Indonesian Journal of Law and Justice Volume: 1, Nomor 2, 2024, *Hal*: 1-9

Pertanggungjawaban Badan Penyelenggara Jaminan Sosial (BPJS) Kesehatan Atas Kebocoran Data Pribadi Pengguna dalam Perspektif Hukum Pidana

One Maulida [1], Hari Utomo [2]

[1] Universitas Muhammadiyah Jember; omaulida2206@gmail.com
[2] Universitas Muhammadiyah Jember; utomohari851@gmail.com

DOI: https://doi.org/10.47134/ijlj.v1i2.2011
*Correspondensi: One Maulida dan Hari Utomo
Email: omaulida2206@gmail.com, utomohari851@gmail.com

Received: 03-10-2023
Accepted: 15-11-2023
Published: 27-12-2023

Abstrak: BPJS Kesehatan merupakan Badan Penyelenggara Jaminan Sosial Kesehatan yang bertanggung jawab dalam menyelenggarakan program jaminan kesehatan bagi masyarakat indonesia. Namun dalam era digitalisasi yang semakin berkembang, kebocoran data pengguna menjadi masalah serius yang harus ditangani dengan sungguh-sungguh. Kebocoran data pengguna telah menjadi isu yang semakin meresahkan dalam era digital ini. Salah satu entitas yang bertanggung jawab dalam menjaga kerahasiaan data pengguna adalah Badan Penyelenggara Jaminan Sosial Kesehatan. Artikel ini bertujuan untuk menganalisis pertanggungjawaban BPJS Kesehatan atas kebocoran data pengguna dari perspektif hukum pidana. Penelitian ini menggunakan metode penelitian normatif dengan pendekatan perundang-undangan dan kasus-kasus terkait dalam analisisnya. Hasil penelitian menunjukkan bahwa kebocoran data pengguna oleh Badan Penyelenggara Jaminan Sosial Kesehatan dapat melanggar beberapa ketentuan pidana sebagaimana tertera dalam Undang-Undang No. 27 tahun 2022 tentang perlindungan data pribadi dan berdasarkan Undang-undang no.11 tahun 2008 tentang Informasi dan Transaksi Elektronik, terutama dalam konteks pelanggaran kerahasiaan dan perlindungan data pribadi. Dapat diambil kesimpulan, BPJS Kesehatan memiliki tanggung jawab hukum pidana atas kebocoran data pengguna. Untuk meminimalkan risiko kebocoran data, Badan Penyelenggara Jaminan Sosial Kesehatan perlu meningkatkan keamanan sistem dan kepatuhan terhadap peraturan perlindungan data pribadi. Selain itu, pemerintah perlu menguatkan pengawasan dan penegakan hukum dalam menghadapi kasus-kasus kebocoran data yang melibatkan entitas publik seperti BPJS Kesehatan.

Keywords: Perlindungan Data Pribadi; Kebocoran Data; Pertanggungjawaban Pidana

Abstract: *BPJS Health is the Health Social Security Organizing Agency which is responsible for administering health insurance programs for the Indonesian people. However, in the era of increasingly digitalization, user data leakage is a serious problem that must be handled seriously. User data leaks have become an increasingly disturbing issue in this digital era. One of the entities responsible for maintaining the confidentiality of user data is the Social Security Administering Agency for Health. This article aims to analyze BPJS Health's responsibility for leaking user data from a criminal law perspective. This research uses normative research methods with a statutory approach and related cases in its analysis. The research results show that leakage of user data by the Health Social Security Administering Agency can violate several criminal provisions as stated in Law no. 27 of 2022 concerning personal data protection and based on Law no. 11 of 2008 concerning Information and Electronic Transactions, especially in the context of violations of confidentiality and protection of personal data. It can be concluded that BPJS Health has criminal legal responsibility for user data leaks. To minimize the risk of data leaks, the Social Security Administering Agency for Health needs to improve system security and compliance with personal data protection regulations. Apart from that, the government needs to strengthen supervision and law enforcement in dealing with cases of data leaks involving public entities such as BPJS Health.*

Keywords: *Personal Data Protection; Data Leakage; Criminal Liability*

Pendahuluan

Di Indonesia terkait dengan penerapan hak as Dunia industri global saat ini telah memasuki era baru yang disebut sebagai era revolusi industri 4.0, yang mana teknologi berkembang begitu pesat dan juga bersamaan dengan penggunaan internet yang semakin besar oleh setiap penduduk di belahan bumi (Amrani & Ali, 2015). Hal ini tentu memberikan dampak yang sangat signifikan terhadap kehidupan manusia. Mulai dari dampak positif hingga dampak negatif. Salah satu dampak positif dari kemajuan teknologi ini ialah kemudahan dalam mengakses informasi (Moghimi, 2020). Kemudahan tersebut tentunya menimbulkan masalah baru yang bisa disebut sebagai dampak negatif dari kemajuan teknologi yakni ialah rentan dilakukannya kejahatan melalui internet yang melanggar hak asasi manusia (Hamzah, 1994). Hak asasi manusia merupakan hak kemanusiaan, berasal dari bahasa asing "Droit De Vhome" (perancis) yang artinya hak manusia dan "Human Right" (inggris). Pengertian Hak Asasi Manusia terdapat dalam Pasal 1 angka l Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia, yang menyatakan bahwa: "Hak asasi manusia adalah seperangkat hak yang melekat pada hakikat dan keberadaan manusia sebagai mahluk Tuhan Yang Maha Esa dan merupakan anugerah-Nya yang wajib dihormati, dijunjung tinggi dan dilindungi oleh negara, hukum dan pemerintah, dan setiap orang demi kehormatan serta perlindungan harkat dan martabat manusia".

Salah satu bagian dari hak asasi manusia yaitu privasi, yakni hak setiap orang untuk leluasa dalam menjalankan kehidupan pribadinya. Dalam hal kejahatan di dunia internet hak asasi manusia yang seringkali dilanggar ialah hak atas perlindungan diri pribadi (hak atas privasi) (Fadillah, 2021). Di Indonesia terkait dengan penerapan hak asasi manusia dalam segala aspek tidak serta merta bebas seperti dalam paham liberalisme, melainkan telah diatur pembatasannya dalam pasal 28J ayat (2) Undang- Undang Dasar Negara Republik Indonesia Tahun 1945 yang menyatakan: "Dalam menjalankan hak dan kebebasannya, setiap orang wajib tunduk kepada pembatasan yang ditetapkan dengan undang-undang dengan maksud semata-mata untuk menjamin pengakuan serta penghormatan atas hak dan kebebasan orang lain dan untuk memenuhi tuntutan yang adil sesuai dengan pertimbangan moral, nilai-nilai agama, keamanan, dan ketertiban umum dalam suatu masyarakat yang demokratis."

Selain itu, terkait dengan perlindungan hukum atas hak untuk melindungi privasi dan data penduduk setiap warga negara indonesia diatur dalam konstitusi negara yakni pada pasal 28G ayat (1) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 yang menyatakan: "setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang dibawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi." Isi pasal tersebut merupakan data pribadi yang dinilai sebagai "privacy rights" dan bagian yang tak terpisahkan dari data diri pribadi warga negara dalam kerangka hak asasi manusia (Zuo, 2019). Penguasaan diri seseorang atas suatu hak yang ada pada dirinya diatur dalam pasal 28H ayat (4) Undang- Undang Dasar Negara Republik Indonesia Tahun 1945 yang menyatakan: "setiap orang berhak mempunyai hak milik pribadi dan hak milik tersebut tidak boleh diambil alih secara sewenangwenang oleh siapapun".

Data pribadi pada dasarnya merupakan suatu privasi yang melekat pada hak seseorang yang tidak boleh diketahui oleh orang lain secara tidak sah. Berdasarkan Pasal 1 ayat (1) Undang-Undang No.27 Tahun 2022 Tentang Perlindungan Data Pribadi, Data Pribadi adalah data tentang perorangan yang teridentifikasi atau dapat di identifikasi secara tersendiri atau kombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik (Hiariej, 2015). Tak jarang ditemukan di berbagai media sosial banyak warganet yang mudah membagikan informasi mengenai dirinya, hal itu membuat peluang terjadinya kejahatan siber semakin besar (Ali, 2018; Patel, 2019).

Kebocoran data atau data leak merupakan salah satu kejahatan cyber crime atau kejahatan dunia maya, dimana data yang penting di akses oleh pihak luar yang tidak memiliki hak untuk melakukan akses data tersebut (Fikri & Alhakim, 2022). Peristiwa Kebocoran data pribadi konsumen 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 rupiah. Raid Forums merupakan sebuah situs jual-beli seperti marketplace yang menjual-belikan database, atau tentang kebocoran database yang disebabkan oleh hacker. Data tersebut berisikan nomor kartu, data keluarga atau data tanggungan, dan status pembayaran yang identik dengan data yang dikelola oleh Badan Penyelenggaraan Jaminan Sosial (BPJS) Kesehatan (Setiyono, 2002). Kebocoran data BPJS Kesehatan terungkap setelah sebuah akun bernama Kotz yang bertindak sebagai pembeli sekaligus penjual data pribadi (reseller) menawarkannya di sebuah forum daring Raid Forums. Penjual mengklaim memiliki 279 juta salinan data identitas warga Indonesia dengan menunjukkan contoh kurang lebih 100.000 data. Hingga saat ini kasus tersebut masih dalam tahap pemeriksaan forensik digital, dengan begitu korporasi BPJS Kesehatan belum dapat dimintai pertanggungjawabannya, sampai hasilnya diketahui dan unsur deliknya dapat dibuktikan.

Bila dikaitkan dengan kebocoran data tersebut terjadi pada aplikasi e- commerce atau perdagangan elektronik, jelas bahwa adanya kewajiban yang tidak dipenuhi oleh pelaku usaha untuk menjaga data pribadi dan privasi konsumen sehingga menimbulkan kerugian yang dialami oleh konsumen (Susanto, 1995). Dalam Pasal 45 ayat 1 undang-undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen menyebutkan bahwa; "setiap konsumen yang dirugikan dapat menggugat pelaku usaha melalui lembaga yang bertugas menyelesaikan sengketa antar konsumen dan pelaku usaha atau melalui peradilan yang berada di lingkungan peradilan umum" (Gupta, 2019).

Perlindungan data pribadi secara khusus ketentuannya diatur dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, keseluruhan upaya untuk melindungi data pribadi dalam rangkaian pemrosesan data pribadi guna menjamin hak konstitusional subjek data pribadi (Johnny, 2006). Dalam Undang- Undang tersebut, apabila terjadi hal yang merugikan subjek data pribadi, pelaku dapat dikenai sanksi pidana penjara dan pidana denda. Hal itu tentunya bisa berdampak serius terhadap orang yang data pribadinya bocor dan tersebar luas. Data pribadi tersebut juga berpotensi digunakan untuk mendapatkan keuntungan pribadi oleh pihak-pihak yang tidak berwenang. Kebocoran data bahkan dapat mengganggu stabilitas negara (Indonesiawan et al., 2021).

Berdasarkan uraian di atas, artikel ini bertujuan untuk mengetahui tentang bagaimana pertanggungjawaban bpjs kesehatan atas kebocoran data pengguna dalam perspektif hukum pidana dan apa saja faktor yang menyebabkan terjadinya kebocoran data.

Metode

Untuk menjamin suatu kebenaran ilmiah, maka dalam suatu penelitian harus mempergunakan metode yang tepat, karena hal tersebut merupakan pedoman dalam rangka melakukan analisis terhadap data atau hasil penelitian. Adapun metode pendekatan yang dipergunakan dalam penelitian ini terdapat 2 macam metode pendekatan adalah sebagai berikut:

a. pendekatan Perundang-Undangan (*Statue Approach)*
   Penelitian ini merupakan jenis penelitian hukum (legal research) yang bersifat normatif preskriptif. 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.
b. pendekatan Konseptual *(conceptual approach*)
   Pendekatan ini beranjak dari pandangan-pandangan dan doktrin- doktrin yang berkembang di dalam ilmu hukum.

Jenis Penelitian yang digunakan adalah yuridis normatif (legal research). Penelitian yuridis normatif sendiri untuk menemukan kebenaran koherensi dengan menggunakan bahan hukum primer seperti undang-Undang sebagai berikut:

a. Undang-Undang Dasar Negara Republik Indonesia Tahun 1945;
b. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi;
c. Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik
d. Undang-Undang Nomor 24 Tahun 2011 Tentang Badan Penyelenggara Jaminan Sosial

Lalu juga menggunakan bahan hukum sekunder seperti jurnal-jurnal, pendapat ahli, dan buku terkait ilmu hukum (Lacharite, 2018).

Teknik Pengumpulan Bahan Hukum dalam penelitian ini penulis menggunakan metode-metode pengumpulan bahan hukum dengan Studi pustaka, yaitu pengumpulan bahan hukum dengan melakukan pengumpulan data yang sumbernya dari bahan-bahan hukum yaitu berupa Peraturan Perundang-Undangan atau studi yang mengulas dari suatu karya tulis, baik dari jurnal-jurnal, buku-buku, atau dari surat kabar serta bahan lainnya.

Teknik analisis data yang digunakan adalah yuridis kualitatif, dimana data primer dan data sekunder yang diperoleh akan dianalisis sesuai dengan rumusan-rumusan masalah yang terkait dengan penelitian.

Hasil dan Pembahasan

Faktor-faktor Penyebab Kebocoran Data Pribadi

Pada setiap penyelenggaraan sistem elektronik tentu terdapat yang namanya resiko, baik itu yang berasal dari faktor manusia atau faktor alamiah dari sistem itu sendiri. Dapat

dipahami bahwa keamanan informasi adalah hal yang menjadi titik perhatian. Setidaknya ada tiga aspek utama dari keamanan informasi, yaitu:

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 tersebut merupakan wujud atas pemenuhan keamanan (*security*) dan privasi *(privacy*) dalam penyelenggaraan sistem elektronik. Kebocoran data pribadi bisa berdampak serius terhadap orang yang data pribadinya bocor dan tersebar luas. Data pribadi tersebut juga berpotensi digunakan untuk mendapatkan keuntungan pribadi oleh pihak-pihak yang tidak berwenang (M. A. Lubis & Siddiq, 2021). Kebocoran data bahkan dapat mengganggu stabilitas negara.

Kebocoran data (*data leakage*) dapat disebabkan oleh faktor internal yakni misalnya, serangan oleh karyawan perusahaan melalui penyalah gunaan wewenang dan kesalahan pada sistem yang disadari dan bisa saja terjadi gangguan teknis dalam proses penyelenggaraan sistem elektronik, yang dapat menyebabkan data rusak (*corrupt*), walaupun tidak ada unsur kesengajaan, hal tersebut merupakan Penyalahgunaan internet yang menganggu ketertiban umum atau pribadi (P. R. F. Lubis, 2022; Marzuki, 2016). Dalam hal terdapat juga faktor eksternal atau faktor luar yang mengakibatkan kebocoran data yang termasuk kejahatan *cyber crime* atau kejahatan dunia maya. Penyelenggaraan sistem elektronik mengandung resiko yang sangat besar terhadap ancaman-ancaman peretasan yang dilakukan oleh oknum hacker (Peng, 2020).

Pada kasus kebocoran data pribadi pengguna BPJS Kesehatan, hasil Investigasi menemukan bahwa akun bernama Kotz menjual data pribadi di Raid Forums. Akun Kotz sendiri merupakan pembeli dan penjual data pribadi (reseller). Dalam kasus kebocoran data pada Badan Penyelenggara Jaminan Sosial (BPJS) Kesehatan belum ditetapkannya tersangka karena masih dalam pemeriksaan forensic digital sebagaimana di katakan oleh Kabareskrim Polri Komjen Polisi Agus Andrianto (Ramadhani, 2020). Upaya Kementerian informasi dan informatika juga telah melakukan pemutusan akses atau takedown terhadap link yang diduga berisi data-data penduduk milik BPJS Kesehatan.

Pertanggungjawaban Korporasi atas Kebocoran Data

Pertanggungjawaban pidana, selain menjadi bentuk penegakan hukum, juga bertujuan untuk memberikan efek jera bagi pelaku tindak pidana, salah satunya dengan menerapkan pemidanaan. Hal tersebut untuk menanggulangi bahkan mencegah terjadinya tindak pidana. Mengenai pertanggungjawaban pidana Secara umum pertanggungjawaban pidana terbagi menjadi tiga macam yaitu:

1. Individual Liability. Dalam teori ini, pertanggungjawaban dijatuhkan kepada individu yang telah melakukan suatu tindak pidana (Lidwina, n.d.). Pidana dijatuhkan sesuai dengan delik kejahatan yang dilakukan oleh individu tersebut sebagai bentuk konskuensi dari perbuatan yang telah diperbuatnya (Rodliyah et al., 2020). Konsep pertanggungjawaban pidana perseorangan merupakan *liability of crime* yang telah diberlalakukan sebagai hukum yang paling lama sudah berlaku dan menjadi bentuk pertanggungjawaban yang paling dasar dari semua jenis bentuk pertanggungjawaban, Dalam pertanggungjawaban individu tidak mengenal pemindahan tanggung jawab terhadap individu lain, karena penjatuhan hukuman menurut prinsip keadilan harus dijalani oleh mereka yang bertanggungjawab.
   Vicarious Liability merupakan bentuk pertanggungjawaban pidana yang mengalihkan tanggung jawab dari individu yang melakukan kesalahan kepada orang lain. Dalam vicarious liability terdapat dua prinsip yang dapat membuat atasan memikul tanggung jawab karena kesalahan bawahannya yaitu prinsip pendelegasian dan prinsip perbuatan buruh merupakan perbuatan majikan. Prinsip pendelegasian berkaitandengan pemberian kewenangan mengenai suatu hal dari atasan kepada bawahan dalam lingkup pekerjaannya. Kewenangan atau tugas yang diberikan kepada bawahan merupakan tanggungjawab dari atasan juga.
2. Pertanggungjawaban Pidana secara Ketat (*StrictLiability) strict liability* adalah pertanggungjawaban pidana tanpa kesalahan atau mens rea dimana pelaku dapat dipidana apabila dia telah melakukan perbuatan pidana sebagaimana dirumuskan dalam undang- undang, tanpa melihat sikap batinnya (Saleh, 2021; Simpson, 1993).
3. Pertanggungjawaban pidana harus memperhatikan bahwa hukum pidana harus digunakan untuk mewujudkan masyarakat adil dan makmur merata materiil dan spirituil. Hukum pidana tersebut digunakan untuk mencegah atau menanggulangi perbuatan yang tidak dikehendaki (Suratman & others, 2014). Khusus mengenai pertanggungjawaban korporasi dalam hukum pidana, terdapat bermacam-macam cara perumusannya yang ditempuh oleh pembuat undang undang. Ada 3 (tiga) sistem kedudukan korporasi dalam hukum pidana yakni:
   a. Pengurus korporasi sebagai pembuat dan pengurus yang bertanggungjawab (Yurizal, 2018)
   b. Korporasi sebagai pembuat dan pengurus yang bertanggungjawab;
   c. Korporasi sebagai pembuat dan yang bertanggungjawab.

Pertanggungjawaban pidana korporasi diatur dalam Pasal 36 Undang-Undang Nomor 27 tahun 2022 tentang Perlindungan Data Pribadi yang menyatakan bahwa dalam melakukan pemrosesan data pribadi, Pengendali data pribadi wajib menjaga kerahasiaan data pribadi. BPJS kesehatan dapat dikatakan lalai dalam hal kurangnya keamanan sistem dan mengakibatkan kebocoran data pribadi milik konsumennya di perjualbelikan oleh akun Bernama kotz (Toruan, 2014; Yuniarti, 2019). Berdasarkan pelanggaran Pasal 36 maka dapat di jatuhi sanksi administratif sebagaimana telah di atur dalam Pasal 57 Ayat 2 Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi berupa:

a. peringatan tertulis

b. penghentian sementara kegiatan pemrosesan data pribadi
c. penghapusan atau pemusnahan data pribadi; dan/atau
d. denda administratif.

Namun apabila akun Bernama Kotz merupakan oknum karyawan dan masih berhubungan langsung dengan perusahaan atau korporasi dalam hal ini BPJS Kesehatan maka BPJS dapat di pidana mengacu dalam Pasal 32 Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Elektronik sebagaimana ketentuan pada Pasal 48 dengan pidana penjara paling lama 8 tahun dan/ atau denda paling banyak 2 miliar rupiah.

Simpulan

Dikaitkan dengan hasil penelitian dan pembahasan maka dapat disimpulkan sebagai berikut:

Peristiwa kebocoran data dapat terjadi disebabkan oleh faktor internal maupun faktor eksternal. faktor internal yaitu perbuatan oleh oknum karyawan perusahaan (insider) melalui penyalahgunaan wewenang dan kesalahan pada sistem yang disadari (system bug, configuration error, improper encryption) dan bisa juga terjadi gangguan teknis dalam proses penyelenggaraan sistem elektronik. Kemudian faktor eksternal dapat disebabkan oleh data breach, virus, malware, phising, dan upaya-upaya peretasan lainnya.

Pertanggungjawaban korporasi (BPJS) Kesehatan apabila terjadi kebocoran data pribadi pengguna dalam perspektif hukum pidana, berdasarkan pada Pasal 32 Ayat (1), (2), (3) Undang-undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, dapat dikenakan sanksi pidana penjara paling lama 8 tahun dan/atau denda paling banyak 2 miliyar. Sedangkan jika berdasarkan Pasal 36 Undang-undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi hanya diberikan sanksi administrative, sebagaimana ditentukan dalam Pasal 57 Ayat 2 Undang-undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi.

Daftar Pustaka

Ali, M. S. (2018). Sampled-Data Stabilization for Fuzzy Genetic Regulatory Networks with Leakage Delays. *IEEE/ACM Transactions on Computational Biology and Bioinformatics*, *15*(1), 271–285. https://doi.org/10.1109/TCBB.2016.2606477

Amrani, & Ali, M. (2015). *Sistem Pertanggungjawaban Pidana*. PT Raja Grafindo.

Fadillah, R. N. (2021). *Pertanggungjawaban Pidana Korporasi Terhadap Pt AkuMobil Sebagai Pelaku Penipuan Dan Tindak Pidana Pencucian Uang Dihubungkan Dengan Konsep Vicarious Liability*.

Fikri, M., & Alhakim, A. (2022). Urgensi Pengaturan Hukum Terhadap Pelaku Tindak Pidana Pencurian Data Pribadi di Indonesia. *YUSTISI*, *9*(1).

Gupta, S. (2019). Low-power near-threshold 10T SRAM bit cells with enhanced data-independent read port leakage for array augmentation in 32-nm CMOS. *IEEE Transactions on Circuits and Systems I: Regular Papers*, *66*(3), 978–988. https://doi.org/10.1109/TCSI.2018.2876785

Hamzah, A. (1994). *Asas-Asas Hukum Pidana*. Rineka Cipta.

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

Indonesiawan, R. C. S., Alroy, M., Suci, T. L., & Prasetyo, B. R. (2021). Analisis Privasi Data Pengguna Dalam Instansi Bpjs Kesehatan. *Sitasi*, *1*(1), 174–182.

Johnny, I. (2006). *Teori dan Penelitian Hukum Normatif*. Bayumedia.

Lacharite, M. S. (2018). Improved Reconstruction Attacks on Encrypted Data Using Range Query Leakage. *Proceedings - IEEE Symposium on Security and Privacy*, *2018*, 297–314. https://doi.org/10.1109/SP.2018.00002

Lidwina, A. (n.d.). *Kebocoran Data Pribadi yang Terus Berulang*. https://katadata.co.id/ariayudhistira/infografik/60b3bbeda4185/kebocoran-data-pribadi-yangterusberulang

Lubis, M. A., & Siddiq, M. (2021). Analisis Yuridis Pertanggungjawaban Pidana Tinjauan Yuridis Penanganan Tindak Pidana. *Jurnal Hukum*, *3*(1), 35–65.

Lubis, P. R. F. (2022). *Perlindungan Hak Asasi Manusia Atas Data Pribadi Di Era Digital Dalam Prinsip Negara Hukum Berdasarkan Pancasila*.

Marzuki, P. M. (2016). *Penelitian Hukum*. Kencana Prenada Media Group.

Moghimi, D. (2020). Medusa: Microarchitectural data leakage via automated attack synthesis. *Proceedings of the 29th USENIX Security Symposium*, 1427–1444.

Patel, S. (2019). Mitigating leakage in secure cloud-hosted data structures: Volume-hiding for multi-maps via hashing. *Proceedings of the ACM Conference on Computer and Communications Security*, 79–93. https://doi.org/10.1145/3319535.3354213

Peng, X. (2020). Analysis of Magnetic-Flux Leakage (MFL) Data for Pipeline Corrosion Assessment. *IEEE Transactions on Magnetics*, *56*(6). https://doi.org/10.1109/TMAG.2020.2981450

Ramadhani, A. P. (2020). *Perlindungan Hukum Pengguna Marketplace dalam Hal Keamanan Data Pribadi Pengguna*.

Rodliyah, R., Suryani, A., & Husni, L. (2020). Konsep pertanggungjawaban pidana Korporasi (Corporate Crime) dalam sistem HuKum pidana indonesia. *Jurnal Kompilasi Hukum*, *5*(1), 191–206.

Saleh, A. R. (2021). Perlindungan Data Pribadi Dalam Perspektif Kebijakan Hukum Pidana. *HUKMY: Jurnal Hukum*, *1*(1), 91–108.

Setiyono, H. (2002). *Kejahatan Korporasi-Analisa Viktimologis dan Pertanggungjawaban Korporasi Dalam Hukum Pidana Indonesia*. Averroes Press.

Simpson, S. S. (1993). Strategy, Structure and Corporate Crime. *Advances In Criminological Theory*, *4*, 171.

Suratman, & others. (2014). *Metode Penelitian Hukum* (Cetakan Kedua). Alfabeta.

Susanto, I. S. (1995). *Kejahatan Korporasi*. Badan Penerbit Universitas Diponegoro.

Toruan, H. D. L. (2014). Pertanggungjawaban pidana korupsi korporasi. *Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional*, *3*(3), 397–416.

Yuniarti, S. (2019). Perlindungan hukum data pribadi di Indonesia. *Business Economic, Communication, and Social Sciences Journal (BECOSS)*, *1*(1), 147–154.

Yurizal. (2018). *Penegakan Hukum Tindak Pidana Cyber Crime di Indonesia*. Media Nusa Kreative.

Zuo, C. (2019). Why does your data leak? uncovering the data leakage in cloud from mobile apps. *Proceedings - IEEE Symposium on Security and Privacy*, *2019*, 1296–1310. https://doi.org/10.1109/SP.2019.00009