IUSTITIA OMNIBUS
JURNAL ILMU HUKUM

Iustitia Omnibus: Jurnal Ilmu Hukum
Volume 5, Number 1, 2023 pp. 53-65
P-ISSN: 2716-1455 E-ISSN: 2716-277X
Open Access: http://jurnal.pasca.unla.ac.id/index.php/iustitiaomnibus/index

PENEGAKKAN HUKUM ATAS TINDAK PIDANA PENCURIAN DATA PADA AKTIVITAS *TELEMEDICINE*

***Wiston Karunna[1], Jafar Sidik[2]**
Program Pascasarjana, Universitas Langlangbuana, Bandung, Indonesia
e-mail: asetrix.bdg@gmail.com

ARTICLE INFO

Article history:
Received November, 2023
Revised November, 2023
Accepted November, 2023
Available online Desember, 2023

Kata Kunci:
Kejahatan Siber, Perlindungan Data, Telehealth, Telemedicine

Keywords:
Cybercrime, Data Protection, Telehealth, Telemedicine

ABSTRAK

Telemedicine mempunyai beberapa keunggulan, seperti efektif memangkas alur birokrasi serta menjamin hak warga negara untuk memperoleh pelayanan kesehatan yang cepat dan akurat, namun kebocoran data/ informasi menjadi efek samping negatif. Pembiaran terhadapnya akan mengancam keberlanjutan Telemedicine itu sendiri. Penelitian ini bertujuan untuk mengetahui bagaimana perlindungan hukum terhadap data pribadi di internet ketika terjadi pencurian data pada aktivitas telemedicine Indonesia dikaitkan dengan Undang-undang Nomor 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik Berdasarkan Asas Kepastian Hukum serta sejauh mana efektifitas sanksi atas pencurian data pribadi dalam praktek telemedicine berdasarkan undang-undang positif di Indonesia. Pendekatan yang digunakan dalam penelitian ini adalah pendekatan normatif, metode penelitian hukum yang mengkaji hukum tertulis dan kepustakaan atau penelitian hukum dari beragam perspektif dengan bahan hukum hukum primer dan bahan hukum sekunder. Analisis ini didasarkan atas metode deskriptif dalam mengumpulkan data dan menghubungkan permasalahan dan contoh kasus dengan analisis berdasarkan teori hukum yang disusun sistematis. Hasil penelitian ini menunjukkan dalam konteks perlindungan privasi atas data pribadi pasien belum sepenuhnya terjamin karena belum pahamnya masyarakat Indonesia akan haknya dan belum merata pemahaman baik pihak pemerintah akan pentingnya perlindungan data pribadi pasien sehingga diperlukan pengaturan yang khusus tentang perlindungan data pribadi pasien dalam program telehealth walaupun telah diatur di dalam beberapa undang-undang.

ABSTRACT

Telemedicine has several advantages, such as effectively cutting bureaucratic flow and guaranteeing citizens' rights to obtain fast and accurate health services, but data/information leaks are a negative side effect. Failure to do so would threaten the very desire of Telemedicine. This research aims to find out how legal protection is for personal data on the internet when data theft occurs in Indonesian telemedicine activities related to Law Number 19 of 2016 concerning Information and Electronic Transactions Based on the Principle of Legal Certainty and to what extent the effectiveness of sanctions for theft of personal data in practice telemedicine based on positive law in Indonesia. The approach used in this research is a normative approach, a legal research method that examines written law and literature or legal research from various perspectives using primary legal material and secondary legal material. This analysis is based on descriptive methods in collecting data and connecting problems and case examples with analysis based on legal theory which is arranged systematically. The results of this research show that in the context of privacy protection for patients' personal data, it is not yet fully guaranteed because the Indonesian people do not yet understand their rights and the government does not have a good understanding of the importance of protecting personal patient data, so that special regulations regarding the protection of patient personal data in the telehealth program are needed even though it has been implemented. regulated in several laws.

PENDAHULUAN

Salah satu produk hukum yang sangat penting menunjang pembangunan di bidang informasi dunia maya dan transaksi elektronik yang menjadi roda penggerak ekonomi negara adalah Undang undang Informasi dan Transaksi Elektronik nomor 19 tahun 2016. Adapun yang menjadi salah satu produk terpentingnya adalah pasal 26 tentang perlindungan data pribadi. Undang-undang ini merupakan revisi undang-undang no 11 tahun 2008. Adapun bunyi Pasal 26 ayat (1) UU 19/2016:

> "Kecuali ditentukan lain oleh peraturan perundang-undangan, penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan Orang yang bersangkutan."

Penjelasan Pasal 26 ayat (1) UU 19/2016 dalam pemanfaatan Teknologi Informasi, perlindungan data pribadi merupakan salah satu bagian dari hak pribadi (*privacy rights*). Hak pribadi mengandung pengertian sebagai berikut:

Hak pribadi merupakan hak untuk menikmati kehidupan pribadi dan bebas dari segala macam gangguan. Hak pribadi merupakan hak untuk dapat berkomunikasi dengan Orang lain tanpa tindakan memata-matai. Hak pribadi merupakan hak untuk mengawasi akses informasi tentang kehidupan pribadi dan data seseorang.

Konsideran Undang-undang ITE ini, menyatakan bahwa adanya kepastian dan perlindungan hukum atas setiap kegiatan yang melibatkan media elektronik untuk mengakses informasi dan transaksi elektronik, sehingga memerlukan kepaseitan hukum atas perlindungan data pribadi yang kuat dan mampu memberi kepastian hukum bagi pihak pihak yang berkepentingan yang dapat mendorong peningkatan partisipasi masyarakat melalui media elektronik dalam pembangunan untuk mewujudkan masyarakat yang sejahtera, adil, dan makmur berdasarkan Pancasila dan Undang undang Dasar 1945.

Seringkali kenyataan yang terjadi di masyarakat tidak seperti yang diharapkan, yang terjadi dalam praktik banyak anggota masyarakat yang mengakses media elektronik menjadi korban pencurian data. Hal ini terjadi bahkan tanpa sepengetahuan pemilik data tersebut. Perlindungan Atas Privasi Data Pribadi Dalam Sistem Elektronik Terhadap Tindak Pencurian Data sudah sejak lama dinantikan dan diidam- idamkan. UU ITE memang belum memuat aturan perlindungan data pribadi secara khusus. Tetapi secara khusus dalam sistem elektronik, ketentuan mengenai privasi dan data pribadi dapat ditemukan dalam Undang- Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik ("UU ITE") sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik ("UU 19/2016"). Pengguna teknologi selalu berinteraksi dengan pihak penyedia jasa informasi sebagai imbas dari perkembangannya. Beberapa sektor kehidupan berdasarkan sistem informasi ini adalah bidang perdagangan (*e-commerce*),

transportasi, industri, pariwisata, bidang pemerintahan (*e-government*) dan industri keuangan (*e-payment*). Dampak langsung dari pemanfaatan teknologi informasi ini adalah meliputi pengumpulan (*collect*), penyimpanan (*store*), pemrosesan, produksi dan pengiriman dari dan ke industri atau masyarakat secara cepat dan efektif.

Perlindungan terhadap hak atas privasi, berarti memberikan perlindungan pula terhadap hak atas kebebasan berbicara. Artinya, hak atas privasi menjamin perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi. Akan tetapi dalam pelaksanaanya masih saja ada hal-hal ataupun suatu kejadian yang menimbulkan data diri dilindungi bocor ke publik yang mana data diri tersebut telah masuk data diri yang bersifat pribadi. Salah satu contohnya kebocoran data diri yang dialami oleh lembaga atau Badan Penyelenggara Jaminan Sosial Kesehatan (BPJS Kesehatan) yang bisa dikatakan kebocoran data diri yang besar.

Seperti telah disinggung sebelumnya, suatu kasus nyata yang terjadi adalah kasus atas Data kesehatan yang merupakan data pribadi yang bersifat spesifik, sensitif, dan rahasia, yang harus dilindungi. Jutaan data dan informasi kesehatan milik penduduk Indonesia sering mengalami kebocoran. Akhir Agustus 2021 lalu, sekitar 1,3 juta data pengguna aplikasi *Health Alert Card (eHAC)* buatan Kementerian Kesehatan Indonesia yang memuat data Covid-19 dibobol. Tindakan ini merupakan aksi *hack* pidana atas pencurian data. Belum diketahui siapa pelakunya. Tiga bulan sebelumnya, data milik 279 juta warga Indonesia yang dikumpulkan bertahun-tahun oleh Badan Pengelola Jaminan Sosial Kesehatan juga bocor. Data itu diperjualbelikan di raidforum.com dan sampai saat ini masih dalam penyelidikan. Jika angka ini benar, akan menjadi rekor baru kasus kebocoran data kesehatan terbesar di dunia. Namun kasus sebesar ini pun hanya berakhir dengan penutupan aplikasi layanan *E-Hac* tersebut. Hal mengejutkan adalah kini layanan tersebut kembali diaktifkan oleh kementrian kesehatan dengan menggandeng aplikasi wajib Peduli Lindungi.

Selama data pribadi para pengguna aplikasi dan pengakses media elektronik tersebut aman dan terlindungi, tidak menimbulkan masalah, akan tetapi bilamana si provider ataupun pihak ketiga lengah dalam perlindungan dan ada pihak lain yang berusaha mendapatkan kunci keamanan data pribadi, baru masalah menjadi besar. Pihak pengkases atau pengguna media elektronik yang tidak terhingga banyaknya seringkali dalam praktiknya hanya bisa pasrah bahwa data pribadinya telah bocor dan dicuri. Dalam berbagai kasus karena masyarakat pengguna disebutkan hanya minor, maka kedudukan yang lemah itu membuat pasrah dan walaupun ingin mengadu tidak terdapat kepastian jalur jelas untuk mengadukan kasusnya. Sementara pemerintah yang berusaha menyediakan kepastian perlindungan hukum dengan Undang-undang ingormasi dan transaksi elektronik (selanjutnya disingkat dengan sebutana UU ITE) pasal 26, tidaklah mampu menjerat para pencuri data dengan sanksi

pidana, dan bahkan untuk sanksi perdata tidak dapat memberikan perlindungan jelas bagi per individu yang mengadukan tanpa adanya bukti jelas bahwa data tersebut telah dicuri ataupun disalahgunakan. Terutama dalam hal data pribadi ini, sangat sering disalahgunakan untuk tindak pidana lanjutan berupa jual beli data, penawaran produk, pengancaman, penipuan kartu kredit (*carding*) hingga pinjaman online atas data tidak valid.

Data kesehatan merupakan data pribadi yang bersifat spesifik, sensitif, dan rahasia, yang harus dilindungi. Sedangkan di sisi lain Tindak Pencurian Data dan Kebocoran Data Dalam Aktivitas *Telemedicine* kerap terjadi. Jutaan data dan informasi kesehatan milik penduduk Indonesia sering mengalami kebocoran. Akhir Agustus 2021 lalu, sekitar 1,3 juta data pengguna aplikasi *Health Alert Card* (eHAC) buatan Kementerian Kesehatan Indonesia yang memuat data Covid-19 dibobol. Tindakan ini merupakan aksi *hack* pidana atas pencurian data. Belum diketahui siapa pelakunya. Tiga bulan sebelumnya, data milik 279 juta warga Indonesia yang dikumpulkan bertahun- tahun oleh Badan Pengelola Jaminan Sosial Kesehatan juga bocor. Data itu diperjualbelikan di raidforum.com dan sampai saat ini masih di dalam penyelidikan. Jika angka ini benar, akan menjadi rekor baru kasus kebocoran data kesehatan terbesar di dunia.

Dua kasus ini saja menandakan bahwa tingkat keamanan data di Indonesia sangat lemah. Data kesehatan merupakan data pribadi yang bersifat spesifik, sensitif, dan rahasia, yang harus dilindungi. Saat data kesehatan yang begitu kompleks didigitalkan dan dipindahkan melintasi batas-batas organisasi dan sistem kesehatan, maka kita dihadapkan pada pertanyaan besar tentang bagaimana tingkat keamanan dan kerahasiaan data kesehatan di Indonesia. Juga apa yang menjadi prioritas pemerintah dan kita untuk meningkatkan keamanannya.

Dalam situasi pandemi, *telemedicine* atau konsultasi *online* disarankan menjadi pilihan meski masyarakat masih bisa menjangkau fasilitas medis. Jadi bukan hanya mereka yang tinggal di daerah terpencil yang bisa memperoleh manfaat *telemedicine*, melainkan masyarakat secara umum. Dalam suatu perlindungan data pribadi dikenal prinsip-prinsip yakni pembatasan pengumpulan, kualitas data, spesifikasi tujuan, penggunaan pembatasan, langkah-langkah pengamanan, keterbukaan, partisipasi individu, serta pertanggungjawaban.

Di Indonesia belum ada regulasi mengenai perlindungan data pribadi dalam suatu peraturan perundang- undangan khusus. Perlindungan terhadap perlindungan data pribadi ini pada dasarnya telah bertumpu pada Pasal 28 G Ayat (1) Undang-undang Dasar Negara Republik Indonesia Tahun 1945, yakni menyatakan bahwa, "setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi." Di samping itu juga, terdapat beberapa peraturan perundang-

undangan yang di dalamnya tercermin mengenai perlindungan data pribadi secara umum.

METODE

Jenis penelitian hukum yang dilakukan secara yuridis normatif adalah yuridis normatif dimana hukum dikonsepkan sebagai apa yang tertulis dalam peraturan perundang-undangan (*law in books*) atau hukum dikonsepkan sebagai kaidah atau norma yang merupakan patokan berperilaku manusia yang dianggap pantas. Penelitian hukum normatif ini didasarkan kepada bahan hukum primer dan sekunder, yaitu penelitian yang mengacu kepada norma-norma yang terdapat dalam peraturan perundang-undangan. Penelitian ini mengkaji dan menguji data sekunder berupa hukum positif yang berkaitan dengan Perlindungan Data Pribadi di Indonesia dan perbandingan dengan Negara lain. Jenis metode penelitian yang dipilih adalah deskriptif analisis, adapun pengertian dari metode deskriptif analitis adalah suatu metode yang berfungsi untuk mendeskripsikan atau memberi gambaran terhadap objek yang diteliti melalui data atau sampel yang telah terkumpul sebagaimana adanya tanpa melakukan analisis dan membuat kesimpulan yang berlaku untuk umum. Penelitian Deskriptif merupakan sebuah metode penelitian yang berusaha menggambarkan dan menginterpretasi objek sesuai dengan apa adanya. Penelitian deskriptif disebut juga penelitian non eksperimen. Disebut penelitian non eksperimen, karena dalam penelitian deskriptif, peneliti tidak melakukan manipulasi variabel dan juga tidak melakukan kontrol terhadap variabel penelitian. Maka penelitian ini menggambarkan dan menganalisis ketentuan-ketentuan hukum, teori-teori hukum dan praktik pelaksanaan hukum positif yang berkaitan dengan perlindungan data pribadi serta kaitannya dengan Rancangan Undang-Undang Perlindungan Data Pribadi.

HASIL DAN PEMBAHASAN

A. Perlindungan Hukum Terhadap Data Pribadi di Internet Ketika Terjadi Pencurian Data Pada Aktivitas *Telemedicine* Indonesia Dikaitkan Dengan Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik Berdasarkan Asas Kepastian Hukum

Kasus kebocoran data bukanlah barang baru di Indonesia. Di tahun 2020, tercatat ada 7 insiden kebocoran data yang dialami pemerintah maupun perusahaan swasta, seperti *platform e- commerce.* Sementara sepanjang 2021 sendiri, terhitung sudah ada tiga kasus terkait dugaan kebocoran data masyarakat Indonesia. Meliputi kebocoran data 279 juta penduduk Indonesia diduga kuat identik dengan data milik Badan Penyelenggara Jaminan Sosial (BPJS) Kesehatan pada Mei lalu. Kemudian, disusul kebocoran data 2 juta nasabah BRI Life Syariah pada Juli 2021. Yang terbaru, adanya dugaan kebocoran data milik 1,3 juta pengguna aplikasi *Electronic Health Alert Card (e-HAC)* versi lama buatan Kementerian Kesehatan (Kemenkes). Meskipun belakangan,

pihak Kemenkes mengeklaim data-data pengguna aplikasi *e-HAC* versi lama itu tidak sampai bocor, serta tidak mengalir ke platform mitra *e-HAC*. Hanya pasrah Terkait maraknya insiden kebocoran data di Indonesia, Konsultan dan peneliti keamanan siber. Pada kenyataannya masyarakat tidak bisa melakukan hal apapun saat terjadi insiden kebocoran data. Dengan kata lain, masyarakat hanya bisa pasrah. Hal ini jelas diungkapkan oleh Pratama Persadha selaku Kepala Lembaga riset siber CISSReC bahwa masyarakat hanya bisa menjadi korban yang tidak berdaya, ketika data pribadi kita sudah diambil orang . Ia melanjutnya, karena pada prinsipnya, masyarakat telah menyetor data pribadinya ke instansi pemerintah atau Penyelenggara Sistem Elektronik (PSE). Termasuk PSE Lingkup Privat yang menggelar layanan digital atau online seperti Facebook, Google, Twitter, Gojek, Grab, Tokopedia, dan sebagainya. Masalahnya, keamanan data masyarakat Indonesia juga belum terjamin.

Pelanggaran data *e-HAC* adalah insiden keamanan siber besar keenam yang melanda Indonesia sejak Mei 2020. Ini termasuk kebocoran data Tokopedia, yang meretas informasi pribadi 15 juta pengguna Indonesia. Insiden keamanan siber di Komisi Pemilihan Umum Indonesia juga mengakibatkan data pemilu 2,3 juta warga negara Indonesia dijual di pasar web gelap *RaidForums*. Perlu dicatat bahwa Pasar semacam itu penuh dengan orang yang memperdagangkan data pasien dari aplikasi pelacakan COVID-19. Adapun setiap oknum dapat menyalahgunakan mereka [data] untuk peniruan identitas, *phishing*, rekayasa sosial, atau upaya pemerasan. Hal ini diasumsikan bahwa ini akan terjadi lebih banyak di masa depan. Miliaran pasien di seluruh dunia akan terpengaruh oleh kegiatan tersebut. Data pada aplikasi pengawasan COVID-19 kemungkinan berisi data GPS, informasi perangkat, dan file media telepon. Mayoritas pembobolan data di Indonesia memengaruhi data milik pemerintah, kata Alia Yofira Karunian, peneliti di Institut untuk Penelitian dan Advokasi Kebijakan atau ELSAM, kata dalam analisis *database e-HAC*. Pemerintah harus memberikan lebih banyak akuntabilitas, tambahnya. Oleh karena itu Pemerintah harus secepatnya membahas RUU Perlindungan Data Pribadi dengan DPR, saran ELSAM.

Pada saat disusunnya tulisan ini, di Indonesia ini belum ada undang-undang umum tentang perlindungan data. Namun, ada peraturan tertentu mengenai penggunaan data elektronik. Sumber utama pengelolaan informasi dan transaksi elektronik adalah Undang- Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (“UU ITE”) sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas UU ITE (“Perubahan UU ITE”), Peraturan Pemerintah No. 71 Tahun 2019 tentang Ketentuan Sistem dan Transaksi Elektronik ("Peraturan 71") dan Peraturan Pelaksanaannya, dan Peraturan Menteri Komunikasi & Informatika No. 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik ("Reg. Menkominfo 20/2016"). Namun, selama beberapa tahun, RUU baru tentang Perlindungan Data Pribadi Pribadi ("RUU") sedang dibahas

tetapi hingga saat ini belum diterbitkan. Meski tanggal pastinya masih belum pasti dan RUU tersebut masih dipertimbangkan oleh DPR, jika disahkan, ini akan menjadi undang- undang komprehensif pertama di Indonesia yang secara khusus menangani masalah privasi data. Selain ketentuan dalam UU ITE, Reg. 71 dan Menkominfo Reg. 20/2016, terdapat juga serangkaian peraturan yang juga mencakup ketentuan tertentu yang mungkin terkait dengan perlindungan data.

B. Perlindungan Hukum Terhadap Data Pengguna Akun Pribadi Dikaitkan Dengan Rancangan Undang- Undang Perlindungan Data Pribadi

Baru-baru ini, Pemerintah Indonesia semakin memperjelas cakupan perlindungan data pribadi dengan menerbitkan Peraturan Pemerintah Nomor 40 Tahun 2019 tentang Pelaksanaan Undang-Undang Nomor 23 Tahun 2006, sebagaimana telah diubah dengan Undang-Undang Nomor 24 Tahun 2013 tentang Administrasi Kependudukan ('PP 40'). PP 40 mulai berlaku pada 24 Mei 2019. Selain itu, kegiatan perdagangan dengan system elektronik diatur dalam Peraturan Pemerintah No. 80 Tahun 2019 tentang Perdagangan Melalui Sistem Elektronik ('PP 80'). Terakhir, pada Oktober 2019, Pemerintah mengeluarkan PP 71, yang mulai berlaku pada 10 Oktober 2019 dan, selain menegaskan kembali konsep perlindungan data pribadi yang ada yang dikemas dalam peraturan perlindungan data Indonesia saat ini, berisi beberapa tambahan yang sebelumnya tidak diakui pada ESP, kewajiban sehubungan dengan perlindungan data pribadi yang sebelumnya ditetapkan dalam PP 82.

Selain Peraturan PDP yang diuraikan di atas, Dewan Perwakilan Rakyat Indonesia ('DPR') sedang dalam proses membahas rancangan Undang-Undang Perlindungan Data Pribadi ('RUU PDP'). Pemberlakuan RUU PDP akan menghasilkan undang-undang komprehensif pertama di Indonesia yang secara khusus mengatur tentang perlindungan data pribadi, khususnya data dalam pengontrol privasi data pribadi. Sampai dengan April 2021, RUU PDP masih dalam pembahasan tahap I (dari 2 tahap pembahasan) oleh DPR dan kementerian terkait yang ditunjuk oleh Presiden. Hasil pembahasan dan pemeriksaan tersebut diharapkan selesai pada awal atau pertengahan tahun 2021, namun hingga saat ini progresnya masih stagnan.

Data pribadi di bidang kesehatan juga diatur dalam Peraturan Menteri Kesehatan No. 269/MENKES/PER/III/2008 tentang Rekam Medis yang mengatur kewajiban yang berkaitan dengan penyimpanan, penghapusan, dan kerahasiaan data. rekam medis. Sementara di bidang perbankan, data pribadi juga diatur dalam Peraturan Bank Indonesia No. 22/20/PBI/2020 tentang Perlindungan Konsumen Bank Indonesia (hanya tersedia dalam bahasa Indonesia di sini) yang mengatur tentang kewajiban bagi entitas perbankan atau non-perbankan. yang berada di bawah pengawasan Bank Indonesia untuk menjaga kerahasiaan dan keamanan data konsumennya (misalnya, persyaratan persetujuan konsumen sebelum mentransfer data pribadinya). Dengan kata lain, Acuan utama perlindungan data pribadi di Indonesia adalah Peraturan PDP,

hingga saat ini belum ada payung hukum yang jelas atau acuan terbaik yang khusus menaungi bidang perlindungan privasi data pribadi.

Terdapat beberapa hal yang menjadi sorotan dalam lingkup aplikasi yang dan dalam RUU PDP. Hal ini menjadi poin penting harus segera disahkannya RUU PDP. RUU PDP terutama berfokus pada informasi elektronik. Dengan demikian, ruang lingkup pribadi Peraturan PDP menjangkau relatif luas seperti yang ditunjukkan melalui definisi ESP di bawah Peraturan PDP, yang tampaknya bersifat generik. Yang dimaksud dengan ESP adalah setiap orang, penyelenggara negara, badan usaha, dan masyarakat yang menyediakan, mengelola, dan / atau mengoperasikan sistem elektronik, baik sendiri-sendiri maupun bersama- sama, bagi pengguna sistem elektronik untuk kepentingan pribadi dan/atau pihak lain. Sehubungan dengan itu, yang dimaksud dengan 'sistem elektronik' dalam PP 71 dan PP 20 adalah seperangkat alat dan prosedur elektronik yang berfungsi untuk menyiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mempublikasikan, mentransmisikan, dan/atau menyebarluaskan informasi elektronik. Dalam hal ini, interpretasi yang diterapkan oleh Kominfo adalah bahwa setiap orang atau badan yang menyimpan data secara elektronik akan dianggap sebagai ESP yang menggunakan sistem elektronik dan oleh karena itu tunduk pada Peraturan PDP.

Selanjutnya, PP 71 membedakan dua jenis ESP: ESP lingkup publik dan ESP lingkup pribadi. ESP lingkup publik adalah lembaga penyelenggara negara, yang didefinisikan dalam PP 71 sebagai legislatif, eksekutif, dan yudikatif di tingkat pusat dan daerah; dan instansi lain yang dibentuk berdasarkan peraturan perundang-undangan; dan lembaga yang ditunjuk oleh badan penyelenggara negara. Yang terakhir mengacu pada lembaga yang menyediakan sistem elektronik dengan ruang lingkup publik atas nama lembaga penyelenggara negara yang ditunjuk. Perlu dicatat bahwa Pasal 2(4) PP 71 mengecualikan ESP ruang lingkup publik yang merupakan otoritas pengatur dan pengawas di sektor keuangan. Sedangkan pengertian ESP lingkup privat meliputi penyediaan sistem elektronik oleh perorangan, badan usaha, dan masyarakat, yang meliputi: ESP diatur atau diawasi oleh kementerian atau lembaga berdasarkan peraturan perundang-undangan; dan ESP dengan portal, situs, atau aplikasi dalam suatu jaringan melalui internet yang digunakan untuk tujuan tertentu, seperti menyediakan, mengelola, dan/atau menyelenggarakan penawaran dan/atau perdagangan barang dan/atau jasa, termasuk ESP yang sistem elektroniknya digunakan dan /atau ditawarkan di Indonesia (Pasal 2(5)(b) PP 71).

Selanjutnya, PP 71 membedakan dua jenis ESP: ESP lingkup publik dan ESP lingkup pribadi. ESP lingkup publik adalah lembaga penyelenggara negara, yang didefinisikan dalam PP 71 sebagai legislatif, eksekutif, dan yudikatif di tingkat pusat dan daerah; dan instansi lain yang dibentuk berdasarkan peraturan perundang-undangan; dan lembaga yang ditunjuk oleh badan penyelenggara negara. Yang

terakhir mengacu pada lembaga yang menyediakan sistem elektronik dengan ruang lingkup publik atas nama lembaga penyelenggara negara yang ditunjuk. Perlu dicatat bahwa Pasal 2(4) PP 71 mengecualikan ESP ruang lingkup publik yang merupakan otoritas pengatur dan pengawas di sektor keuangan. Sedangkan pengertian ESP lingkup privat meliputi penyediaan sistem elektronik oleh perorangan, badan usaha, dan masyarakat, yang meliputi: ESP diatur atau diawasi oleh kementerian atau lembaga berdasarkan peraturan perundang-undangan; dan ESP dengan portal, situs, atau aplikasi dalam suatu jaringan melalui internet yang digunakan untuk tujuan tertentu, seperti menyediakan, mengelola, dan/atau menyelenggarakan penawaran dan/atau perdagangan barang dan/atau jasa, termasuk ESP yang sistem elektroniknya digunakan dan /atau ditawarkan di Indonesia (Pasal 2(5)(b) PP 71).

Ketentuan RUU PDP akan mengatur dan berlaku bagi orang perseorangan, badan hukum, badan usaha, lembaga pemerintah, badan publik, dan organisasi masyarakat sipil.

1. Lingkup Material Peraturan PDP berlaku Peraturan Kominfo 20 mengatur proses berikut:
   - akuisisi dan koleksi;
   - memproses dan menganalisis;
   - penyimpanan;
   - tampilan, publikasi, transmisi, diseminasi, dan/atau pembukaan akses;
   - penghancuran.

Di sisi lain, Pasal 56(4) PP 40 memberikan akses ke data pribadi untuk tujuan keamanan nasional dan penegakan hukum, dengan persetujuan dari Menteri Dalam Negeri. Ketentuan RUU PDP mengatur secara khusus mengenai data pribadi yang bersifat sensitif, yang terdiri dari data yang berkaitan dengan agama, kesehatan, kondisi fisik dan mental, kehidupan seksual, data keuangan pribadi, serta data pribadi lainnya yang dapat membahayakan membahayakan privasi subjek data. Namun DPR telah mengkonfirmasi bahwa data yang berkaitan dengan orientasi seksual dapat dihapus dari RUU PDP dan oleh karena itu tidak dapat diatur di dalamnya.

Lingkup aplikasi juga terdapat hal penting yang menjadi sorotan dalam lingkup aplikasi yang diubah dan diatur dalam RUU PDP. Hal ini menjadi poin sangat penting segera disahkannya RUU PDP. Adapun lingkup tersebut adalah otoritas perlindungan data, yakni Regulator utama untuk perlindungan data pribadi, dimana Regulator utama untuk perlindungan data pribadi Peraturan PDP berlaku Saat ini tidak ada otoritas perlindungan data umum, badan pengatur, atau organisasi yang secara khusus bertanggung jawab untuk melindungi informasi pribadi dan memastikan bahwa subjek hukum (misalnya, individu dan perusahaan) mematuhi undang-undang perlindungan data. Apalagi, di Indonesia belum ada database pusat arsip. Namun demikian, Kominfo diberi wewenang untuk menyelenggarakan urusan

pemerintahan di bidang komunikasi dan teknologi informasi, berdasarkan Peraturan Presiden Nomor 54 Tahun 2015 tentang Kementerian Komunikasi dan Informatika dan Peraturan Kominfo Nomor 6 Tahun 2018 tentang Organisasi dan Tata Kerja Kementerian Komunikasi dan Informatika. Selanjutnya, berdasarkan Pasal 85 Undang-Undang Kependudukan, data pribadi warga negara harus dipelihara secara akurat dan dilindungi oleh administrator dan badan eksekutif.

RUU PDP memang memberikan otoritas perlindungan data yang akan memiliki kewenangan untuk memastikan bahwa pelaksanaan data pribadi sesuai dengan ketentuan dalam RUU PDP. Dalam hal ini, otoritas perlindungan data adalah Komisi Informasi Pusat berdasarkan Undang- Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik.

Pemerintah dibebani tugas pengawasan, advokasi, evaluasi, penegakan, dan tindakan lain yang diperlukan untuk memastikan perlindungan data pribadi. Lebih lanjut, baik UU Informasi Elektronik maupun PP71 memuat ketentuan yang mewajibkan Pemerintah untuk melindungi kepentingan publik di bidang komunikasi elektronik. Secara khusus, Pemerintah diberikan kewenangan antara lain untuk menetapkan strategi keamanan siber nasional dan mengatur standar keamanan informasi. Selanjutnya Kominfo berwenang antara lain merumuskan dan melaksanakan kebijakan serta bimbingan teknis dan pengawasan di bidang komunikasi dan teknologi informasi. Adapun pengurus dan badan pelaksana sebagaimana dimaksud dalam Undang-Undang Kependudukan, Pasal 1(6) dan (7) Undang-Undang Kependudukan mengatur bahwa badan penyelenggara terdiri dari pemerintah pusat, pemerintah provinsi, dan pemerintah kabupaten atau kota yang bertanggung jawab atas dan berwenang menyelenggarakan urusan pemerintahan kependudukan, sedangkan badan pelaksana terdiri atas perangkat pemerintah kabupaten/kota yang bertanggung jawab dan berwenang menyelenggarakan pelayanan yang berkaitan dengan urusan administrasi kependudukan.

RUU PDP memang memberikan otoritas perlindungan data yang akan memiliki kewenangan untuk memastikan bahwa pelaksanaan data pribadi sesuai dengan ketentuan dalam RUU PDP. Dalam hal ini, otoritas perlindungan data adalah Komisi Informasi Pusat berdasarkan Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik.

KESIMPULAN

Telemedicine mempunyai beberapa keunggulan, seperti efektif memangkas alur birokrasi serta menjamin hak warga negara untuk memperoleh pelayanan kesehatan yang cepat dan akurat, namun kebocoran data/ informasi menjadi efek samping negatif. Pembiaran terhadapnya akan mengancam keberlanjutan *Telemedicine* itu sendiri. Dalam konteks perlindungan privasi atas data pribadi pasien belum sepenuhnya terjamin karena belum pahamnya masyarakat Indonesia akan haknya dan

belum merata pemahaman baik pihak pemerintah akan pentingnya perlindungan data pribadi pasien sehingga diperlukan pengaturan yang khusus tentang perlindungan data pribadi pasien dalam program *telehealth* walaupun telah diatur di dalam beberapa undang-undang, Peraturan Pemerintah, maupun Peraturan Menteri menyatakan Setiap orang yang menyebarluaskan data pribadi tanpa hak atau tidak sesuai dengan ketentuan dalam peraturan perundang-undangan dikenai sanksi administratif sesuai dengan ketentuan peraturan perundang-undangan meliputi peringatan lisan, peringatan tertulis, penghentian sementara kegiatan, pengumuman di situs alam jaringan. Korban kebocoran data pribadi yang mengalami kerugian ataupun dirugikan karena data pribadinya dipergunakan tanpa persetujuan dapat mengajukan gugatan ganti rugi ke pengadilan yang berwenang.

Upaya perlindungan data pribadi yang bersifat elektronik oleh penegak hukum hingga saat ini masih minim dan tidak efektif, lahirnya Undang-Undang informasi dan transaksi elektronik bertujuan untuk meminimalisir kejahatan baru dan perlindungan hukum yang dilakukan dengan sarana pemanfaatan teknologi pada sistem elektronik. Perlindungan atas data elektronik hanya sebatas pada adanya illegal akses dan gangguan data (data interference) dalam memberikan perlindungan terhadap sistem keamanan, tidak termasuk data yang bersifat khusus yang ada dalam sistem elektronik. Di samping itu menurut penulis dalam hal ini justru terkendala juga pada beberapa pasal yang kurang menjangkau dan tidak adanya aturan yang jelas atas perlindungan data pribadi pada Undang- Undang ITE. Padahal tujuan dari pembentukan Undang-Undang ITE untuk memberikan jaminan perlindungan atas informasi/data elektronik, kepastian hukum dan keadilan di masyarakat atas dampak perbuatan pelanggaran yang merugikan masyarakat. Hal ini terlihat jelas dari penerapan prinsip perlindungan data pribadi dalam kasus BPJS, *e-HAC*, bahkan Peduli Lindungi yang belum sepenuhnya diterapkan. Faktor penyebab kurang efektifnya penerapan prinsip perlindungan data pribadi pada kasus *telemedicine* di Indonesia adalah belum adanya peraturan perlindungan data pribadi yang komprehensif di Indonesia sehingga Kominfo saat ini merangkap sebagai pengontrol data pribadi sekaligus pengawas data pribadi. Tanpa adanya regulasi yang komprehensif dan terjadinya peran ganda oleh Kominfo, penegakan prinsip perlindungan data pribadi di Indonesia belum dapat berjalan secara maksimal.

Penulis melihat terdapat 2 (dua) hal besar yang dapat dilakukan Pemerintah untuk mengantisipasi dampak berkelanjutan, khususnya terhadap kerahasiaan data pribadi pasien. Pertama, pemerintah perlu mendorong percepatan pengesahan Rancangan Undang- Undang (RUU) Perlindungan Data Pribadi Tahun 2020. Kedua, Kementerian Kesehatan Republik Indonesia selaku leading sektor, perlu membangun suatu mekanisme pencegahan dan instrument pengawasan yang masif. Upaya ini, jika perlu dapat melibatkan kontribusi dan koordinasi lintas lembaga seperti Kementerian

Komunikasi dan Informatika Republik Indonesia, serta Komisi Informasi Pusat Republik Indonesia dan bahkan Kementrian Kesehatan Indonesia.

DAFTAR PUSTAKA

Al, Wisnubroto. *Konsep Hukum Pidana Telematika*. Cetakan Pertama. Yogyakarta: Universitas Atma Jaya, 2011.

Amiruddin & Zainal Asikin. *Pengantar Metode Penelitian Hukum*. Jakarta: Raja Grafindo Persada, 2012.

Aulia, M. Zulfa. "Hukum Pembangunan dari Mochtar Kusuma-atmadja: Mengarahkan Pembangunan atau Mengabdi pada Pembangunan?." *Undang: Jurnal Hukum* 1, no. 2 (2018): 363-392.

Barda Nawawi Arief. *Bunga Rampai Kebijakan Hukum Pidana*. Jakarta: Kencana, 2016.

Barda Nawawi Arief. *Perkembangan Sistem Pemidanaan Di Indonesia*. Semarang: Pustaka Magister, 2015.

Beyleveld, Deryck, et.al. *Law as A Moral Judgment*. London: Sweet & Maxwell, 2019.

Bradford, Laura, Mateo Aboy, and Kathleen Liddell. "COVID-19 contact tracing apps: a stress test for privacy, the GDPR, and data protection regimes." *Journal of Law and the Biosciences* 7, no. 1 (2020): lsaa034.

Budhijanto, D. 2019. *Cyber Law dan Revolusi Industri 4.0*. Bandung: Logoz Publishing, 2019

Butarbutar, Russel. "Initiating new regulations on personal data protection: Challenges for personal data protection in indonesia." *3rd International Conference on Law and Governance (ICLAVE 2019)*. Atlantis Press, 2020.

Danrivanto Budhijanto. *Cyber Law Dan Revolusi Industri 4.0*. Bandung: Logoz Publishing, 2019.

Dewi, Sinta. "Privasi atas Data Pribadi: Perlindungan Hukum dan Bentuk Pengaturan di Indonesia." *Jurnal De Jure* 15, no. .2 (2015): 23.

Hoofnagle, Chris Jay, Bart Van Der Sloot, and Frederik Zuiderveen Borgesius. "The European Union general data protection regulation: what it is and what it means." *Information & Communications Technology Law* 28, no. 1 (2019): 65-98.

James Adams and Richard Kletter. *Artificial Intelligence: Confronting The Revolution*. California: Endeavour Media Ltd, 2018.

Jang-Jaccard, Julian, and Surya Nepal. "A survey of emerging threats in cybersecurity." *Journal of computer and system sciences* 80, no. 5 (2014): 973-993.

Karo, Rizky. *Penegakan Hukum Kejahatan Dunia Maya (Cybercrime) Melalui Hukum Pidana*. Tanggerang: Penerbit Fakultas Hukum Universitas Pelita Harapan, 2019.

Kementrian Pertahanan Indonesia, *Pedoman Pertahanan Siber*, tanpa cetakan, Kemenhan RI, Jakarta, 2014.

Kletter, J. A. and R. *Artificial Intelligence: Confronting The Revolution*. California: Endeavour Media Ltd, 2018.

Kwarto, Febrian, and Madya Angsito. "Pengaruh Cyber Crime Terhadap Cyber Security Compliance Di Sektor Keuangan." *Jurnal Akuntansi Bisnis* 11, no. 2 (2018).

Mewengkang, Marchellino Christian Nathaniel. "Penerapan Asas Kekhususan Sistematis Sebagai Limitasi Antara Hukum Pidana dan Hukum Pidana Administrasi." *LEX CRIMEN* 7, no. 8 (2018).

Ozeran, Larry, Anthony Solomonides, and Richard Schreiber. "Privacy versus convenience: a historical perspective, analysis of risks, and an informatics call to action." *Applied Clinical Informatics* 12, no. 02 (2021): 274-284.

Politou, Eugenia, et al. "Backups and the right to be forgotten in the GDPR: An uneasy relationship." *Computer Law & Security Review* 34, no. 6 (2018): 1247-1257.

Sidik, Jafar. "Penyelesaian Sengketa Kesehatan Melalui Alternatif Dispute Resolution dalam Perspektif Hukum Positif Indonesia." (2015).

Vickya, Alvansa, and Reshina Kusumadewi. "Kewajiban Data Controller dan Data Processor Dalam Data Breach Terkait Pelindungan Data Pribadi Berdasarkan Hukum Indonesia dan Hukum Singapura: Studi Kasus Data Breach Tokopedia." *Padjadjaran Law Review* 9, no. 1 (2021).