomor telepon seluler.

VII. SARAN

Penyedia Jasa Layanan Telekomunikasi dan Pemerintah dapat melakukan Pembentukan Badan Hukum yang menangani secara khusus terhadap data pribadi dan sistem yang dapat mendeteksi terhadap keabsahan dari data yang diberikan saat melakukan registrasi nomor seluler. Sehingga apabila mengalami kejadian yang tidak diinginkan yang dialami oleh warga Negara Indonesia akibat keocoran datanya dapat mengambil tindakan yang jelas dengan melakukan pelaporan dan dijamin bahwa haknya tidak diambil secara illegal oleh orang lain.

Apabila pemerintah memiliki lembaga khusus dalam mengelola data pribadi dan sistem elektronik yang aman, maka penegakan hukum terhadap pelaku penyebaran data pribadi pengguna nomor telepon seluler dapat dilakukan dengan sebagaimana mestinya.

DAFTAR PUSTAKA

Peraturan Perundang-Undangan

Undang-Undang Dasar Negara Republik Inodesia Tahun 1945

Undang-Undang Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen. Undang-Undang Nomor 36 Tahun 1999 Tentang Telekomunikasi

Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. Undang-Undang Nomor 23 Tahun 2006 Tentang Adinistrasi Kependudukan

Undang-Undang Nomor 24 Tahun 2013 Tentang Perubahan Atas Undang-Undang Nomor 23 Tahun 2006 Tentang Administrasi Kependudukan.

Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi Peraturan Menteri Komunikasi dan Informaika Republik Indonesia Nomor 23 Tahun

2005 Tentang Registrasi Terhadap Pelanggan Jasa Telekomunikasi.

Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 20 Tahun 2016 Tentang Perlindungan Data Pribadi Dalam Sistem Elektronik.

Peraturan Menteri Komunikasi dan Informatika Nomor 12 Tahun 2016 tentang Registrasi Pelanggan Jasa Telekomunikasi sebagaimana telah diubah dengan Peraturan Menteri Komunikasi Nomor 14 Tahun 2017

Ardi Saputra Gulo, Sahuri Lasmadi, Kabib Nawawi, "Cyber Crime dalam Bentuk Phising Berdasarkan Undang- Undang Informasi dan Transaksi Elekrtronik"

Asa Intan Primanta, "Pertanggungjawaban Pidana pada Penyalahgunaan Data Pribadi", Jurist-Diction Volume 3 Nomor 4, 2020

Christian Judhita, "Pola Komunikasi dalam Cybercrime", 2015

Dararida Fandra Mahira, Emilia Yofita, Lisa Nur Azizah, "Consumer Protection System (CPS): Sistem Perlindungan Data Pribadi Konsumen Melalu Collaboration Concept", Legislatif Volume 3 Nomor 3, Juni 2020

Data penggua Telepon seluler menurut Tomato Digital Indonesia pada https://www.tomato.co.id/data-digital-indonesia-2019/

Dian Rachmawati, "Phising Sebagai Salah Satu Bentuk Ancaman Dalam Dunia Cyber", Jurnal Ilmiah Saintikom

Gaston L'Huillier, Sebastian A. Rios, Hector Alvarez, Felipe Aguilera, "Topic-Based Social Network Analysis for Virtual Communities of Interests in the Dark Web"

Glen Wijaya, "Perlindungan Data Pribadi Indonesia: Ius Constitutum dan Ius Constituendum", Law Review, Volume XIX, Nomor 3, 2020

Helmi, "Perlindungan Hukum Bagi Pengguna Jasa Operator Seluler Atas Adanya Short Message Service (SMS) Spam."

Kasus yang banyak dieluhkan di Twitter https://twitter.com/askDita/status/1618830855639818241?t=uTLe7B7_F4_oopB ysie_IQ&s=19

Lia Sautunnida, "Urgensi Undang-Undang Pelindungan Data Pribadi di Indonesia: Studi Perlindungan Hukum Inggris dan Malaysia", Kanun Jurnal Hukum Volume 20 Nomor 2, 2018

Michael Enrick, "Pembobolan ATM Menggunakan Teknik Skimming Kaitannya dengan Pengajuan Restitusi", 2019

Muttaqin, "Kesadaran Pengguna Jasa Telekomunikasi Seluler Dalam Melindungi Data Kependudukan Setelah Pemberlakuan Registrasi Nomor MSISDN."

Selvi Marlina, "Kajian Hukum Perlindungan Hak Privasi Pengguna SIM Card Terkait Registrasi SIM Card berdasarkan Permen Kominfo Nomor 14 Tahun 2017 Tentang Registrasi Pelanggan Jasa Elektronik".

Suhardi Rustam, "Analisa Clustering Phising dengan K-Means dalam Meningkatkan Keamanan Komputer"