Perlindungan Hukum Atas Kebocoran Data Pribadi Ditinjau dari Undang Undang Nomor 19 Tahun 2019 tentang Informasi dan Transaksi Elektronik dan Implementasinya terhadap Kebocoran Data Pengguna Electronic Healcth Alert Card

Herlan Solehudin[*], Neni Ruhaeni

Prodi Ilmu Hukum, Fakultas Hukum, Universitas Islam Bandung, Indonesia.

[*]herlansolehudin9@gmail.com, nenihayat@unisba.ac.id

Abstract. The government through the Ministry of Health made an eHAC (Electronic Health Alert Card) application and required people traveling outside the city to register for eHAC. Electronic Health Alert Card is an application that functions to verify passengers while traveling. Existing laws and regulations have not been effectively implemented, so there are still many cases of leakage of personal data at the practical level, including the leakage of personal data of users of the EHAC application.Based on the explanation above, this study aims to find out how the implementation of legal protection for leakage from personal users of the electronic health alert card application is reviewed from law number 19 of 2016 concerning Electronic Information and Transactions.This research method uses normative juridical and this research is Descriptive Analysis. Meanwhile, the data used in this study are secondary data obtained from the results of the literature and using the Qualitative Descriptive analysis method.So the result was obtained that the Provisions regarding Personal Data as previously stated were a provision that placed the Electronic System Provider Company as a party that was obliged to always maintain all Personal Data of its consumers. Violations of the provisions of Personal Data have been regulated by Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law).

Keywords: *Legal Protection, Victims, Information and Electronic Transaction.*

Abstrak. Pada tahun 2021 pemerintah melalui kemenkes membuat aplikasi eHAC (Electronic Health Alert Card) dan mewajibkan masyarakat yang bepergian ke luar kota wajib mendaftar eHAC. Electronic Health Alert Card merupakan aplikasi yang berfungsi untuk melakukan verifikasi penumpang selama bepergian. Aplikasi ini wajib untuk setiap wisatawan dari Negara atau wilayah tertentu yang terkena penyakit, misalnya Covid-19.. Berdasarkan pemaparan diatas, bahwa penelitian ini bertujuan untuk mengetahui bagaimana impelentasi perlindungan hukum atas kebocoran dari pribadi pengguna aplikasi electronic health alert card ditinjau dari undang undang nomor 19 tahun 2016 tentang Informasi dan Transaksi Elektronik. Metode penelitian ini menggunakan yuridis normatif dan penelitian ini bersifat Deskriptif Analisis. Sedangkan data yang digunakan dalam penelitian ini adalah data sekunder yang diperoleh dari hasil kepustakaan dan menggunakan metode analisis Deskriptif Kualitatif. Maka diperoleh hasil bahwa ketentuan-ketentuan mengenai Data Pribadi sebegaimana telah di kemukakan sebelumnya merupakan suatu ketentuan yang menempatkan. Pelanggaran terhadap ketentuan Data Pribadi telah diatur oleh Undang-Undang Nomor 19 tahun 2016 tentang Perubahan Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE).

Kata Kunci: *Perlindungan Hukum, Korban, Informasi dan Transaksi Elektronik.*

Corresponding Author
Email: nenihayat@unisba.ac.id

A. Pendahuluan

Pesatnya perkembangan teknologi telah masuk ke berbagai aspek kehidupan manusia, baik dalam aspek kehidupan sosial, budaya, ekonomi, politik, maupun hukum. Penggunaan teknologi juga telah secara signifikan mengubah pola komunikasi, interaksi, bahkan sampai dalam rangka pelayanan pemerintah kepada masyarakatnya Menurut Kotler menyatakan bahwa, "Iklan adalah segala bentuk presentasi non-pribadi dan promosi gagasan, barang, atau jasa oleh sponsor tertentu yang harus dibayar." Menurut Saladin menyatakan bahwa, "*Advertising* adalah salah satu alat promosi, biasanya digunakan untuk mengarahkan komunikasi persuasif pada pembeli sasaran dan masyarakat dimana bentuk penyajian iklan ini bersifat non-personal".

Kemajuan serta perkembangan teknologi khususnya internet sendiri telah banyak memberikan pengaruh bagi kehidupan sosial masyarakat seperti dapat dengan mudah untuk mendapatkan informasi, dapat dengan mudah berinteraksi dengan pengguna internet lainnya. Kehadiran internet saat ini dirasa telah mampu untuk memenuhi tuntutan masyarakat yang menggunakan internet. Berkembangnya internet juga menyebabkan dampak negatif bagi pengguna internet salah satunya yaitu terjadinya tindakan Kejahatan Dunia Maya (*Cybercrime)*.

Berbicara mengenai data pribadi adalah data perseorangan tertentu yang disimpan, dirawat, dan dijaga kebenaran serta dilindungi kerahasiaannya. Data perseorangan tertentu adalah setiap keterangan yang benar dan nyata yang melekat dan dapat diidentifikasi, baik langsung maupun tidak langsung, pada masing-masing individu yang pemanfaatannya sesuai ketentuan peraturan perundang-undangan.

Disisi lain hukum memungkinkan semua kepentingan dari orang (manusia, dan badan hukum/korporasi) yang telah menjadi subyek hukum itu mewujudkan diri dalam kerja sama melakukan perbuatan melawan hukum karena manusia, badan hukum tidak dapat hidup sendiri tanpa perasanan manusia /badan hukum lainnya.

Teknologi internet memudahkan kehidupan manusia, baik dalam komunikasi, melakukan transaksi elektronik, berbelanja, melakukan video *conferensi*, melakukan peradilan secara elektronik (*e-court, e-litigation*). Teknologi membuat hubungan masyarakat menjadi tidak terbatas (*borderless, cyberspace*), pengembang teknologi memiliki peluang untuk melakukan tinggi prinsip persaingan usaha sehat dan prinsip kehati-hatian (*prudential principle*). Namun, dibalik pengembangan teknologi internet yang baik, terdapat dampak negatif dari penggunaan internet yaitu:

Dampak Negatif Penggunaan Internet secara umum adalah sebagai berikut:

1. Cybercrime Adalah kejahatan yang di lakukan seseorang dengan sarana internet di dunia maya yang bersifat.
2. Melintasi batas Negara
3. Perbuatan dilakukan secara illegal
4. Kerugian sangat besar
5. Sulit pembuktian secara hukum

Bentuk-bentuk *cybercrime* sebagai berikut :

1. Hacking

Usaha memasuki sebuah jaringan dengan maksud mengeksplorasi atau mencari kelemahan system jaringan.

2. Cracking

Usaha memasuki secara illegal sebuah jaringan dengan maksud mencuri, mengubah atau menghancurkan file yang di simpan padap jaringan tersebut.

Banyak yang tidak menyadari akan pengaruh negatif internet khususnya jejaring sosial. Mungkin karena sudah kecanduan dengan internet atau jejaring sosial. Tapi justru inilah yang berbahaya, yang tidak disadari. Pengguna internet atau khususnya jejaring sosial di dominasi oleh para remaja usia 14- 24 tahun sebanyak 61,1%.

Berikut ini dampak negatif internet khususnya:

1. Tidak peduli dengan lingkungan sekitarnya. Orang yang terlalu asyik dengan dunia yang diciptakannya sendiri sehingga tidak peduli dengan orang-orang disekitarnya. Hal ini sering dilakukan orang yang kecanduan internet atau Jejaring Sosial. Tidak peduli dengan lingkungan sekitar, dunianya berubah menjadi dunia internet atau dunia maya.

2. Minimnya sosialisasi dengan lingkungan. Ini dampak dari terlalu sering dan terlalu lama bermain internet atau jejaring sosial. Ini cukup mengkhawatirkan bagi perkembangan kehidupan sosial pelajar. Mereka yang seharusnya belajar sosialisai dengan lingkungan justru lebih banyak menghabiskan waktu lebih banyak di dunia maya bersama teman teman facebook-nya yang rata rata membahas sesuatu yang nggak penting. Akibatnya kemampuan verbal pelajar menurun.
3. Boros. Akses internet khususnya untuk membuka jejaring sosial jelas berpengaruh terhadap kondisi keuangan (terlebih kalau akses dari warnet). Ini sudah bisa dikategorikan sebagai pemborosan, karena tidak produktif. Lain soal jika mereka menggunakannya untuk kepentingan bisnis.
4. Mengganggu kesehatan. Terlalu banyak melihat di depan monitor tanpa melakukan kegiatan apa pun, tidak pernah olah raga sangat beresiko bagi kesehatan. Penyakit akan mudah datang. Telat makan dan tidur tidak teratur. Obesitas (kegemukan), penyakit lambung (pencernaan), dan penyakit mata adalah gangguan kesehatan yang paling mungkin terjadi.
5. Waktu belajar berkurang. Ini sudah jelas, bagi pelajar, terlalu lama bermain internet atau jejaring sosial akan mengurangi jatah waktu belajar si pelajar. Bahkan ada beberapa yang masih asyik bermain internet saat di sekolah.
6. Kurangnya perhatian untuk keluarga Keluarga di rumah adalah nomor satu. Slogan tersebut tidak lagi berlaku bagi para pecandu internet. Buat mereka temen temen di dunia maya adalah nomor satu. Tidak jarang perhatian mereka terhadap keluarga menjadi berkurang.
7. Tersebarnya data pribadi. Beberapa pengguna jejaring sosial memberikan data mengenai dirinya dengan sangat detail. Biasanya ini untuk orang yang baru kenal di internet hanya sebatas jejaring sosial saja. Mereka tidak tahu resikonya menyebarkan data pribadi di internet. Ingat data data di internet mudah sekali bocor, apalagi yang gampang sekali di hack.

Rawan penipuan Jejaring sosial juga rawan terhadap penipuan seperti media media lainnya, Bagi si penipu sendiri, kondisi dunia maya yang serba anonim jelas sangat menguntungkan. Belakangan penipuan via facebook kian merajalela.

Pada tahun 2021 pemerintah melalui kemenkes membuat aplikasi eHAC (*Electronic Health Alert Card*) dan mewajibkan masyarakat yang bepergian ke luar kota wajib mendaftar eHAC. *Electronic Health Alert* Card merupakan aplikasi yang berfungsi untuk melakukan verifikasi penumpang selama bepergian. Aplikasi ini wajib untuk setiap wisatawan dari Negara atau wilayah tertentu yang terkena penyakit, misalnya Covid-19. Pemerintah Indonesia mewajibkan masyarakat untuk mengisi data di aplikasi eHAC sebagai upaya untuk mendeteksi, mencegah, dan mengendalikan Kedaruratan Kesehatan Masyarakat melalui Titik Masuk (Bandara, Pelabuhan, dan Pos Perbatasan Daratan).

Mengutip panduan pengguna Aplikasi eHAC adalah Kartu Kewaspadaan Kesehatan, merupakan versi modern dari kartu manual yang digunakan sebelumnya. Untuk diketahui, sistem e-HAC dikembangkan oleh Kementerian Kesehatan Indonesia (Kemenkes RI), dalam hal ini Direktorat Surveilans dan Karantina Kesehatan, Direktur jenderal Pencegahan dan Pengendalian Penyakit, untuk menjawab tantangan di era digital.

Mengisi eHAC merupakan salah satu syarat wajib untuk melakukan perjalanan selama masa pandemi Covid-19. eHAC atau electronic-Health Alert Card (e-HAC) ialah Kartu Kewaspadaan Kesehatan Elektronik yang ditujukan pada semua pelaku perjalanan domestik dan internasional selama pandemi Covid-19.

Pemerintah Indonesia pernah membuat aplikasi (e-HAC) Kesehatan namun pada tanggal 2 juli 2021 aplikasi tersebut sudah tidak dipergunakan dan pemerintah menghimbau untuk meng *uninstall* aplikasi tersebut, akan tetapi tidak ada tindak lanjut dalam pengamanan data yang sudah ada, padahal dalam ketentuan undang-undang seharusnya pemerintah lebih menindak lanjuti hal tersebut.

Menurut VPN Mentor, mereka mengugkapkan data eHAC yang bocor sebesar 2 Gigabyte. Jumlah data warga Indonesia dan warga Negara asing yang menginstal eHAC dan

bocor diperkirakan mencapai lebih dari 1.4 juta orang. Sedangkan data eHAC yang terekspos saat ini mencapai 1.3 juta orang. Maraknya kasus kebocoran data ini menunjukkan lemahnya proteksi data pribadi di Negeri ini. Kabarnya, di kalangan peretas, situs-situs milik Pemerintah Indonesia memang dikenal "mudah dibobol". Kebocoran data pribadi ini akan terus terjadi selama pengelolaan dilakukan serampangan dan mengabaikan aspek keamanan.

B. Metodologi Penelitian

Berdasarkan pemaparan diatas, bahwa penelitian ini bertujuan untuk mengetahui bagaimana impelentasi perlindungan hukum atas kebocoran dari pribadi pengguna aplikasi electronic health alert card ditinjau dari undang undang nomor 19 tahun 2016 tentang Informasi dan Transaksi Elektronik.

Metode penelitian ini menggunakan yuridis normatif dan penelitian ini bersifat Deskriptif Analisis. Sedangkan data yang digunakan dalam penelitian ini adalah data sekunder yang diperoleh dari hasil kepustakaan dan menggunakan metode analisis Deskriptif Kualitatif.

C. Hasil Penelitian dan Pembahasan

Dalam laporan yang dirilis ke khalayak umum, VPN Mentor menyebut pihaknya menemukan data-data eHAC tanpa rintangan pada 15 Juli 2021. Menurut VPN Mentor, pembuat aplikasi menggunakan database *Elasticsearch* yang tidak dienskripsi dan tidak memiliki tingkat keamanan yang rumit sehingga mudah dan rawan diretas.

Pemerintah melalui Kementrian Kesehatan membuat aplikasi eHAC (*Electronic Health Alert Card*) dan mewajibkan masyarakat yang bepergian ke luar kota wajib mendaftar eHAC. *Electronic Health Alert* Card merupakan aplikasi yang berfungsi untuk melakukan verifikasi penumpang selama bepergian. Aplikasi ini wajib untuk setiap wisatawan dari Negara atau wilayah tertentu yang terkena penyakit, misalnya Covid-19. Pemerintah Indonesia mewajibkan masyarakat untuk mengisi data di aplikasi eHAC sebagai upaya untuk mendeteksi, mencegah, dan mengendalikan Kedaruratan Kesehatan Masyarakat melalui Titik Masuk (Bandara, Pelabuhan, dan Pos Perbatasan Daratan).

Mengutip panduan pengguna Aplikasi eHAC adalah Kartu Kewaspadaan Kesehatan, merupakan versi modern dari kartu manual yang digunakan sebelumnya. Untuk diketahui, sistem e-HAC dikembangkan oleh Kementerian Kesehatan Indonesia (Kemenkes RI), dalam hal ini Direktorat Surveilans dan Karantina Kesehatan, Direktur jenderal Pencegahan dan Pengendalian Penyakit, untuk menjawab tantangan di era digital.

Mengisi eHAC merupakan salah satu syarat wajib untuk melakukan perjalanan selama masa pandemi Covid-19. eHAC atau electronic-Health Alert Card (e-HAC) ialah Kartu Kewaspadaan Kesehatan Elektronik yang ditujukan pada semua pelaku perjalanan domestik dan internasional selama pandemi Covid-19.

Data yang bocor tidak hanya mengungkap data pribadi 1,3 juta pengguna eHAC, menurut VPN Mentor. Kebocoran ini juga mengungkap seluruh infrastruktur seputar eHAC, termasuk catatan pribadi dari berbagai rumah sakit hingga tenaga kesehatan yang menangani pelaku perjalanan.

Pada Mei 2021, data sekitar 279 juta warga Indonesia termasuk mereka yang sudah meninggal dunia diduga diretas dan dijual di forum daring. Data itu diduga berasal dari badan penyelenggara layanan kesehatan, BPJS Kesehatan.

Lantas pada Mei tahun lalu, data kependudukan milik sekitar 2,3 juta warga Indonesia yang memuat nomor induk kependudukan (NIK) serta nama dan alamat lengkap, diduga bocor dan dibagikan lewat forum komunitas hacker. Data itu diduga bersumber dari Komisi Pemilihan Umum (KPU).

Adapun Informasi Pengguna Yang Bocor Di eHAC Mencakup Antara Lain:

1. Data tes Covid-19
2. Kartu identitas pelaku perjalanan
3. Identitas rumah sakit
4. Nomor antrean

5. Nomor referensi
6. Alamat
7. Tipe tes Covid (PCR, rapid antigen, lainnya), tanggal dan lokasi
8. Hasil tes Covid dan tanggal dikeluarkan
9. Identitas dokumen eHAC

Kebocoran Juga Mencakup Data Dari 226 Rumah Sakit Dan Klinik Di Indonesia:

1. Rincian rumah sakit (nama, nomor lisensi, lokasi pasti dilengkapi koordinat, nomor WhatsApp, jam operasional).
2. Nama penanggung jawab bagi pelaku perjalanan
3. Nama dokter yang menangani sang pelaku perjalanan
4. Daya tampung rumah sakit
5. Jenis tes yang dilakukan rumah sakit tersebut
6. Jumlah tes yang dilakukan setiap hari
7. Jenis pelaku perjalanan yang ditangani rumah sakit tersebut

Identitas Pengguna Pun Bocor, Antara Lain:

1. Detail pelaku perjalanan (nomor paspor/KTP, nama lengkap, nomor telepon, pekerjaan, jenis kelamin, dan lainnya)
2. Paspor dan foto profil di akun eHAC
3. Detail hotel pelaku perjalanan
4. Detail tentang akun eHAC perjalanan dan kapan dibuat.

Dalam sebuah laporannya mereka mengemukakan telah menemukan adanya kebocoran data pada aplikasi eHAC yang digunakan sebagai *'test and trace'* bagi orang-orang yang masuk ke Indonesia untuk memastikan mereka tidak membawa virus. Vpn mentor memaparkan kebocoran data ini mengekspos seluruh infrastruktur di sekitar eHAC, termasuk catatan pribadi dari rumah sakit dan pejabat Indonesia yang menggunakan aplikasi tersebut. Vpn mentor juga menunjukkan data-data pribadi yang bocor tersebut mulai dari nomor identitas, telepon, serta detail mengenai hasil tes COVID-19 dan sejumlah tempat yang dikunjungi.

Kebocoran data ini disebutnya sebagai ancaman nyata terhadap privasi warga negara. Data mereka dapat diperjualbelikan, sehingga seseorang tidak lagi punya kedaulatan atas data dan kehidupan pribadinya karena rentan disalahgunakan.

Kepala Pusat Data dan Informasi Kemenkes Anas Ma'ruf dalam kesempatan yang sama mengatakan dugaan kebocoran data pada aplikasi eHAC kemungkinan disebabkan adanya kebocoran pada pihak mitra pemerintah.

Sebagai langkah mitigas atas adanya dugaan kebocoran data ini, kata Anas, eHAC yang lama sudah dinonaktifkan. Sementara eHAC yang baru tetap dilakukan dan terintegrasi atau berada dalam aplikasi PeduliLindungi. Anas menjamin eHAC yang baru dan terintegrasi dengan PeduliLindungi itu telah dijaga keamanan datanya. Data tersebut semuanya satu paket dengan seluruh informasi tentang pengendalian COVID-19 yang ada di Pusat Data Nasional.

Namun hal ini menyadarkan kita tentang kurang terjaminnya perlindungan terhadap data pribadi seseorang. Perlindungan terhadap keamanan informasi pribadi pengguna jasa internet sangat diperlukan, hal ini dikarenakan data pribadi tersebut merupakan *privacy* seseorang yang apabila disalahgunakan akan merugikan pemilik data yang diretas tersebut terlebih lagi apabila informasi tersebut digunakan untuk menguntungkan kepentingan bisnis ataupun dengan tujuan melakukan suatu perbuatan melawan hukum.

Dalam Penjelasan Umum Undang-undang informasi dan transaksi elektronik ditegaskan pemanfaatan teknologi informasi tanpa mengabaikan perlindungan data pribadi sebagai bagian dari hak pribadi. Dengan begitu, kasus penyalahgunaan data pribadi masyarakat oleh pihak tidak bertanggungjawab tidak terlepas dari kelalaian pemerintah dalam menjamin perlindungan hak pribadi masyarakat.

Seyoginya *Electronic Health Alert Card* atau eHAC Indonesia yang merupakan kartu kewaspadaan kesehatan dalam bentuk digital adalah aplikasi seluler milik Kementerian Kesehatan Republik Indonesia yang memberikan layanan pelaporan perjalanan Warga Negara Indonesia (WNI) atau Warga Negara Asing (WNA) di Indonesia, dengan tujuan untuk melakukan pendataan dan pemantauan terhadap risiko kesehatan masyarakat terutama

penyebaran penyakit infeksi emerging selama berada di wilayah Indonesia. Aplikasi eHAC berjalan pada dua platform yaitu Android dan iOS. Pengguna aplikasi eHAC Indonesia adalah WNI atau WNA yang sedang/akan melakukan perjalanan ke luar negeri dan di wilayah Indonesia, pekerja migran Indonesia, dan pengguna umum lainnya, tidak terbatas pada individu yang akan/sedang melakukan perjalanan di luar negeri dan dalam negeri.

Perlindungan Hukum Atas Kebocoran Data Pribadi Ditinjau Dari Undang–Undang Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik

Upaya perlindungan hukum dalam teori dan praktik hukum terdapat 2 (dua) macam, yaitu upaya hukum biasa dan upaya hukum luar biasa. Perbedaan antara keduanya adalah bahwa dalam upaya hukum biasa, eksekusi ditangguhkan kecuali dakwaan diberikan terhadap suatu keputusan. Sebaliknya, upaya hukum luar biasa tidak menangguhkan eksekusi.

Undang undang informasi dan transaksi elektronik telah memberikan definisi atas tindak penyalahgunaan data pribadi dalam media elektronik, yaitu sebagai tindakan dengan sengaja mengakses komputer dan/atau sistem komputer milik orang lain secara tidak sah dan tanpa izin dengan bermaksud untuk mendapatkan Informasi Elektronik dan/atau Dokumen Elektronik serta melakukan pembobolan atas sistem keamanan komputer tersebut.

Istilah mengakses dalam definisi ini adalah istilah yang sangat populer digunakan dalam bidang Informasi dan Transaksi Elektronik (selanjutnya disebut ITE). Kata dasar mengakses adalah akses. Undang-undang informasi dan transaksi elektronik memberi tafsir otentik tentang akses, yaitu sebuah kegiatan melakukan interaksi dengan sistem elektronik yang berdiri sendiri atau jaringan.

Dalam Pasal 30 UU ITE menitik beratkan kepada para pelaku peretasan (*Hacker*). Sebagai upaya perlindungan hukum represif yang di tujukan untuk para konsumen agar ada kepastian hukum ketika Data Pribadi yang mereka miliki di gunakan secara melawan hukum demi kepentingan-kepentingan tertentu

Dalam pasal 26 ayat 4 undang undang transaksi elektronik tahun 2016 menjelaskan bahwa: “Setiap penyelenggara sistem elektronik wajib menghapus informasi elektronik dan/atau Dokumen elektronik yang tidak relevan yang berada dibawah kendalinya atas permintaan orang yang bersangkutan berdasarkan penepatan pengadilan.”

Implementasi Perlindungan Hukum Atas Kebocoran Data Pribadi Undang–Undang Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik Terhadap Pengguna Aplikasi Ehac (Electronic Health Alert Card) Di Indonesia

Pasal 31 merumuskan dua bentuk tindak pidana ITE, sebagaimana dalam ayat 1 dan ayat 2. Ancaman pidana nya dirumuskan dalam pasal 47. Bila dirumusan tindak pidana pasal 31 yang dirumuskan dalam satu naskah dengan pasal 47 selengkapnya sebagai berikut.

1. Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakuknan intersepti atau penyadapan atas Informasi Elektronik dan/atau Dokumen Elektronik dalam suatu komputer dan/atau Sisterm Elektronik tertentu milik orang lain, dipadana dengan pidana penjara paling lama 10 tahun dan/atau dengan paling banyak Rp 800.000.000 (delapan ratus juta rupiah).
2. Dipidana yang sama seperti ayat pertama, setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atas transmisi Informasi Elektronik dan/atau Dokumen Elektronik yang tidak bersifat publik dari, ke, dan didalam suatu Komputer dan/atau Sistem Elektronik tertentu milik orang lain, baik yang tidak menyebabkan perubahan apapun maupun yang menyebabkan adanya perubahan, penghilangan, dan/atau penghentian informasi Elektronik dan/atau Dokumen Elektronik yang ditransimisikan.
3. Kecuali intersepsi sebagiamana dimaksud pada ayat 1 dan 2, intersesi yang dilakukan dalam rangka penegakan hukum atas permintaan kepolisian, kejaksaan, dan/atau institusi penegak hukum lainnya yang ditetapkan berdasarkan undang-undang.
4. Ketentuan lebih lanjut mengenai tata cara intersepsi sebagaimana dimaksud pada ayat 3 diatur dengan peraturan pemerintah.

Tindak Pidana Intersepsi Pasal 31 Ayat 1

Tindak pidana intersepsi yang pertama terdiri dari unsur unsur berikut:

1. Kesalahan (dengan sengaja)
2. Melawan hukum (tanpa hak atau melawan hukum)
3. Perbuatan (intersepsi atau penyadapan)
4. Objek (Informasi Elektronik dan/atau Dokumen Elektronik dalam Komputer dan/atau sisterm elektronik tertentu milik orang lain.

Mengenai dua macama sifat melawan hukumnya perbuatan (objektif dan subjektif) ini wajib di buktikan oleh Jaksa. Pertama bahwa informasi elektronik dan/atau Dokumen Elektronik dalam komputer dan/atau sistem elektronik yang disadap milik orang lain (Objektif). Milik orang lain harus diartikan bukan miliknya. Orang disini harus diartikan secara luas, termasuk korposasi/badan. Milik korporasi/atau badan termasuk badan hukum (*rechtpersoon*) juga disebut bukan milik si pembuat. Kedua, tidak adanya ijin dari si pemilik komputer atau sisterm elektronik. Kemudian dibuktikan bahwa ketika perbuatan dilakukan, jiwa si pembuat dalam keadaan normal. Hanya orang yang berjiwa normal saja yang dapat meyadari perbuatan yang dilakukannya sebagai tercela atau melawan hukum. Oleh karena berjiwa normal maka si pembuat menyadari bahwa perbuatannya mengandung sifat celaan, terlarang atau melawan hukum.

D. Kesimpulan

Berdasarkan pembahasan dalam penelitian ini, peneliti menyimpulkan beberapa hasil penelitian sebagai berikut:

1. Diperlukannya kepastian hukum oleh Lembaga Pemerintah bagi korban tindak pidana kebocoran data pribadi lebih lanjut. Karena di Negara Indonesia belum adanya hukum yang mengatur secara kongkrit mengeai perlindungan data milik pribadi. Indonesia belum memiliki Undang-undang yang khusus membahas mengenai privasi dan perlindungan data pribadi. Tetapi perlindungan privasi dan data pribadi dapat ditemukan di beberapa peraturan perundangundangan. Khusus untuk perlindungan data pribadi yang secara spesifik berada di lingkup media elektronik terdapat dalam Pasal 26 Undang undang No. 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE).
2. Penyalahgunaan data pribadi merupakan perbuatan yang memenuhi unsur-unsur perbuatan pidana seperti unsur tindak pidana pencurian dan unsur tindak pidana penipuan serta tindak pidana lainnya baik dari sisi unsur objektif maupun unsur subjektif. Dengan terpenuhinya unsur-unsur tersebut, maka sanksi administratif, sanksi perdata maupun sanksi pidana belum cukup untuk mengakomodir tindak pidana penyalahgunaan data pribadi yang senyatanya merupakan bentuk kejahatan yang sempurna.

Acknowledge

Pertama peneliti mengucapkan syukur atas terlaksananya penelitian ini dalam membahas perlindungan hukum atas kebocoran data pribadi ditinjau dari undang undang nomor 9 tahun 2016 tentang informasi dan transaksi elektronik. Tak lupa terimakasih kepada orang tua, keluarga serta dosen fakultas hukum UNISBA yang telah membimbing selama penelitian ini berlangsung. Sangat diharapkan apabila ada saran di penelirian ini. Peneliti ucapkan terima kasih.

Daftar Pustaka

[1] Rachel Silcock. 2001. What Is e-Government. Parliamentary Government

[2] Alcianno G. Gani “Pengenalan Teknologi Internet Serta Dampaknya” Jurnal Vol 2 No 2

[3] Soerjono Soekanto dan Sri Mamudji, Penelitian Hukum Normatif Suatu Tinjauan Singkat, Rajawali Pers, Jakarta, 2010

[4] Wahyu Sasongko, Ketentuan-ketentuan Pokok Hukum Perlindungan Konsumen. Universitas Lampung, Bandar Lampung, 2007

[5] Rohaedi, Rosalia Alima Utami. (2021). *Tanggung Jawab Bank terhadap Simpanan Deposito Berjangka yang Tidak Tercatat dihubungkan dengan Perlindungan Hukum*

Nasabah menurut Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan. Jurnal Riset Ilmu Hukum, 1(1), 44-51.

[6] R Abdoel Jamal, "Pengantar Hukum Indonesia", PT Raja Grafindo Persada, Jakarta

[7] Satijipto Raharjo, Ilmu Hukum, (Bandung: PT Citra Aditya Bakti, 2000)

[8] Undang undang nomor 19 tahun 2016 tentang informasi dan transaksi elektronik