Jurnal Penelitian Hukum De Jure
Volume 23, Nomor 1, Maret 2023
P-ISSN: 1410-5632, E-ISSN: 2579-8561
Diakreditasi No: 10/E/KPT/2019

KETIDAKAMANAN PERLINDUNGAN DATA KONSUMEN DI SEKTOR *eHealth*

Insecurity to Consumer Data Protection in The eHealth Sector

Edy Santoso[1], Andriana[2]
Magister Ilmu Hukum, Universitas Langlangbuana, Bandung, Indonesia[1]
Fakultas Teknik Elektro, Universitas Langlangbuana, Bandung, Indonesia[2]
Email: edys39768@gmail.com

Diserahkan: 28-1-10-2022; Diterima: 30-03-2023
DOI: http://dx.doi.org/10.30641/dejure.2023.V23.115-130

ABSTRACT

In Indonesia, the eHealth application has been widely used. It has also been recognized by World Health Organization (WHO) that Information and Communication Technology (ICT) provides a cost-effective and secure value to support various health sectors. The research method uses normative research which more emphasizes the use of positive law and comparisons of law with other countries. Meanwhile, the approach used in this study is a "qualitative empirical". A primary legal material implementing statutory regulation in the field of Cyber law, and practically discusses how it is implemented in eHealth. This research examines two things in depth. Firstly; Is a "Data breach" committed by the electronic service providers? Secondly; Is a "Data theft" modus operandi achieved by the perpetrator? This study concludes that a "data breach" can occur due to "carelessness" or "bad faith" on the part of the service provider. Thus, bad faith behavior may intentionally process the data for illegal commercial purposes, either by processing it alone or by cooperating with other parties who use the data. Meanwhile, "Data theft" caused by "illegal access" activities there are carried out by the perpetrator, causing data can be changed, damaged, and deleted. Data related to eHealth is included in the category of special data that is protected by the laws and regulations in Indonesia. Thus, service providers should participate in providing data protection efforts by making "self-regulation" and providing training to service users, in an effort to avoid crime under Law Number. 27 of 2022 on Personal Data Protection.

Keywords: data breach; data protection; data theft; eHealth.

ABSTRAK

Di Indonesia, aplikasi *eHealth* sudah banyak digunakan. Hal ini telah pula diakui oleh Organisasi Kesehatan Dunia (WHO) bahwa Teknologi Informasi dan Komunikasi (TIK) memberikan nilai yang hemat biaya dan aman untuk mendukung berbagai sektor kesehatan. Metode penelitian menggunakan penelitian normatif yang lebih menekankan penggunaan hukum positif dan perbandingan hukum dengan negara lain. Sementara itu, pendekatan yang digunakan dalam penelitian ini adalah "empiris kualitatif". Merupakan bahan hukum utama pelaksana peraturan perundang-undangan di bidang Hukum Siber, dan secara praktis membahas bagaimana penerapannya di *eHealth*. Penelitian ini mengkaji dua hal secara mendalam. Pertama; Apakah "pelanggaran data" dilakukan oleh penyedia layanan elektronik? Kedua; Apakah modus operandi "pencurian data" dilakukan oleh pelaku? Studi ini menyimpulkan bahwa "pelanggaran data" dapat terjadi karena "kecerobohan" atau "itikad buruk" dari pihak penyedia layanan. Dengan demikian, perilaku itikad buruk dapat dengan sengaja memproses data untuk tujuan komersial secara ilegal, baik dengan memprosesnya sendiri atau dengan bekerja sama dengan pihak lain yang menggunakan data tersebut. Sementara itu, "pencurian data" yang disebabkan oleh aktivitas "akses secara ilegal" ada yang dilakukan oleh pelaku sehingga menyebabkan data dapat diubah, rusak, dan terhapus. Data terkait *eHealth* termasuk dalam kategori data khusus yang dilindungi oleh peraturan perundang-undangan di Indonesia. Oleh karena itu, sebaiknya penyedia layanan turut serta memberikan upaya perlindungan data dengan membuat "self-regulation" dan memberikan pelatihan kepada pengguna layanan, sebagai upaya menghindari tindak pidana berdasarkan Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi.

Kata kunci: pelanggaran data; perlindungan data; pencurian data; eHealth.

1. PENDAHULUAN

Pada tahun 1999 sebuah studi nasional tentang telemedis di Australia mempromosikan konsep kesehatan elektronik (*eHealth*).[1] Di sini, Mitchell juga menunjukkan bahwa "*eHealth* dapat dianggap sebagai industri kesehatan yang setara dengan e-commerce.[2] Ini adalah e-commerce di bidang pelayanan yang mengkhususkan diri pada bidang kesehatan. Sektor ini merupakan sektor yang berkembang sangat pesat di masa depan. Teknologi terbaru yang digunakan, seperti e-commerce, net banking, layanan kesehatan, dan data pribadi pada penyimpanan cloud membutuhkan keamanan yang tinggi.[3]

Merujuk data dari Ikatan Penyelenggara Jasa Internet Indonesia (IISPA). Di Indonesia, penetrasi internet tahun 2021-2022 mencapai 77,02%.[4] Mengacu pada jumlah penetrasi internet diatas 70%, penulis optimis pengguna jasa di bidang *eHealth* akan terus meningkat sejalan dengan perkembangan e-commerce di bidang jasa ini. Padahal, pada tahun 2019, pengguna aplikasi kesehatan baru mencapai 10% dari total populasi di Indonesia.[5]

Berdasarkan data dari Statista untuk Indonesia, pendapatan di segmen *eHealth* diproyeksikan mencapai US$989,80 juta pada tahun 2023. Diperkirakan akan menunjukkan tingkat pertumbuhan tahunan (CAGR 2023-2027) sebesar 13,32%, menghasilkan proyeksi volume pasar sebesar US$1.632,00 juta pada tahun 2027. Sementara itu, penetrasi pengguna akan mencapai 20,08% pada tahun 2023 dan diperkirakan akan mencapai 26,23% pada tahun 2027. Dengan data ini, pendapatan rata-rata per pengguna (ARPU) diperkirakan mencapai US$17.49[6].

Data ini menunjukkan perkembangan yang signifikan dalam penggunaan aplikasi *eHealth*. Munculnya *eHealth* merupakan salah satu gaya baru pelayanan medis. Hal ini memungkinkan fasilitas kesehatan dengan mudah mengelola data rekam medis, apotek, dan rumah sakit dengan harga yang terjangkau baik untuk klinik maupun rumah sakit melalui platform ICT. Dapat dikatakan sebagai inovasi teknologi dalam pelayanan medis yang memberikan banyak kemudahan untuk kegiatan medis, seperti konsultasi, pengobatan, dan transaksi. Di sini, *eHealth* berperan sebagai kemudahan dalam memberikan pelayanan kesehatan di seluruh dunia.

---

1 John Mitchell, "Increasing the Cost-Effectiveness of Telemedicine by Embracing e-Health," *Sage Joulnals* 6, no. 1 (2000), https://journals.sagepub.com/doi/10.1258/1357633001934500

2 Vincenzo Della Mea, "What Is E-Health (2): The Death of Telemedicine?," *Journal of Medical Internet Research* 3, no. 2 (2001): 6–7.

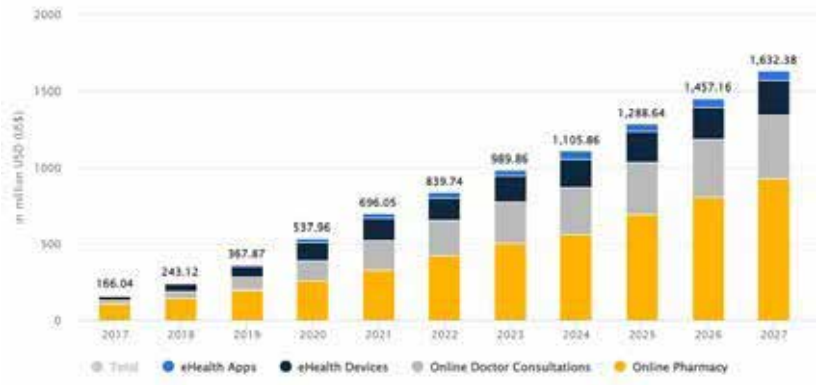
3 Charu Virmani et al., "Analysis of Cyber Attacks and Security Intelligence: Identity Theft," *Indian Journal of Science and Technology* 13, no. 25 (2020): 2529–2536

4 APJII, "APJII Di Indonesia Digital Outloook 2022," last modified 2022, accessed February 14, 2023, https://apjii.or.id/berita/d/apjii-di-indonesia-digital-outloook-2022_857

5 Media Infokes, "Penggunaan Aplikasi Kesehatan Digital Di Indonesia, Hanya 10% Dari Total Penduduk," last modified 2019, accessed October 4, 2022, https://media-infokes.com/2019/08/22/penggunaan-aplikasi-kesehatan-digital-di-indonesia-hanya-10-dari-total-penduduk/

6 Statista, "EHealth - Indonesia," last modified 2022, accessed March 26, 2023, https://www.statista.com/outlook/dmo/digital-health/ehealth/indonesia.

Gambar 1. *eHealth* di Indonesia



Pada tahun 2001, G Eysenbach mendefinisikan istilah dan konsep *eHealth* sebagai "mengacu pada layanan kesehatan dan informasi yang disampaikan atau ditingkatkan melalui Internet dan teknologi terkait.[7] Definisi ini diharapkan dapat memberikan arti yang cukup luas untuk diterapkan pada lingkungan yang dinamis seperti internet. Hal lain yang dapat disampaikan adalah sekaligus menyadari bahwa *eHealth* mencakup lebih dari sekedar "Internet dan Kedokteran".[8] Dalam hal ini, WHO mendefinisikan *eHealth* sebagai penggunaan TIK yang hemat biaya dan aman dalam mendukung kesehatan.[9] Dalam 2020, Dymyt, dan Malgorzata, menyatakan bahwa "Kemajuan teknologi digital berkontribusi pada perkembangan dinamis *eHealth*.[10] Selanjutnya, *eHealth* dapat memberikan layanan kesehatan berkualitas tinggi yang secara signifikan mempengaruhi keselamatan pasien.[11]

Dalam Keputusan Menteri Kesehatan RI (KepMenKes) Nomor 192/MENKES/SK/VI/2012[12] disebutkan bahwa *eHealth* adalah pemanfaatan TIK dalam bidang kesehatan, khususnya untuk meningkatkan pelayanan kesehatan. Perda ini mengandung visi untuk mewujudkan Indonesia Sehat 2025, maka disusunlah Desain Besar Reformasi Sistem Informasi Kesehatan yang terbagi dalam tiga *roadmap*.

Gambar 2. Kerangka Dasain Besar Reformasi Sistem Informasi Kesehatan (SIK)

Roadmap 2011-2014 berfokus pada Penguatan Landasan Reformasi Sistem Informasi Kesehatan (SIK) baik dari sisi Regulasi/Kebijakan, Sumber Daya, dan Proses Integrasi SIK. Sedangkan roadmap 2015-2019

7 Gunther Eysenbach, "What Is E-Health?," *Journal of Medical Internet Research* 3, no. 2 (2001): 1–5
8 Ibid.
9 WHO, "EHealth," last modified 2022, http://www.emro.who.int/health-topics/ehealth/.
10 Malgorzata Dymyt, "The Role of EHealth in the Management of Patient Safety," Journal of e-health Management 2020 (2020): 1–13, https://ibimapublishing.com/articles/JEHM/2020/341252/.
11 Ibid
12 *Decree of the Minister of Health Number 192/MENKES/SK/VI/2012 Regarding Roadmap of Strengthening Action Plan Indonesian Health Information System*, n.d.

dan 2020-2024: lanjutkan, pertahankan/pertahankan dan sempurnakan integrasi dan penguatan SIK. Peraturan ini merupakan tindak lanjut terkait kebijakan Sistem Kesehatan Nasional (SKN) yang diatur dalam Keputusan Menteri Kesehatan (KepMenKes) RI No. 374/MENKES/SK/V/2009 tentang Sistem Kesehatan Nasional (NHS)[13].

Namun, teknologi memiliki peran untuk mengubah perilaku sosial dalam berbagai aktivitas masyarakat. Di sini inti dari layanan jejaring sosial adalah mengungkapkan privasi dan berbagi informasi pribadi.[14] Dengan demikian, dampak yang akan muncul tidak hanya positif tetapi juga negatif sekaligus mengubah perilaku manusia. Sebaliknya, Internet dapat dikatakan sebagai "alat yang sangat diperlukan" dalam menciptakan Masyarakat Informasi.[15] Sementara itu, dari sisi yang berlawanan muncul jenis kejahatan baru yang sebenarnya dapat merugikan masyarakat.

Dalam hal ini, Howard mengingatkan aliran data pribadi pengguna internet terus terjadi pada perusahaan penyedia layanan digital (media sosial, mesin pencari, e-commerce, dan lainnya)—selama pengguna internet aktif menggunakan layanan tersebut.[16] Dengan demikian, masyarakat harus waspada dalam penggunaan media digital berbasis internet, karena data pribadi mereka sangat rentan digunakan oleh pihak yang tidak bertanggung jawab. Di sini pelaku bisnis tidak hanya memiliki kewajiban untuk melindungi data selama pemrosesan data pribadi, tetapi juga memiliki kewajiban untuk melindunginya seperti melindungi aset.[17] Seperti yang dikatakan Almunia bahwa "Saat ini, data pribadi merupakan salah satu jenis aset bagi perusahaan.".[18]

Dalam kaitan ini, Martin, Kelly D. dkk berpendapat bahwa konsumen berpandangan bahwa data sangat rentan terhadap pelanggaran privasi.[19] Kekhawatiran di sini terkait dengan privasi data yang diabaikan oleh pelaku bisnis. Oleh karena itu, penulis sangat prihatin agar setiap pelaku usaha memperhatikan aspek perlindungan data konsumen khususnya terkait data rekam medis yang merupakan bagian dari layanan *eHealth*.

Di sektor kesehatan, risiko yang terkait dengan pelanggaran data dan pencurian data tidak dapat dihindari. Risiko pertama kasus "pelanggaran data" di AS antara tahun 2009 dan 2021 adalah sekitar 4.419 pelanggaran data layanan kesehatan dari 500 catatan. Sementara itu, pada tahun 2021, rata-rata 1,95 pelanggaran data layanan kesehatan dari 500 atau lebih catatan dilaporkan setiap hari.[20] Selanjutnya, layanan kesehatanitnews.com menulis bahwa, di web gelap, data rekam medis dapat dijual hingga $1000 per dokumen. Ini adalah dampak dari kebocoran data. Penjualan data, dalam kasus di atas, akan memiliki banyak resiko. Hal ini dapat

---

13 *Decree of the Minister of Health of the Republic of Indonesia No. 374/MENKES/SK/V/2009 Concerning the National Health System (NHS)*, n.d.

14 Anahiby Anyel Becerril, "The Value of Our Personal Data in the Big Data and the Internet of All Things Era," *ADCAIJ: Advances in Distributed Computing and Artificial Intelligence Journal* 7, no. 2 (2018): 71–80.in which we transit, is preceded by a digital economy based fundamentally on information. And although estimates have been made on whether the data moving in the digital economy flow are from sensors or machines or come from each of us, one thing is certain, all information has a monetary value. Within this flow of information are our personal data. Every moment that we use an electronic device we leave behind vestiges of our life, which are collected by the machines to generate value to the companies. In this way our information is subject to market rules, supply and demand. We have become intangible beings, mercantilized, giving our bodies of data to the science, innovation and technological development. With the use of technologies such as Big Data and IoT, more information less is better. The speed with which our information is collected and treated as well as commercialized is undermining confidencein the digital market. Concern about the misuse of our personal data, or about the information we know about us, raises fundamental questions about privacy, ownership of information and human rights. The question of who shouldbenefit from products and services based on digital data (generated by users

15 M. Castells, *The Information Age*, III. (Oxford: Blackwell, 1998), 336.

16 Agus Sudibyo, *Jagad Digital* (Jakarta: Kepustakaan Populer Gramedia, 2019), 174

17 Maria Bottis and George Boucha, "Personal Data v. Big Data: Challenges of Commodification of Personal Data," *Open Journal of Philosophy* 8 (2018): 206–215, http://www.scirp.org/journal/ojpp.

18 Joaquín Almunia, "Speech - Competition and Personal Data Protection, Commissioner Joaquín Almunia," *European Commission*, last modified 2012, https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_12_860

19 Kelly D. Martin, Abhishek Borah, and Robert W. Palmatier, "Data Privacy: Effects on Customer and Firm Performance," *Journal of Marketing* 81, no. 1 (2017): 36–58

20 HIPAA Journal, *Healthcare Data Breach Statistics*, 2022, https://www.hipaajournal.com/healthcare-data-breach-statistics/.

berdampak pada sektor keuangan. Dengan kepemilikan data tersebut, pelaku kejahatan dapat mengakses data keuangan korban dan mencurinya. Hal ini merupakan salah satu resiko yang akan dialami oleh korban, belum lagi penggunaan data untuk kepentingan tertentu yang dapat merugikan korban.

Di sini, saluran komunikasi dan perdagangan yang disediakan oleh Internet dengan mudah melampaui batas-batas negara.[21] Namun, masalah di bidang yurisdiksi, misalnya, yurisdiksi pribadi berlaku dengan terdakwa yang setuju dengan yurisdiksi kita jika orang tersebut hadir di sini.[22] Sangat sulit untuk membuktikan keberadaan pelaku di dunia maya. Hal yang mengkhawatirkan di Indonesia juga akan terjadi. Kasus seperti pencurian data administrasi, peretasan untuk penipuan klaim asuransi, penipuan kartu asuransi, penipuan resep obat, dan Penggunaan informasi kesehatan untuk pemerasan.

Sehubungan dengan hal tersebut, Solove (2008) berpendapat bahwa permasalahan di atas disebabkan oleh tidak adanya regulasi dalam pengelolaan informasi pribadi.[23] Menurut penulis, hal ini akan menjadi masalah besar di kemudian hari jika diabaikan. Oleh karena itu, penelitian terkait masalah hukum di *eHealth* sangat penting untuk dilakukan terkait dengan pelanggaran dan kejahatan penggunaan data pribadi secara ilegal.

Untuk mengantisipasi permasalahan hukum di atas, pada tanggal 20 September 2022, melalui Rapat Paripurna DPR RI disahkan Rancangan Undang-Undang Perlindungan Data Pribadi menjadi undang-undang (Undang-Undang PDP 2022).[24] Peraturan baru ini diharapkan dapat digunakan sebagai sebuah "payung hukum" di sektor digital. Pengesahan Rancangan Undang-Undang menjadi undang-undang juga merupakan keberhasilan dan kemajuan besar dalam mewujudkan tata kelola data pribadi di Indonesia. Dengan demikian, bagi penyedia layanan *eHealth*, baik publik maupun swasta, untuk meningkatkan sistem keamanan, mematuhi tanggung jawab, dan memelihara data pribadi yang mereka kelola, baik data umum maupun khusus, sebagai kepatuhan mutlak terhadap peraturan perlindungan data pribadi. Selanjutnya standar dan kriteria data kesehatan diatur dalam Peraturan Menteri Kesehatan Nomor 18 Tahun 2022 Tentang Penyelenggaraan Data Bidang One Health Melalui Sistem Informasi Kesehatan (PerMenKes 18/2022).

Untuk mengkaji upaya perlindungan data konsumen dalam kegiatan *eHealth*, penulis akan mengkaji berbagai peraturan perundang-undangan yang memungkinkan memberikan perlindungan dari sisi regulasi nasional. Selain itu, penting juga untuk meninjau langkah-langkah perlindungan yang diambil oleh penyedia layanan elektronik terkait *eHealth*. Dimana dalam hal ini, pelaku usaha juga dituntut untuk berusaha memberikan perlindungan terhadap data pribadi pasiennya, sebagai konsumen.

Oleh karena itu, salah satu permasalahan yang diangkat umumnya berkaitan dengan pencurian dan penyalahgunaan data pasien yang dalam hal ini adalah konsumen. Hal inilah yang menjadi fokus penelitian ini. Dengan demikian, penelitian ini mengkaji dua hal secara mendalam. Pertama, apakah "Pelanggaran Data" dilakukan oleh penyedia layanan elektronik? Kedua, adalah modus operandi "Pencurian Data" yang dilakukan oleh pelaku.

2. METODE PENELITIAN

Pendekatan "empiris kualitatif" diterapkan dalam penelitian ini. Sehingga tidak dilakukan pengumpulan data primer melalui kuesioner. Sebagai bahan hukum primer merupakan peraturan perundang-undangan di bidang hukum siber. Penelitian ini juga akan menyentuh bagaimana hukum dapat diterapkan dalam praktik.[25] Metode "socio-legal" akan digunakan. Ini akan memeriksa prinsip-prinsip hukum, dan memeriksa peraturan tertulis serta mempertimbangkan realitas sosial. Tujuan terungkap, dan mengetahui apa yang sedang dihadapi.[26]

---

21 Clive Walker and David Wall, *The Internet, Law and Society* (UK: Person Education Limited, 2000), 14

22 Walker and Wall, *The Internet, Law and Society*

23 Rita O. Koyame-Marsh and John L. Marsh, "Data Breaches and Identity Theft: Costs and Responses," *IOSR Journal of Economics and Finance (IOSR-JEF)* 5, no. 6 (2014): 36–45, www.iosrjournals.org.

24 Kominfo, "Rapat Paripurna DPR Sahkan RUU PDP," last modified 2022, accessed October 16, 2022, https://aptika.kominfo.go.id/2022/09/rapat-paripurna-dpr-sahkan-ruu-pdp/

25 Philip Langbroek et al., "Methodology of Legal Research: Challenges and Opportunities," *Utrecht Law Review* 13, no. 3 (2017): 1–8

26 Soerjono Soekanto, *Pengantar Penelitian HUkum* (Jakarta: UI Press, 1986), 3

Kenyataannya, masyarakat sering mengalami permasalahan hukum terkait penggunaan *eHealth*. Oleh karena itu, sangat erat kaitannya dengan hukum siber. Dimana, penggunaan TIK sangat dominan di masyarakat dan secara tidak langsung sangat mempengaruhi gaya hidup masyarakat. Ini digunakan oleh penjahat untuk menargetkan mangsanya menggunakan aplikasi. Hal ini membutuhkan penerapan hukum yang bersifat "lex specialist". Itu harus mencerminkan sikap dan perilaku sosial dan kemudian mengalir ke saluran yang tepat.[27]

Penelitian ini menggunakan pendekatan normatif. Hal-hal yang dibahas akan mengacu pada peraturan perundang-undangan yang relevan. Selain itu, pendekatan studi hukum komparatif juga akan digunakan, khususnya terkait dengan regulasi yang berlaku di Uni Eropa. Selain itu, penelitian ini juga menggunakan jenis data sekunder yang berasal dari bahan hukum primer dan bahan hukum sekunder.[28] Di sini perlu diperhatikan keterpaduan antara penelitian sosial dan penelitian hukum. Sosial terkait dengan perilaku manusia dan hukum terkait dengan hukum normatif. Ini akan sangat penting dalam menciptakan administrasi publik yang lebih baik di masyarakat.[29]

Bahan hukum primer adalah bahan yang hukumnya mempunyai kekuatan hukum mengikat. Ini akan mencakup berbagai peraturan perundang-undangan di bidang hukum siber, seperti Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (Undang-Undang PDP),[30] dan Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (Undang-Undang ITE).[31] Untuk membahas lebih dalam terkait perlindungan data, kajian ini juga menggunakan Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik (Permen DP)[32] dan Peraturan Menteri Kesehatan Republik Indonesia Nomor 24 Tahun 2022 tentang Rekam Medis[33] serta Peraturan Menteri Kesehatan Nomor 18 Tahun 2022 Tentang Implementasi Data Sektor One Health Melalui Sistem Informasi Kesehatan (Permen 18/2022)[34].

3. PEMBAHASAN DAN ANALISIS

Pencurian data sangat menakutkan. Penyediaan informasi data di area publik seperti surat kabar, majalah, media sosial, aplikasi seluler, dan situs web harus mendapat perhatian. Memberikan informasi kepada publik dapat menjadi risiko yang terkait dengan keamanan data. Tidak hanya media elektronik tetapi juga media cetak yang memiliki resiko tersendiri. Kasus Vereniging Weekblad Bluf! v. Netherlands,[35] 9 Februari 1995, dalam hal kerahasiaan informasi telah diumumkan karena tindakan surat kabar itu sendiri.[36]

Ketidakamanan di dunia maya lebih mengerikan. Kemudahan mengakses data secara ilegal terhadap sistem teknologi informasi yang dimiliki organisasi atau individu sangat rentan untuk dibobol. Dengan demikian, masalah keamanan untuk sebuah sistem informasi merupakan prioritas yang paling penting untuk dijaga. Menyebabkan data ini sangat mudah untuk diakses yang akan berhubungan dengan perlindungan data.

Mengacu pada laporan survei Deloitte 2019, responden menyatakan 84,4% puas, sedangkan 15,6% lainnya menyatakan tidak puas dengan aplikasi layanan kesehatan digital. Namun, terdapat beberapa kekhawatiran yang dimiliki responden antara lain: privasi data, miskomunikasi, akurasi diagnostik, dokter yang tidak

27 S. N Jain, "Legal Research and Methodology," *Journal of the Indian Law Institute* 14, no. 4 (1972): 487–500, https://www.jstor.org/stable/43950155.

28 Z Amiruddin & Asikin, *Pengantar Metode Penelitian Hukum* (Jakarta: Raja Grafindo Persada, 2003), 118

29 Pradeep M.D., "Legal Research- Descriptive Analysis on Doctrinal Methodology," *International Journal of Management, Technology, and Social Sciences* 4, no. 2 (2019): 95–103

30 *The Law Number. 27 of 2022 on Personal Data Protection*, n.d

31 *The Law Number 19 of 2016 Concerning Amendments to Law Number 11 of 2008 on Information and Electronic Transactions*, n.d

32 *Regulation of the Minister of Communication and Informatics No. 20 of 2016 Concerning Protection of Personal Data in Electronic Systems*, n.d

33 *The Regulation of the Minister of Health of the Republic of Indonesia Number 24 of 2022 Concerning Medical Records*, n.d

34 *Regulation of the Minister of Health, No 18 of 2022 Concerning Implementation of One Data in the Health Sector Through the Health Information System.*, n.d

35 European Court of Human Rights, *Vereniging Weekblad Bluf! V. the Netherlands*, Series A v (1995)

36 Geoffrey Robertson and Andrew Nicol, *Media Law*, Fifth Edit. (London, UK: Penguin Books, n.d.).

berpengalaman, dan perlindungan hukum. Dalam survei ini, masih ada sekitar 16% yang mempermasalahkan masalah regulasi & keamanan hukum.

Gambar 3. Alasan Tidak Menggunakan Aplikasi *eHealth*

Keberadaan data baik melalui sistem penyimpanan data di komputer[37] maupun yang berhubungan dengan internet harus mendapatkan prioritas keamanan tertinggi. Sebab, data ini akan rentan digunakan untuk berbagai kepentingan seperti bisnis, profesionalisme, dan kepentingan lainnya. Tentunya hal tersebut akan menyebabkan pemilik data dirugikan baik secara materiil maupun immateriil.

Mengacu pada Pasal 8 PermenKes 18/2022 tentang Penyelenggaraan Data Bidang One Health Melalui Sistem Informasi Kesehatan. Informasi Kesehatan tergolong informasi rahasia, informasi terbatas; dan informasi publik yang harus mendapat perlindungan. Mengingat data ini sangat rentan disalahgunakan oleh pihak yang tidak bertanggung jawab.

Selain itu, negara berkembang harus menyiapkan infrastruktur TIK yang baik. Tragedi kasus pemadaman listrik (blackout) di sebagian besar wilayah Indonesia pada 4-5 Agustus 2019, membuat seluruh sistem layanan berbasis TIK lumpuh total. Masyarakat tidak dapat mengambil uangnya di ATM dan juga tidak dapat menggunakan transaksi elektronik berbasis internet yang tidak dapat digunakan. Ini merupakan peristiwa yang memberikan pelajaran, ada resiko yang dialami oleh masyarakat yang menyimpan uangnya berbasis TIK.[38] Bisa juga terjadi pada pengguna *eHealth* yang menggunakan fasilitas TIK.

Mengenai pencurian data, ada kasus penjualan CD. Mungkin juga terkait dengan penjualan data yang berisi rekam medis. Pada tahun 2019, kasus pelanggaran jual beli data pribadi secara ilegal terjadi di Indonesia. Pengadilan Negeri Tangerang menjatuhkan hukuman 9 bulan penjara dan denda Rp 1 miliar kepada Adi Warnadi Ismentin.[39] Pelaku terbukti menjual database pelanggan dan divonis oleh Undang-Undang Informasi dan Transaksi Elektronik (Undang-Undang ITE). Pelaku mengumpulkan data konsumen dari situs domain www.database.org. Data nasabah dari berbagai bank, antara lain nama, nomor telepon, alamat, tanggal lahir, nomor kartu, dan jenis kartu.

Harga per CD dijual mulai Rp 500 ribu hingga Rp 3 jutaan. Dalam setahun, pelaku bisa mendapatkan keuntungan sekitar Rp 60 juta lebih. Dalam hal ini, Majelis Hakim menyatakan bahwa pelaku dengan sengaja dan tanpa hak atau melawan hukum memindahkan informasi elektronik dan/atau dokumen elektronik ke sistem elektronik orang lain yang tidak berhak melakukan perbuatan tersebut. Melanggar Pasal 48 ayat 2 juncto Pasal 32 (2) Undang-Undang ITE.[40] Dimana pelanggaran tersebut apabila pelaku, dengan sengaja dan melawan hukum memindahkan atau memindahtangankan Informasi Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik Orang Lain yang bukan haknya.

Kasus di atas merupakan contoh pentingnya memberikan perlindungan data. Di bawah Uni Eropa sebagaimana tercantum dalam Peraturan Perlindungan Data Umum (*General Data Protection Regulation* - GDPR), definisi 'data pribadi' adalah 'informasi apa pun yang berkaitan dengan orang alami yang teridentifikasi atau dapat diidentifikasi sebagai subjek data'. Dalam Pasal 4, Data Pribadi terdiri atas Data Pribadi khusus dan Data Pribadi umum. Di sini, data pribadi terkait sektor keuangan merupakan bagian dari data pribadi yang termasuk dalam data spesifik. Hal inilah yang ditekankan untuk mendapat perlindungan dalam Undang-Undang PDP.

Berkaitan dengan kondisi tersebut, tidak heran jika permasalahan hukum di era digital menjadi perhatian dunia, salah satunya adalah permasalahan perlindungan data. Dimulai dari reformasi regulasi perlindungan

37 Ibid

38 Nik Martin, "Indonesia's Jakarta Hit by Major Power Blackout," last modified 2019, accessed October 2, 2019, https://www.dw.com/en/indonesias-jakarta-hit-by-major-power-blackout/a-49884728.

39 Andi Saputra, "Jual Database Nasabah Perbankan, Warga Tangsel Dibui 9 Bulan," *Detik News*, last modified 2019, accessed October 2, 2022, https://news.detik.com/berita/d-4588549/jual-database-nasabah-perbankan-warga-tangsel-dibui-9-bulan

40 *The Law Number 19 of 2016 Concerning Amendments to Law Number 11 of 2008 on Information and Electronic Transactions*

data di Uni Eropa sebagaimana tertuang dalam GDPR pada tahun 2016. Regulasi ini memberikan upaya perlindungan data baik di dalam maupun di luar Kawasan Uni Eropa. Peraturan tersebut, menginspirasi negara-negara lain untuk melakukan penyempurnaan peraturan di negaranya dengan mempertimbangkan perkembangan teknologi informasi terkini.

Konsumen yang dalam hal di atas disebut sebagai pengguna jasa, tentunya akan membiarkan data pribadi atau data medisnya diolah dan disimpan dalam sistem yang dimiliki oleh penyedia jasa. Di sini, menurut penulis, terdapat 2 (dua) risiko yang dihadapi oleh konsumen, yaitu pertama, risiko "pembobolan data" dimana pelaku usaha menyalahgunakan data yang akan digunakan untuk kepentingan bisnis penyedia layanan, dan kedua, risiko bocornya data yang disimpan dalam sistem yang dimiliki oleh penyedia layanan.

Risiko kedua sering disebut risiko yang terkait dengan "pencurian data". *eHealth* yang difasilitasi oleh infrastruktur TIK tentunya sangat rentan terhadap kejahatan jenis ini. Penjahat akan mencoba mengambil data, untuk tujuan bisnis maupun untuk tujuan keuangan. Melihat situasi ini, beberapa negara maju sangat memperhatikan masalah ini. Beberapa negara telah membuat atau merevisi aturan perlindungan data pribadi, dan beberapa negara juga telah menyiapkan aturan perlindungan data terkait kegiatan *eHealth* ini.

Adapun resiko kedua yaitu "pencurian data" banyak terjadi di Indonesia. Pada Januari 2022, sebanyak 6 juta data pasien dari banyak rumah sakit di Indonesia bocor dan dijual di RaidForums. Data yang bocor tidak hanya data kependudukan tetapi juga data medis pasien seperti foto medis, data administrasi pasien, hasil pemeriksaan laboratorium, EKG, dan data radiologi.[41]

Menurut Alfons Tanujaya, "Data medis yang bocor dapat disalahgunakan dan mengakibatkan kerugian yang sangat besar bagi pemiliknya".[42] Menurut hemat penulis, jika pengelola aplikasi *eHealth* tidak memperhatikan sistem keamanannya, maka akan terjadi resiko "pencurian data" yang akan merugikan pengguna jasa.

3.1 Pelanggaran Data

Dalam konsep perlindungan data konsumen, Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 Tentang Perlindungan Data Pribadi Dalam Sistem Elektronik (Permen Perlindungan Data)[43] telah mengatur "Hak Dirahasiakan" dan "Hak Penghapusan". Ini memberikan upaya perlindungan data, terutama untuk organisasi yang menyediakan layanan elektronik. Menurut hemat penulis, prinsip-prinsip tersebut meliputi hal-hal sebagai berikut:

1. Pemberian hak untuk menjaga kerahasiaan data konsumen agar tidak bocor ke pihak lain;
2. Pemberian hak untuk menghapus data jika sudah tidak terkait lagi dengan layanan yang diberikan;
3. Pemberian hak atas sistem keamanan yang memadai untuk menghindari akses secara ilegal oleh pihak lain.
4. Pemberian hak atas keutuhan data yang telah diinput, diproses, dan disimpan.
5. Pemberian hak untuk memberikan edukasi kepada konsumen untuk selalu menjaga kode rahasia seperti "username" dan "kata sandi".

Secara teori, pelanggaran data didefinisikan sebagai pengungkapan yang tidak sah atau tidak disengaja oleh organisasi yang mengakibatkan hilangnya informasi identitas pribadi (PII) pelanggan,[44] seperti nomor rahasia keuangan. Organisasi yang menyediakan layanan adalah "wali" untuk menjaga data pribadi, khususnya di bidang *eHealth*. Hal inilah yang menjadi perhatian penulis pada resiko pertama, dalam menggunakan layanan *eHealth* ini. Basis data dan perangkat elektronik ini rentan terhadap serangan peretas. Ini memungkinkan

41 Herman Herman, "6 Juta Data Pasien RS Bocor, Ini Risiko Yang Mengintai," *7 January 2022*, last modified 2022, accessed September 28, 2022, https://www.beritasatu.com/lifestyle/876043/6-juta-data-pasien-rs-bocor-ini-risiko-yang-mengintai.

42 Ibid

43 *Regulation of the Minister of Communication and Informatics No. 20 of 2016 Concerning Protection of Personal Data in Electronic Systems*

44 K. K. Peretti, "Data Breaches: What the Underground World of Carding Reveals," *Santa Clara Computer & High Tech* 25, no. 2 (2008): 375–413

penjahat untuk mendapatkan akses ke informasi pribadi jutaan orang dan menjualnya kepada penawar tertinggi. Mode ini memungkinkan terjadinya pencurian identitas.[45] Pelanggaran data membahayakan privasi konsumen dan memiliki dampak negatif yang signifikan terhadap keputusan terkait privasi pasien dalam layanan *eHealth*.

Seperti yang dikutip oleh Shankar, Nithya, dan Mohammed, Zareef[46] bahwa Culnan dan Williams (2009) memandang pelanggaran data merupakan bagian dari masalah privasi yang tidak bisa dianggap remeh. Merupakan tantangan bagi pengontrol data untuk menciptakan budaya yang peduli dengan perlindungan privasi dan menerapkan proses tata kelola yang baik untuk memastikan bahwa pelanggaran data ini tidak terjadi di masa mendatang.[47] Untuk alasan ini, pendekatan sistem dan pendidikan bagi konsumen sangat penting untuk pengendali data yang harus dilakukan.

Kasus ini dapat terjadi bahkan pada organisasi yang bonafid, seperti Yahoo. Pada tahun 2016, Yahoo mengonfirmasi bahwa setidaknya 500 juta akun penggunanya telah bocor ke publik.[48] Dalam hal ini, menurut Trautman dan Ormerod (2017), pengontrol data gagal melakukan investigasi. Ini menunjukkan kemampuan manajemen pengontrol data yang buruk.[49] Dalam hal ini, penulis mengidentifikasi alasan organisasi dapat mengalami pelanggaran data, yang disebabkan sebagai berikut:

A. Kesalahan Karyawan

Menurut Laporan Investigasi Pelanggaran Data Verizon 2022, sebanyak 82% pelanggaran data melibatkan unsur manusia.[50] Di sini, kesalahan manusia adalah salah satu ancaman keamanan terbesar yang dihadapi organisasi.[51] Hal ini termasuk insiden di mana karyawan mengungkapkan informasi secara langsung (misalnya, oleh misconfiguring databases) atau dengan membuat kesalahan yang memungkinkan penjahat dunia maya mengakses sistem organisasi.[52] Karyawan masih melakukan kesalahan yang dapat menyebabkan pelanggaran data, penyebab berikut:[53]

1. Salah mengirim data berharga melalui email ke penerima yang tidak berhak;
2. Kecerobohan dalam mengirim email dokumen dengan data sensitif;
3. Tidak sengaja mempublikasikan data rahasia di situs web publik;
4. Salah mengonfigurasi aset untuk mengizinkan akses yang tidak diinginkan

Masalah ini menjadi perhatian bagi suatu organisasi. Karyawan yang memiliki tanggung jawab untuk melindungi data konsumen harus memiliki integritas yang tinggi untuk tidak membocorkan data konsumen baik sengaja maupun tidak sengaja sehingga menimbulkan kerugian bagi konsumen baik materil maupun immateriil. Hal ini telah diatur dalam Pasal 3 Undang-Undang ITE bahwa penggunaan Teknologi Informasi dilakukan berdasarkan salah satunya dengan menerapkan "prinsip kehati-hatian". Dan prinsip penting lainnya dalam penggunaan teknologi informasi juga adalah "itikad baik".

---

45 Rita O. Koyame-Marsh and John L. Marsh, "Data Breaches and Identity Theft: Costs and Responses," *IOSR Journal of Economics and Finance (IOSR-JEF)* 5, no. 6 (2014): 36–45

46 Zareef Shankar, Nithya Mohammed, "Surviving Data Breaches: A Multiple Case Study Analysis," *Journal of Comparative International Management* 23, no. 1 (2020): 35–54

47 Culnan, M. J. and C. C. Williams, "How Ethics Can Enhance Organizational Privacy: Lessons from the Choicepoint and TJX Data Breaches," *MIS Quarterly* 33, no. 4 (2009): 673–687.

48 Jamie White, "Yahoo Announces 500 Million Users Impacted by Data Breach," *2021*, last modified 2021, accessed October 4, 2022, https://lifelock.norton.com/learn/data-breaches/company-data-breach

49 L. J. Trautman and P Ormerod, "Corporate Directors' and Officers' Cybersecurity Standard of Care: The Yahoo Data Breach," *American University Law Review* 66 (2017): 1231–1291

50 verizon.com, "2022 Data Breach Investigations Report," last modified 2022, accessed October 4, 2022, https://www.verizon.com/business/resources/reports/dbir/

51 Luke Irwin, "Human Error Is Responsible for 82% of Data Breaches," last modified 2022, accessed October 4, 2022, https://www.grcelearning.com/blog/human-error-is-responsible-for-85-of-data-breaches#:~:text=According to Verizon's 2022 Data,to access the organisation's systems

52 Ibid

53 Ekran, "How to Prevent Human Error: Top 4 Employee Cybersecurity Mistakes," last modified 2019, accessed October 9, 2022, https://www.ekransystem.com/en/blog/how-prevent-human-error-top-5-employee-cyber-security-mistakes

B. Rekayasa Sosial

Menurut *U.S. Department of Justice*, yang dikutip oleh Fatima Salahdine, dan Naima Kaabouch, serangan rekayasa sosial merupakan salah satu ancaman paling berbahaya di dunia.[54] Menurut mereka, rekayasa sosial dapat diklasifikasikan menjadi dua (2), yaitu berbasis manusia atau berbasis komputer. Di sini, rekayasa sosial mengelabui korban untuk mendapatkan data spesifik yang dapat digunakan untuk menguntungkan pelaku kejahatan secara finansial. Tentu saja, barang-barang tersebut dapat digunakan untuk tujuan tertentu, atau bahkan dijual di pasar gelap dan web gelap.[55]

Sedangkan *human-based* (berbasis manusia) menggunakan pendekatan tradisional yang mengandalkan hubungan komunikasi antar individu sehingga pelaku kejahatan dapat menggali informasi dan berusaha mencurinya. Sedangkan pendekatan berbasis komputer menekankan pada penggunaan sistem. Hal ini dapat dilakukan dengan menggunakan teknologi komputer dan teknologi telekomunikasi. Penggunaan perangkat lunak yang digunakan akan berupaya mencuri data konsumen yang penting.

Pada tahun 2020, Abeer F. AL-Otaibi dan Emad S Alsuwat dalam kesimpulan penelitiannya menyatakan bahwa "ancaman rekayasa sosial telah menjadi ancaman utama dan dianggap sebagai ancaman keamanan terbesar dan paling berbahaya yang merupakan pelanggaran yang dihadapi oleh individu dan institusi".[56] Melalui rekayasa sosial, sebuah organisasi dapat kehilangan data dan informasi penting. Rekayasa sosial akan menyerang dengan seni dan teknik memanipulasi atau memikat pengguna dan institusi untuk mendapatkan data penting yang diinginkan penjahat.

Oleh karena itu, pasal 36 Undang-Undang PDP mengatur bahwa Pengontrol Data Pribadi wajib mencegah Data Pribadi tersebut diakses secara tidak sah. Pencegahan dapat dilakukan dengan menggunakan sistem pengamanan Data Pribadi yang diolah dan/atau diolah dengan menggunakan sistem elektronik secara handal, aman dan bertanggung jawab. Oleh karena itu, diperlukan sistem keamanan yang memadai, mengingat "serangan siber" saat ini akan menyasar sistem keamanan yang lemah dan memberikan keuntungan bagi para pelaku kejahatan.

C. Orang Dalam yang Berbahaya

Dalam berbagai kegiatan organisasi tentunya ada karyawan yang memiliki niat buruk. Itu juga dapat terjadi pada organisasi yang terkait dengan penyedia layanan elektronik. Pelanggaran karyawan dapat berupa mencari keuntungan sendiri dengan mengabaikan kepentingan organisasi, maupun konsumen. Mereka dapat memposisikan diri mereka sebagai, orang dalam yang jahat, orang dalam, informan, dan *whistle-blower* semuanya mampu membocorkan data ke luar.[57]

Mengingat perannya sebagai "*inside person*", mereka akan lebih mengetahui apa yang dilakukan organisasi, isu yang sedang tren, data penting terkait data konsumen dan data perusahaan, serta hal-hal rahasia lainnya. Orang dalam, diberi tanggung jawab dan kepercayaan untuk menjaga hal-hal tersebut. Oleh karena itu, orang dalam lebih berbahaya melakukan pelanggaran daripada orang luar, terutama dalam hal pembocoran data rahasia.

Dalam hal ini, serangan orang dalam menyumbang 34% dari semua pelanggaran data pada tahun 2018 seperti yang ditangani oleh IBM.[58] Untuk suatu organisasi bisnis, ini merupakan jumlah yang signifikan, dan dapat mempengaruhi kepercayaan publik dalam pemberian layanan, terutama terkait dengan masalah menjaga kerahasiaan data konsumen. Selain itu, ancaman orang dalam yang berbahaya dapat terjadi dalam berbagai bentuk seperti sabotase Teknologi Informasi (TI) orang dalam dan penipuan oleh orang dalam.[59]

---

54 Fatima Salahdine and Naima Kaabouch, "Social Engineering Attacks: A Survey," *Future Internet* 11, no. 4 (2019)

55 Ibid

56 Abeer F. AL-Otaibi and Emad S Alsuwat, "A Study on Social Engineering Attacks: Phishing Attack," *International Journal of Recent Advances in Multidisciplinary Research* 07, no. 11 (2020): 6374–6380

57 Diogo A.B. Fernandes et al., "Chapter 25 - A Quick Perspective on the Current State in Cybersecurity," in *Emerging Trends in ICT Security*, 2014, 423–442, https://www.sciencedirect.com/science/article/pii/B9780124114746000256.

58 Abolaji B. Akanbi et al., "A Stacked Ensemble Framework for Detecting Malicious Insiders," *International Journal of Innovative Research in Computer Science & Technology* 8, no. 4 (2020)

59 Ibid

Orang dalam inilah yang menyebabkan tersebarnya data atau informasi elektronik kepada orang yang tidak berwenang. Perlu merujuk pada Pasal 32 (2) Undang-Undang ITE telah mengatur pelanggaran tersebut bahwa setiap orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apapun memindahtangankan Informasi Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik milik orang lain yang tidak berhak.

3.2 Pencurian Data

Menurut Kaspersky, definisi "pencurian data" adalah tindakan mencuri informasi digital yang disimpan di komputer, server, atau perangkat elektronik untuk mendapatkan informasi rahasia atau membahayakan privasi.[60] Ini adalah aktivitas secara ilegal yang dilakukan oleh pelaku untuk mengakses sumber data dan mencuri mereka. Dengan demikian, berbagai perangkat seperti database bisnis, desktop, perangkat genggam, telepon, flash drive, dan kamera semuanya dapat digunakan oleh pencuri untuk mencuri data.[61]

Pencurian Identitas (ID) terjadi ketika seseorang mencuri informasi pribadi Anda untuk melakukan penipuan.[62] Penyedia layanan harus memiliki komitmen untuk memberikan perlindungan data untuk mencegah akses secara ilegal. Hal itu bisa diwujudkan dengan memperkuat sistem keamanan yang tangguh. Dalam perjanjian online, komitmen ini harus dituangkan. Bukan hanya untuk kepentingan konsumen tetapi juga untuk kepentingan penyedia jasa. Di sini, pencurian data merupakan masalah utama bagi banyak bisnis karena keamanan, reputasi, dan kerugian finansial.[63]

Secara historis, sejak tahun 1997, *Federal Trade Commission* (FTC) mengidentifikasi bahwa jumlah pengaduan terkait "pencurian identitas" telah meningkat. Dalam hal ini, *Consumer Sentinel Network* (CSN) yang merupakan bagian dari FTC melaporkan bahwa pada tahun 2013 telah menerima lebih dari 2 juta pengaduan dari konsumen. 14% masuk dalam kategori "pencurian identitas".[64] Data yang dicuri umumnya berupa data spesifik, seperti informasi rekening bank dan kartu kredit, termasuk data rekam medis. Terkait layanan *EHealth*, resiko bagi konsumen yang menggunakan fasilitas ini adalah pencurian data berupa "Rekam Medis".

Hal tersebut adalah sesuatu yang perlu dilindungi. Rekam medis berisi dokumen yang memuat data identitas pasien, pemeriksaan, pengobatan, tindakan, dan pelayanan lain yang telah diberikan kepada pasien. Untuk itu secara khusus dilindungi dengan Peraturan Menteri Kesehatan Republik Indonesia Nomor 24 Tahun 2022 tentang Rekam Medis.[65]

Di sini, Laporan medis berarti setiap laporan yang dihasilkan oleh konsultan luar Pengguna yang terlibat untuk melakukan pengujian atau pemeriksaan medis atau terkait medis pada atau pasien tersebut.[66] Jika sistem keamanan yang dimiliki oleh penyedia layanan kesehatan tidak kuat, maka pelaku dapat mengaksesnya. Mereka memiliki akses ke data pribadi untuk menghapus, mengubah, memodifikasi, atau mencegah akses ke data tersebut secara ilegal.

Dalam hal ini, penulis mengidentifikasi upaya "pencurian data" terkait layanan *eHealth*, yang dapat berupa, sebagai berikut:

A. Serangan dunia maya

Serangan dunia maya yang berhasil mengenai sasaran akan berdampak pada berbagai tingkat dampak, mulai dari pengguna individu, organisasi penyedia layanan, bahkan sistem komputasi yang digunakan. Dampak paling signifikan biasanya dirasakan pada data yang disimpan dalam sistem atau data yang dikirimkan melalui

60 Kaspersky, "What Is Data Theft and How to Prevent It," accessed October 2, 2022, https://www.kaspersky.com/resource-center/threats/data-theft.

61 Source Defense, "What Is Data Theft?," last modified 2022, accessed October 3, 2022, https://sourcedefense.com/glossary/what-is-data-theft/

62 usa.gov, "Identity Theft," last modified 2022, accessed October 3, 2022, https://www.usa.gov/identity-theft.

63 Source Defense, "What Is Data Theft?"

64 Koyame-Marsh and Marsh, "Data Breaches and Identity Theft: Costs and Responses."

65 *The Regulation of the Minister of Health of the Republic of Indonesia Number 24 of 2022 Concerning Medical Records*

66 Law Insider, "Medical Reports Definition," last modified 2022, accessed October 4, 2022, https://www.lawinsider.com/dictionary/medical-reports

jaringan. Dampak tersebut dapat terkait dengan kerahasiaan, integritas, atau ketersediaannya.[67] Secara umum, serangan siber ini telah diatur dalam Undang-Undang ITE. Khususnya dalam Pasal 30 yang mengatur larangan akses tanpa izin dan menerobos, menyalip, atau membobol sistem keamanan.

B. Peretasan

Peretasan digunakan sebagai metode untuk melakukan kejahatan lain seperti pencurian identitas di dunia maya.[68] Modus kejahatan ini mengancam data pribadi yang sensitif dengan cara yang berbeda dari modus lainnya. Modus operandi lain melibatkan kelalaian konsumen, tetapi untuk modus ini, subjek aktif pencurian data adalah pelakunya sendiri. Modusnya bisa dilakukan secara online, melalui jaringan internet, maupun offline tidak melalui jaringan lain.

Pelaku harus memiliki keahlian di bidang IT dan jaringan, untuk menerobos sistem keamanan organisasi keuangan. Kuncinya memang ada di sistem keamanannya, apakah bisa dengan mudah ditembus atau tidak. Bagi penyedia layanan *eHealth* yang tidak memiliki sistem yang relatif aman, akan mudah ditembus. Ancamannya adalah data konsumen dapat diketahui oleh pelakunya, termasuk penggunaan sistem cloud computing. Di sini, komputasi awan adalah istilah umum untuk segala hal yang melibatkan pengiriman layanan yang dihosting melalui internet. Layanan ini dibagi menjadi tiga kategori utama yaitu infrastruktur, platform, dan perangkat lunak.[69]

Pasal 16 (2e) Undang-Undang PDP, mengatur bahwa pengendali data pribadi harus melindungi keamanan Data Pribadi dari akses yang tidak sah, pengungkapan yang tidak sah, modifikasi yang tidak sah, penyalahgunaan, perusakan, dan/atau kehilangan data pribadi. Tindakan tersebut dapat dilakukan oleh orang yang memiliki pengetahuan di bidang teknologi informasi yang mumpuni, sehingga dapat mengetahui bahwa sistem keamanan tersebut dimiliki oleh pihak lain.

Lebih lanjut, menurut Norton Cybersecurity Insights Report, pada tahun 2015 sebanyak 594 juta orang di seluruh dunia telah menjadi korban. Dari data tersebut, sebanyak 21% email orang Amerika telah diretas. Selain itu, sebanyak 12% data keuangan mereka dicuri setelah berbelanja melalui platform online. Kasus-kasus tersebut merupakan bagian dari risiko penggunaan layanan Wi-Fi publik, yang tidak menjamin keamanan data pengguna.[70]

C. *Deceptive Phishing*

Bentuk kejahatan lain yang terkait dengan kejahatan siber adalah *phishing*. Secara umum, phishing adalah tindakan mencoba mengelabui penerima pesan, dengan mengirimkan email dengan niat jahat. Hal ini dilakukan agar penerima membuka dan mengikuti petunjuk yang diberikan oleh pelaku. Modus operandinya tidak hanya bisa dikirim melalui email, tapi juga SMS dan media sosial. Tujuan utamanya adalah mengelabui pemilik data pribadi yang sensitif, dan mengakses data korban. Secara khusus, apa yang merupakan bagian dari kejahatan dunia maya disebut *Deceptive Phishing*. *Deceptive Phishing* adalah mengelabui seseorang agar mengeklik tautan berbahaya dalam email phishing yang tampaknya sah daripada menerobos pertahanan komputer.[71]

Korban akan menduga bahwa email tersebut berasal dari organisasi secara legal. Kerugian konsumen di sini adalah mereka tidak berhati-hati untuk memeriksa nama domain asli dari organisasi hukum mereka. Hal yang sangat berbahaya adalah email phishing mungkin memiliki konten berbahaya, seperti dokumen berupa

---

67 Kenneth Okereafor and Oluwasegun Adelaiye, "Randomized Cyber Attack Simulation Model: A Cybersecurity Mitigation Proposal for Post COVID-19 Digital Era," *International Journal of Recent Engineering Research and Development (IJRERD)* 05, no. 07 (2020): 61–72, www.ijrerd.com.

68 Rizal Rahman, Nazura Abdul Manap, and Sohaib Mukhtar, "Hacking in Cyberspace Identity Theft: A Comparative Analysis of Malaysia, United Kingdom, and Iran," *Baltica* 23, no. 11 (2020): 67–86, https://www.researchgate.net/publication/347935764

69 Wesley Chai and Stephen J. Bigelow, "Cloud Computing," last modified 2022, accessed February 14, 2023, https://www.techtarget.com/searchcloudcomputing/definition/cloud-computing.

70 Norton, "Why Hackers Love Public Wi-Fi," last modified 2019, accessed October 12, 2022, https://us.norton.com/blog/wifi/why-hackers-love-public-wifi#.

71 Alexander S. Gillis, "Phishing," last modified 2020, accessed October 16, 2022, https://www.techtarget.com/searchsecurity/definition/phishing

dokumen PDF atau Word yang berisi perangkat lunak berbahaya (*malware*). Bahaya yang terkait dengan phishing adalah, adanya kejahatan 'typo squatting' yang memungkinkan pelaku membuat 'nama domain palsu' yang membuat pengguna salah memasukkan nama domain.

Umumnya, berita yang dimuat dalam email atau media sosial berisi berita yang memaksa pengguna untuk mengakses 'situs palsu', dan memasukkan data keuangan sensitif mereka. Ini mungkin berisi program atau file yang berbahaya bagi pengguna komputer. Jenis malware yang dapat dipasang di "situs web palsu" antara lain virus komputer, worm, trojan horse, dan spyware. Perangkat lunak yang dirancang untuk melakukan aktivitas secara ilegal dapat berfungsi untuk melakukan pencurian, penghapusan, pengubahan, dan melakukan aktivitas spionase.

Data pribadi yang sensitif seperti rekam medis, terancam karena segala aktivitas yang dilakukan melalui internet, terutama yang berhubungan dengan keuangan akan diketahui oleh pelaku kejahatan. Rekam medis berisi dokumen yang memuat data identitas pasien, pemeriksaan, pengobatan, tindakan, dan pelayanan lain yang telah diberikan kepada pasien. Untuk itu secara khusus dilindungi dengan Peraturan Menteri Kesehatan Republik Indonesia Nomor 24 Tahun 2022 tentang Rekam Medis.[72]

Informasi yang disampaikan umumnya mengharuskan pengguna memasukkan sejumlah data pribadi sensitif yang kemudian akan diketahui oleh pelaku. Dengan demikian, pelaku akan leluasa memasukkan data pribadi yang sensitif untuk mengakses nama domain resmi, tempat pengguna menyimpan uang. Oleh karena itu, istilah phishing tidak hanya untuk mendapatkan detail akun pengguna, tetapi sekarang mencakup akses ke data semua pribadi dan keuangan.[73] Dengan demikian, penyelenggara sistem elektronik harus mengikuti peraturan yang diatur dalam Permen 18/2022, karena standar pengelolaan kesehatan data melalui sistem informasi telah diatur. Hal yang paling krusial adalah faktor keamanan data. Disini peran administrator sistem informasi memiliki kewajiban untuk memberikan edukasi dan menyediakan sistem keamanan yang memadai.

4. KESIMPULAN

Dengan hadirnya layanan *eHealth* memberikan berbagai kemudahan bagi pengguna untuk mendapatkan berbagai fasilitas kesehatan melalui platform elektronik. Ini memberikan solusi tempat dan jarak yang akan mempengaruhi biaya mendapatkan pelayanan kesehatan. Namun, hal ini juga berdampak negatif dengan munculnya permasalahan hukum akibat ancaman pelaku kejahatan terhadap data konsumen.

Studi ini menyimpulkan bahwa ancaman kebocoran data konsumen dapat muncul karena "pelanggaran data" dan "pencurian data". Pelanggaran data dapat terjadi karena "kecerobohan" atau "itikad buruk" dari pengelola data pribadi, seperti kelalaian pegawai yang kurang hati-hati dalam menjaga data sehingga data secara tidak sengaja tersebar ke pihak yang tidak bertanggung jawab. Sedangkan karyawan yang "beriktikad buruk" dapat dengan sengaja mengolah data tersebut secara tidak sah untuk tujuan komersial, baik dengan mengolahnya sendiri maupun dengan melakukan kerjasama dengan pihak lain. Berbagai perbuatan melawan hukum dalam kategori ini antara lain kesalahan karyawan, Social Engineering, dan *Malicious Insiders*.

Sedangkan "pencurian data" disebabkan oleh kegiatan "akses secara ilegal" yang dilakukan oleh pelaku agar data dapat diubah, dirusak, dan dihapus. Berbagai perbuatan melawan hukum dalam kategori ini antara lain serangan siber, hacking, dan *Deceptive Phishing*. Data terkait *eHealth* termasuk dalam kategori data khusus yang dilindungi oleh peraturan perundang-undangan di Indonesia. Pengesahan Undang-Undang PDP, akan memberikan "kepastian hukum" sebagai upaya memberikan perlindungan data. Perlindungan data yang diatur oleh Undang-Undang PDP telah mengadopsi prinsip dasar perlindungan data yang diatur oleh GDPR di Uni Eropa (UE).

Di sini, budaya hukum di UE saat ini sangat berhati-hati dalam memberikan data pribadi orang lain. Khususnya lembaga sangat berhati-hati mengingat konsekuensi sanksi yang sangat berat. Hal inilah yang perlu dikembangkan di Indonesia, mengingat budaya hukum masih sangat mudah untuk mendapatkan data pribadi dari pihak tertentu. Maka, jangan heran, ada yang dengan mudah menawarkan hal-hal tertentu, seperti kartu kredit dan asuransi.

---

72 *The Regulation of the Minister of Health of the Republic of Indonesia Number 24 of 2022 Concerning Medical Records*

73 Gunter Ollmann, *The Phishing Guide*, *IBM*, 2007, https://www.scribd.com/document/219802442/The-Phishing-Guide-Understanding-Preventing-Phishing-Attacks-IBM-Internet-Security-Systems

5. UCAPAN TERIMA KASIH

Pertama-tama, penulis mengucapkan puji syukur kepada Allah SWT atas selesainya penelitian ini, Kemendikbudristek Republik Indonesia atas dukungan dananya. Dan terima kasih kepada Program Pascasarjana Hukum, Universitas Langlangbuana dan Badan Pengembangan Sumberdaya Manusia (BPSDM), Kementerian Hukum dan Hak Asasi Manusia, Republik Indonesia atas dukungan yang berharga.

6. SPONSOR

Penulisan ini mendapatkan dana hibah penelitian dasar dari Kementerian Pendidikan, Kebudayaan, Ristek, pada tahun 2022

DAFTAR PUSTAKA

Akanbi, Abolaji B., Adewale O. Adebayo, Sunday A. Idowu, and Ebunoluwa E. Okediran. "A Stacked Ensemble Framework for Detecting Malicious Insiders." *International Journal of Innovative Research in Computer Science & Technology* 8, no. 4 (2020).

Almunia, Joaquín. "Speech - Competition and Personal Data Protection, Commissioner Joaquín Almunia." *European Commission*. Last modified 2012. https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_12_860.

APJII. "APJII Di Indonesia Digital Outloook 2022." Last modified 2022. Accessed February 14, 2023. https://apjii.or.id/berita/d/apjii-di-indonesia-digital-outloook-2022_857.

Asikin, Z Amiruddin &. *Pengantar Metode Penelitian Hukum*. Jakarta: Raja Grafindo Persada, 2003.

Becerril, Anahiby Anyel. "The Value of Our Personal Data in the Big Data and the Internet of All Things Era." *ADCAIJ: Advances in Distributed Computing and Artificial Intelligence Journal* 7, no. 2 (2018): 71–80.

Bottis, Maria, and George Boucha. "Personal Data v. Big Data: Challenges of Commodification of Personal Data." *Open Journal of Philosophy* 8 (2018): 206–215. http://www.scirp.org/journal/ojpp.

Castells, M. *The Information Age*. III. Oxford: Blackwell, 1998.

Chai, Wesley, and Stephen J. Bigelow. "Cloud Computing." Last modified 2022. Accessed February 14, 2023. https://www.techtarget.com/searchcloudcomputing/definition/cloud-computing.

Culnan, M. J., and C. C. Williams. "How Ethics Can Enhance Organizational Privacy: Lessons from the Choicepoint and TJX Data Breaches." *MIS Quarterly* 33, no. 4 (2009): 673–687.

Dymyt, Malgorzata. "The Role of EHealth in the Management of Patient Safety." *Journal of e-health Management* 2020 (2020): 1–13. https://ibimapublishing.com/articles/JEHM/2020/341252/.

Ekran. "How to Prevent Human Error: Top 4 Employee Cybersecurity Mistakes." Last modified 2019. Accessed October 9, 2022. https://www.ekransystem.com/en/blog/how-prevent-human-error-top-5- employee-cyber-security-mistakes.

European Court of Human Rights. *Vereniging Weekblad Bluf! V. the Netherlands*, Series A v (1995).

Eysenbach, Gunther. "What Is E-Health?" *Journal of Medical Internet Research* 3, no. 2 (2001): 1–5.

F. AL-Otaibi, Abeer, and Emad S Alsuwat. "A Study on Social Engineering Attacks: Phishing Attack." *International Journal of Recent Advances in Multidisciplinary Research* 07, no. 11 (2020): 6374–6380.

Fernandes, Diogo A.B., Liliana F.B. Soares, João V. Gomes, Mário M. Freire, and Pedro R.M. Inácio. "Chapter 25 - A Quick Perspective on the Current State in Cybersecurity." In *Emerging Trends in ICT Security*, 423–442, 2014. https://www.sciencedirect.com/science/article/pii/B9780124114746000256.

Gillis, Alexander S. "Phishing." Last modified 2020. Accessed October 16, 2022. https://www.techtarget.com/searchsecurity/definition/phishing.

Herman, Herman. "6 Juta Data Pasien RS Bocor, Ini Risiko Yang Mengintai." *7 January 2022*. Last modified 2022. Accessed September 28, 2022. https://www.beritasatu.com/lifestyle/876043/6-juta-data-pasien-rs-bocor-ini-risiko-yang-mengintai.

Irwin, Luke. “Human Error Is Responsible for 82% of Data Breaches.” Last modified 2022. Accessed October 4, 2022. https://www.grcelearning.com/blog/human-error-is-responsible-for-85-of-data-breaches#:~:text=According to Verizon’s 2022 Data,to access the organisation’s systems.

Jain, S. N. “Legal Research and Methodology.” *Journal of the Indian Law Institute* 14, no. 4 (1972): 487–500. https://www.jstor.org/stable/43950155.

Journal, HIPAA. *Healthcare Data Breach Statistics*, 2022. https://www.hipaajournal.com/healthcare-data-breach-statistics/.

Kaspersky. “What Is Data Theft and How to Prevent It.” Accessed October 2, 2022. https://www.kaspersky.com/resource-center/threats/data-theft.

Kominfo. “Rapat Paripurna DPR Sahkan RUU PDP.” Last modified 2022. Accessed October 16, 2022. https://aptika.kominfo.go.id/2022/09/rapat-paripurna-dpr-sahkan-ruu-pdp/.

Koyame-Marsh, Rita O., and John L. Marsh. “Data Breaches and Identity Theft: Costs and Responses.” *IOSR Journal of Economics and Finance (IOSR-JEF)* 5, no. 6 (2014): 36–45. www.iosrjournals.org.

———. “Data Breaches and Identity Theft: Costs and Responses.” *IOSR Journal of Economics and Finance (IOSR-JEF)* 5, no. 6 (2014): 36–45.

Langbroek, Philip, Kees van den Bos, Marc Simon Thomas, Michael Milo, and Wibo van Rossum. “Methodology of Legal Research: Challenges and Opportunities.” *Utrecht Law Review* 13, no. 3 (2017): 1–8.

Law Insider. “Medical Reports Definition.” Last modified 2022. Accessed October 4, 2022. https://www.lawinsider.com/dictionary/medical-reports.

M.D., Pradeep. “Legal Research- Descriptive Analysis on Doctrinal Methodology.” *International Journal of Management, Technology, and Social Sciences* 4, no. 2 (2019): 95–103.

Martin, Kelly D., Abhishek Borah, and Robert W. Palmatier. “Data Privacy: Effects on Customer and Firm Performance.” *Journal of Marketing* 81, no. 1 (2017): 36–58.

Martin, Nik. “Indonesia’s Jakarta Hit by Major Power Blackout.” Last modified 2019. Accessed October 2, 2019. https://www.dw.com/en/indonesias-jakarta-hit-by-major-power-blackout/a-49884728.

Della Mea, Vincenzo. “What Is E-Health (2): The Death of Telemedicine?” *Journal of Medical Internet Research* 3, no. 2 (2001): 6–7.

Media Infokes. “Penggunaan Aplikasi Kesehatan Digital Di Indonesia, Hanya 10% Dari Total Penduduk.” Last modified 2019. Accessed October 4, 2022. https://media-infokes.com/2019/08/22/penggunaan-aplikasi-kesehatan-digital-di-indonesia-hanya-10-dari-total-penduduk/.

Mitchell, John. “Increasing the Cost-Effectiveness of Telemedicine by Embracing e-Health.” *Sage Joulnals* 6, no. 1 (2000). https://journals.sagepub.com/doi/10.1258/1357633001934500.

Norton. “Why Hackers Love Public Wi-Fi.” Last modified 2019. Accessed October 12, 2022. https://us.norton.com/blog/wifi/why-hackers-love-public-wifi#.

Okereafor, Kenneth, and Oluwasegun Adelaiye. “Randomized Cyber Attack Simulation Model: ACybersecurity Mitigation Proposal for Post COVID-19 Digital Era.” *International Journal of Recent Engineering Research and Development (IJRERD)* 05, no. 07 (2020): 61–72. www.ijrerd.com.

Ollmann, Gunter. *The Phishing Guide*. *IBM*, 2007. https://www.scribd.com/document/219802442/The-Phishing-Guide-Understanding-Preventing-Phishing-Attacks-IBM-Internet-Security-Systems.

Peretti, K. K. “Data Breaches: What the Underground World of Carding Reveals.” *Santa Clara Computer & High Tech* 25, no. 2 (2008): 375–413.

Rahman, Rizal, Nazura Abdul Manap, and Sohaib Mukhtar. “Hacking in Cyberspace Identity Theft: A Comparative Analysis of Malaysia, United Kingdom, and Iran.” *Baltica* 23, no. 11 (2020): 67–86. https://www.researchgate.net/publication/347935764.

Robertson, Geoffrey, and Andrew Nicol. *Media Law*. Fifth Edit. London, UK: Penguin Books, n.d.

Salahdine, Fatima, and Naima Kaabouch. “Social Engineering Attacks: A Survey.” *Future Internet* 11, no. 4 (2019).

Saputra, Andi. “Jual Database Nasabah Perbankan, Warga Tangsel Dibui 9 Bulan.” *Detik News*. Last modified 2019. Accessed October 2, 2022. https://news.detik.com/berita/d-4588549/jual-database-nasabah-perbankan-warga-tangsel-dibui-9-bulan.

Shankar, Nithya Mohammed, Zareef. “Surviving Data Breaches: A Multiple Case Study Analysis.” *Journal of Comparative International Management* 23, no. 1 (2020): 35–54.

Soekanto, Soerjono. *Pengantar Penelitian HUkum*. Jakarta: UI Press, 1986.

Source Defense. “What Is Data Theft?” Last modified 2022. Accessed October 3, 2022. https://sourcedefense.

com/glossary/what-is-data-theft/.

———. “What Is Data Theft?”

Statista. “EHealth - Indonesia.” Last modified 2022. Accessed March 26, 2023. https://www.statista.com/

outlook/dmo/digital-health/ehealth/indonesia.

Sudibyo, Agus. *Jagad Digital*. Jakarta: Kepustakaan Populer Gramedia, 2019.

Trautman, L. J., and P Ormerod. “Corporate Directors’ and Officers’ Cybersecurity Standard of Care: The

Yahoo Data Breach.” *American University Law Review* 66 (2017): 1231–1291.

usa.gov. “Identity Theft.” Last modified 2022. Accessed October 3, 2022. https://www.usa.gov/identity-theft. verizon.com. “2022 Data Breach Investigations Report.” Last modified 2022. Accessed October 4, 2022.

https://www.verizon.com/business/resources/reports/dbir/.

Virmani, Charu, Neha Kaushik, Mohak, Vishnu Mathur, and Sanskar Saxena. “Analysis of Cyber Attacks and Security Intelligence: Identity Theft.” *Indian Journal of Science and Technology* 13, no. 25 (2020): 2529–2536.

Walker, Clive, and David Wall. *The Internet, Law and Society*. UK: Person Education Limited, 2000.

White, Jamie. “Yahoo Announces 500 Million Users Impacted by Data Breach.” *2021*. Last modified 2021.

Accessed October 4, 2022. https://lifelock.norton.com/learn/data-breaches/company-data-breach.

WHO. “EHealth.” Last modified 2022. http://www.emro.who.int/health-topics/ehealth/.

Decree of the Minister of Health Number 192/MENKES/SK/VI/2012 Regarding Roadmap of Strengthening Action Plan Indonesian Health Information System, n.d.

Decree of the Minister of Health of the Republic of Indonesia No. 374/MENKES/SK/V/2009 Concerning the National Health System (NHS), n.d.

Regulation of the Minister of Communication and Informatics No. 20 of 2016 Concerning Protection of Personal Data in Electronic Systems, n.d.

Regulation of the Minister of Health, No 18 of 2022 Concerning Implementation of One Data in the Health Sector Through the Health Information System., n.d.

The Law Number. 27 of 2022 on Personal Data Protection, n.d.

The Law Number 19 of 2016 Concerning Amendments to Law Number 11 of 2008 on Information and Electronic Transactions, n.d.

The Regulation of the Minister of Health of the Republic of Indonesia Number 24 of 2022 Concerning Medical Records, n.d.