

Urgensi Realisasi Pengaturan *Data Protection Officer* (DPO) pada Sektor Kesehatan Ditinjau dari Hukum Pelindungan Data Pribadi

Muhammad Izzar Damargara¹, Muhammad Alhidayah², Muhammad Raihan Faiqy³, Jatnika Maulana⁴

Abstrak

Layanan kesehatan berbasis digital menjadi salah satu inovasi dalam perkembangan teknologi informasi saat ini yang semakin dilirik masyarakat sejak pandemi *covid-19* menerpa. Pada penggunaan layanan kesehatan berbasis digital ini membutuhkan data pribadi penggunanya, hal ini menjadi hal yang sensitif dan berpotensi menimbulkan permasalahan hukum sehingga diperlukan pengaturan terkait pelindungan data pribadi. Indonesia telah mengatur ketentuan pelindungan data pribadi pada sektor kesehatan melalui berbagai instrumen hukum. Namun, dalam implementasinya, jaminan atas keamanan data pribadi pengguna pada digitalisasi sektor kesehatan ini tidaklah terwujud. Hal ini dapat dilihat dengan terjadinya kasus kebocoran data pribadi peserta Badan Penyelenggara Jaminan Sosial Kesehatan (BPJS Kesehatan). Penelitian ini menggunakan metode penelitian hukum yuridis normatif. Berdasarkan hasil yang diperoleh, diperlukan pengaturan dan pengawasan yang ketat dalam instansi kesehatan, khususnya pada sektor digital. Realisasi peran *Data Protection Officer* di instansi layanan kesehatan menjadi jawaban terhadap permasalahan tersebut yang harus diwujudkan sebagai pelindungan data pribadi secara digital di sektor kesehatan.

Kata kunci: data pribadi, *data protection officer*, kebocoran data, sektor kesehatan publik

The Urgency of Realizing Data Protection Officer (DPO) Regulation in the Health Sector in Terms of Personal Data Protection Law

Abstract

Digital-based health service is one of the innovations in the current development of information technology which the public has increasingly looked at since the covid-19 pandemic hit. The use of digital-based health services requires users' personal data, which is a sensitive matter and has the potential to cause legal problems, so arrangements related to personal data protection are needed. Indonesia has regulated the provisions for personal data protection in the health sector through various legal instruments. However, in practice, the guarantee for personal data protection in the digital health sector has not been materialized. This is apparent in the case of personal data breach of participants from the Health Social Security Administering Agency (BPJS Kesehatan). This study uses a normative juridical legal research method. Based on the results obtained, strict regulation and supervision are needed in health agencies, particularly in the digital sector. The realization of the Data Protection Officer role in health service agencies is the answer to these problems which must be realized as digital personal data protection in the health sector.

Keywords: *personal data, data protection officer, digital service, data breach, public health sector.*

¹ Fakultas Hukum Universitas Padjadjaran, Jl. Raya Bandung Sumedang KM. 21, muhammad19201@mail.unpad.ac.id, Mahasiswa Strata 1.

² Fakultas Hukum Universitas Padjadjaran, Jl. Raya Bandung Sumedang KM. 21, muhammad19013@mail.unpad.ac.id, Mahasiswa Strata 1.

³ Fakultas Hukum Universitas Padjadjaran, Jl. Raya Bandung Sumedang KM. 21, muhammad19100@mail.unpad.ac.id, Mahasiswa Strata 1.

⁴ Fakultas Hukum Universitas Padjadjaran, Jl. Raya Bandung Sumedang KM. 21, jatnika19001@mail.unpad.ac.id, Mahasiswa Strata 1.

A. Pendahuluan

Peningkatan aktivitas sistem informasi dan keadaan teknologi saat ini telah mencerminkan konstelasi masyarakat dunia yang berorientasi kepada informasi.⁵ Terlebih dengan kehadiran era disrupsi telah mengubah gaya hidup dan cara kerja masyarakat yang semula dilakukan secara konvensional menjadi modern dengan menggunakan pendekatan digital. Bahkan masyarakat kini telah memasuki fase transisi meninggalkan era disrupsi revolusi industri 4.0 karena keberadaan revolusi industri 5.0 yang hadir lebih cepat dengan dipicu oleh teknologi telekomunikasi 5G serta masifnya platform digital.⁶ Sejalan dengan hal tersebut, apabila berkaca pada kondisi Indonesia berdasarkan data pada tahun 2021 dapat diketahui bahwasanya pengguna internet tercatat berjumlah 202,6 juta pengguna, yang mana angka tersebut mengalami peningkatan 11% dibanding tahun sebelumnya yang berjumlah 175,4 juta pengguna.⁷ Selain itu, kondisi pandemi *covid-19* juga telah menginspirasi banyak orang untuk beralih pada penggunaan teknologi digital.

Keadaan-keadaan demikian tentu memberikan dampak signifikan terhadap kemajuan inovasi dan efisiensi dalam transformasi digital. Salah satu inovasi yang hadir dalam perkembangan saat ini ialah layanan kesehatan berbasis digital seperti *electronic health (e-health)* yang semakin dilirik dan menjadi perhatian masyarakat

sejak pandemi *covid-19* menerpa. Pemanfaatan teknologi digital pada sektor layanan kesehatan dapat mendorong ketersediaan, kemampuan, kedayagunaan, serta mutu prosedur medis dengan mengikutsertakan *stakeholder* pelayanan medis terkait.⁸ Namun, menggunakan layanan kesehatan digital akan memerlukan informasi pribadi konsumen, yang menjadi persoalan rumit dan dapat mengakibatkan masalah hukum jika tidak diselenggarakan dengan baik. Dengan demikian, negara perlu hadir dalam mengikuti perkembangan teknologi di era digital dengan memberikan perlindungan terhadap data pribadi pengguna layanan kesehatan berbasis digital.

"Data is the new oil", istilah ini memberi gambaran betapa pentingnya data pada era digital saat ini sehingga perlu dilindungi sedemikian rupa. Hal serupa juga disampaikan oleh Presiden Joko Widodo yang menjelaskan bahwa data menjadi jenis kekayaan baru bagi bangsa sehingga Indonesia perlu mewujudkan kedaulatan data (*data sovereignty*).⁹ Sebagai negara hukum, Indonesia telah memberikan jaminan atas perlindungan data pribadi melalui konstitusi negara yaitu Undang-Undang Dasar Negara Republik Indonesia 1945. Hal tersebut sebagaimana dimuat dalam pasal 28G yang menentukan bahwa perlindungan diri pribadi dan rasa aman menjadi landasan konstitusional untuk perlindungan data pribadi sebagai bagian dari hak asasi.

⁵ Danrivanto Budhijanto, *Hukum Telekomunikasi, Penyiaran & Teknologi Informasi, Regulasi dan Konvergensi*, Bandung: PT. Refika Aditama, 2013, hlm 1.

⁶ Disampaikan oleh Prof. Dr. Ahmad M. Ramli, S.H., M.H., FCB., Arb. pada *Studium Generale* Dampak Transformasi Digital terhadap Pendidikan Tinggi Hukum dan Profesi Hukum 30 Agustus 2021.

⁷ Aptika Kominfo, "Warganet Meningkat, Indonesia Perlu Tingkatkan Nilai Budaya di Internet", <https://aptika.kominfo.go.id/2021/09/warganet-meningkat-indonesia-perlu-tingkatkan-nilai-budaya-di-internet/>, diunduh 10 Maret 2022.

⁸ Handryas Prasetyo Utomo, dkk, "Urgensi Perlindungan Hukum Data Pribadi Pasien dalam Pelayanan Kesehatan Berbasis Teknologi di Indonesia", *Jurnal Ilmiah Galuh Justisi*, Volume 8, Nomor 2, 2020, hlm. 173.

⁹ Danrivanto Budhijanto, "*Data as New Oil* dalam Konstruksi Hukum Ekonomi Digital di Indonesia", <https://www.hukumonline.com/berita/baca/lt5db1470b9d036/data-as-new-oil-dalam-konstruksi-hukum-ekonomi-digital-di-indonesia>, diunduh 10 Maret 2022.

Pada sektor kesehatan, data kesehatan termasuk data spesifik atau sensitif sehingga data pribadi pasien sebagai konsumen sangat perlu dilindungi karena berisi informasi yang sifatnya rahasia seperti hasil tes kesehatan, jenis penyakit yang diderita, keterangan tempat tinggal, nomor telepon, dan lainnya.¹⁰ Oleh karena itu, mengenai data-data tersebut dilindungi dengan adanya Undang-Undang Nomor 29 Tahun 2004 tentang Praktik Kedokteran ("UU Praktik Kedokteran"), Undang-Undang Nomor 36 Tahun 2009 tentang Kesehatan ("UU Kesehatan"), serta Undang-Undang Nomor 44 Tahun 2009 tentang Rumah Sakit ("UU Rumah Sakit"). Sementara itu, pada sektor digital, perlindungan atas data pribadi dimuat dalam ketentuan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik ("UU ITE").

Walaupun telah termaktub pada ketentuan undang-undang terkait, dalam implementasinya, jaminan atas perlindungan data pribadi pada sektor kesehatan secara digital ini tidaklah terwujud. Hal ini dapat dilihat dengan terjadinya kasus kebocoran data pribadi dari kepesertaan Badan Penyelenggara Jaminan Sosial ("BPJS") Kesehatan. *In casu* diyakini terdapat 279 juta catatan informasi pribadi peserta BPJS Kesehatan tersebar dan diperjualbelikan pada *Raid Forums*. Dedy Permadi sebagai perwakilan dari Kementerian Komunikasi dan Informatika mengungkapkan bahwa telah dilakukan pengkajian terhadap sampel data yang mengalami kebocoran tersebut dan telah terkonfirmasi informasi pribadi yang tersebar tersebut diduga berasal dari data

BPJS Kesehatan. Dedy juga menyebutkan bahwa klaim tersebut semakin meyakinkan setelah melihat berbagai informasi yang tersebar, termasuk nomor kartu peserta BPJS, kode kantor BPJS, informasi keluarga, tanggungan yang ditanggung oleh asuransi kesehatan, dan status pembayaran.¹¹ Keadaan demikian menggambarkan bahwa ketentuan instrumen hukum yang ada saat ini belum dapat memberikan jaminan atas perlindungan data pribadi pada sektor kesehatan secara digital. Oleh karena itu, diperlukan suatu upaya inovasi sebagai strategi perlindungan data pribadi di era digital khususnya pada sektor kesehatan.

Hal tersebut menandakan urgensi dibuatnya tulisan ini yang akan mengulas lebih lanjut mengenai perlindungan data pribadi pada sektor kesehatan secara digital. Tulisan ini akan membahas problematika perlindungan data pribadi pada sektor kesehatan, dasar hukum perlindungan data pribadi di sektor kesehatan, penerapan peran *data protection officer* pada instansi layanan kesehatan, serta urgensi realisasi pengaturan *data protection officer* sebagai strategi perlindungan data pribadi secara digital pada sektor kesehatan.

B. Metode Penelitian

Penelitian ini disusun dalam bentuk penelitian deskriptif dengan metode yuridis normatif. Dimana penelitian hukum dilakukan dengan cara meneliti bahan pustaka atau data sekunder.¹² Penggunaan data sekunder tersebut meliputi bahan hukum primer, bahan hukum sekunder dan bahan hukum

¹⁰ Aulia Naslah Mahira, "Perlindungan Hukum terhadap Kerahasiaan Data Kesehatan Pasien berdasarkan Undang-Undang Nomor 36 Tahun 2009 tentang Kesehatan", *Dinamika Jurnal Ilmiah Ilmu Hukum*, Volume 27, Nomor 10, 2021, hlm. 1502.

¹¹ CNN Indonesia, "Kebocoran Data Pribadi, BPJS Kesehatan Bakal Digugat", <https://www.cnnindonesia.com/teknologi/20210606200515-185-650991/kebocoran-data-pribadi-bpjs-kesehatan-bakal-digugat>, diunduh 10 Maret 2022.

¹² Soerjono Soekanto, *Penelitian Hukum Normatif: Suatu Tinjauan Singkat*, Jakarta: PT RajaGrafindo Persada, 2009, hlm. 13.

tersier. Bahan hukum primer yang digunakan adalah peraturan perundang-undangan. Bahan hukum sekunder yang digunakan adalah buku, jurnal, dan hasil-hasil penelitian. Lalu, bahan hukum tersier yang digunakan adalah surat kabar dan artikel internet.

C. Pembahasan dan Analisis

1. Peran Platform Digital pada Sektor Kesehatan

Pandemi *covid-19* yang berawal dua tahun lalu telah mengubah tatanan kehidupan secara umum dan secara khusus telah menyebabkan pergeseran kebiasaan masyarakat dalam pelayanan kesehatan. Perhimpunan Rumah Sakit di Indonesia ("PERSI") menyebutkan bahwa setelah terjadinya pandemi *covid-19*, penurunan pendapatan rumah sakit mencapai 40% dari rata-rata pendapatan bulanan.¹³ Hal ini dikarenakan adanya himbauan untuk tidak berkunjung ke rumah sakit, pasien yang ragu untuk mendatangi rumah sakit, pembatasan jumlah pasien rumah sakit, serta jumlah praktik dokter yang berkurang. Solusinya, masyarakat menjadi lebih terbuka terhadap konsultasi kesehatan melalui platform berbasis elektronik. Dalam hal ini, penggunaan layanan aplikasi *telemedicine* mengalami kenaikan hingga 600%.¹⁴ Berbagai pilihan layanan *telemedicine* yang disediakan terdiri dari konsultasi dokter, pemesanan

janji temu dengan dokter, hingga transaksi pembelian obat-obatan secara online.¹⁵

Awal perkembangan platform layanan *telemedicine* atau layanan kesehatan digital di era pandemi *covid-19* didukung oleh Keputusan Menteri Nomor HK.01.07/MENKES/4829/2021 tentang Pedoman Pelayanan Kesehatan Melalui Telemedicine Pada Masa Pandemi *Corona Virus Disease* 2019 (COVID-19) ("Kepmenkes 4829/2021"), dewasa ini telah berperan sebagai landasan hukum beroperasinya platform *telemedicine* yang bisa ditunjukkan untuk pengidap *covid-19* yang melakukan isolasi mandiri. Secara garis besar, Kepmenkes 4829/2021 memberikan seperangkat pedoman komprehensif yang digunakan sebagai acuan oleh Pemerintah Indonesia, serta tenaga medis, fasilitas penyedia layanan berbasis kesehatan, penyedia layanan platform kesehatan digital dan *stakeholder* terkait sehubungan dengan penyediaan layanan berbasis kesehatan melalui platform kesehatan digital selama era pandemi *covid-19*. Berdasarkan diktum ketiga Kepmenkes 4829/2021, *telemedicine* sebagai platform digital pada sektor kesehatan sendiri pada pokoknya dapat dimaknai sebagai layanan yang ada pada bidang kesehatan secara *online* yang melibatkan sarana teknologi informasi dan komunikasi dalam penyediaan informasi kesehatan meliputi pengobatan, diagnosis, penilaian kondisi kesehatan pasien, pencegahan perburukan dan/atau layanan di sektor farmasi, meliputi pula *monitoring* kondisi pengidap *covid-19* yang sedang

¹³ Daniel Budi Wibowo, "Optimisme Rumah Sakit di Masa Pandemi Covid-19", https://persi.or.id/wp-content/uploads/2020/05/materi_drdanielbw.pdf, diunduh 4 Juli 2022

¹⁴ Fahmi Ahmad Burhan, "Kunjungan ke Aplikasi Alodokter & Halodoc Naik 600% Efek Virus Corona", <https://katadata.co.id/desysetyowati/digital/5e9a421548005/kunjungan-ke-aplikasi-alodokter-halodoc-naik-600-efek-virus-corona>, diunduh 4 Juli 2022

¹⁵ EuroCham, "Position Paper: Pharmaceutical & Medical Technology", <http://www.eurocham.id/publications>, diunduh 4 Juli 2022

melaksanakan isolasi mandiri. Layanan *telemedicine* harus dilaksanakan oleh tenaga medis melalui fasilitas penyedia layanan kesehatan sebagaimana kemampuan serta kewenangan mereka, dengan melihat mutu layanan serta kondisi kesehatan pasien pengguna layanan *telemedicine*.

Kehadiran platform digital pada sektor kesehatan ini turut mendukung penyediaan layanan kesehatan yang lebih baik dan lebih efektif. Ketua Ikatan Dokter Indonesia (“IDI Bogor”) mengemukakan bahwa transformasi digital pada sektor kesehatan memberikan manfaat, yakni semakin mudahnya masyarakat dalam menjangkau pelayanan, efektivitas sumber daya manusia, mendorong peningkatan mutu layanan, dan dapat menekan biaya pada layanan kesehatan.¹⁶ Melihat peran dan perkembangan platform digital tersebut, Kementerian Kesehatan melalui Peraturan Menteri Kesehatan Republik Indonesia Nomor 21 Tahun 2020 tentang Rencana Strategis Kementerian Kesehatan Tahun 2020-2024 menginginkan adanya transformasi digital pada layanan kesehatan. Upaya tersebut dilakukan melalui pengintegrasian sistem informasi, penelitian, serta peningkatan kesehatan. Sistem Kesehatan Nasional Berbasis Individu sebagai Rekam Medis dan Kesehatan Elektronik Terpadu sedang dikembangkan sebagai hasil dari transformasi digital yang terjadi di industri perawatan kesehatan. Pengintegrasian layanan platform kesehatan tersebut nantinya akan menitikberatkan pada berbagai layanan seperti tanggap darurat kesehatan, layanan primer, farmasi dan alat kesehatan, pelayanan kesehatan

rujukan, pendanaan kesehatan, vaksinasi *covid-19*, serta tata kelola internal dan infrastruktur Kementerian Kesehatan.¹⁷ Akan tetapi, untuk mewujudkan peran platform digital yang baik pada sektor kesehatan ini perlu memperhatikan beberapa hal, salah satunya ialah terkait aspek keamanan yang dapat menjamin perlindungan data pribadi pengguna layanan tersebut.

2. Problematika Pelindungan Data Pribadi pada Sektor Kesehatan

Di Indonesia, pelindungan hukum dinilai masih belum optimal terkait dengan data pribadi. Pada persoalan penyalahgunaan data pribadi misalnya yang masih marak terjadi tanpa diketahui oleh pemiliknya. Problematika penyalahgunaan data pribadi ini akan memunculkan adanya pelanggaran privasi yang dapat saja terjadi pada seseorang. Dari hal tersebut menunjukkan adanya celah pengawasan dan kelemahan sistem yang memungkinkan terjadinya penyalahgunaan informasi data pribadi dan dapat merugikan pemilik data. Hal ini terlihat pada persoalan kebocoran data pasien BPJS Kesehatan yang mana menurut juru bicara Kementerian Kominfo, Dedy Permadi mengatakan adanya dugaan kebocoran 279 juta data milik BPJS Kesehatan yang juga diperjualbelikan pada sebuah forum.

Timboel Siregar selaku Koordinator Bidang Advokasi BPJS Watch menjelaskan bahwa terdapat dua dugaan penyebab kebocoran data pada kasus BPJS Kesehatan. Pertama, kebocoran data disebabkan oleh peretasan di aplikasi pihak ketiga. Berdasarkan hasil analisisnya, banyaknya aplikasi yang dimiliki oleh BPJS Kesehatan yang diantaranya terdiri atas

¹⁶ Aptika Kominfo, “Digitalisasi Pelayanan Kesehatan dengan Penerapan Revolusi Industri”, <https://aptika.kominfo.go.id/2019/04/digitalisasi-pelayanan-kesehatan-dengan-penerapan-revolusi-industri-4-0/>, diunduh 4 Juli 2022.

¹⁷ Kementerian Kesehatan Republik Indonesia, *Cetak Biru Strategi Transformasi Digital Kesehatan 2024*, Jakarta: Kementerian Kesehatan Republik Indonesia, 2021, hlm. 28-33.

delapan aplikasi pada sistem informasi manajemen penjaminan pelayanan kesehatan, enam aplikasi pada sistem informasi layanan publik, dan enam aplikasi untuk mendukung sistem informasi manajemen kepesertaan. Meninjau banyaknya aplikasi yang dimiliki BPJS Kesehatan, ia menduga kebocoran yang disebabkan oleh peretasan khususnya pada aplikasi sistem informasi manajemen kepesertaan dan juga pada aplikasi pelayanan kesehatan. Kemudian dugaan yang kedua yaitu terdapat kebocoran data yang dilakukan oleh pihak internal. Timboel menimbang peretasan tersebut membuktikan rendahnya pengamanan pada aplikasi BPJS Kesehatan.¹⁸ Beberapa kerangka dan standar pengoperasian IT diterapkan guna melindungi keamanan aplikasi tidak bisa dipastikan oleh instansi pemerintah. Dengan itu, instansi perlu menyederhanakan jumlah aplikasi di BPJS Kesehatan dan pengamanan data yang ketat agar dapat efektif dan efisien dalam menjamin kerahasiaan data pribadi dan data kesehatan masyarakat.

Pada kasus kebocoran data BPJS Kesehatan diatas menjadi bukti data pribadi pasien pada sektor kesehatan tidak terlepas dari kemungkinan penyalahgunaan. Data pribadi pasien terdapat pertalian antara pasien dan juga penyelenggara jasa layanan kesehatan yang tidak terpaku pada informasi ketika proses registrasi saja, namun termasuk juga data-data lainnya. Dewasa ini di Indonesia telah banyak digunakannya bantuan teknologi oleh penyelenggara jasa pelayanan kesehatan dalam pengolahan informasi data pasien sehingga menjadi secara digital.¹⁹ Dengan demikian, hal ini

menjadi perhatian serius untuk memberikan perlindungan hukum terhadap data pribadi dan data kesehatan dimana data tersebut tidak boleh diterbitkan atau diumumkan pada khalayak umum kecuali jika undang-undang memberikan kewenangan tersebut, sebab jika kerahasiaan data pasien dibuka atau diumumkan ke masyarakat umum tentunya hal tersebut telah jelas melanggar pada ketentuan undang-undang.

Pengaturan terkait dengan perlindungan data pribadi dimana pengaturannya terpisah dalam berbagai instrumen hukum di Indonesia membuat pengaturan ini menjadi lemah dan sifatnya umum dalam menggambarkan aturan perlindungan data pribadi ini.²⁰ Pada UU ITE misalnya, pengaturan perlindungan data pribadi belum mencakup aturan perlindungan data pribadi yang jelas dan juga lengkap, yang mana pada aturan ini tidak menguraikan berbagai pokok masalah yang banyak diperbincangkan perihal perlindungan data pribadi. Pada ketentuan UU ITE ini tidak terdapat jaminan terhadap perlindungan data pribadi pada sektor kesehatan seperti yang sedang dibahas dalam tulisan ini, dimana ketentuan-ketentuan yang telah ada masih belum mengakomodir hal tersebut. Ketentuan peraturan-peraturan yang telah ada juga masih menjadi problematika terlebih lagi saat ini tidak ada undang-undang di Indonesia yang secara eksklusif memberikan pengaturan perlindungan data pribadi dengan jelas, tegas dan juga komprehensif.

Data pribadi pada sektor kesehatan yang bersifat rahasia dan privasi ini terdiri atas identitas pribadi pasien, seperti nama, nomor telepon, alamat, dan lain-lain. Selain itu juga terkait rahasia medis yang

¹⁸ Arie Dwi Budiati, "Dua Dugaan Penyebab Kebocoran 279 Juta Data Pribadi Diklaim Peserta BPJS" <https://www.dream.co.id/dinar/2-hal-ini-diduga-jadi-biang-kerok-kebocoran-data-penduduk-210524f.html>, diunduh 13 Maret 2022.

¹⁹ Handryas Prasetyo Utomo, dkk. *Op.cit.*, hlm. 177.

²⁰ Lia Sautunnida, "Urgensi Undang-Undang Perlindungan Data Pribadi di Indonesia: Studi Perbandingan Hukum Inggris dan Malaysia", *Kanun Jurnal Ilmu Hukum*, Volume 20, Nomor 2, 2018, hlm. 380.

menjadi hasil pemeriksaan pada pasien tersebut. Dengan begitu, pasien memiliki hak dalam memperoleh jaminan privasi serta kerahasiaan penyakit yang dialami pasien termasuk juga informasi medisnya sehingga kerahasiaan pasien menjadi penting. Termasuk dalam pelayanan kesehatan berbasis digital seperti halnya dalam pengumpulan data pribadi pasien yang sifatnya sensitif tentu perlu adanya perlindungan sampai seberapa jauh penyelenggara jasa kesehatan bisa memproteksi data pribadi pasien pada *e-health*. Dengan begitu, perlu adanya pengaturan yang dapat mengakomodir hal tersebut serta pengawasan yang memadai sebagai jaminan perlindungan data pribadi pada sektor kesehatan.

3. Dasar Hukum Pelindungan Data Pribadi di Sektor Kesehatan

"Medical record ten times more valuable to hackers than credit card information". Berharganya suatu data pribadi di sektor kesehatan terletak pada bagaimana lengkapnya suatu data yang terdapat di dalamnya karena pada umumnya data pribadi yang dikendalikan oleh penyelenggara pelayanan kesehatan memuat identitas pasien, data keuangan, serta rekam medis pasien.²¹ Pentingnya data pribadi di sektor kesehatan ini perlu mendapatkan suatu proteksi yang optimal berdasarkan instrumen hukum yang berlaku di Indonesia. Sehubungan dengan data pribadi di sektor kesehatan, disebutkan pada pasal 57 UU Kesehatan menegaskan pada intinya bahwa pasien memiliki hak atas kerahasiaan keadaan kesehatan pribadi masing-masing yang sudah diberikan kepada penyedia fasilitas layanan kesehatan kecuali ditentukan lain secara limitatif sebagaimana kondisi serta pihak-pihak yang termuat dalam pasal

tersebut.²² Selain itu, pasal 47 Ayat (2) UU Praktik Kedokteran pada pokoknya mewajibkan dokter dan para pemimpin fasilitas pelayanan kesehatan untuk memberikan proteksi sifat rahasia dari hasil rekam medis setiap orang yang di dalamnya terdapat sejumlah dokumen serta catatan mengenai informasi kesehatan apapun yang ditunjukkan kepada pasien. Selanjutnya, pada pasal 40 Ayat (3) UU ITE jo. pasal 99 Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik ("PP PSTE"), institusi di sektor kesehatan dikategorikan sebagai pemegang data pribadi strategis yang wajib dilindungi. Dalam konteks perlindungan data pribadi pada sektor kesehatan di era digital, dalam pasal 26 UU ITE termuat bahwa pemanfaatan seluruh data pribadi serta informasi elektronik berkenaan dengan data pribadi tiap individu di Indonesia wajib dilaksanakan berdasarkan consent orang tersebut atau mengacu pada landasan hukum positif sebagai bentuk *lawful data processing*.²³

Mengacu pada pengaturan di atas, dapat dipahami bahwa hukum positif di Indonesia telah menegaskan kewajiban pihak yang menyediakan sarana layanan kesehatan untuk melindungi data kesehatan milik pasien. Akan tetapi, sejumlah kasus kebocoran data di Indonesia seperti yang dialami oleh BPJS Kesehatan menjadi bukti lemahnya perlindungan data pribadi pada sektor kesehatan di Indonesia. Dengan demikian, sudah semestinya optimalisasi perlindungan data pribadi pada sektor kesehatan menjadi prioritas bersama untuk menyelesaikan permasalahan seputar data dan informasi kesehatan.

²¹ Pusat Studi Forensika Digital UII, "Data Kesehatan", <https://forensics.uii.ac.id/data-kesehatan/>, diunduh 17 Maret 2022.

²² Aulia Naslah Mahira, *Op.cit.*, hlm. 1504-1505.

²³ Handryas Prasetyo Utomo, dkk, *Op.cit.*, hlm. 179.

4. Data Protection Officer dalam Pengaturan General Data Protection Regulation

General Data Protection Regulation ("GDPR") ialah instrumen pengaturan hukum berkenaan dengan perlindungan data pribadi yang dibuat oleh negara-negara anggota dari Uni Eropa. Instrumen ini dijadikan referensi oleh komunitas internasional dalam mengatur hukum nasional mereka. Berdasarkan GDPR, organisasi tertentu diharuskan untuk menunjuk *Data Protection Officer* ("DPO") sebagai cara untuk memfasilitasi kepatuhan mereka terhadap aturan dalam GDPR.

GDPR dalam hal ini memperkenalkan konsep DPO dalam 3 pasal pada Bagian 4 GDPR, yaitu pasal 37, pasal 38, serta pasal 39.

a. Pasal 37 - Designation of the DPO (Penunjukan DPO)

Berkaitan dengan penunjukan DPO, pasal 37 ayat (1) GDPR mengatur kewajiban penunjukan DPO dan menetapkan jenis organisasi seperti apa yang tunduk pada kewajiban tersebut. Dalam hal ini, kewajiban penunjukan DPO tersebut tidak berlaku secara langsung, namun hanya organisasi tertentu yang termasuk dalam kriteria yang sudah ditetapkan oleh pasal 37 ayat (1) yang wajib untuk menunjuk DPO. Organisasi yang memenuhi salah satu dari kriteria berikut tunduk pada kewajiban penunjukan DPO:

- 1) dimana otoritas atau badan publik yang melakukan pemrosesan data (hal ini tidak termasuk pengadilan yang bertindak dalam kapasitasnya);
- 2) dimana kegiatan inti terdiri dari operasi pemrosesan data yang, berdasarkan sifat, ruang lingkup dan/atau tujuannya,

membutuhkan peninjauan subjek data yang teratur dan sistematis dalam skala besar; atau

- 3) dimana kegiatan inti tersebut meliputi pemrosesan kategori data khusus dalam skala besar dan data pribadi yang berkaitan dengan tindak pidana.

Melihat ketentuan diatas, terdapat beberapa terminologi yang digunakan seperti Kegiatan Inti (*Core Activities*) dan Kategori Data Khusus (*Special Categories of Data*). Untuk mengetahui maksud dari terminologi yang digunakan tersebut, kita dapat melihat ketentuan dari GDPR dan penjelasan dalam *Guidelines on Data Protection Officers* oleh *Data Protection Working Party*.

Di mana dinyatakan bahwa *core activities* "....tidak boleh (i) mengecualikan pemrosesan informasi pribadi yang terkait erat dengan tujuan utama organisasi...."²⁴ Contohnya, suatu layanan kesehatan perlu mengolah data kesehatan agar dapat mencapai tujuan utama dalam memberikan pelayanan kesehatan. Karena pemrosesan data tersebut penting bagi layanan kesehatan tersebut, maka kegiatan pengolahan data kesehatan harus dianggap sebagai salah satu kegiatan inti layanan kesehatan, yang berarti layanan kesehatan tersebut tunduk pada aturan penunjukan DPO.²⁵ Sedangkan, *special categories of data* merupakan data pribadi yang berkaitan dengan kesehatan, asal ras atau etnis, pendapat politik, kepercayaan, ideologi, keanggotaan serikat pekerja, dan kategori data khusus lainnya.²⁶

²⁴ Pasal 29 Data Protection Working Party, *Guidelines on Data Protection Officers*, 16/EN WP 243, diadopsi pada 13 Desember 2016, hlm. 6-7.

²⁵ M. Iqsan Sirie, "The Mandatory Designation of a Data Protection Officer in Indonesia's Upcoming Personal Data Protection Law", *Padjadjaran Journal of Law*, Volume 5, Nomor 1, 2018, hlm. 29.

²⁶ Pasal 9 General Data Protection Regulation.

b. Pasal 38 - *Position of the DPO* (Posisi DPO)

Berkenaan dengan posisi DPO dalam organisasi, hal ini diatur dalam pasal 38 GDPR. Posisi yang dimaksud disini tidak serta merta berarti posisi DPO dalam struktur perusahaan dari sebuah organisasi, namun berkaitan dengan keterlibatan DPO dalam aktivitas pemrosesan data organisasi.²⁷ Pengendali dan prosesor wajib memastikan DPO untuk terlibat dengan benar dalam semua isu terkait dengan perlindungan data pribadi.²⁸ Berikut penjelasan terkait posisi DPO:²⁹

1) Keterlibatan DPO pada Semua Isu Terkait Perlindungan Data Pribadi

Peran DPO sebagai pihak yang berhadapan dengan isu perlindungan data pribadi terkait, sangat penting bagi DPO untuk terlibat di semua isu terkait perlindungan data pada tahap sedini mungkin.

2) Independensi

Dalam menjalankan tugas dan tanggung jawabnya, DPO tidak diperkenankan untuk diberikan instruksi. Selain itu, DPO juga memiliki hak dalam pengambilan keputusan diluar tugas-tugas yang diberikan kepadanya

3) *Conflict of Interest* (Benturan Kepentingan)

DPO diperbolehkan untuk melaksanakan fungsi lain, asalkan fungsi tersebut tidak mengakibatkan benturan kepentingan. Demi mencegah terjadinya benturan kepentingan, Pengendali atau Prosesor harus:

- a) Mengidentifikasi posisi-posisi yang tidak kompatibel dengan fungsi DPO;
- b) Membuat aturan internal demi menghindari benturan kepentingan;
- c) Membuat penjelasan umum yang menjelaskan tentang benturan kepentingan;
- d) Menyatakan bahwa DPO mereka tidak memiliki benturan kepentingan sehubungan dengan perannya sebagai DPO untuk meningkatkan kesadaran akan persyaratan ini; dan
- e) Memasukan perlindungan di semua rangkaian aturan internal.

c. Pasal 39 - *Tasks of the DPO* (Tugas DPO)

Ketentuan terakhir dalam Bagian 4 GDPR, pasal 39 mengatur mengenai tugas-tugas dari DPO. Dalam menjalankan tugasnya, DPO wajib memastikan bahwa mereka secara penuh menyadari risiko-risiko terkait pemrosesan data pribadi. Secara khusus, GDPR mewajibkan DPO untuk melakukan tugas-tugas berikut:³⁰

- 1) Memberitahukan dan menyarankan Pengendali atau Prosesor dan pegawai yang bersangkutan terkait kewajibannya, sebagaimana telah ditetapkan dalam ketentuan mengenai perlindungan data;
- 2) Memantau kepatuhan Pengendali atau Prosesor terhadap GDPR, sebagaimana ditetapkan dalam kebijakan perlindungan data pribadi mereka;
- 3) Memberikan saran sesuai dengan DPIA;

²⁷ Pasal 29 Guidelines on Data Protection Officers, *Op.Cit.*, hlm. 13.

²⁸ Pasal 38 (1) General Data Protection Regulation.

²⁹ Pasal 29 Guidelines on Data Protection Officers, *Op.Cit.*, hlm. 13.

³⁰ Pasal 39 (1) General Data Protection Regulation.

- 4) Bekerja sama dengan otoritas pengawas; dan
- 5) Bertindak sebagai titik penghubung untuk otoritas pengawas terkait pemrosesan data pribadi.

5. Penerapan Peran *Data Protection Officer* pada Instansi Layanan Kesehatan

Mengingat urgensi optimalisasi perlindungan data pribadi pada sektor kesehatan, pemerintah perlu merealisasikan peran pejabat yang berwenang untuk melakukan pengawasan terhadap aktivitas perlindungan data pribadi di setiap instansi dan/atau perusahaan yang bergerak di bidang kesehatan baik konvensional maupun digital. Adapun tugas terkait perlindungan data pribadi di sektor kesehatan ini dapat diserahkan kepada DPO. Konsep DPO ini pada awalnya dikenalkan oleh pasal 37 GDPR. Pada pasal tersebut, telah ditegaskan bahwa apabila suatu kegiatan pengolahan data dilakukan oleh badan atau badan publik, maka wajib untuk menunjuk DPO.³¹ Kemudian pengaturan tersebut diadopsi dalam pasal 45 dan 46 Rancangan Undang-Undang Pelindungan Data Pribadi ("RUU PDP"). pasal 45 Ayat (2) huruf a dan Ayat (3) RUU PDP mengharuskan tersedianya pejabat yang melaksanakan fungsi dalam upaya melindungi data pribadi pada aspek pemrosesan data pribadi yang berorientasi pada kepentingan publik, yang dipilih dengan landasan mutu profesionalitas, wawasan terkait hukum serta praktik perlindungan data pribadi, dan kompetensi

untuk bertanggungjawab atas tugas-tugas yang dimilikinya.

Realisasi peran DPO di perusahaan/instansi layanan kesehatan harus diwujudkan dalam rangka perlindungan data pribadi di sektor kesehatan yang berkaitan dengan kepentingan publik. Adapun fungsi dari DPO berdasarkan pasal 46 RUU PDP menunjukkan bahwa peran DPO dalam optimalisasi perlindungan data pribadi sangat penting karena DPO memiliki wewenang untuk mengawasi segala aktivitas pemrosesan data yang dilakukan oleh prosesor data pribadi. Oleh sebab itu, berbagai perusahaan/instansi yang bergerak di bidang kesehatan seperti instansi kesehatan publik, rumah sakit, platform layanan kesehatan digital, laboratorium kesehatan, asuransi kesehatan serta sarana layanan kesehatan lainnya yang melaksanakan pemrosesan data pribadi untuk layanan publik harus memiliki DPO. Hal ini bertujuan untuk memastikan aktivitas pemrosesan data pribadi tetap berorientasi pada perlindungan data pribadi yang optimal dengan tetap mengacu pada koridor hukum positif di Indonesia.

Selain itu, DPO yang ada di perusahaan dan/atau instansi layanan kesehatan juga bertanggung jawab atas kinerja prosesor data pribadi dengan memberikan pelatihan dan audit secara berkala agar perlindungan data pribadi pasien di perusahaan dan/atau instansi layanan kesehatan tetap terjaga. Tugas selanjutnya yang dapat dibebankan kepada DPO di perusahaan dan/atau instansi layanan kesehatan adalah melakukan mitigasi risiko pada

³¹ Cliza, Marta Claudia dan Negura, Laura Cristiana Spataru "The General Data Protection Regulation: What Does The Public Authorities and Bodies Need to Know and to do? The Rise of The Data Protection Officer", *Juridical Tribune*, Volume 8, Nomor 2, 2018, hlm. 492.

pemrosesan data dan informasi kesehatan demi meminimalisir celah kebocoran data pribadi yang merugikan pasien/pengguna layanan kesehatan. Berdasarkan fungsi-fungsi DPO tersebut, dapat disimpulkan bahwa DPO memegang peran vital dalam rangka optimalisasi perlindungan data pribadi pada sektor kesehatan, khususnya perusahaan dan/atau instansi layanan kesehatan publik.

6. Urgensi Realisasi Pengaturan *Data Protection Officer* sebagai Strategi Pelindungan Data Pribadi secara Digital pada Sektor Kesehatan

Dalam menjamin perlindungan data pribadi secara digital khususnya pada sektor kesehatan, realisasi atas DPO menjadi suatu bahasan yang fundamental. Realisasi atas DPO tersebut dapat terjadi apabila dijamin oleh hukum yang mampu mengawal perubahan yang terjadi dalam masyarakat pada era digital saat ini guna mewujudkan perlindungan atas data pribadi sebagai bentuk kedaulatan data (*data sovereignty*). Mencermati hal tersebut, apabila merujuk pada Teori Hukum Pembangunan, maka dapat dipahami bahwa hukum berperan sebagai cara pembaharuan masyarakat (*a tool of social engineering*). Hukum harus memastikan bahwa perubahan yang tengah berlangsung dalam masyarakat dapat terlaksana dengan teratur.³² Berdasarkan hal tersebut, terdapat fungsi dinamis hukum sebagai alat pembaharuan yang mesti menjadi pemandu utama (*the prime mover*) dari pembangunan,³³ khususnya pada perubahan yang terjadi di era digital

saat ini. Dengan demikian, diperlukan regulasi yang dapat merealisasikan DPO tersebut sebagai upaya perlindungan atas data pribadi khususnya pada sektor kesehatan sehingga perubahan yang terjadi pada masyarakat di era digital saat ini dapat berjalan secara teratur.

Dalam upaya melindungi data pribadi termasuk pada sektor kesehatan, pemerintah Indonesia perlu dengan sesegera mungkin untuk mengesahkan RUU PDP. Pada RUU PDP terdapat jaminan perlindungan data pribadi pada sektor kesehatan terkait dengan data yang bersifat spesifik menurut pasal 3 Ayat (1) RUU PDP yang meliputi salah satunya terkait data serta informasi kesehatan yang termaktub pada Ayat (2). Pada Ayat (2) tersebut dijelaskan bahwa catatan atau keterangan individu yang bertalian baik itu kesehatan fisik, mental, atau pelayanan kesehatan termasuk ke dalam data dan informasi kesehatan. Dalam RUU PDP ini terdapat juga peran dari pejabat atau petugas DPO yaitu menjalankan fungsi dari perlindungan data pribadi sehingga hal tersebut menjadi jaminan perlindungan data pribadi. Hal ini tentunya perlu direalisasikan dimana instansi layanan kesehatan selaku pengelola data pribadi serta pemroses data pribadi wajib mengangkat DPO guna menjalankan fungsi dari perlindungan data pribadi.

Selain dengan disegerakannya pengesahan RUU PDP, alternatif lainnya yaitu dengan pembentukan Peraturan Pemerintah terkait realisasi DPO sebagai strategi perlindungan data pribadi secara digital pada sektor kesehatan. Berdasarkan ketentuan pasal 12 Undang-Undang Nomor 12 Tahun 2011 tentang Pembentukan Peraturan Perundang-undangan ("UU P3") mengatur isi peraturan pemerintah ini agar undang-undang dapat dilaksanakan sebagaimana mestinya. Dengan begitu artinya dengan penetapan terkait

³² Mochtar Kusumaatmadja, *Pembinaan Hukum dalam Rangka Pembangunan Nasional*, Bandung: Bina Cipta, 1975, hlm. 4.

³³ Atip Latipulhayat, "Khazanah: Mochtar Kusumaatmadja", *Padjadjaran Jurnal Ilmu Hukum*, Volume 1, Nomor 3, 2014, hlm. 629."

peraturan pemerintah tersebut guna menjalankan undang-undang sejauh mana diperlukan dan tidak adanya penyimpangan dari muatan materi yang diatur pada undang-undang terkait. Dalam hal ini, pembentukan peraturan pemerintah mengenai realisasi DPO tersebut diajukan untuk menjalankan pasal 47 Ayat (2) UU Praktik Kedokteran yang mengatur keharusan para pelaku sarana pelayanan kesehatan dalam hal melakukan penyimpanan dan penjagaan kerahasiaan terhadap dokumen rekam medis. Lebih lanjut, berdasarkan ketentuan pasal 27 UU P3 dapat diketahui bahwasannya rancangan peraturan pemerintah berasal dari baik itu kementerian maupun non kementerian yang sejalan dengan bidang dari tugasnya. Oleh sebab itu, pada hal ini diperlukan kolaborasi antara Kementerian Kesehatan dan Kementerian Kominfo untuk membentuk rancangan peraturan pemerintah mengenai realisasi DPO sebagai upaya menciptakan pengaturan yang dapat mengakomodir perlindungan data pribadi pada sektor kesehatan secara digital.

Informasi yang tercakup dalam peraturan pemerintah yang menangani DPO ini berkaitan dengan unsur-unsur penting dalam menetapkan tanggung jawab pejabat atau pejabat yang melaksanakan tugas melindungi data pribadi serta peraturan terkait lainnya, seperti:

- 1) Kewajiban penyediaan DPO di setiap instansi layanan kesehatan yang menyimpan data pribadi pasien (sebagai contoh: rumah sakit; perusahaan layanan asuransi kesehatan, klinik kesehatan, laboratorium kesehatan);
- 2) Ketentuan mengenai kriteria persyaratan dan pengangkatan DPO di instansi layanan kesehatan;
- 3) Kewajiban dan tanggung jawab DPO di sektor pelayanan kesehatan;
- 4) Peran dan fungsi DPO dalam memroses data pribadi termasuk data pribadi spesifik serta data pribadi umum berupa data dan informasi kesehatan pasien (meliputi: identitas pribadi; alamat, data keuangan, rekam medis pasien, dan data lain yang terdapat kaitan erat dengan data pribadi seseorang yang menggunakan fasilitas kesehatan) antara lain:
 - a) Memberikan informasi serta saran yang ditujukan kepada instansi layanan kesehatan agar mematuhi ketentuan dalam regulasi pada sektor perlindungan data pribadi di sektor kesehatan;
 - b) Kegiatan *monitoring* dan mengontrol kepatuhan terhadap instrumen hukum yang berkenaan dengan perlindungan data pribadi di sektor kesehatan dan

kebijakan instansi layanan kesehatan, meliputi, tanggung jawab, penugasan, meningkatkan pemahaman dan arahan semua pihak yang terlibat dalam penanganan data pribadi di bidang kesehatan, serta melakukan pemeriksaan dan pengawasan terkait;

- c) Menyampaikan masukan tentang cara mengevaluasi dampak penyimpanan data pribadi di sektor kesehatan serta *monitoring* performa instansi layanan kesehatan; dan
- d) berkoordinasi serta berperan sebagai narahubung pada topik yang berkaitan dengan pemrosesan data pribadi di instansi layanan kesehatan, termasuk melaksanakan konsultasi mengenai mitigasi risiko, menjalin kerjasama dengan instansi pengamanan data pribadi, dan/atau hal lainnya.

Kasus kebocoran data BPJS Kesehatan mencerminkan tidak terwujudnya perlindungan data pribadi pada sektor kesehatan di Indonesia. Pengaturan terkait dengan perlindungan data pribadi yang mana pengaturannya masih terpisah dalam beberapa peraturan perundang-undangan membuat pengaturan bersifat umum dan lemah. Berdasarkan hal tersebut, perlu adanya pengaturan dan pengawasan yang ketat dalam instansi kesehatan, khususnya pada sektor digital. Realisasi peran DPO di instansi layanan kesehatan menjadi jawaban terhadap permasalahan tersebut yang harus diwujudkan sebagai perlindungan data pribadi secara digital di sektor kesehatan.

Akan tetapi, urgensi realisasi peran DPO dalam rangka optimalisasi perlindungan data pribadi di sektor kesehatan secara digital tidak didukung dengan regulasi yang mengatur mengenai peran DPO. Oleh sebab itu, RUU PDP sebagai dasar hukum komprehensif mengenai perlindungan data pribadi yang memuat payung hukum penerapan peran DPO harus segera disahkan. Dalam alternatif RUU PDP tak kunjung disahkan, maka pemerintah perlu membuat peraturan pemerintah tentang DPO yang mengacu pada ketentuan umum perlindungan data pribadi di sektor kesehatan yang bersumber dari berbagai peraturan perundang-undangan.

Daftar Pustaka **Buku**

- Danrivanto Budhijanto, *Hukum Telekomunikasi, Penyiaran & Teknologi Informasi, Regulasi dan Konvergensi*, PT. Refika Aditama, Bandung, 2013.
- Kementerian Kesehatan Republik Indonesia, *Cetak Biru Strategi Transformasi Digital Kesehatan 2024*, Kementerian Kesehatan Republik Indonesia, Jakarta, 2021.

D. Penutup

Mochtar Kusumaatmadja, *Pembinaan Hukum dalam Rangka Pembangunan Nasional*, Bina Cipta, Bandung, 1975.
Soerjono Soekanto, *Penelitian Hukum Normatif: Suatu Tinjauan Singkat*, PT RajaGrafindo Persada, Jakarta, 2009.

Dokumen Lain

Aptika Kominfo, "Digitalisasi Pelayanan Kesehatan dengan Penerapan Revolusi Industri",
<https://aptika.kominfo.go.id/2019/04/digitalisasi-pelayanan-kesehatan-dengan-penerapan-revolusi-industri-4-0/>.

Aptika Kominfo, "Warganet Meningkatkan, Indonesia Perlu Tingkatkan Nilai Budaya di Internet",
<https://aptika.kominfo.go.id/2021/09/warganet-meningkat-indonesia-perlu-tingkatkan-nilai-budaya-di-internet/>.

Arie Dwi Budiati, "Dua Dugaan Penyebab Kebocoran 279 Juta Data Pribadi Diklaim Peserta BPJS",
<https://www.dream.co.id/dinar/2-hal-ini-diduga-jadi-biang-kerok-kebocoran-data-penduduk-210524f.html>.

Atip Latipulhayat, "Khazanah: Mochtar Kusumaatmadja", *Padjadjaran Jurnal Ilmu Hukum*, Volume 1, Nomor 3, 2014.

Aulia Naslah Mahira, "Perlindungan Hukum terhadap Kerahasiaan Data Kesehatan Pasien berdasarkan Undang-Undang Nomor 36 Tahun 2009 tentang Kesehatan", *Dinamika Jurnal Ilmiah Ilmu Hukum*, Volume 27, Nomor 10, 2021.

Cliza, Marta Claudia dan Negura, Laura Cristiana Spataru "The General Data Protection Regulation: What Does The Public Authorities and Bodies Need to Know and to do? The Rise of The Data Protection Officer", *Juridical Tribune*, Volume 8, Nomor 2, 2018.

CNN Indonesia, "Kebocoran Data Pribadi, BPJS Kesehatan Bakal Digugat",
<https://www.cnnindonesia.com/teknologi/20210606200515-185->

[650991/kebocoran-data-pribadi-bpjs-kesehatan-bakal-digugat](https://www.cnnindonesia.com/teknologi/20210606200515-185-650991/kebocoran-data-pribadi-bpjs-kesehatan-bakal-digugat).

Daniel Budi Wibowo, "Optimisme Rumah Sakit di Masa Pandemi Covid-19",
https://persi.or.id/wp-content/uploads/2020/05/materi_drda_nielbw.pdf.

Danrivanto Budhijanto, "Data as New Oil dalam Konstruksi Hukum Ekonomi Digital di Indonesia",
<https://www.hukumonline.com/berita/baca/lt5db1470b9d036/data-as-new-oil-dalam-konstruksi-hukum-ekonomi-digital-di-indonesia>.

EuroCham, "Position Paper: Pharmaceutical & Medical Technology",
<http://www.eurocham.id/publications>,
diunduh 4 Juli 2022.

Fahmi Ahmad Burhan, "Kunjungan ke Aplikasi Alodokter & Halodoc Naik 600% Efek Virus Corona",
<https://katadata.co.id/desysetyowati/digital/5e9a421548005/kunjungan-ke-aplikasi-alodokter-halodoc-naik-600-efek-virus-corona>.

Handryas Prasetyo Utomo, dkk, "Urgensi Perlindungan Hukum Data Pribadi Pasien dalam Pelayanan Kesehatan Berbasis Teknologi di Indonesia", *Jurnal Ilmiah Galuh Justisi*, Volume 8, Nomor 2, 2020.

Lia Sautunnida, "Urgensi Undang-Undang Perlindungan Data Pribadi di Indonesia: Studi Perbandingan Hukum Inggris dan Malaysia", *Kanun Jurnal Ilmu Hukum*, Volume 20, Nomor 2, 2018.

M. Iqsan Sirie, "The Mandatory Designation of a Data Protection Officer in Indonesia's Upcoming Personal Data Protection Law", *PADJADJARAN Journal of Law*, Volume 5, Nomor 1, 2018.

Pusat Studi Forensika Digital UII, "Data Kesehatan",
<https://forensics.uui.ac.id/data-kesehatan/>.

Dokumen Hukum

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.

Undang-Undang Nomor 29 Tahun 2004 tentang Praktik Kedokteran.

Undang-Undang Nomor 36 Tahun 2009 tentang Kesehatan.

Undang-Undang Nomor 44 Tahun 2009 tentang Rumah Sakit.

Undang-Undang Nomor 12 Tahun 2011 tentang Pembentukan Peraturan Perundang-Undangan.

Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

Peraturan Menteri Kesehatan Republik Indonesia Nomor 21 Tahun 2020 tentang Rencana Strategis Kementerian Kesehatan Tahun 2020-2024.

Rancangan Undang-Undang tentang Pelindungan Data Pribadi.

Keputusan Menteri No. HK.01.07/MENKES/4829/2021 tentang Pedoman Pelayanan Kesehatan Melalui Telemedicine Pada Masa Pandemi *Corona Virus Disease* 2019 (COVID-19).

General Data Protection Regulation.

Data Protection Working Party, Guidelines on Data Protection Officers.