Jurnal Hukum Adigama

Volume 4 Nomor 2, Desember 2021
E-ISSN: 2655-7347 | P-ISSN: 2747-0873



# PERTANGGUNGJAWABAN PIDANA KORPORASI SEBAGAI PENYELENGGARA SISTEM ELEKTRONIK DALAM TERJADINYA KEBOCORAN DATA PENGGUNA SISTEM ELEKTRONIK

**Rony Mart Panjaitan**

(Fakultas Hukum Universitas Tarumanagara)

(E-mail: ronymartp@gmail.com)

## Abstract

*Based on reliable sources, it is to be found that Indonesia has experienced an increase in the number of active internet users between the time period of 2020 to 2021 with an estimate of 27 million users. Not forgetting the dangers of personal data leakage also goes hand in hand. One of the main factors that can pose a danger of personal data leakage is the lack of digital security in Indonesia, creating loop holes for telematics crimes. However, this does not rule out the possibility that the leakage of public personal data is carried out or caused by the corporation operating the internet system. This study examines the form of corporate criminal liability for electronic system operators in relation to the leakage of user data. The type of research used is prescriptive normative which is generally used to identify the law in accordance with legal principles in Indonesia. The research approach used is a conceptual approach, which refers to legal principles based on legal doctrine. Reinforced by sources, this research also uses primary, secondary and non-legal materials. Through this research we get to generate the idea of investigating data leakage occurrence through forensic examination, which may help us in identifying whether corporation managing the system is responsible of the criminal act or not. In this case, the corporation can be sentenced based on Article 52 of the Electronic Information and Transaction Law, if the corporation is found guilty, then the corporation must carry out administrative sanctions in accordance with the Electronic Information and Transaction Law and Government Regulations 71 of 2019. However, there are a few obligations in proving the same such as difficulty in proving the element of offense violated by the corporation and the fact that Indonesia highly upholds the principle of legality, which is one of the challenges in dealing with computer crime.*

***Keywords****: electronic system, corporation, data leakage*

## I. PENDAHULUAN

### A. Latar Belakang

Perkembangan teknologi informasi dan komunikasi yang telah memberikan banyak kemudahan dan peningkatan terhadap kualitas hidup manusia. Inovasi dan perkembangan komputer yang kini semakin ringkas dan semakin baik dari hari ke hari kini membuat hidup manusia bergerak lebih cepat, dinamis, dan lebih baik dari sebelumnya. Salah satu instrumen vital dalam perkembangan ini adalah

internet. Internet kini hadir dan memengaruhi setiap aspek kehidupan manusia modern. Berdasarkan data dari *Digital 2021 April Global Statshot Report* yang dirilis oleh *Hootsuite* dan *We Are Social* pengguna internet di seluruh dunia mengalami pertumbuhan sebanyak lebih dari 330 juta dalam kurun waktu setahun terakhir, dan telah mencapai total lebih dari 4,7 miliar pengguna internet aktif pada awal April 2021.[1)]

Internet memungkinkan manusia memiliki akses tak terbatas terhadap informasi, mengalami peningkatan terhadap cara berkomunikasi, dan mengalami peningkatan terhadap cara beraktivitas. Aktivitas yang dilakukan manusia kini tidak lagi dilaksanakan secara konvensional, melainkan melalui sebuah sistem komputer, internet, atau media elektronik lain yang kemudian diselenggarakan melalui sebuah sistem elektronik. Sistem elektronik tersebut diselenggarakan oleh penyelenggara sistem elektronik, yang pada intinya melakukan pengoperasian sebuah sistem elektronik.[2)]

Keberadaan korporasi sebagai penyelenggara sistem elektronik ini menjadi penting karena layanan berbasis sistem elektronik yang diselenggarakan oleh korporasi-korporasi semacam ini sudah merambah ke hampir semua aspek kehidupan sosial. Beberapa bukti nyata yang dapat dilihat adalah kemunculan berbagai sistem pembayaran elektronik, sistem perbankan elektronik, perkembangan industri *e-commerce*, akses terhadap layanan kesehatan secara elektronik, pendidikan, dan sebagainya. Dalam penyelenggaraan layanan-layanan ini, terdapat informasi elektronik milik pengguna sistem elektronik yang masuk untuk diproses dan dikelola oleh korporasi penyelenggara sistem elektronik tersebut. Informasi elektronik merupakan elemen penting dalam sebuah sistem elektronik karena proses verifikasi *(verification)* dan autentikasi

[1)] Simon Kemp, "Digital 2021 April Statshot Report", https://datareportal.com/reports/digital-2021-april-global-statshot, diakses tanggal 11 Agustus 2021.
[2)] Indonesia, *Undang-Undang Republik Indonesia 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)*, Pasal 1 ayat (6a).

*(authentication)* terhadap seseorang di sebuah sistem elektronik dilakukan melalui dokumen atau informasi elektronik.

Hal ini tentu berdampak baik apabila dilihat dari efisiensi dan efektifitas karena memangkas birokrasi. Namun, ada sisi lain yang perlu mendapat perhatian khusus mengingat untuk dapat menggunakan layanan sistem elektronik ini, ada informasi pribadi pengguna, data pribadi, preferensi pribadi, hingga tanda tangan digital yang masuk ke dalam sistem yang diselenggarakan oleh penyelenggara sistem elektronik tersebut. Keberadaan informasi elektronik berupa data pribadi pengguna layanan yang dikelola oleh penyelenggara sistem elektronik inilah yang perlu mendapat perhatian serius dari semua pihak.

Dalam beberapa tahun belakangan, kasus kebocoran data kian marak terjadi. Salah satu kasus yang cukup menggemparkan dunia adalah skandal kebocoran data pribadi Facebook dan Cambridge Analytica. Dalam laporannya, *The New York Times* mengatakan bahwa Cambridge Analytica telah mengambil data pribadi sekitar 50 juta akun Facebook secara ilegal pada tahun 2014 dan 2016 lalu. Atas insiden ini Komisi Perdagangan Federal (FTC) Amerika Serikat menjatuhkan denda sebesar 5 miliar USD atau sekitar 70 triliun rupiah kepada Facebook.[3)] Tidak cukup sampai disitu, Facebook kembali disorot mengenai kebocoran data pribadi sebanyak 533 juta pengguna dari 106 negara pada awal tahun 2021 lalu. Hal ini diungkapkan oleh *Chief Technology Officer* (CTO) sebuah perusahaan intelijen yang bernama Hudson Rock.[4)]

Di Indonesia sendiri kasus kebocoran data pribadi juga sudah semakin marak terjadi. Pada bulan Mei 2021 lalu, Indonesia dihebohkan dengan dugaan kebocoran data pengguna BPJS Kesehatan. Sebanyak 279 juta data pribadi pengguna diperjualbelikan di *Raid Forums* dengan harga jual hingga 80 juta

[3)] Bhaskar Chakravorti, "Why Facebook's new 'privacy cop' is doomed to fail", https://theconversation.com/why-facebooks-new-privacy-cop-is-doomed-to-fail-120960, diakses tanggal 13 Agustus 2021.
[4)] Novina Putri Bestari, "Data Facebook Bocor, 533 Juta User Terancam Dibegal Hacker" https://www.cnbcindonesia.com/tech/20210405101044-37-235223/data-facebook-bocor-533-juta-user-terancam-dibegal-hacker, diakses tanggal 13 Agustus 2021.

rupiah. Sebelumnya, pada tahun 2020 sebanyak 91 juta data pengguna dan 7 juta data *merchant* perusahaan *e-commerce* terbesar di Indonesia, Tokopedia, juga mengalami kebocoran dan disebar secara gratis di forum internet. Masih di tahun yang sama, sebanyak 2,3 juta data pemilih Komisi Pemilihan Umum (KPU) dan sebanyak 230 ribu data pasien *covid-19* juga diretas dan dijual di situs dan forum *online*.[5)]

Berkaca dari rentetan kasus kebocoran data yang terjadi, dapat dilihat bahwa kebocoran data *(data leakage)* dapat terjadi pada setiap sistem elektronik milik penyelenggara dikarenakan sebuah sistem elektronik yang terhubung dengan jaringan atau internet sangat rentan akan upaya-upaya peretasan yang berpotensi menyebabkan terjadinya kebocoran data *(data leakage)*. Maraknya kasus kebocoran data terjadi karena sistem elektronik ini tidak didukung dengan sistem keamanan digital yang mumpuni, maka sistem itu akan sangat rentan disusupi. Bahkan, terjadinya kebocoran data sering kali diketahui dari pihak ketiga, dalam artian informasi mengenai terjadinya kebocoran data ini terlebih dahulu diketahui melalui pemberitaan di media, dikarenakan penyelenggara sistem elektronik tidak menyadari bahwa telah terjadi peretasan dan kebocoran di dalam sistem yang mereka kelola. Keadaan ini terjadi dikarenakan adanya celah dan kelemahan pada sistem keamanan milik penyelenggara sistem elektronik sehingga data pribadi milik pengguna dapat dicuri oleh pihak yang tidak bertanggung jawab.[6)]

Terkait dengan penyelenggaraan sistem elektronik ini, hukum positif Indonesia melalui Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik (UU ITE) dan beberapa aturan sektoral mengatur mengenai kewajiban-kewajiban yang harus dipenuhi dalam rangka

---

5 ) Andrea Lidwina, "Kebocoran Data Pribadi yang Terus Berulang" https://katadata.co.id/ariayudhistira/infografik/60b3bbeda4185/kebocoran-data-pribadi-yang-terus-berulang, diakses tanggal 13 Agustus 2021.

6) Rudi Natamiharja, "A Case Study on Facebook Data Theft in Indonesia," *Fiat Justitia,* Nomor 12 Tahun 2018, 3.

penyelenggaraan sistem elektronik. Kewajiban-kewajiban tersebut dapat dilihat pada Pasal 15 dan Pasal 16 UU ITE, Pasal 3 sampai Pasal 5 Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem Dan Transaksi Elektronik, dan Pasal 5 sampai Pasal 6 Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 20 Tahun 2016 Tentang Perlindungan Data Pribadi Dalam Sistem Elektronik. Selain itu, UU ITE juga mengatur tentang perbuatan yang dilarang di dalam dalam Pasal 27 sampai dengan Pasal 35. Sedangkan ketentuan pidananya diatur di dalam dalam Pasal 45 sampai dengan Pasal 51. Namun, dalam hal terjadinya kebocoran data yang khususnya yang tidak disengaja dan tidak disadari, UU ITE tidak mengatur secara eksplisit karena UU ITE bersifat preventif. Hal ini dilihat dari adanya pengaturan mengenai kewajiban-kewajiban penyelenggara sistem elektronik akan tetapi tidak ditemukan adanya sanksi pidana apabila melanggar atau tidak melakukan kewajiban-kewajiban tersebut. Dalam hal pertanggungjawaban, hukum positif Indonesia hanya mengatur tentang pertanggungjawaban perdata melalui gugatan ganti rugi.

Maka dari itu, perlu adanya kajian mengenai delik kelalaian dan kegagalan pemenuhan kewajiban korporasi serta relevansi pemidanaan terhadap hal tersebut, mengingat korporasi penyelenggara sistem elektronik juga merupakan subjek hukum dalam ketentuan pidana peraturan perundang-undangan tentang transaksi dan sistem elektronik. Sehingga apabila terjadi kebocoran data pengguna yang diakibatkan oleh kelalaian atau tidak dipenuhinya kewajiban tersebut, korporasi penyelenggara sistem elektronik itu dapat dimintakan pertanggungjawaban pidana.

Berdasarkan uraian di atas, maka yang menjadi kajian dalam tulisan ini adalah mengenai delik dan pertanggungjawaban pidana korporasi sebagai penyelenggara sistem elektronik dalam terjadinya kebocoran data pengguna sistem elektronik.

## B. Perumusan Masalah

Berdasarkan pemaparan latar belakang permasalahan di atas, maka permasalahan yang akan dibahas dalam tulisan ini adalah bagaimana bentuk pertanggungjawaban pidana korporasi penyelenggara sistem elektronik dalam kebocoran data pengguna sistem elektronik?

## C. Metode Penelitian

1. Jenis Penelitian

   Jenis penelitian ini adalah penelitian hukum *(legal research)* yang bersifat normatif preskriptif.[7)] Penelitian hukum ini dilakukan dengan tujuan untuk menemukan kebenaran koherensi, yang menyoroti tentang apakah ada aturan hukum sesuai norma hukum dan apakah ada norma yang berupa perintah atau larangan yang sesuai dengan prinsip hukum, serta apakah perbuatan *(act)* seseorang sesuai dengan norma hukum atau prinsip hukum.[8)] Akan tetapi dalam hal ini bukan sekadar menerapkan aturan yang ada, melainkan juga menciptakan hukum untuk mengatasi masalah yang dihadapi.

2. Sumber Penelitian

   Untuk memecahkan permasalahan yang diangkat dan untuk memberikan preskripsi mengenai apa yang seharusnya, maka diperlukan sumber-sumber penelitian sebagai berikut:

   a. Bahan hukum primer, terdiri dari perundang-undangan, catatan-catatan resmi, atau risalah dalam pembuatan perundang-undangan dan putusan-putusan hakim.
   b. Bahan hukum sekunder, merupakan publikasi tentang hukum yang bukan merupakan dokumen-dokumen resmi, yang terdiri dari buku teks

[7)] Peter Mahmud Marzuki, *Penelitian Hukum* (Jakarta:Prenada Media Group, 2015), 55.
[8)] *Ibid*, 47.

hukum, kamus hukum, jurnal hukum, dan komentar atas putusan pengadilan. [9)]

## II. PEMBAHASAN

### A. Korporasi sebagai Penyelenggara Sistem Elektronik, Kebocoran Data *(Data Leakage)*, dan Forensik Digital *(Digital Forensics)*

Di era teknologi informasi saat ini, korporasi memiliki peran yang sangat besar bagi kepentingan manusia maupun bagi kepentingan negara. Eksistensi korporasi bagi manusia dapat dilihat dari fakta bahwa korporasi mencukupi dan kehidupan manusia pada saat ini. Sedangkan bagi negara, korporasi berperan meningkatkan penerimaan negara melalui pajak, membuka lapangan pekerjaan, dan pemanfaatan teknologi. Salah satu bentuk pemanfaatan teknologi oleh korporasi adalah pemanfaatan dan pengelolaan data, seperti lahirnya uang digital *(e-money)*, cek elektronik, kartu kredit, hingga dompet digital *(e-wallet)*, yang semuanya merupakan produk korporasi yang memanfaatkan basis data sebagai inti *(core)* operasional bisnisnya.[10)]

Di era digital saat ini, data telah mengalami perubahan menjadi data digital dan tersimpan secara *online*.[11)] Data dan/atau informasi ini dikumpulkan oleh situs-situs pemerintah dan korporasi swasta dengan tujuan tertentu. Pengumpulan dan pengelolaan data oleh pemerintah dilakukan untuk mendukung pelayanan publik. Sedangkan bagi korporasi sebagai penyelenggara sistem elektronik, data dan/atau informasi pribadi milik pengguna sistem elektronik dipergunakan sebagai alat verifikasi dan autentikasi atas pelayanan yang diberikan oleh penyelenggara, namun di sisi lain data dan informasi pribadi pengguna juga kini telah menjadi komoditas yang diperjualbelikan dan bernilai jutaan dollar.[12)] Data dan informasi pribadi telah dianggap sebagai aset perusahaan yang bernilai ekonomi tinggi dan

---

[9)] *Ibid*, 181.
[10)] Josua Sitompul, *Cyberspace, Cybercrimes, Cyberlaw*, (Jakarta: Tatanusa, 2014), 61.
[11)] Starkey, L., & Eppel, E, "Digital Data in New Zealand Schools: Policy Reform and School Leadership", *Educational Management Administration & Leadership*, 2017, 1-19.
[12)] Edmon Makarim, *Kompilasi Hukum Telematika*, (Jakarta: Raja Grafindo Perkasa,2003), 3.

dapat memberikan pemasukan kepada perusahaan tersebut.[13)] Namun di sisi lain menjadi tantangan tersendiri bagi korporasi karena potensi nilai ekonomi inilah yang menjadi motif para pelaku kejahatan siber untuk melakukan pencurian data *(data breach)* dan informasi milik pengguna yang dikelola oleh korporasi penyelenggara sistem elektronik.

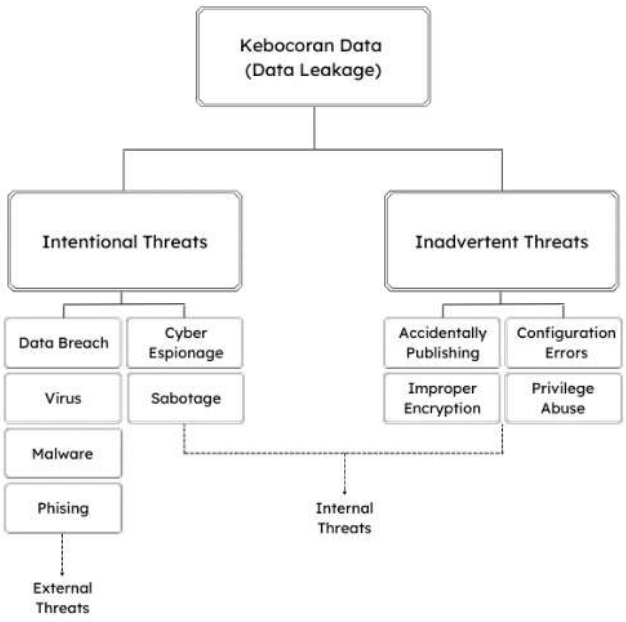
Pada dasarnya setiap penyelenggaraan sistem elektronik memiliki risiko. Risiko ini bisa berasal dari manusia, faktor alamiah, hingga sistem elektronik itu sendiri. Dalam rangka manajemen resiko ini, sistem pengamanan dalam penyelenggaraan sistem elektronik harus dilaksanakan melalui Sistem Manajemen Pengaman Informasi (SMPI) yang diatur di dalam Peraturan Badan Siber dan Sandi Negara Nomor 8 Tahun 2020 tentang Sistem Pengamanan Dalam Penyelenggaraan Sistem Elektronik ("**Peraturan BSSN 8/2020**"). Badan Siber dan Sandi Negara (BSSN) sendiri merupakan lembaga pemerintah yang menyelenggarakan tugas pemerintahan di bidang keamanan siber.[14)]

*Data breach* adalah serangan siber *(cyber attack)* yang memang bertujuan untuk mencuri data yang sifatnya sensitif dan rahasia dengan cara membobol atau meretas sistem elektronik milik penyelenggara. Sedangkan, kebocoran data *(data leakage)* adalah sebuah kondisi dimana terekspos nya sebuah data yang sifatnya sensitif dan rahasia. Kebocoran data *(data leakage)* dapat diklasifikasikan menjadi dua berdasarkan faktor penyebab terjadinya yaitu secara sengaja *(intentional)* dan secara tidak sengaja *(inadvertently)*. Selain itu dapat pula diklasifikasikan berdasarkan pihak yang terlibat, yaitu pihak dalam/internal *(insider)* pihak luar/eksternal *(outsider).* Kebocoran data karena faktor ancaman eksternal atau pihak luar biasanya disebabkan oleh serangan *hacker* seperti *data breach*, penyebaran *malware*, *virus, phising* dengan tujuan untuk mengeksploitasi sebuah sistem. Hal ini biasanya dilakukan untuk mendapatkan kontrol akses untuk

[13)] *Ibid.*, 185.
[14)] *Indonesia, Peraturan Badan Siber dan Sandi Negara Nomor 8 Tahun 2020 tentang Sistem Pengamanan Dalam Penyelenggaraan Sistem Elektronik, (Berita Negara Republik Indonesia Tahun 2020 Nomor 1375*), Pasal 1 angka (17).

melewati *(bypass)* mekanisme verifikasi *(verification)* dan autentikasi *(authentication)* sistem elektronik tersebut.

Sedangkan karena faktor ancaman internal, kebocoran data bisa terjadi karena perbuatan yang disengaja seperti spionase *(cyber espionage)*, dan kesalahan yang tidak disengaja (kelalaian), seperti terekspos nya *(accidentally publishing)* dan transmisi data sensitif yang tidak disengaja dan tanpa enkripsi yang kuat *(improper encryption)*. Untuk menggambarkan lebih jelas mengenai pengklasifikasian mengenai kebocoran data *(data leakage)*, dapat dilihat dalam bagan berikut ini:[15)]




*Bagan 1. Klasifikasi Kebocoran Data*

Berdasarkan hal tersebut dapat dilihat bahwa kebocoran data memiliki beberapa faktor penyebab yang tentunya harus diperhatikan dalam rangka

[15)] Long Cheng, Fang Liu dan Danfeng Yao, *Enterprise data breach: causes, challenges, prevention, and future directions*, (by John Wiley & Sons, Ltd: WIREs Data Mining and Knowledge Discovery, 2017), 2.

menuntut pertanggungjawaban pidana bagi korporasi penyelenggara sistem elektronik. Maka dari itu perlu dilakukan pemeriksaan forensik digital *(digital forensics)* untuk mengetahui apa yang menjadi penyebab terjadinya kebocoran data dalam sebuah sistem elektronik tersebut. Faktor inilah yang kemudian coba diidentifikasi melalui forensik digital, sehingga menjadi dasar untuk menganalisis pertanggungjawaban pidana korporasi sebagai penyelenggara elektronik dalam terjadinya kebocoran data pengguna sistem elektronik tersebut.

## B. Pertanggungjawaban Pidana Korporasi sebagai Penyelenggara Sistem Elektronik dalam Terjadinya Kebocoran Data Pengguna Sistem Elektronik

Pada dasarnya setiap penyelenggaraan sistem elektronik memiliki risiko. Risiko ini bisa berasal dari manusia, faktor alamiah, hingga sistem elektronik itu sendiri. Permasalahan yang muncul kemudian adalah terkait dengan bagaimana pengelolaan terhadap risiko dan siapa yang bertanggung jawab atas terjadinya risiko tersebut. Ghadeer Neama dkk. (2016) menerbitkan sebuah tulisan yang berjudul *Privacy, Security Risk, and Trust Concern in e-Commerce*, tentang prinsip kehati-hatian dalam penyelenggaraan sistem elektronik. Dalam tulisan tersebut dikatakan bahwa:

> *"Due to such growth, businesses owners should realize that it is vital to improve online services provided to their customers. Currently, many companies are gathering customers' information (e.g., name, address, interest, etc.) through registration, online transactions, or cookies in order to achieve such improvement in provided services. Privacy and security concerns are the major barriers from adopting e-commerce services."*[16)]

[16)] Ghadeer Neama, Rana W. Alaskar, M. Alkandari, "Privacy, Security Risk, and Trust Concern in e-Commerce", *Proceedings of the 17th International Conference on Distributed Computing and Networking*, January 2016, 1.

Dari pernyataan di atas dapat dipahami bahwa keamanan informasi adalah hal yang menjadi titik perhatian. Setidaknya ada tiga aspek utama dari keamanan informasi, yaitu:[17)]

1. Kerahasiaan *(Confidentiality)*, yaitu sebuah informasi hanya dapat diakses oleh pihak yang berhak, berwenang. Artinya ada pembatasan akses untuk mengungkap informasi tersebut.
2. Keutuhan *(Integrity)*, artinya informasi dalam kondisi yang murni *(genuine)*, tidak ada modifikasi atau perubahan tanpa izin atau persetujuan dari pemilik dan pemegak hak atas informasi tersebut.
3. Ketersediaan *(Availability)*, yaitu informasi tersebut dapat diakses oleh pihak yang berhak dan berwenang.

Ketiga aspek di atas adalah wujud dari pemenuhan atas keamanan *(security)* dan privasi *(privacy)* dalam penyelenggaraan sistem elektronik. Dalam kaitannya dengan teori pelindungan data pribadi, keamanan dan privasi adalah hal yang paling penting sebagai jaminan hak atas privasi *(privacy rights)* dan kepentingan hukum pengguna sistem elektronik, karena di era digital saat ini data pribadi pengguna sangat rentan akan penyalahgunaan.

Terjadinya kebocoran data *(data leakage)* yang disebabkan oleh faktor eksternal diantaranya *data breach, virus, malware, phising*, dan upaya-upaya peretasan lainnya. Dalam hal ini, apabila sistem elektronik milik penyelenggara berhasil dibobol sehingga menyebabkan terjadinya kebocoran data, maka korporasi penyelenggara sistem elektronik tersebut tidak bisa langsung dituntut pertanggungjawaban pidananya. Hal ini menjadi penting mengingat belum tentu ada *mens rea*, sehingga korporasi tersebut tidak bisa langsung dipersalahkan, mengingat semua perbuatan yang dilarang oleh UU ITE merupakan kesalahan yang bentuknya adalah kesengajaan. Namun, korporasi penyelenggara sistem elektronik tersebut harus mampu membuktikan bahwa korporasi tersebut telah menjalankan kewajiban-kewajibannya seperti yang telah diatur di dalam UU ITE,

[17)] Kyosti Pennanen, Taina Kaapu, dan Minna Paakki, "Trust, Risk, Privacy, and Security in w-Commerce", *Frontiers of e-Business Research*, 2006, 23.

PP 71/2019, dan Peraturan BSSN 8/2020. Salah satu yang harus dibuktikan keamanan sistem elektronik tersebut seperti yang tertuang dalam Pasal 15 UU ITE j.o Pasal 3 PP 71/2019, yang mengatakan bahwa sistem elektronik harus diselenggarakan secara andal dalam artian memiliki kemampuan yang sesuai dengan kebutuhan penggunaannya, dan aman atau terlindungi secara fisik dan non fisik.[18)] Selain itu, sistem elektronik tersebut juga harus menerapkan standar SNI ISO/IEC 27001 sebagaimana diatur dalam Peraturan BSSN 8/2020.

Selain disebabkan oleh faktor eksternal, kebocoran data juga bisa terjadi diakibatkan oleh faktor internal. Faktor internal ini seperti misalnya, serangan oleh karyawan perusahaan *(insider)* melalui penyalahgunaan wewenang dan kesalahan pada sistem yang disadari *(system bug, configuration error, improper encryption).* Korporasi penyelenggara sistem elektronik, dalam operasionalnya juga bisa saja mengalami ganguan teknis seperti yang telah disebutkan di atas, yang menyebabkan data rusak *(corrupt)* walaupun tidak ada unsur kesengajaan. Seperti yang telah dijelaskan sebelumnya, penyelenggaraan sistem elektronik mengandung risiko yang sangat besar terhadap ancaman-ancaman peretasan yang hingga kini terus berkembang seiring semakin majunya teknologi informasi. Hal inilah yang perlu diantisipasi oleh penyelenggara dengan cara turut melakukan *upgrade* dan perbaikan berkala terhadap sistem elektronik yang mereka kelola. Hal ini disebabkan karena sebuah sistem akan selalu memiliki *bug* yang apabila tidak segera diperbaiki akan menimbulkan kerentanan untuk disusupi. Jika *bug* ini ditemukan oleh pihak lain yang memiliki niat jahat, maka dapat masuk ke dalam sistem dan melakukan tindak kejahatan seperti pencurian data hingga pengrusakan.[19)]

Maka terhadap hal tersebut korporasi penyelenggara sistem elektronik harus melakukan perawatan *(maintenance)* dan evaluasi berkala terhadap sistem yang mereka kelola dalam rangka menjamin keamanan. Apabila dalam evaluasi ditemukan celah *(loophole)* atau *bug* yang dapat mengganggu keamanan sistem,

[18)] Penjelasan Umum Pasal 3, PP 71/2019.
[19)] Josua Sitompul, *Op. Cit*., 84.

maka penyelenggara harus melakukan langkah-langkah antisipatif untuk memperbaiki dan mengamankan sistem mereka, karena jika tidak dilakukan, hal ini dapat dikatakan sebagai kelalaian yang disadari.

Dalam hal kemudian kebocoran data dilakukan dengan kesengajaan, seperti yang diatur di dalam Pasal 27 sampai Pasal 37, maka korporasi penyelenggara sistem elektronik dipidana dengan pidana pokok ditambah dua pertiga. Perbuatan oleh korporasi ini mencakup pula pengurus dan/atau staff yang memiliki kapasitas untuk mewakili korporasi, mengambil keputusan dalam korporasi, melakukan pengawasan dan pengendalian dalam korporasi, dan melakukan kegiatan demi keuntungan korporasi.[20)]

Selanjutnya mengenai pertanggungjawaban pidana dalam terjadinya kebocoran data, apabila berdasarkan hasil forensik digital menunjukkan bahwa sistem elektronik milik korporasi penyelenggara tidak diselenggarakan dengan andal dan aman sesuai dengan standar yang ditetapkan oleh peraturan perundang-undangan, maka korporasi penyelenggara sistem elektronik tersebut dapat dimintakan pertanggungjawaban pidana. Hal ini dapat dilihat dari bentuk kesalahannya, yaitu kealpaan *(imperitia culpae annumeratur)*, yang artinya kealpaan adalah kesalahan.[21)] Dalam terjadinya kebocoran data maka kealpaan dapat dilihat dari penyelenggaraan yang harus menerapkan prinsip kehati-hatian. Hal ini dikarenakan kealpaan meliputi ketidakhati-hatian, kurang perhatian, dan tidak melakukan sesuatu. Kurang penghati-hatian disini dapat dilihat karena tidak adanya penelitian, kebijaksanaan, kemahiran, dan usaha pencegahan yang nyata dalam keadaan tertentu, dalam hal ini kebocoran data.[22)]

Pengaturan mengenai kealpaan penyelenggara sistem elektronik yang dapat menyebabkan kebocoran data inilah yang belum ditemukan pengaturannya dalam peraturan pidana di Indonesia *(rechtvacuum)*. Maka dari itu ketika kebocoran data

---

[20)] Indonesia, *Undang-Undang Republik Indonesia 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)*, Pasal 52 ayat (4) dan Penjelasannya.
[21)] Eddy O.S Hiariej, *Prinsip-Prinsip Hukum Pidana*, (Yogyakarta: Cahaya Atma Pustaka, 2015), 195.
[22)] *Ibid*, 192.

terjadi, korporasi penyelenggara sistem elektronik tidak dapat dimintakan pertanggungjawaban pidana karena kesulitan dalam pembuktian unsur delik yang dilanggar oleh korporasi tersebut. Selain itu, terdapat kendala karena dalam prakteknya Indonesia sangat menjunjung tinggi asas tiada pidana tanpa kesalahan atau asas legalitas. Hal inilah kemudian yang menjadi salah satu tantangan dalam menghadapi kejahatan komputer *(computer related crime)* karena asas legalitas cenderung membatasi ruang gerak penegak hukum untuk melakukan penyelidikan dan penyidikan terhadap kejadian tersebut.

## C. Pemidanaan Korporasi Penyelenggara Sistem Elektronik dan Pendekatan Hukum Progresif sebagai Upaya Mengatasi Kejahatan Telematika

Kebocoran data *(data leakage)* adalah salah satu bentuk pelanggaran terhadap hak atas privasi. Kebocoran data juga menyebabkan kerugian bagi masyarakat luas karena tersebarnya data pribadi milik pengguna sehingga pengguna tersebut rentan terhadap tindak kejahatan, khususnya kejahatan berbasis teknologi atau kejahatan telematika. Dalam hal inilah kemudian hukum pidana berperan sebagai salah satu alat untuk mengatasi masalah sosial termasuk dalam penegakan hukum yang tujuannya adalah kesejahteraan masyarakat.[23)] Dalam terjadinya kebocoran data yang disebabkan oleh kealpaan atau kelalaian oleh penyelenggara sistem elektronik, maka korporasi penyelenggara tersebut dikenai sanksi administratif. Mengingat hal ini telah melanggar hak atas privasi dan korbannya sangat luas, maka perlu dipertimbangkan pemidanaan terhadap korporasi penyelenggara sistem elektronik. Hal ini perlu menjadi pertimbangan mengingat masalah kejahatan merupakan permasalahan kemanusiaan dan permasalahan sosial. Salah satu upaya untuk menanggulanginya adalah melalui kebijakan kriminal *(criminal policy)*. Kebijakan kriminal sendiri dapat dimaknai sebagai upaya rasional dari negara untuk mengatasi kejahatan, yang dalam hal ini bertujuan untuk

[23)] Teguh Prasetyo, *Kriminalisasi Dalam Hukum Pidana*, (Bandung: Nusa Media, 2010), 19.

perlindungan masyarakat *(social defense planning)* serta untuk mencapai kesejahteraan.[24)]

Dalam tatanan teori, pemidanaan dilakukan dilakukan mencapai tujuan yang bermanfaat untuk melindungi masyarakat menuju kesejahteraan. Inilah yang disebut sebagai teori pemidanaan relatif *(doel theorien)* yang menekankan pada pencegahan bukan pembalasan. Dalam hal pemidanaan terhadap korporasi penyelenggara sistem elektronik, maka teori relatif *(doel theorien)* bisa dipandang sebagai teori yang relevan, mengingat kebocoran data merupakan *public wrongs* yang melibatkan korban yang sangat luas. Sehingga prospek kemakmuran masyarakat yang ingin dicapai oleh teori ini relevan terhadap fenomena kebocoran data ini. Pemidanaan terhadap korporasi penyelenggara sistem elektronik ini bukan semata-mata untuk menghukum, namun lebih kepada tujuan lain yaitu untuk menegakkan kepatuhan korporasi penyelenggara sistem elektronik dalam rangka melindungi dan mencapai kesejahteraan dan keamanan masyarakat sebagai pengguna sistem elektronik.

Selanjutnya terhadap terjadinya kebocoran data pengguna sistem elektronik yang pada pemaparan sebelumnya menunjukkan bahwa telah terjadi kekosongan hukum *(rechtvacuum)* yang menunjukkan ketidakmampuan hukum pidana positif mengikuti perkembangan ilmu pengetahuan dan teknologi yang demikian pesatnya. Dalam hal inilah kemudian gagasan hukum progresif menjadi relevan dan strategis. Perlu diketahui bahwa progresivisme tidak mengharamkan hukum positif. Dalam ajarannya progresivisme tetap berpegang pada hukum positif, akan tetapi pemaknaan terhadap hukum positif tersebut harus dilakukan secara luas dan tajam.[25)] Sebagai contoh, perbuatan *hacking* dan *cracking* yang merupakan salah satu bentuk kejahatan telematika yang muncul seiring berkembangnya teknologi komputer. Namun, apabila dimaknai secara dalam, perbuatan *hacking* ini sendiri

[24)] Yenti Garnasih, "Kriminalisasi Pencucian Uang (Money Laundering)", *Pascasarjana FH-UI, Jakarta*, 2003, 12.
[25)] Al Wibisono, *Strategi Penanggulangan Kejahatan Telematika*, (Yogyakarta: Atma Jaya, 2010), 80.

pada dasarnya sama dengan perbuatan *trespass* di dalam pasal 167 KUHP, dan *cracking* atau perbuatan merusak pada Pasal 406 KUHP.

Progresivisme sendiri bukanlah hal yang baru dalam dunia hukum Indonesia. Hal ini dapat dibuktikan dengan adanya yurisprudensi terkait kejahatan-kejahatan berbasis teknologi, diantaranya sebagai berikut:

1. Putusan Pengadilan Negeri Jakarta Barat pada tahun 1989 yang menerapkan Pasal 362 KUHP tentang pencurian dalam kasus *data diddling* PT Bank Bali cabang Jakarta Barat.[26)]
2. Putusan Pengadilan Negeri Sleman pada tahun 2002 yang menerapkan Pasal 378 KUHP tentang penipuan dalam kasus *carding*.[27)]
3. Putusan Pengadilan Negeri Semarang pada tahun 2003 yang menerapkan Pasal 362 tentang pencurian dalam kasus *carding.*[28)]

Berdasarkan yurisprudensi di atas, dapat dilihat bahwa putusan-putusan tersebut tergolong progresif karena penegak hukum dalam perkara tersebut memiliki keberanian untuk melakukan pencarian, yaitu terobosan yang dilakukan aparat penegak hukum untuk menggunakan hukum positif secara kreatif dalam penyelesaian kasus yang belum diatur secara khusus. Selain itu penegak hukum juga melakukan upaya pembebasan, yang tampak dari sikap membebaskan diri dari stigma corong undang-undang atau kekakuan atas hukum positif. Serta upaya pencerahan yang terlihat dari dampak yang ditimbulkan atas putusan tersebut dalam penyelesaian masalah kejahatan di bidang teknologi, yang menunjukkan bahwa keadilan dapat terjadi tanpa harus menunggu terciptanya hukum positif.[29)]

Pada akhirnya, progresivisme tidak serta merta dapat menyelesaikan permasalahan kejahatan telematika, khususnya dalam kebocoran data pengguna sistem elektronik, karena dalam kenyataannya saat ini Indonesia masih menempatkan hukum positif sebagai landasan utama dalam penegakan hukum.

[26)] Putusan Pengadilan Negeri Jakarta Barat No. 1050/Pid.S/1989/PN.Jkt.Bar. 20 November 1989.
[27)] Putusan Pengadilan Negeri Sleman No. 94/Pid.B/2002/PN. Slmn.
[28)] Putusan Pengadilan Negeri Semarang No. 504/Pid.B/2003/PN.Smg.
[29)] Al Wibisono, *Op. Cit*., 83.

Sehingga pendekatan hukum progresif dalam ranah praktek tidak dapat dilakukan secara ekstrim dengan mengabaikan aspek normatif. Namun, berkaitan dengan permasalahan ini semangat progresivisme perlu dikembangkan dalam kebijakan dan penerapan hukum positif untuk mencapai keadilan dan kesejahteraan masyarakat.

## III. PENUTUP

### A. Kesimpulan

Berdasarkan analisis permasalahan yang telah dilakukan, maka dapat ditarik kesimpulan bahwa terjadinya kebocoran data *(data leakage)* disebabkan beberapa faktor yang dapat diketahui dari hasil pemeriksaan forensik digital *(digital forensics)* sebagaimana telah disampaikan di dalam analisis permasalahan. Dalam hal kemudian terjadi peretasan atau pembobolan terhadap sistem yang menyebabkan terjadinya kebocoran data, yang apabila dilakukan secara sengaja, maka korporasi sebagai subjek tindak pidana di dalam UU ITE, dapat dijatuhi pertanggungjawaban pidana. Hal ini dapat dilihat dari pengaturan dalam Pasal 52 UU ITE.

Sedangkan dalam terjadinya kebocoran data yang yang diakibatkan oleh adanya kelalaian terhadap kewajiban-kewajiban penyelenggara sistem elektronik, UU ITE dan PP 71/2019 hanya mengatur tentang penjatuhan sanksi administratif bagi penyelenggara sistem elektronik. Pengaturan mengenai pidananya sendiri tidak ditemukan *(rechtvacuum)* sehingga ketika kebocoran data terjadi, korporasi penyelenggara sistem elektronik tidak dapat dimintakan pertanggungjawaban pidana karena kesulitan dalam pembuktian unsur delik yang dilanggar oleh korporasi tersebut. Kriminalisasi terhadap korporasi penyelenggara sistem elektronik yang gagal memenuhi kewajibannya sebagaimana diatur dalam peraturan perundang-undangan perlu dipertimbangkan karena dampak kebocoran data dirasakan oleh masyarakat luas.

### B. Saran

Berdasarkan analisis permasalahan yang telah dilakukan, maka adapun hal-hal yang dapat dilakukan adalah sebagai berikut:

1. Bagi korporasi pengguna sistem elektronik, dalam terjadinya kebocoran data *(data leakage)* pengguna, maka perlu dilakukan pemeriksaan forensik digital *(digital forensics)*. Hal ini perlu dilakukan untuk mengetahui bagaimana mekanisme pertanggungjawabannya. Hasil forensik digital juga sebaiknya diberitahukan kepada pengguna sistem elektronik yang dalam hal ini sebagai korban data yang mengalami kebocoran.
2. Bagi aparat penegak hukum, hak atas privasi *(privacy rights)* di era teknologi saat ini sangat terancam keberadaannya. Perlindungan terhadap hak atas privasi perlu ditegakkan dengan sungguh-sungguh untuk memberikan rasa aman dan kesejahteraan bagi masyarakat luas.

## IV. DAFTAR PUSTAKA

### A. Buku

Garnasih, Yenti. *Kriminalisasi Pencucian Uang (Money Laundering)*. (Jakarta: Pascasarjana FH-UI, 2003).

Hiariej, Eddy O.S. *Prinsip-Prinsip Hukum Pidana*. (Yogyakarta: Cahaya Atma Pustaka, 2015).

Makarim, Edmon. *Kompilasi Hukum Telematika,* (Jakarta: Raja Grafindo Perkasa, 2003).

Marzuki, Peter Mahmud. *Penelitian Hukum* (Jakarta: Prenada Media Group, 2015).

Prasetyo, Teguh. *Kriminalisasi Dalam Hukum Pidana*. (Bandung: Nusa Media, 2010).

Sitompul, Josua. *Cyberspace, Cybercrimes, Cyberlaw*. (Jakarta: Tatanusa, 2014).

Wibisono, Al. *Strategi Penanggulangan Kejahatan Telematika*. (Yogyakarta: Atma Jaya, 2010).

**B. Peraturan Perundang-undangan**

*Indonesia, Peraturan Badan Siber dan Sandi Negara Nomor 8 Tahun 2020 tentang Sistem Pengamanan Dalam Penyelenggaraan Sistem Elektronik, (Berita Negara Republik Indonesia Tahun 2020 Nomor 1375*).

Indonesia, *Undang-Undang Republik Indonesia 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).*

**C. Artikel Jurnal**

Cheng, Long. et al. *Enterprise Data Breach: Causes, Challenges, Prevention, and Future Directions*. (John Wiley & Sons, Ltd: WIREs Data Mining and Knowledge Discovery, 2017).

L, Starkey dan Eppel, E. "Digital Data in New Zealand Schools: Policy Reform and School Leadership". *Educational Management Administration & Leadership*. (2017).

Natamiharja, Rudi. "A Case Study on Facebook Data Theft in Indonesia," *Fiat Justitia,* Edisi No. 12 Tahun 2018.

Neama, Ghadeer. et. al. "Privacy, Security Risk, and Trust Concern in e-Commerce". *Proceedings of the 17th International Conference on Distributed Computing and Networking.* Edisi No. 46 Tahun 2016.

Pennanen, Kyosti. et. al. "Trust, Risk, Privacy, and Security in e-Commerce". *Frontiers of e-Business Research*. Tahun 2006.

**D. Putusan**

Putusan Pengadilan Negeri Jakarta Barat No. 1050/Pid.S/1989/PN.Jkt.Bar.

Putusan Pengadilan Negeri Semarang No. 504/Pid.B/2003/PN.Smg.

Putusan Pengadilan Negeri Sleman No. 94/Pid.B/2002/PN. Slmn.

**E. *Website***

Bestari, Novina Putri. "Data Facebook Bocor, 533 Juta User Terancam Dibegal Hacker" https://www.cnbcindonesia.com/tech/20210405101044-37-235223/data-facebook-bocor-533-juta-user-terancam-dibegal-hacker, 13 Agustus 2021.

Chakravorti, Bhaskar. "Why Facebook's new 'privacy cop' is doomed to fail", https://theconversation.com/why-facebooks-new-privacy-cop-is-doomed-to-fail-120960, 13 Agustus 2021.

Kemp, Simon. "Digital 2021 April Statshot Report", https://datareportal.com/reports/digital-2021-april-global-statshot, 11 Agustus 2021.

Lidwina, Andrea. "Kebocoran Data Pribadi yang Terus Berulang" https://katadata.co.id/ariayudhistira/infografik/60b3bbeda4185/kebocoran-data-pribadi-yang-terus-berulang, 13 Agustus 2021.