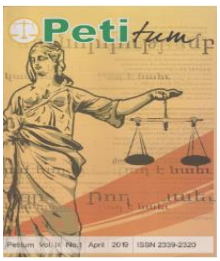

PETITUM
https://uit.e-journal.id/JPetitum
Vol 10, No, 1, April 2022 pp, 70-76
p-ISSN:2339-2320 dan e-ISSN: 2716-0017

Tinjauan Yuridis Perlindungan Data Pribadi Terkait Kebocoran Data Dalam Ruang *Cyber Crime*

Bolu HB[1], Djaenab [2]

[1] Fakultas Hukum, Universitas Islam Makassar, Email: hb.hasanbasri.dty@uim-makassar.ac.id
[2] Fakultas Agama, Universitas Islam Makassar, Email: djaenabusman20@gmail.com

Artikel info

Artikel history:
Received: 29-06-2022
Revised: 04-07-2022
Published: 24-07-2022

Keywords:
Legal Protection, Personal Data Leakage, Cyber Crime.

Kata Kunci:
Perlindungan Hukum, Kebocoran Data Pribadi, Cyber Crime.

ABSTRACT: *The research method in this thesis uses a method with a Normative Legal Research Approach which refers to the amalgamation of the statutory approach and the case approach. The sources of data used in this study are secondary data. Data collection techniques in this study were carried out by literature study of legal materials and secondary data sources. Analysis of the data used in this study is the analysis of qualitative data obtained by a systematic process. Based on the research results obtained from the decision of the criminal case no. 1229/Pid.Sus/2020/PN Mks, shows that the cause of the leakage of personal data is the negligence of the Electronic System User and the intelligence of the perpetrators of criminal acts. The settlement of cases is by the ITE Law, but these rules have not been able to have a major effect on technology users in protecting personal data leakage.*

ABSTRAK: Metode penelitian dalam skripsi ini menggunakan metode dengan Pendekatan Penelitian Hukum Normatif yang mengacu pada penggabungan pendekatan perundang-undangan *(statute approach)* dan pendekatan kasus *(case approach)*. Sumber data yang digunakan dalam penelitian ini adalah data sekunder. Teknik pengumpulan data dalam penelitian ini dilakukan dengan studi pustaka terhadap bahan-bahan hukum sumber data sekunder. Analisis data yang digunakan dalam penelitian ini adalah analisis data kualitatif yang diperoleh dengan proses sistematis. Berdasarkan hasil penelitian yang diperoleh dari putusan perkara pidana No. 1229/Pid.Sus/2020/PN Mks, menunjukkan bahwa penyebab terjadinya kebocoran data pribadi adalah kelalaian Pengguna Sistem Elektronik dan kecerdasan pelaku tindak pidana. Penyelesaian perkara sesuai dengan Undang-Undang ITE, namun aturan tersebut belum mampu memberikan efek yang besar terhadap pengguna teknologi dalam perlindungan kebocoran data pribadi. pelaku usaha yang tidak terdaftar sehingga upaya untuk menemukan pemilik barang sangat susah teridentifikasi.

Coresponden author:
Email: hb.hasanbasri.dty@uim-makassar.ac.id

PENDAHULAN

Memasuki era revolusi industri 5.0, perkembangan teknologi komputer, telekomunikasi dan informasi telah berjalan sedemikian rupa sehingga pada saat ini sudah sangat jauh berbeda dengan puluhan tahun yang lalu. Pemanfaatan teknologi tersebut telah mendorong pertumbuhan bisnis yang pesat, karena berbagai informasi telah disajikan dengan canggih dan mudah diperoleh. Dengan memanfaatkan teknologi telekomunikasi dalam hubungan jarak jauh, pihak-pihak yang terkait dalam transaksi tidak perlu bertemu *face to face* untuk perencanaan langkah bisnis selanjutnya, cukup melalui peralatan komputer dan telekomunikasi. Kondisi yang demikian merupakan pertanda dimulainya era siber dalam bisnis.

Dampak positif tersebut tidak berlangsung demikian, di sisi lain timbul pikiran pihak-pihak lain yang dengan itikad tidak baik mencari keuntungan dengan melawan hukum, yang berarti melakukan pelanggaran dan kejahatan (Suparni, 2009). Hal inilah yang menjadi dasar timbulnya salah satu cyber crime saat ini, yaitu kebocoran data. Kebocoran data atau data leakage merupakan salah satu bentuk cyber crime. Cyber crime atau kejahatan dunia maya masih banyak terjadi akibat lemahnya regulasi hukum di Indonesia. Jika permasalahan kita terus berpatokan pada kekuatan hukum saat ini, sebaiknya melihat siklus kebocoran data selama dua tahun terakhir.

Dilansir dari CNN, pada tahun 2020 kurang lebih sebanyak 404.249.978 juta pengguna data mengalami kasus kebocoran data (Tim CNN, 2020). Sedangkan di tahun 2021 kurang lebih sebanyak 282.430.002 yang dipublikasi oleh Techbiz.go.id, belum dengan angka kebocoran data lainnya yang tidak dipublikasi (Khairuddin, 2021). Maraknya kasus kebocoran data pribadi yang signifikan terus berlanjut tersebut menandakan data penduduk Indonesia rawan disalahgunakan sebab lemahnya regulasi hukum pada aspek cyber space atau dunia siber lantaran belum adanya regulasi perlindungan data pribadi yang lebih spesifik. Berdasarkan latar belakang masalah di atas, maka penulis memilih judul 'Tinjauan Yuridis Perlindungan Data Pribadi Terkait Kebocoran Data Dalam Ruang *Cyber Crime*.

METODE PENELITIAN

Penulis memilih metode dan pendekatan penelitian hukum normatif ini dengan menggabungkan pendekatan perundang-undangan (statute approach) dan pendekatan kasus (case approach). Pendekatan perundang- undangan (statute approach) merupakan pendekatan yang objek penelitiannya undang-undang, peneliti menelaah peraturan perundang-undangan dan regulasi yang sifatnya comprehensive (norma hukum di dalamnya saling berkaitan), all-inclusive (norma hukum yang ada mampu menampung permasalahan hukum. Sehingga tidak ada kekurangan hukum) dan systematic (norma hukum tersusun secara hierarki) yang bersangkutan dengan isu hukum yang dihadapi hukum, sedangkan pendekatan kasus (case approach) merupakan pendekatan yang objek penelitiannya kasus- kasus yang telah menjadi putusan pengadilan yang berkekuatan tetap, penulis melakukan telaah terhadap kasus-kasus yang berkaitan dengan isu yang dihadapi.

HASIL DAN PEMBAHASAN

A. Penyebab Terjadinya Kebocoran Data Pribadi Dalam Ruang *Cyber Crime*

Kehidupan seseorang seakan transparan sebab kepercayaan akan tujuannya mengumbar kehidupan pribadi di sosial media. Dalam banyak hal, media online sangat bermanfaat seperti persaingan ilmu manajemen media, pasar online (*e-commerce*), dan yang terutama menjadi sumber informasi ter-update. Sayangnya, masih banyak orang yang memuat privasinya di berbagai kancah media online, mayoritas di antaranya karena lalai atau tidak tahu menahu terhadap akibat atau ancaman apa saja yang dapat ditimbulkan kedepannya jika mengumbar privasi. Berbagai ekspresi yang dipertunjukkan di ranah media online seperti facebook, instagram, twitter, youtube, tiktok, game dan berbagai aplikasi ataupun media sosial lainnya rentan terhadap pengaruh buruk, bahkan diskriminasi sosial kerap terjadi. Hal ini bermula dari 'bad mind' sehingga menyebabkan terjadinya kejahatan dalam dunia siber *(cyber crime)*, salah satunya kebocoran data (data leakage).

Pembahasan di atas tersebut memberikan gambaran perkembangan sosial globalisasi dan kemajuan teknologi informasi 2yang akan terus berkelanjutan dan menjadi konsumsi manusia. Teknologi memberikan tuntutan dalam berbagai sendi kehidupan, mulai dari keperluan hidup hingga keamanan elektronik sebagai bentuk perlindungan penggunaan media elektronik. Jika melihat Ius Constitutum (hukum yang berlaku) negara kita saat ini, kita sebaiknya mempertimbangkan Ius Constituendum (Arief Mansur & Gultom, 2005) (hukum yang harus ditetapkan). Sangat perlu menetapkan hukum yang lebih komprehensif dengan memuat khusus perlindungan data pribadi sebab undang-undang siber yang sampai sekarang kita gunakan masih tergolong umum fungsinya, belum merujuk pada perlindungan data pribadi secara spesifik, yaitu Undang-Undang No. 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang No. 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik dan aturan turunannya. Berdasarkan hasil kajian pustaka putusan Pengadilan Negeri Makassar terkait jenis perkara ITE ada sebanyak 19 putusan di tahun 2019, sebanyak 19 putusan di tahun 2020, dan sebanyak 20 putusan di tahun 2021, dengan begitu ada selisih satu putusanperkara di antara tahun 2020 dan tahun 2021. Merujuk pada pembahasan rumusan masalah pertama, yaitu penyebab terjadinya kebocoran data pribadi dalam ruang *cyber crime*. Peneliti mengambil satu sampel kasus terkait kebocoran data yang terjadi pada tahun 2020.

Perkara dengan Nomor Putusan 1229/Pid.Sus/2020/PN Mks. (Direktori Putusan Mahkamah Agung RI, 2020) Nama terdakwa : Akbar Bin Rusli. Locus Delicti : Jl. Mawar Blok FG No.5 Nusa Tamalanrea Indah, Kel. Kapasa, Kec.Tamalanrea, Kota Makassar.Tempus Delicti : Kamis, 4 Juni 2020 sekitar pukul 14.00 wita saat tim Subdit V Cyber Crime Dit Reskrimsus Polda Sulsel melakukan patrol tentang maraknya tindak pidana carding.

Penulis terbatas mengikuti Jan Remelink mengidentifikasi teori kausalitas atau teori sebab akibat sebagai salah satu teori hukum dalam hukum pidana. Teori kausalitas digunakan agar dapat menjawab persoalan siapa yang dapat dimintai pertanggungjawaban atas akibat dari suatu perbuatan pidana. (Gede Atmadja & Putu Budhiarta, 2018) Merujuk pada perkara nomor putusan 1229/Pid.Sus/2020/PN Mks, dalam kausalitas perkaranya

Sebab :

Terdakwa melakukan tindak pidana ITE dengan menggunakan kartu kredit atau Credit Card (CC) milik orang lain untuk melakukan pembelian top up diamond game, top up gift bigo dan top up coin line atau yang lebih dikenal dengan nama carding.

- Terdakwa menggunakan laptop miliknya yang bermerek asus dalam melancarkan aksinya.
- Terdakwa melakukan spam dengan cara mengirim kata-kata yang berisikan link phising menggunakan email orang asing (resultUki@yandex.com) yang dicuri atau diambil alih dari pemilik email, yakni seseorang bernama Uki.
- Terdakwa mendapatkan data credit card orang lain dengan cara mengarahkan target yang menerima link untuk mengisi data email dan informasi data kartu kredit pribadinya, setelah target mengisi data-data tersebut dan dikirim akan tersimpan otomatis di email yang dicuri tadi.

Data credit card yang terdapat pada email tadi, yaitu nomor kartu kredit, masa aktif kartu kredit, CVV (Card Verification Number), nama dan alamat pemilik kartu kredit.

Kemudian terdakwa melakukan top up dengan masuk ke aplikasi line, bigo dan game menggunakan pembayaran yang melalui kartu kredit dengan cara memasukkan data nomor kartu kredit, yakni CVV Number (Card Verification Value Number) yang sudah tersimpan pada email tadi. Keuntungan dari top up game dan bigo, yaitu untuk kesenangan pribadi terdakwa sedangkan top up coin line dilakukan oleh terdakwa untuk dijual kembali.

Akibat :

Tagihan top up diamond game, top up coin line dan top up gift bigo dibebankan kepada si pemilik kartu kredit. Perbuatan terdakwa telah merugikan orang lain (pemilik email dan pemiliki data credit card) secara materiil. Sehingga terdakwa terbukti secara sah dan meyakinkan bersalah dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik dengan cara apapun dengan tujuan untuk memperoleh informasi elektronik dan/atau dokumen elektronik sesuai Pasal 30 Ayat (2) UU No.19 Tahun 2016 Tentang Perubahan atas UU No.11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik.

Kemungkinan yang dapat terjadi dalam proses dilakukannya tindak pidana carding berdasarkan kajian dan analisis kasus di atas, yakni awal mula email korban diretas yaitu dengan cara meminta kode OTP (On Time Password) melalui nomor telepon korban yang tertaut dengan email korban. Terdapat dua opsi untuk mendapatkan kode OTP tersebut, yaitu menggunakan pesan teks dan menggunakan panggilan telepon. Jalur yang paling mudah digunakan pelaku adalah jalur telepon. Jika menggunakan jalur telepon, korban meminta kode OTP melalui telepon, kemudian pelaku melakukan pengalihan panggilan dari nomor telepon korban untuk dialihkan ke nomor telepon pelaku sehingga kode OTP tersebut diterima secara langsung oleh pelaku. Untuk mendapatkan data pribadi korban, pelaku menggunakan verifikasi keamanan yang dimana setiap aplikasi dapat diketahui kata sandinya dari kode OTP tersebut.

B. Bentuk Perlindungan Hukum Data Pribadi Sebagai Upaya Menanggulangi Kebocoran Data Dalam Ruang *Cyber Crime*

Dalam penyelesaian perkara tindak pidana carding ini, setelah ditentukan jenis dakwaan perkara adalah dakwaan tunggal, terdakwa telah terbukti memenuhi unsur-unsur dari rumusan pasal yang didakwakan, yaitu :

Setiap orang. Sengaja dan tanpa hak atau melawan hukum. Mengakses komputer dan/atau sistem elektronik dengan cara apapun dengan tujuan untuk memperoleh informasi elektronik dan/atau dokumen elektronik. Terdakwa telah diadili dan terbukti secara sah dan meyakinkan bersalah melanggar Pasal 46 Ayat (2) Jo. Pasal 30 Ayat (2) UU No.19 Tahun 2016 Tentang Perubahan atas UU No.11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik (ITE).

Sebagaimana terdakwa dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik dengan cara apapun dengan tujuan untuk memperoleh informasi elektronik dan/atau dokumen elektronik sesuai Pasal 30 Ayat (2) UU No.19 Tahun 2016 Tentang Perubahan atas UU No.11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik.

Terdakwa dijatuhi pidana penjara selama 8 (delapan) bulan dan denda sebesar Rp 10.000.000.- (sepuluh juta rupiah), bila tidak dibayar diganti dengan kurungan selama 2 (dua) bulan. Dalam Pasal 46 Ayat (2) Undang-Undang ITE diuraikan sanksi pelanggaran Pasal 30 Ayat (2), yaitu pidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp 700.000.000,00 (tujuh ratus juta rupiah), namun alasan penjatuhan pidana penjara dan denda dalam putusan tersebut lebih kecil daripada sanksi yang terdapat di dalam Pasal 46 Ayat (2) UU ITE adalah karena hakim dalam memutus perkara wajib mempertimbangkan tuntutan yang didakwakan oleh jaksa penuntut umum (JPU) sebagaimana kaidah hukum yang diangkat sebagai dasar pemeriksaan oleh hakim dalam mengadili suatu perkara pidana harus sesuai dengan kaidah hukum yang ada pada surat dakwaan. Dalam memberikan penuntutan, jaksa penuntut umum tidak boleh melewati batas maksimal sanksi yang terdapat pada suatu pasal. Sebelum mengadili atau menjatuhkan putusan kepada terdakwa, hakim terlebih dahulu mempertimbangkan hal yang memberatkan dan hal yang meringankan terdakwa.

Hakim telah menetapkan masa penahanan terdakwa dikurangi seluruhnya dari pidana penjara yang dijatuhkan. Masa penahanan terdakwa sebelumnya, antara lain:

Sejak tanggal 5 Juni – 24 Juni 2020 oleh penyidik.

Sejak tanggal 25 Juni – 3 Agustus 2020 perpanjangan oleh penuntut umum.

Sejak tanggal 28 Juli – 16 Agustus 2020 oleh penuntut umum.

Sejak tanggal 11 Agustus – 9 September 2020.

Sejak tanggal 10 September – 8 November 2020 perpanjangan oleh ketua Pengadilan Negeri Makassar.

Sehingga total jumlah penahanan terdakwa sebelumnya sebanyak 5 (lima) bulan 3 hari. Setelah penetapan putusan oleh hakim pada tanggal 14 Oktober 2020, sisa masa penahanan terdakwa terhitung mulai tanggal penetapan putusan hingga 8 November 2020 sebanyak 25 hari dikurangi seluruhnya.

KESIMPULAN

Berdasarkan uraian-uraian dan pembahasan pada hasil penelitian di atas, maka dapat ditarik kesimpulan bahwa aturan mengenai data pribadi di Indonesia belum mampu memberikan efek yang besar terhadap pengguna teknologi dalam perlindungan kebocoran data pribadi karena meskipun dalam penyelesaian perkara di ranah peradilan telah dilakukan sebagaimana mestinya, namun jika penyebab kebocoran data bukan hanya karena usaha peretas *(hacker)* atau pelaku tindak pidana cyber tetapi karena kelalaian dan kurangnya pengetahuan pemilik data pribadi terkait cyber crime juga ikut terkombinasi sehingga mudahnya terjadi kebocoran data (data leakage). Hukum yang digunakan sekarang *(Ius Constitutum*) masih tergolong umum penggunaannya dalam ruang atau lingkup cyber. Jika melihat perkembangan teknologi yang semakin pesat, maka, semakin besar peluang terjadinya cyber crime. Kemungkinan semakin banyaknya bentuk-bentuk cyber crime juga tidak bisa dihindari terutama kebocoran data (data leakage). Oleh karena itu, hukum yang harus ditetapkan (Ius Constituendum) harus lebih spesifik dan komprehensif menguraikan perlindungan data pribadi secara khusus karena lebih mudah memberikan efek jera terhadap pelaku sekaligus mencegah peretas melancarkan aksinya. Jadi, meskipun banyak cara yang peretas dapat lakukan dengan kemampuan dan perkembangannya, aturan perlindungan data pribadi juga sejalan dengan perkembangan peretas dalam menggunakan sistem elektronik.

SARAN

Sistem Elektronik juga wajib diperhatikan oleh Pengguna Sistem Elektronik atau pemilik data pribadi itu sendiri karena peretas juga cerdas dalam melakukan tindak pidana. Maka, sebaiknya Pengguna Sistem Elektronik lebih teliti dalam protecting data dan update terhadap informasi mengenai perlindungan data pribadi, dan peran pemerintah dalam mengembangkan informasi terkait teknologi dan dampaknya secara materi dan praktik terhadap masyarakat sembari lembaga legislatif membuat dan melakukan upgrade terhadap aturan yang terkait data pribadi serta mengesahkan Rancangan Undang-Undang Perlindungan Data Pribadi sebagai *improvement*.

UCAPAN TERIMA KASIH

Pertama penulis ingin mengucapkan terima kasih kepada Tuhan Yang Maha Esa, karena tanpa bantuan dari-Nya artikel ini tidak akan pernah selesai. Kedua, terima kasih kepada diri sendiri karena telah berjuang melawan rasa malas dan bekerja keras untuk menyelesaikan artikel ini. Dan yang terakhir, terima kasih kepada orang tua, dosen pembimbing, teman-teman dan seluruh pihak yang telah membantu dalam penulisan artikel ini baik secara langsung maupun tidak langsung.

DAFTAR PUSTAKA

Arief Mansur, D., & Gultom, E. (2005). *Cyber Law Aspek Hukum Teknologi Informasi.* Bandung: PT. Refika Aditama.

Direktori Putusan Mahkamah Agung RI. (2020). *Putusan PN MAKASSAR Nomor 1229/Pid.Sus/2020/PN Mks.* putusan3.mahkamahagung.go.id.

Gede Atmadja, I., & Putu Budhiarta, I. (2018). *Teori-Teori Hukum.* Jawa Timur: Setara Press.

Khairuddin, I. (2021). *Rapor Merah Kebocoran Data di Indonesia.* https://techbiz.id.

Suparni, N. (2009). *Cyberspace Problematika & Antisipasi Pengaturannya.* Jakarta: Sinar Grafika.

Tim CNN. (2020). *Rentetan Kebocoran Data di Indonesia Sejak 2020.* www.cnnindonesia.com.