Analisis Yuridis Kebocoran Data Pada Sistem Perbankan Di Indonesia (Studi Kasus Kebocoran Data Pada Bank Indonesia)

Aditama Candra Kusuma, Ayu Diah Rahmani
Fakultas Hukum, Universitas Pembangunan Veteran Jakarta
aditamacandrak@upnvj.ac.id, ayudiahrahmani@upnvj.ac.id

Abstrak

Pencurian data merupakan masalah serius yang dihadapi di era digital saat ini. Jika data yang dicuri jatuh ke tangan yang salah, dapat berdampak negatif dan dapat merugikan banyak pihak. Pencurian data terjadi pada bank sentral di Indonesia yaitu Bank Indonesia. Metode penelitian yang digunakan yaitu penelitian hukum normatif, sifat penelitian ini adalah kepustakaan *(library research)*, sumber data bersumber dari data sekunder yang terdiri dari bahan hukum primer, bahan hukum sekunder dan bahan hukum tersier. Teknik analisis data secara kualitatif disajikan secara deskriptif-analitis. Teknik pengambilan kesimpulan secara deduktif. Kesimpulan dalam penelitian ini yaitu regulasi yang mengatur perlindungan data telah diatur dalam beberapa regulasi di Indonesia. Pelaku kejahatan diancam dengan pidana penjara dan denda. Namun, belum dapat mengakomodir dan memberikan perlindungan dan kepastian hukum. Penindakan kejahatan siber harus dikenakan hukuman yang berat. Urgensi untuk dapat segera mungkin mengesahan Rancangan Undang-Undang Perlindungan Data Pribadi demi melindungi masyarakat apalagi mengingat kondisi masyarakat yang berhadapan dengan teknologi dan perkembangan internet yang semakin canggih dan pesat, maka pengesahan sesegera mungkin ini sangat penting. Pemerintah seyogyanya bertanggung jawab untuk melindungi hak-hak rakyat, termasuk privasi terkait data pribadi.
Kata kunci : Bank Indonesia, Kebocoran data, perbankan

Abstract

Data leakkage is a serious peoblem faced in today's digital era. If the stolen data falls into the worng hands,it can bring negative impact and prejudice many parties. Data leakage occurred at the central bank of Indonesia, named Bank Indonesia. The research method used is normative legal reasearch, the nature of this reasearch is library (library reasearch), the data sourcce comes from secondary legal materials and tertiary legal materials. Using dedcutibe inference technique. The conclusions in this study is that regulations governing data protection have been regulated in several regulations in Indonesia. Offenders are thereatened with imprisonment and fines. However, it hasn't been able to accommodate and provide lgal protection and certainty. Cybercrime should be punished suverly. The urgency to be able to ratify the draft bill of Personal Data Protection as soon as possible in order to protect the public, especially considering the condition of the people who are dealing with technology and the development of the internet which is increasingly sophisticated and rapid, so ratification as soos as possible is very important. The govenrment should be responsible for protecting people's rights, including privacy regarding personal data.

Keywords *: Bank Indonesia, Data leakage, banking*

1. PENDAHULUAN

Kemajuan teknologi sangat membantu manusia dalam melakukan apapun. Kemajuan tersebut dapat kita rasakan sehari-hari, seperti telepon genggam yang sering digunakan untuk berkomunikasi dengan orang lain dengan jarak jauh. Dengan ditemukannya internet, kemajuan teknologi telah memudahkan masyarakat tidak hanya di Indonesia tetapi di seluruh dunia ikut merasakan dampak dengan adanya internet. Perkembangan internet juga semakin canggih dengan banyaknya aplikasi yang sangat membantu untuk mempermudah aktivitas banyak orang.

Peran teknologi informasi, media, komunikasi dan sistem elektronik sangat bermanfaat bagi perubahan perilaku masyarakat secara global. Sistem elektronik yang dimaksud yaitu perangkat keras, perangkat lunak komputer, jaringan telekomunikasi dan sistem komunikasi elektronik.[1] Kegagalan dan kesalahan dalam teknologi informatika dan sistem elektronik adalah salah satunya kurangnya penjagaan yang dilakukan dalam upaya melindungi data pribadi nasabah atau pelanggan yang sudah meregistrasi data-data pribadinya ke pelantar dunia internet.

Dalam dunia maya, semua data baik berupa tulisan, gambar bahkan video tidak akan pernah bisa dihapus secara permanen, dan hal ini disebut sebagai rekam jejak digital, dimana dari pengunggahan tersebut meninggalkan jejak yang kemudian masih bisa ditelusuri informasinya. Tentu hal ini sangat berbahaya apabila tidak diberikan perlindungan yang baik dalam rangka menghindari kebocoran dari data-data pribadi yang telah diunggah. Untuk menghindari digunakannya sebagai senjata yang membahayakan di kemudian hari dikarenakan identitas yang tidak dilindungi tersebut digunakan oleh oknum yang tidak bertanggung jawab.

Kekhawatiran masyarakat Indonesia selaku pelanggan *e-commerce*, pemilik akun aplikasi media sosial dan nasabah bank di Indonesia akan keamanan data mereka. Rupanya kekhawatiran tersebut terbukti dengan banyaknya berita di media yang menginformasikan bahwa data-data pelanggan Tokopedia, Shopee, Yahoo, Instagram dan lainnya mengalami kebocoran akibat tindakan pembobolan yang dilakukan oleh oknum jahat yang menginginkan informasi atau data pribadi pelanggan untuk dikumpulkan dan kemudian diperjualbelikan sebagai data-data palsu agar mendapat perizinan peminjaman online dan kegiatan ilegal menggunakan data pribadi orang lain sehingga pelacakan terkadang salah sasaran karena informasi yang sudah diunggah berbeda dengan data pelaku tersebut.

Akhir-akhir ini kebocoran data terjadi pada bank sentral di Indonesia yaitu Bank Indonesia. Diketahui Bank Indonesia mengalami kebocoran data berdasarkan berita yang ramai di sosial media. Berita kebocoran data yang dialami Bank Indonesia ramai beredar di sosial media pada awal tahun 2022. Didapati satu akun twitter atas nama @darktracer_int mengunggah potongan layar yang lengkap

[1] Bala Tim PY, *Undang-Undang Informasi Dan Transaksi Elektronik: Seri Perundangundangan* (Yogyakarta: Pustaka Yustisia, 2019), hal 33–34.

dengan keterangan file di dalamnya, tertulis bahwa file tersebut berasal dari situs www.bi.go.id.[2] Setelah ditelusuri lebih lanjut ternyata kebocoran data ini terjadi secara berkala diperkirakan awal mula terjadi pada tahun 2021 sampai pada tahun 2022. Dalam kurun waktu dua tahun jumlah kebocoran data Bank Indonesia terus bertambah dan perangkat yang diretas juga semakin meningkat.

Pencurian data merupakan masalah serius yang dihadapi di era digital saat ini. Jika data yang dicuri jatuh ke tangan yang salah, dapat berdampak negatif dan dapat merugikan banyak pihak. Tidak hanya terjadi pada Bank Indonesia, kasus serupa juga banyak terjadi di Indonesia. Modus operandi yang dilakukan oleh *hacker* Rusia adalah dengan mengunci sistem dan mengambil data Bank Indonesia. Tentunya kebocoran data ini sangat mengkhawatirkan banyak pihak, mengingat peran Bank Indonesia sebagai bank sentral yang membawahi bank lain dan menjadi pusat peredaran uang di Indonesia.

Terdapat beberapa penelitian terdahulu yang telah membahas terkait tema dan permasalahan yang penulis angkat, adapun uraiannya sebagai berikut: Sebagai bentuk orisinalitas penelitian ini, maka penulis melakukan riset penelitian terdahulu dengan tema serupa dan mencari perbedaan dari pokok bahasan dalam penelitian. Penulis menemukan beberapa karya ilmiah dengan tema serupa diantaranya ***Pertama,*** penelitian Muhamad Bayu Satrio dan Men Wih Widiatno yang berjudul *Perlindungan Hukum Terhadap Data Pribadi Dalam Media Elektronik (Analisis Kasus Kebocoran Data Pengguna Facebook Di Indonesia),*[3] ***Kedua,*** penelitian Muhammad Fathur yang berjudul *Tanggung Jawab Tokopedia Terhadap Kebocoran Data Pribadi Konsumen.*[4] ***Ketiga,*** penelitian Deanne Destriani Firmansyah Putri dan Muhammad Helmi Fahrozi yang berjudul *Upaya Pencegahan Kebocoran Data Konsumen Melalui Pengesahan Ruu Perlindungan Data Pribadi (Studi Kasus E-Commerce Bhinneka.Com).*[5]

Berdasarkan uraian di atas, maka penelitian ini berbeda dengan penelitian-penelitian terdahulu yang mengangkat tema serupa. Adapun perbedaan dengan antara penelitian pertama adalah penelitian pertama membahas perlindungan hukum

[2] C. N. N. Indonesia, "Kebocoran Data Bank Indonesia Belum Selesai, Naik Jadi 74GB," *teknologi*, accessed January 20, 2022, https://www.cnnindonesia.com/teknologi/20220124163634-185-750569/kebocoran-data-bank-indonesia-belum-selesai-naik-jadi-74gb.

[3] Muhamad Bayu Satrio and Men Wih Widiatno, "PERLINDUNGAN HUKUM TERHADAP DATA PRIBADI DALAM MEDIA ELEKTRONIK (ANALISIS KASUS KEBOCORAN DATA PENGGUNA FACEBOOK DI INDONESIA)," *JCA of Law* 1, no. 1 (July 15, 2020), accessed March 4, 2022, https://jca.esaunggul.ac.id/index.php/law/article/view/6.

[4] Muhammad Fathur, "TANGGUNG JAWAB TOKOPEDIA TERHADAP KEBOCORAN DATA PRIBADI KONSUMEN," *National Conference on Law Studies (NCOLS)* 2, no. 1 (November 19, 2020), hal 43–60.

[5] Deanne Destriani Firmansyah Putri and Muhammad Helmi Fahrozi, "UPAYA PENCEGAHAN KEBOCORAN DATA KONSUMEN MELALUI PENGESAHAN RUU PERLINDUNGAN DATA PRIBADI (STUDI KASUS E-COMMERCE BHINNEKA.COM)," *National Conference on Law Studies (NCOLS)* 2, no. 1 (November 19, 2020), hal 255–273.

terhadap data pribadi bagi pengguna media online ditinjau dari Undang-Undang Nomor 11 tahun 2008 sebagaimana telah diubah dengan Undang-Undang Nomor 19 tahun 2016 Tentang Informasi dan Transaksi Elektronik (UU ITE) dan dikaitkan dengan studi kasus kebocoran data pengguna *Facebook* di Indonesia. Sedangkan penelitian ini tidak membahas perlindungan hukum dan tidak memilih studi kasus kebocoran data pada platform sosial media. Perbedaan dengan antara penelitian kedua adalah membahas pertanggungjawaban *Tokopedia* terhadap kebocoran data pribadi konsumennya, sedangkan dalam penelitian ini membahas bentuk pertanggungjawaban semua aspek terhadap kebocoran data. Perbedaan antara penelitian ketiga adalah pada variabel penelitiannya, dalam pembahasan penelitian ketiga variabel penelitian berupa studi kasus kebocoran data pada *e-commerce* sedangkan dalam penelitian ini studi kasus kebocoran data pada Bank Indonesia.

Secara umum tujuan penelitian ini sebagai sumbangsih pemikiran dan gagasan terhadap ilmu hukum pidana khususnya dalam tindak pidana siber yang berkaitan dengan pencurian data melalui jaringan internet. Tujuan khusus penelitian ini, untuk mengetahui bentuk penindakan kejahatan peretas data di Indonesia serta untuk mengetahui upaya pemerintah untuk mengambil tindakan terhadap pencuri data dan akuntabilitas untuk semua aspek yang terlibat.

2. METODE PENELITIAN

Dalam penelitian ini penulis menggunakan metode penelitian hukum normatif. Oleh karena itu sifat penelitian ini adalah kepustakaan *(library research)*, artinya sebuah studi dengan mengkaji buku-buku atau kitab-kitab terkait dengan artikel ini yang berasal dari perpustakaan (bahan pustaka) yang berkaitan dengan tema yang diangkat. Dalam metode normatif ini, pendekatan hukum yang digunakan adalah pendekatan perundang-undangan atau yang biasa dikenal sebagai *statute approach*.

Sumber data yang digunakan adalah sumber data sekunder yang terdiri dari sumber bahan hukum primer berupa peraturan perundang-undangan terkait kebocoran data, bahan hukum sekunder berupa buku-buku dan jurnal terkait tema penelitian, dan bahan hukum tersier berupa kamus, ensiklopedia, koran, sumber internet lainnya. Teknik Penyajian data dalam penelitian ini disajikan secara deskriptif-analitis. Teknik analisis data dilakukan secara kualitatif, dan teknik pengambilan kesimpulan secara deduktif.

3. HASIL DAN PEMBAHASAN

A. Bentuk Penindakan Kejahatan Peretas Data Di Indonesia

Informasi pribadi yang sudah diunggah ke sistem elektronik akan menjadi jejak digital yang mustahil untuk dimusnahkan, sehingga harus dilakukan

perlindungan untuk meminimalisasi risiko kebocoran data pribadi agar tidak disalahgunakan. Akan tetapi, faktanya di lapangan masih saja ada kesalahan yang terjadi secara tidak sengaja dikarenakan sistem proteksi yang kurang memadai sehingga terdapat celah bagi predator informasi pribadi orang lain dibobol dan diperjualbelikan, atau digunakan untuk hal-hal yang melanggar hukum. Kasus-kasus kebocoran data dan penjualan data pribadi yang terjadi di Indonesia :

1) Kasus pembobolan data pengguna akun Tokopedia mencapai 91 juta data dan tersebar di forum internet.[6]

   Awal tahun 2021 Tokopedia ramai dibicarakan, ketika dikabarkan sebanyak 15 juta akun pengguna Tokopedia mengalami kebocoran. Tokopedia sebagai salah satu marketplace yang memiliki nama cukup besar dan berpengaruh bagi kegiatan jual beli *online* di Indonesia tentu harus memberikan tindakan yang tepat kepada para pengguna akun. Kemudian tidak sampai di situ, bahkan data sebesar 91 juta data pengguna telah dimiliki oleh akun bernama @cellibis dari platform bernama *Raids Forum*. Presiden Lembaga Penelitian Keamanan Siber Indonesia Cissrec menjelaskan, tanpa regulasi yang ketat bagi setiap penyelenggara sistem elektronik, baik publik maupun swasta, tidak akan ada tekanan untuk menciptakan sistem perawatan terbaik.[7] Kebocoran data pengguna Tokopedia dengan jumlah besar tentu mengakibatkan banyaknya kerugian dari pihak pengguna. Keamanan dan privasi data pengguna menjadi suatu hal yang disebarluaskan bahkan sampai diperjualbelikan. Data pengguna yang tersebar bisa saja digunakan sebagai identitas untuk melakukan tindak kriminal oleh orang-orang yang tidak bertanggung jawab.

2) Kasus pembobolan data penumpang Lion Air Group, dengan jumlah penumpang diperkirakan mencapai 7,8 juta data.[8]

   Beberapa waktu lalu Lion Air mengalami kebocoran data penumpang. Kasus kebocoran ini melibatkan beberapa maskapai seperti Malindi Air, Thai Lion Air, dan Batik Air yang tergabung dalam Lion Air Group. Setelah dilakukan penelusuran diketahui pencurian data tersebut dilakukan oleh dua karyawan GoQuo Sdn Bhd, perusahaan *e-commerce* yang menjadi pernah menjadi pemasok bagi Malindo Air. Kedua mantan karyawan Go Quo Sdn Bhd ini melakukan aksi mereka

[6] JawaPos.com, "91 Juta Data Akun Tokopedia Bocor dan Disebar Di Forum Internet," *JawaPos.com*, last modified July 5, 2020, accessed February 10, 2022, https://www.jawapos.com/oto-dan-tekno/teknologi/05/07/2020/91-juta-data-akun-tokopedia-bocor-dan-disebar-di-forum-internet/.
[7] Ibid.
[8] Liputan6.com, "Malindo: Kebocoran Data Gara-Gara Mantan Staf Perusahaan Kontraktor," *liputan6.com*, last modified September 23, 2019, accessed February 20, 2022, https://www.liputan6.com/tekno/read/4069498/malindo-kebocoran-data-gara-gara-mantan-staf-perusahaan-kontraktor.

melalui pusat data di India dengan mengakses data penumpang tanpa izin dari pihak Lion Air Group. Keduanya diketahui melakukan pencurian data melalui server maskapai atau penyedia *Cloud Amazon Web Sevice* dari Malindo Air dan bukan dari GoQuo. Malindo Air kemudian meminta bantuan dari ahli forensik dan keamanan siber untuk kembali memastikan keamanan infrastruktur milik Malindo Air sebagai bentuk pertanggungjawaban dari pihak maskapai. Untuk menghindari hal-hal yang tidak diinginkan di kemudian hari para penumpang Malindo Air kemudian juga diminta pihak maskapai untuk mengubah kata sandi mereka.[9]

3) Peretasan data pengguna Bukalapak mencapai 13 juta pengguna terjadi pada Maret 2019. Kabarnya data yang sudah diretas oleh *hacker* dengan username Startexmislead juga diperjualkan di dark web.[10]

Pada tahun 2019 Bukalapak mengalami kebocoran data. Diperkirakan kebocoran data berjumlah 13 juta data pengguna aktif Bukalapak. Diketahui peretas asal Pakistan yang terkenal dengan nama Gnosticplayers telah menjual data-data tersebut. Saat itu, data-data tersebut dijual dengan harga 1.2431 Bitcoin atau setara dengan sekitar 5.000 USD atau Rp 70,5 juta rupiah dengan delapan website secara terpisah. Kemudian pada tahun 2020 Bukalapak juga mengalami kebocoran data. Data milik Bukalapak ini dijual oleh akun bernama Asian Boy. Asian Boy diketahui menjual basis data milik Bukalapak.com sebanyak 12.960.526 pengguna. Asian Boy menjual beragam data mulai dari Email, Nama Pengguna, Kata Sandi, Saldo, Login Terakhir, Email Facebook dengan Hash, Alamat Pengguna, Tanggal Lahir, dan Nomor Telepon. Peretas lain dengan akun Startexmislead juga menawarkan 12 juta data Bukalapak.com. Startexmislead bahkan meretas data dari pendiri Bukalapak seperti Fajrin Rasyid hingga Ahmad Zaky. Dua peretas menjual data Bukalapak.com dengan tidak mencantumkan harga, sebab keduanya meminta untuk dikontak secara langsung untuk menanyakan perihal harga.[11]

Kasus kebocoran data kembali terjadi pada tahun 2022 ini. Kebocoran data yang terjadi pada bank sentral milik Indonesia yaitu Bank Indonesia.

[9] idxchannel, "Pembobol Data Penumpang Lion Air Group Akhirnya Terungkap," *https://www.idxchannel.com/*, accessed February 21, 2022, https://www.idxchannel.com/market-news/pembobol-data-penumpang-lion-air-group-akhirnya-terungkap.

[10] "Bukalapak Akui 13 Juta Data yang Dijual Hacker adalah Peretasan di Maret 2019," *kumparan*, accessed February 21, 2022, https://kumparan.com/kumparantech/bukalapak-akui-13-juta-data-yang-dijual-hacker-adalah-peretasan-di-maret-2019-1tMRTr1UR0G.

[11] "13 Juta Data Bocor Bukalapak Dijual Di Forum Hacker," accessed February 22, 2022, https://www.cnnindonesia.com/teknologi/20200506065657-185-500477/13-juta-data-bocor-bukalapak-dijual-di-forum-hacker.

Kebocoran data ini terntu kembali menarik perhatian dari masyarakat. Perhatian masyarakat tertuju pada kemanan data pribadi milik mereka yang berada atau terdaftar pada sistem Bank Indonesia. Kemudian Badan Siber dan Sandi Negara, BSSN, telah mengonfirmasi kebenaran bahwa data Bank Indonesia mengalami kebocoran. BSSN menyatakan bahwa data yang bocor merupakan data milik Bank Indonesia cabang Bengkulu. Melalui juru BSSN yaitu Aton Setiawan juga menyatakan kepada publik bahwa data yang bocor bukanlah data kritikal.[12] Namun jika dilihat lebih jauh walaupun kebocoran bukan terjadi pada data kritikal, keadaan kebocoran-kebocoran data ini tetap mengancam keberadaan dan kepercayaan masyarakat terhadap keamanan Bank Indonesia. Mengingat Bank Indonesia merupakan bank sentral yang menjadi pusat peredaran bank lain serta uang masyarakat di Indonesia.

Setelah dilakukan penelusuran lebih lanjut diketahui bahwa peretasan data milik Bank Indonesia diketahui dilakukan oleh peretas asal Rusia, Conro Ransomware. Mereka telah mengatakan dan mengkonfirmasi kebenaran bahwa Bank Indonesia adalah korban peretasan data mereka. Peretasan itu terjadi tahun lalu, peretasan disinyalir awalnya menyerang Personal Computer Bank Indonesia di cabang Bengkulu. Para *hacker* ini melakukan penyerangan dengan melakukan modus mengunci sistem kemudian mengambil data Bank Indonesia. Diketahui Conro Ransomware telah melakukan peretasan data sampai dengan kapasitas 487 MB dari 16 *personal computer* (PC) pada 21 Januari 2022. Kemudian selang 3 hari kemudian, melalui akun twitternya @darktracker_int kembali menyatakan bahwa kebocoran data Bank Indonesia ke kelompok *hacker* tersebut telah bertambah menjadi 52.767 dokumen dengan kapasitas 74 GB. Data yang diretas dari 237 unit PC di jaringan komputer BI. Walaupun BSSN telah melakukan upaya dengan mitigasi,[13] tetap terjadi peningkatan jumlah yang sangat besar dalam kurun waktu 3 hari yang dilakukan oleh para *hacker*. Dalam waktu singkat mereka telah menunjukan bahwa adanya sistem keamanan milik data Bank Indonesia yang telah mereka kuasai.

Maka tidak kecil kemungkinan para *hacker* ini dapat terus menambah jumlah data pencurian Bank Indonesia jika tidak dilakukan pencegahan. Berdasarkan informasi yang didapat selama 3 hari setelah peretasan pertama dari pihak Bank Indonesia maupun dari BSSN belum ada pergerakan untuk mencegah sehingga terjadi lagi peretasan dengan jumlah yang lebih banyak. Jika pihak-pihak yang berkaitan dengan hal tersebut bisa mengatasi masalah ini

[12] "Benarkan Ada Kebocoran Data Milik Bank Indonesia, BSSN Pastikan Bukan Data Kritikal," *KOMPAS.tv*, accessed January 20, 2022, https://www.kompas.tv/article/253628/benarkan-ada-kebocoran-data-milik-bank-indonesia-bssn-pastikan-bukan-data-kritikal.

[13] "Kebocoran Data Bank Indonesia Terus Bertambah, Naik Jadi 74 GB! | Databoks," accessed January 21, 2022, https://databoks.katadata.co.id/datapublish/2022/01/25/kebocoran-data-bank-indonesia-terus-bertambah-naik-jadi-74-gb.

dengan cara mencegah tidak akan ada peretasan kedua dengan jumlah yang lebih banyak. Maka seharusnya dilakukan tindakan yang lebih cepat dan maksimal untuk melindungi data-data yang lain. Namun yang juga perlu diperhatikan adalah menjadikan prioritas keamanan siber sejak awal mula membangun sistem dan faktor keamanan.

Regulasi di Indonesia turut mengatur perusahaan yang memang membangun bisnisnya dengan menggaet publik untuk mendaftarkan informasi diri yang sensitif ke perusahaan tersebut sehingga perusahaan harus memahami aturan, prinsip prinsip dan praktik perlindungan data pribadi. Pemerintah juga mengatur hubungan kontraktual antara bank dengan nasabah yang merupakan pengguna jasa bank, dalam hal nasabah memberikan informasi dan data pribadi yang sangat sensitif khususnya dalam hal perbankan dan keuangan harus siap menerapkan prinsip kerahasiaan.[14]

Beberapa regulasi yang mengatur tentang perlindungan data pribadi konsumen dan nasabah yang berlaku di Indonesia:

1. Undang-Undang Nomor 7 Tahun 1992 Tentang Perbankan dengan perubahan Undang-Undang Nomor 10 Tahun 1998, yang menentukan bahwa Bank sebagai pihak yang menawarkan jasanya sebagai penyimpanan keuangan dan kegiatan keuangan lainnya harus merahasiakan keterangan terkait nasabahnya, penyimpannya dan simpanannya;
2. Undang-Undang Nomor 43 Tahun 2009 tentang Kearsipan, yang mengatur mengenai arsip data-data nasabah dan pelanggan yang merupakan warga negara Indonesia yang memiliki hak untuk dilindungi;
3. Undang-Undang Nomor 8 Tahun 1997 tentang Dokumen Perusahaan, yang mengatur mengenai dokumen berkaitan dengan data pribadi para pengguna;
4. Undang-Undang Nomor 36 Tahun 2009 tentang Kesehatan, yang dalam perannya memiliki kedudukan hukum atas keamanan data pribadi pasien;
5. Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi (UU Telekomunikasi), yang mengatur berbagai macam tindakan yang kemungkinan berpeluang membahayakan penggunaan data pribadi pelanggan dan nasabah di sistem elektronik;
6. Undang-Undang Nomor 24 Tahun 2013 tentang Perubahan Atas Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan (UU Adminduk);
7. Undang-Undang Nomor 19 Tahun 2016 Tentang perubahan atas

[14] Marnia Rani, "Perlindungan Otoritas Jasa Keuangan Terhadap Kerahasiaan Dan Keamanan Data Pribadi Nasabah Bank," *Jurnal Selat* 2, no. 1 (2014), hal 172.

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

8. Peraturan Pemerintah Nomor 82 Tahun 2012 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik.
9. Peraturan Menteri Komunikasi dan Informasi Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik
10. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

Dengan adanya peraturan-peraturan tersebut maka secara otomatis pengolahan data dan informasi harus dikelola secara baik, jelas dan terarah. Apabila tidak dikelola dengan tepat, maka akibatnya bisa fatal dan berbahaya karena berujung dengan penyalahgunaan dan penyerangan kejahatan *cyber crime*. Maka dari hal tersebut diperlukan analisis manajemen risiko guna menghadapi serangan *cyber crime.*[15] Karena *cyber crime* memiliki potensi terhadap hilangnya sistem informasi dan kendali data pribadi dan hal tersebut sulit untuk diatasi. Kejahatan pencurian data yang dilakukan oleh *hacker* yang tidak bertanggung jawab tentu menimbulkan kerugian bagi korbannya. Begitupun dengan korban atas tindakan *phising* yang membuat data-data pribadi korban dengan bebas diperjual belikan dengan risiko yang harus ditanggung korban sangat besar. Maka penindakan kejahatan siber harus dikenakan hukuman yang berat.

Dalam Undang-Undang Telekomunikasi mengatur beberapa hal yang berkaitan dengan kerahasiaan data pribadi, yakni pada Pasal 22 dituliskan setiap orang dilarang melakukan perbuatan tanpa hak, tidak sah atau manipulasi akses ke jaringan telekomunikasi pada sistem elektronik, baik umum maupun khusus. Bagi pelanggar peraturan tersebut diancam pidana penjara maksimal 6 (enam) tahun dan/atau denda maksimal Rp 600.000.000 (enam ratus juta rupiah). Pada Pasal 40 menyatakan setiap orang dilarang melakukan penyadapan informasi yang diunggah lewat jaringan telekomunikasi dalam bentuk apapun. Apabila melanggar ketentuan tersebut, akan diancam pidana penjara maksimal 15 (lima belas) tahun. Pada pasal 42 ayat (1) menyatakan kewajiban penyelenggara jasa telekomunikasi untuk merahasiakan informasi dan apabila melanggar diancam pidana penjara maksimal 2 (dua) tahun dan/atau denda maksimal Rp 200.000.000 (dua ratus juta rupiah).

Dijelaskan pula di dalam Undang-Undang Informasi dan Telekomunikasi Elektronik mengenai sanksi yang diberikan kepada pelaku kejahatan pembobolan data pribadi. Dinyatakan di dalam Pasal 26 UU ITE bahwa setiap

[15] Ineu Rahmawati, "ANALISIS MANAJEMEN RISIKO ANCAMAN KEJAHATAN SIBER (CYBER CRIME) DALAM PENINGKATAN CYBER DEFENSE," *Jurnal Pertahanan & Bela Negara* 7, no. 2 (October 3, 2017), hal 53.

orang dapat melakukan gugatan terhadap perolahan data pribadi tanpa persetujuannya. Maka setidaknya pelaku kejahatan yang telah melakukan pelanggaran PDP dapat digugat sebagai Perbuatan Melawan Hukum (PMH) atas dasar kesalahan berdasarkan ketentuan UU (1365 KUHPerdata), maupun atas dasar ketidakpatutan atau ketidakhati-hatian (1366 KUHPerdata). Kemudian pada Pasal 3 UU ITE juga menjelaskan harus ada prinsip kehati-hatian dan memberikan tanggung jawab pihak korporasi maupuan pemerintah yang dinyatakan sebagai Penyelenggara Sistem Elektonik (PSE), yakni setidak-tidaknya harus andal, aman dan bertanggung jawab.

Kemudian masih di dalam UU ITE Pasal 30 yang menjelaskan bahwa setiap orang dengan sengaja dan melawan hukum mengakses komputer dan/atau sistem elektronik orang lain untuk tujuan memperoleh informasi elektronik dan/atau dokumen elektronik dengan melakukan pelanggaran, penyusupan, penimpaan, atau pembobolan keamanan sistem dapat dipidana. Pidana yang diberikan kepada pelaku adalah dengan mendapatkan pidana penjara paling lama 6 (enam) sampai dengan 8 (delapan) tahun dan/atau denda paling banyak Rp 600.000.000,00 (enam ratus juta rupiah) sampai dengan Rp 800.000.000,00 (delapan ratus juta rupiah).

Kemudian bagi pelaku kejahatan yang juga memperjualbelikan hasil data retasan yang telah mereka dapatkan juga diatur di dalam UU ITE. Di dalam Pasal 34 bahwa setiap orang yang dengan sengaja dan tanpa hak atau melawan hukum memproduksi, menjual, mengadakan, untuk dilakukan mengimpor, mendistribusikan, menyediakan atau memiliki perangkat komputer atau sistem informasi maka menurut Pasal 45 dapat dipidana dengan pidana penjara paling lama 6 (enam) tahun dan.atau denda paling banyak Rp 1.000.000.000,00 (satu miliar rupiah).

B. Upaya Pemerintah Dalam Menindak Pelaku Kebocoran Data Dan Pertanggungjawaban Semua Aspek Yang Terlibat.

Meningkatnya jumlah pengguna internet tidak terlepas dari meningkatnya kejahatan siber. Adanya pandemi global yaitu *Covid-19* memaksa segala bentuk kegiatan dialihkan dari jarak jauh maka faktor ini sangat relevan dengan meningkatnya jumlah pengguna internet beberapa tahun ini. Tercatat sebesar 18 laporan mengenai peretasan data dalam sistem elektronik pada bulan Januari-September 2020 yang dilaporkan oleh rangkuman Databoks milik Kepolisian Republik Indonesia (POLRI) dalam data Laporan Kasus Kejahatan Siber Indonesia.[16] Kemudian pada tahun 2021 jumlah kehatan ini terus bertambah

[16] Sandryones Palinggi and Erich C. Limbongan, "Pengaruh Internet Terhadap Industri Ecommerce Dan Regulasi Perlindungan Data Pribadi Pelanggan Di Indonesia," *Semnas Ristek (Seminar Nasional Riset dan Inovasi Teknologi)* 4, no. 1 (January 27, 2020): 226, accessed March 4, 2022, http://www.proceeding.unindra.ac.id/index.php/semnasristek/article/view/2543.

dengan meningkat menjadi 43 kasus dengan dugaan kegagalan perlindungan data pribadi masyarakat.[17] Maka besar kemungkinan terjadinya pertambahan jumlah pada kasus serupa akan terus terjadi jika tidak ada pergerakan untuk mengesahkan RUU Perlindungan Data Pribadi oleh pemerintah.

Dengan melihat ke belakang, pasti terdapat beberapa alasan yang mendorong sehingga menyebabkan banyak orang menjadi berani dan nekat dalam melakukan kejahatan siber. Tentunya dengan adanya faktor yang mendukung untuk melakukan hal tersebut menjadi dorongan banyaknya jumlah kejahatan siber yang terjadi. Kejahatan siber ini tentunya tidak hanya mengancam dan merugikan satu pihak saja mengingat jika pencurian data yang dilakukan dapat pula merugikan perorangan, kelompok bahkan satu negara. Tidak sampai pada subjek yang dirugikan tetapi juga objek yang dirugikan akibat pencurian data. Akibat pencurian data kerugian-kerugian yang dialami bisa menyebar sampai dengan bidang ekonomi, perbankan, politik bahkan kerugian kepada keamanan nasional.[18]

Faktor ekonomi menjadi salah satu faktor yang paling banyak mendorong adanya kejahatan siber yang dilakukan oleh para pelaku kejahatan pada bidang siber. Mengingat adanya rasa keinginan serta adanya kesempatan yang dilihat oleh pelaku kejahatan siber untuk melakukan kejahatan demi mendapatkan keuntungan bagi diri sendiri. Salah satu kejahatan mereka adalah melakukan pembobolan data yang seharusnya bersifat rahasia dengan kemudian memperjualbelikan data pribadi yang berhasil mereka retas ke pasar web ilegal. Adanya kemajuan teknologi yang sangat pesat juga menjadi faktor pendorong sehingga terus menimbulkan banyak kejahatan baru di dunia siber. Selain adanya dorongan faktor ekonomi dan kemajuan teknologi, juga dapat dilihat berdasarkan kasus yang pernah terjadi adalah akibat dari kurangnya kesiap siagaan dalam menangani pelaku kejahatan siber oleh aparat penegak hukum. Maka dari itu aparat penegak hukum dengan kualitas yang mumpuni pada bidangnya sangat diperlukan keberadannya agar dapat menangani berbagai kejahatan siber. Mengingat kedepannya akan terus terjadinya kehatan seperti ini dan terus marak terjadi serta keberadannya yang akan berkembang diiringi dengan perubahan zaman.[19]

Jika tercipta sebuah masalah yang menimbulkan keresahan maka menuntut adanya sebuah jalan keluar yang tepat, maka dalam kasus ini pertanggungjawaban dari pihak yang bersangkutan merupakan jalan keluar dan solusi yang bijaksana bagi para pihak yang dirugikan. Bagi pihak yang telah memberikan data pribadinya di sebuah sistem informasi maka harus melakukan tanggung jawab atas

[17] "Tercatat, Kominfo Selesaikan 43 Kasus Kebocoran Data Pribadi Sepanjang 2021," *suara.com*, last modified December 31, 2021, accessed February 22, 2022, https://www.suara.com/tekno/2021/12/31/104557/tercatat-kominfo-selesaikan-43-kasus-kebocoran-data-pribadi-sepanjang-2021.

[18] Barda Nawawi Arief, *Tindak Pidana Mayantara Perkembangan Kajian Cyber Crime Di Indonesia* (Jakarta: PT Raja Grafindo, 2006), hal 52.

[19] Ibid.

data yang diberikan kepada pihak yang bersangkutan, apakah data yang diberikan sudah benar dan sesuai dengan data pribadi miliknya dan bukanlah data pribadi milik orang lain. Kemudian bentuk pertanggung jawaban dari pihak yang memegang data pribadi milik orang lain harus menunjukan pertanggung jawabannya dengan cara melindungi dan memberikan keamanan terhadap data pribadi milik orang lain, mereka harus bisa mempertanggung jawabkan data pribadi milik orang lain terhadap pengamanan dan perlindungan sarana dan prasarana sistem elektronik.[20] Dijelaskan melalui Pasal 21 Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia bahwasannya setiap orang berhak atas keutuhan pribadi, baik rohani maupun jasmani, dan karena itu tidak boleh menjadi obyek penelitian tanpa persetujuan. Diperjelas lagi bahwa yang dimaksud obyek penelitian di dalam pasal tersebut adalah kegiatan yang menempatkan seseorang sebagai yang dimintai komentar, pendapat atau keterangan yang menyangkut kehidupan pribadi dan data-data pribadinya serta direkam gambar dan suaranya. Urgensi diperlukannya Undang-Undang yang mengatur mengenai permasalahan data pribadi berangkat dari harus adanya persetujuan terlebih dahulu dari pemilik data untuk menggunakan datanya. Namun didapati kesalahan yang marak terjadi adalah digunakannya data pribadi mereka tanpa adanya persetujuan dari pemilik data pribadi terlebih dahulu.

Menghasilkan sebuah produk hukum yaitu Undang-Undang yang berasal dari sebuah Rancangan Undang-Undang tentu membutuhkan waktu dan proses yang panjang. Butuh banyak hal yang dipertimbangkan oleh banyak pihak sebelum memformulasikan Rancangan Undang-Undang menjadi sebuah Undang-Undang yang sah yang mana isinya dapat dijadikan hukum positif yang bermanfaat dan melindungi kewajiban serta hak dari pihak-pihak yang bersangkutan. Maka pengharmonisasian merupakan salah satu proses yang dapat ditempuh. Dijelaskan bahwa mengharmoniasasikan Undang-Undang merupakan salah satu bentuk upaya untuk diselarasakannya suatu Peraturan Perundang-Undangan yang satu dengan Peraturan Perundang-Undangan yang lain di dalam suatu hierarki Peraturan Perundang-Undangan. Konsep penyelarasan ini dikemukakan oleh Padma Widyantari dan Adi Sulistiyono dalam salah satu tulisan mereka.[21] Namun, urgensi untuk dapat sesegera mungkin mengesahan RUU PDP demi melindungi masyarakat apalagi mengingat kondisi masyarakat yang berhadapan dengan teknologi dan perkembangan internet yang semakin canggih dan pesat, maka pengesahan sesegera mungkin ini sangat penting. Maka dalam hal ini pemerintah memiliki desakan untuk segera melakukan pertanggungjawaban

[20] *Peraturan Pemerintah No. 71 Tahun 2019 Tentang Penyelenggaran Sistem Dan Transaksi Elektronik*.
[21] Padma Widyantari and Adi Sulistiyono, "PELAKSANAAN HARMONISASI RANCANGAN UNDANG-UNDANG PERLINDUNGAN DATA PRIBADI (RUU PDP)," *Jurnal Privat Law* 8, no. 1 (February 2, 2020), hal 117–123.

yang diharapkan oleh masyarakat untuk segera mengesahkan RUU Perlindungan Data Pribadi.

Adanya asas pertanggungjawaban yang dimaksudkan di dalam Rancangan Undang-Undang Perlindungan Data Pribadi pun menjelaskan agar semua pihak yang terkait dengan proses dan pengawasan data pribadi untuk dapat bertindak secara bertanggung jawab sehingga mampu menjamin keseimbangan hak dan kewajiban para pihak yang terkait termasuk pemilik data pribadi.[22] Secepat mungkin dengan pertimbangan yang sangat matang pemerintah harus mengesahkan Rancangan Undang-Undang Perlindungan Data Pribadi. Dengan mengesahan RUU PDP ini dapat menjadi bentuk dari pertanggung jawaban yang dapat diberikan oleh pemerintah. Mengingat akan terjaminnya perlindungan terhadap pemilik data pribadi dari disahkannya RUU PDP. Pihak Pemerintah seharusnya juga dapat melakukan pengupayaan lebih lanjut sebagai bentuk penindakan terhadap pelaku kebocoran data dengan menerapkan sanksi. Seperti yang sudah dijelaskan menurut hukum pidana di dalam Bab XIII dalam Rancangan Undang-Undang Perlindungan Data Pribadi mengenai Ketentuan Pidana yang sudah dijabarkan di atas. Dengan memberikan sanksi sehingga dapat diharapkan pelaku kejahatan kebocoran data mendapat efek jera atas tindakannya. Kemudian para korban kebocoran data bisa mendapatkan kepastian hukum sehingga dapat menuntut hak dan kewajiban yang seharusnya mereka dapatkan. Para korban juga dapat melaporkan permasalahannya agar diselesaikan oleh aparat penegak hukum sesuai dengan hukum yang berlaku. Sehingga sesuai dengan prinsip-prinsip pengelolaan data pribadi, para pelapor maupun korban kebocoran data pribadi dan pemilik sistem informasi yang berperan sebagai pengelola data pribadi milik pengguna dapat mempertanggung jawabkan pengelolaan data pribadi dan dapat memiliki dasar dan sumber hukum yang kuat. Masyarakat mengharapkan adanya upaya dan kontribusi dari pemerintah yang besar dengan segera mengesahkan RUU Perlindungan Data Pribadi terlebih dahulu, mengingat dengan disahkannya RUU ini menjadi sebuah Undang-Undang, akan menimbulkan wewenang yang dimiliki aparat penegak hukum dan badan pemerintahan lain yang terkait terhadap penegakan perlindungan data pribadi. Sehingga aparat penegak hukum dan badan pemerintah lain yang terkait dapat menindaklanjuti pelaku kebocoran data sesuai dengan hukum yang berlangsung.

Selain upaya pemerintah melalui pengesahan RUU Perlindungan Data Pribadi Kementerian Komunikasi dan Informatika Republik Indonesia (KOMINFO) juga melakukan penyuluhan kepada masyarakat mengenai kebocoran data. KOMINFO sebagai menteri yang erat bergerak di bagian siber Indonesia juga harus turut andil dalam menyelesaikan permasalahan PDP.

[22] *RUU Perlindungan Data Pribadi, Rancangan Penjelasan Tentang Perlindungan Data Pribad Secara Umum.*

Mengingat terus bertambahnya jumlah kebocoran data yang terjadi kepada Bank Indonesia tentunya menimbulkan kekhawatiran baru kepada masyarakat. KOMINFO menyatakan guna mencegah kerentanan terhadap pencurian data pribadi, generasi muda perlu memahami jenis data pribadi dan relevansinya. Mencermati jenis produk jasa, layanan yang disediakan, serta memeriksa ketentuan kebijakan privasi. Melihat saat ini tindakan pencegahan kebocoran data pribadi bisa dilakukan dengan cara jangan menyerahkan data diri pada situs web untuk mendapatkan suatu hadiah. KOMINFO juga menegaskan kepada masyarakat untuk berhati-hati dengan pesan *e-mail* yang meminta data pribadi ataupun pesan *e-mail* yang tidak terduga.

4. PENUTUP

a. Kesimpulan

1. Ketentuan yang mengatur perlindungan data telah diatur dalam beberapa regulasi di Indonesia. Salah satunya adalah yang termuat di dalam UU Telekomunikasi yangmana mengancam kejahatan peretasan data dengan pidana penjara dan juga denda. Seperti yang tertuang di dalam Pasal 40 UU Telekomunikasi meyatakan bahwa penyadapan informasi yang diunggah dalam bentuk apapun diancam dengan pidana penjara maksimal 15 (lima belas) tahun. Kemudian di dalam Pasal 30 UU ITE juga menyatakan bahwa barang siapa yang dengan sengaja mengakses sistem orang lain untuk memperoleh infomasi seseorang diancam dengan pidana penjara paling lama 8 (delapan) tahun dan denda maksimal Rp 8.000.000,00 (delapan ratus juta rupiah). Namun, regulasi ini belum dapat mengakomodir dan memberikan perlindungan dan kepastian hukum saat terjadi sebuah peretasan data.

2. Bank Indonesia selaku pihak yang menawarkan jasanya sebagai penyimpanan keuangan dan kegiatan keuangan lainnya harus merahasiakan keterangan terkait nasabahnya, penyimpanan dan simpanannya, serta memberikan rasa keamanan terkait data nasabahnya. Mengingat posisi Bank Indonesia sebagai bank sentral sudah seharusnya keamanan data milik Bank Indonesia terjaga secara ketat dan terkontrol oleh pihak terkait. Peretasan data sebanyak dua kali dan jumlah peretasan data yang terus meningkat menjadikan bukti adanya kelalaian dan keterlambatan dalam menangani kasus tersebut. Keterlambatan dalam penanganan kebocoran data milik Bank Indonesia juga menjadi suatu hal yang perlu diperbaiki dan menjadi catatan penting dalam upaya perlindungan data di dunia siber.

b. Saran

Adapun saran dari penelitian ini adalah

1. Pemerintah dapat bertanggung jawab untuk melindungi hak-hak rakyat, termasuk privasi terkait data pribadi, sehingga diharapkan melalui penelitian ini, pemerintah, khususnya DPR sebagai lembaga yang berwenang membuat Rancangan Undang-Undang, dapat menyelesaikan RUU Perlindungan Data Pribadi.
2. Rancangan Undang-Undang ini sudah menjadi Undang-Undang yang sah, pemerintah serta aparat penegak hukum dan instansi pemerintah yang berwenang lainnya seperti Kementerian Informasi dan Komunikasi, Badan Perlindungan Konsumen Nasional, Kementerian Perdagangan, POLRI serta Badan Siber dan Sandi Negara memiliki landasan dan dasar hukum untuk menindaklanjuti pelaku kebocoran data sehingga pengguna *e-commerce* dapat merasa terlindungi dan merasakan keamanan dan kenyamanan dalam berinternet.

DAFTAR PUSTAKA

Buku

Asikin, Zainal, and Dkk. *Dasar-Dasar Hukum Perburuhan*. Jakarta: PT. Raja Grafindo Persada, 2010.

Barda Nawawi Arief. *Tindak Pidana Mayantara Perkembangan Kajian Cyber Crime Di Indonesia*. Jakarta: PT Raja Grafindo, 2006.

Tim PY, Bala. *Undang-Undang Informasi Dan Transaksi Elektronik: Seri Perundangundangan*. Yogyakarta: Pustaka Yustisia, 2019.

Jurnal

Fathur, Muhammad. "TANGGUNG JAWAB TOKOPEDIA TERHADAP KEBOCORAN DATA PRIBADI KONSUMEN." *National Conference on Law Studies (NCOLS)* 2, no. 1 (November 19, 2020): 43–60.

Palinggi, Sandryones, and Erich C. Limbongan. "Pengaruh Internet Terhadap Industri Ecommerce Dan Regulasi Perlindungan Data Pribadi Pelanggan Di Indonesia." *Semnas Ristek (Seminar Nasional Riset dan Inovasi Teknologi)* 4, no. 1 (January

27, 2020). Accessed March 4, 2022. http://www.proceeding.unindra.ac.id/index.php/semnasristek/article/view/2543.

Putri, Deanne Destriani Firmansyah, and Muhammad Helmi Fahrozi. "UPAYA PENCEGAHAN KEBOCORAN DATA KONSUMEN MELALUI PENGESAHAN RUU PERLINDUNGAN DATA PRIBADI (STUDI KASUS E-COMMERCE BHINNEKA.COM)." *National Conference on Law Studies (NCOLS)* 2, no. 1 (November 19, 2020): 255–273.

Rahmawati, Ineu. "ANALISIS MANAJEMEN RISIKO ANCAMAN KEJAHATAN SIBER (CYBER CRIME) DALAM PENINGKATAN CYBER DEFENSE." *Jurnal Pertahanan & Bela Negara* 7, no. 2 (October 3, 2017): 35–50.

Rani, Marnia. "Perlindungan Otoritas Jasa Keuangan Terhadap Kerahasiaan Dan Keamanan Data Pribadi Nasabah Bank." *Jurnal Selat* 2, no. 1 (2014): 168–181.

Satrio, Muhamad Bayu, and Men Wih Widiatno. "PERLINDUNGAN HUKUM TERHADAP DATA PRIBADI DALAM MEDIA ELEKTRONIK (ANALISIS KASUS KEBOCORAN DATA PENGGUNA FACEBOOK DI INDONESIA)." *JCA of Law* 1, no. 1 (July 15, 2020). Accessed March 4, 2022. https://jca.esaunggul.ac.id/index.php/law/article/view/6.

Widyantari, Padma, and Adi Sulistiyono. "PELAKSANAAN HARMONISASI RANCANGAN UNDANG-UNDANG PERLINDUNGAN DATA PRIBADI (RUU PDP)." *Jurnal Privat Law* 8, no. 1 (February 2, 2020): 117–123.

Berita

"13 Juta Data Bocor Bukalapak Dijual Di Forum Hacker." Accessed February 22, 2022. https://www.cnnindonesia.com/teknologi/20200506065657-185-500477/13-juta-data-bocor-bukalapak-dijual-di-forum-hacker.

"Benarkan Ada Kebocoran Data Milik Bank Indonesia, BSSN Pastikan Bukan Data Kritikal." *KOMPAS.tv*. Accessed January 20, 2022. https://www.kompas.tv/article/253628/benarkan-ada-kebocoran-data-milik-bank-indonesia-bssn-pastikan-bukan-data-kritikal.

"Bukalapak Akui 13 Juta Data yang Dijual Hacker adalah Peretasan di Maret 2019." *kumparan*. Accessed February 21, 2022. https://kumparan.com/kumparantech/bukalapak-akui-13-juta-data-yang-dijual-hacker-adalah-peretasan-di-maret-2019-1tMRTr1UR0G.

"Kebocoran Data Bank Indonesia Terus Bertambah, Naik Jadi 74 GB! | Databoks." Accessed January 21, 2022. https://databoks.katadata.co.id/datapublish/2022/01/25/kebocoran-data-bank-indonesia-terus-bertambah-naik-jadi-74-gb.

"Tercatat, Kominfo Selesaikan 43 Kasus Kebocoran Data Pribadi Sepanjang 2021." *suara.com*. Last modified December 31, 2021. Accessed February 22, 2022. https://www.suara.com/tekno/2021/12/31/104557/tercatat-kominfo-selesaikan-43-kasus-kebocoran-data-pribadi-sepanjang-2021.

idxchannel. "Pembobol Data Penumpang Lion Air Group Akhirnya Terungkap." *https://www.idxchannel.com/*. Accessed February 21, 2022. https://www.idxchannel.com/market-news/pembobol-data-penumpang-lion-air-group-akhirnya-terungkap.

Indonesia, C. N. N. "Kebocoran Data Bank Indonesia Belum Selesai, Naik Jadi 74GB." *teknologi*. Accessed January 20, 2022.

https://www.cnnindonesia.com/teknologi/20220124163634-185-750569/kebocoran-data-bank-indonesia-belum-selesai-naik-jadi-74gb.

JawaPos.com. "91 Juta Data Akun Tokopedia Bocor dan Disebar Di Forum Internet." *JawaPos.com*. Last modified July 5, 2020. Accessed February 10, 2022. https://www.jawapos.com/oto-dan-tekno/teknologi/05/07/2020/91-juta-data-akun-tokopedia-bocor-dan-disebar-di-forum-internet/.

Liputan6.com. "Malindo: Kebocoran Data Gara-Gara Mantan Staf Perusahaan Kontraktor." *liputan6.com*. Last modified September 23, 2019. Accessed February 20, 2022. https://www.liputan6.com/tekno/read/4069498/malindo-kebocoran-data-gara-gara-mantan-staf-perusahaan-kontraktor.

Peraturan Perundang-undangan

Undang-Undang Nomor 8 Tahun 1997 tentang Dokumen Perusahaan. Lembaran Negara Republik Indonesia Tahun 1997 Nomor 18, Tambahan Lembaran Negara Republik Indonesia Nomor 3674.

Undang-Undang Nomor 10 Tahun 1998 tentang Perubahan atas Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan. Lembaran Negara Republik Indonesia Tahun 1998 Nomor 182, Tambahan Lembaran Negara Republik Indonesia Nomor 3790.

Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi (UU Telekomunikasi). Lembaran Negara Republik Indonesia Tahun 1999 Nomor 154, Tambahan Lembaran Negara Republik Indonesia Nomor 3881.

Undang-Undang Nomor 36 Tahun 2009 tentang Kesehatan. Lembaran Negara Republik Indonesia Tahun 2009 Nomor 144, Tambahan Lembaran Negara Republik Indonesia Nomor 5063.

Undang-Undang Nomor 43 Tahun 2009 tentang Kearsipan. Lembaran Negara Republik Indonesia Tahun 2009 Nomor 152, Tambahan Lembaran Negara Republik Indonesia Nomor 5071.

Undang-Undang Nomor 24 Tahun 2013 tentang Perubahan Atas Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan (UU Adminduk). Lembaran Negara Republik Indonesia Tahun 2013 Nomor 232, Tambahan Lembaran Negara Republik Indonesia Nomor 5475.

Undang-Undang Nomor 19 Tahun 2016 Tentang perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251, Tambahan Lembaran Negara Republik Indonesia Nomor 5952.

Peraturan Pemerintah Nomor 82 Tahun 2012 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Lembaran Negara Republik Indonesia Tahun 2012 Nomor 189, Tambahan Lembaran Negara Republik Indonesia Nomor 5348.

Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Lembaran Negara Republik Indonesia Tahun 2019 Nomor 185, Tambahan Lembaran Negara Republik Indonesia Nomor 6400.

Peraturan Menteri Komunikasi dan Informasi Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik. Berita Negara Republik Indonesia Tahun 2016 Nomor 1829.

RUU Perlindungan Data Pribadi, Rancangan Penjelasan Tentang Perlindungan Data Pribadi Secara Umum.