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

PERLINDUNGAN HUKUM TERHADAP DATA KESEHATAN MELALUI PENGESAHAN RANCANGAN UNDANG-UNDANG PERLINDUNGAN DATA PRIBADI

Endison Ravlindo

(Fakultas Hukum Universitas Tarumanagara)

(*E-mail* : endison.205180009@stu.untar.ac.id)

Ariawan Gunadi

(Fakultas Hukum Universitas Tarumanagara. Meraih Sarjana Hukum pada Fakultas Hukum Universitas Tarumanagara, Magister Hukum pada Fakultas Hukum Universitas Tarumanagara, Doktor (Dr.) pada Fakultas Hukum Universitas Indonesia)

(*E-mail* : ariawangun@gmail.com)

Abstract

The development of an increasingly sophisticated era, now personal data has become a commodity that has a high economic value that must receive proper and optimal protection in the practices that exist in society. Some of the regulations regarding the protection of personal data in Indonesia have regulated this, but have not been able to face the challenges that arise regarding the problems that occur. Where this makes the creation of legal certainty as one of the objectives of the law itself. There have been a number of cases that have occurred in recent years, namely the alleged leakage of public personal data that was hacked by third parties irresponsibly for unilateral gain. In this case, because there is no specific and comprehensive regulation that accommodates the protection of personal data itself. In this study, it is intended to examine how legal protection is according to current positive law and according to the Personal Data Protection Bill.

Keywords : *Data Protection; Personal Data; Privacy Rights; Personal Data Leak.*

I. PENDAHULUAN

A. Latar Belakang

Perkembangan teknologi informasi dan komunikasi berkembang cukup pesat sehingga mengubah sejumlah kehidupan masyarakat yang semula secara luring dan kemudian menjadi daring. Sejatinya, kehidupan masyarakat pada dasarnya hanya dapat dilakukan secara fisik dengan waktu yang dikorbankan menjadi semakin efisien karena pengaruh dari perkembangan teknologi informasi dan komunikasi. Perkembangan teknologi informasi dan komunikasi yang sangat pesat ditandai dengan lahirnya komputer, telefon ponsel *smartphone*, laptop dan lain sebagainya yang dapat memperoleh data, mengolah data dan memproses data seseorang secara aman dan terlindungi.

Seiring dengan kecanggihan teknologi menjadikan data atau informasi pribadi yang terdaftar pada media elektronik merupakan suatu komoditas bernilai tinggi dan rentan terhadap kebocoran data yang dilakukan oleh pihak ketiga. Tetapi, dengan adanya kecanggihan tersebut, akan memberikan kemudahan kepada masyarakat dalam melaksanakan aktivitas sehari-hari secara praktis dan efisien.

Perkembangan teknologi informasi dan komunikasi telah memasuki segala sektor yang salah satunya adalah *electronic health* (*e-Health*) yang memberikan sejumlah pelayanan pengobatan, konsultasi, layanan apotek online, dan berbagai informasi kesehatan dalam bentuk aplikasi berbasis internet. e-Health di ciptakan untuk memberikan kemudahan kepada pasien dalam mengakses terhadap layanan kesehatan secara efektif, efisien waktu dan biaya.

Namun, informasi kesehatan dan data pasien yang tercantum dalam aplikasi tersebut tidak terjamin terhadap keamanannya, mengingat Indonesia belum memiliki pengaturan hukum yang mengatur secara khusus dalam mengakomodir permasalahan yang timbul dalam masyarakat terkait perlindungan data pribadi terutama pada bidang *e-Health*.

Indonesia merupakan negara hukum sebagaimana yang diatur di dalam Undang-Undang Dasar Negara Republik Indonesia Tahun 1945. Negara Indonesia melalui suatu lembaga pemerintahan melaksanakan kewajiban konstitusional

dengan berlandaskan atas hukum terutama memasuki era globalisasi yang ditandai dengan adanya teknologi informasi.

Salah satu hak konstitusional yang terdapat pada setiap warga negara yaitu ha katas perlindungan diri pribadi. Pada konstitusi Negara Indonesia telah mengatur bahwa setiap hak asasi seseorang harus mendapatkan perlindungan sebagaimana tercantum dalam bunyi Pasal 28G ayat (1) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 (UUD 1945) yang menyatakan setiap orang berhak atas perlindungan diri pribadi, berhak atas rasa aman serta perlindungan dari ancaman ketakutan.[1]

Perlindungan data pribadi memiliki keterkaitan dengan konsep privasi yang wajib mendapatkan perlindungan atas kerahasiaannya. Warren dan Brandeis merupakan tokoh yang mengemukakan konsep privasi untuk pertama kalinya dalam karya jurnal ilmiah yang berjudul "*The Right to Privacy*" yang berarti hak untuk tidak diganggu. Dalam jurnal tersebut, dikatakan bahwa setiap orang dalam melaksanakan kegiatan memiliki hak untuk dilindungi privasinya.[2]

Konsep privasi yaitu sebuah gagasan untuk menjamin integritas, martabat dan taraf hidup seseorang, dan setiap orang berhak untuk menentukan siapa, untuk apa dan bagaimana informasi mengenai diri mereka digunakan untuk kepentingan tertentu.[3] Upaya dalam melindungi hak privasi seseorang sama halnya perlindungan terhadap hak atas kebebasan berbicara yang notabene harus menjamin perlindungan dari penyalahgunaan data pribadi yang bagian dari hak asasi manusia.[4]

Perlindungan data pribadi merupakan bagian dari hak asasi manusia yang fundamental, yaitu hak seseorang untuk mendapatkan perlindungan serta pengamanan terhadap informasi pribadi mereka, dan apabila terjadi suatu

[1] Indonesia, *Undang-Undang Dasar Negara Republik Indonesia Tahun 1945*, Pasal 28G Ayat (1)

[2]Latumahina RE, *Aspek Hukum Perlindungan Data Pribadi Di Dunia Maya*, (Jakarta: Gema Aktualita Vol.3 No. 2, 2014), Hal. 14-25.

[3]Wahyudi Djafar dan Asep Komarudin, *Perlindungan Hak Atas Privasi di Internet Beberapa Penjelasan Kunci*, (Jakarta: Elsam, 2014), Hal 2.

[4]Cynthia H, "Registrasi Data Pribadi Melalui Kartu Prabayar Dalam Perspektif Hak Asasi Manusia", Jurnal HAM Vol.9 No.2, 2018, Hal.191

permasalahan, pemilik data pribadi berhak atas pembenaran dan pembelaan.[5] Hak privasi merupakan hak pribadi yang lebih sensitif karena informasi yang terkandung di dalamnya berisi sejumlah informasi pribadi yang krusial.

Berbagai negara telah memiliki pengaturan khusus yang mengatur secara spesifik dan komprehensif mengenai perlindungan data pribadi antara lain Jerman sebagai negara pertama yang telah mengatur terkait perlindungan data pribadi, kemudian diikuti oleh negara Swedia, Amerika Serikat, dan negara Inggris.[6]

Pengaturan mengenai perlindungan data pribadi yang menjadi suatu standar dunia yaitu terdapat pada seluruh Uni Eropa Regulation (EU) 2016/*679 on the protection of personal data* yang dikenal sebagai *General Data Protection Regulation* (GDPR). Pada GDPR telah menganut 6 (enam) prinsip perlindungan data umum, pengertian data pribadi lebih luas, serta terdapat hak baru yaitu untuk portabilitas data individu yang mengharuskan pengendali data memproses sesuai dengan tujuan dan kepentingan pemilik data pribadi.

Pengertian data pribadi dalam GDPR yaitu, suatu data yang dapat mengidentifikasi pengguna seperti nama, data demografi, nomor telepon, alamat IP, nama pengguna online, orientasi seksual, data kesehatan dan lain sebagainya. Sedangkan, pengertian data pribadi pada Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik (Permenkominfo 20/2016) yaitu data perseorangan tertentu yang di simpan, di rawat, dan dijaga kebenarannya serta mendapatkan perlindungan atas kerahasiaannya.

Dalam GDPR juga memiliki pengaturan terhadap pengawasan oleh pihak terkait yaitu adanya suatu lembaga khusus "*The European Data Protection Board*" yang bertugas dalam mengawasi pelaksanaan GDPR pada negara-negara di Uni Eropa.[7] Sedangkan, pada pengaturan di Indonesia belum memiliki lembaga khusus yang melakukan pengawasan terhadap pelindungan data pribadi secara menyeluruh melainkan hanya terbatas pada pengawasan sektoral.

---

[5]Graham Greenleaf, "*76 Global Data Protection Laws, Privacy Laws & Business Special Report*", Law Article, 2011, Hal.20.

[6] Edmond Makarim, *Pengantar Hukum Telematika (Suatu Kompilasi Kajian)*, (Jakarta: RajaGrafindo Persada, 2005), Hal.35

[7] Normand Edwin Elnizar, "Ini 4 Perbedaan GDPR dan Perlindungan Data Pribadi di Indonesia", HukumOnline Berita, Indonesia, 20 Agustus 2021, Hal.1.

Uni Eropa dengan GDPR telah menjadi suatu standar dunia dan telah mempengaruhi sejumlah kebijakan perlindungan data pribadi di seluruh dunia, diharapkan Indonesia dapat ikut berkiblat pada GDPR dalam merancang pengaturan khusus yang mengatur secara komprehensif mengenai perlindungan data pribadi dan segera mengesahkannya.

Dalam hal pihak yang bertanggung jawab dalam GDPR yaitu pengendali dan pengelola data pribadi sebagai pihak yang bertanggung jawab serta menjamin perlindungan data dengan fungsi yang lebih luas dari istilah pengguna yang terdapat pada Permenkominfo 20/2016. Terhadap data kesehatan, GDPR juga membenarkan pengungkapan identitas pasien dengan kewajiban menerapkan nama samara (pseudonymisation) terhadap data yang diambil demi menjamin keamanan informasi subjek data.

Selain itu, GDPR juga mengatur terkait denda yaitu terhitung dari 4% (empat persen) pendapat total global jika telah melanggar ketentuan GDPR dan juga terdapat hak kompensasi bagi pihak yang dirugikan terhadap pelanggaran tersebut. Sedangkan, peluang kompensasi kepada pihak yang dirugikan pada pengaturan di Indonesia hanya dapat melalui gugatan perdata atas kerugian yang ditimbulkan. Sehingga, perolehan kompensasi bagi korban dalam GDPR di rasakan dapat diimplementasikan dalam pengaturan di Indonesia guna menjamin pemenuhan hak dari orang tersebut.

Selain GDPR, pengaturan pada sejumlah negara lain juga telah mengakomodir permasalahan terkait perlindungan data pribadi secara optimal. Negara Inggris memiliki *Data Protection Act 1998*, Negara Switzerland memiliki *Federal Act on Data Protection of Switzerland 1992*, Republik Lithuania memiliki *The Lithuanian Cybersecurity Law* dan lain sebagainya. Negara Indonesia hingga saat ini belum memiliki undang-undang khusus yang tegas dan komprehensif mengatur terkait perlindungan data pribadi.

Dengan absennya pengaturan ini, mengakibatkan banyak terjadi permasalahan yang timbul dalam masyarakat karena tidak tersedianya payung hukum dan/atau kekosongan hukum yang secara tegas dan komprehensif mengatur terhadap data pribadi. Di Indonesia sendiri, apabila kita melihat dari seluruh peraturan perundang-undangan yang berlaku di Indonesia, hanya sedikit yang menyinggung

terkait dengan perlindungan data pribadi, dapat terlihat dari 30-an (tiga puluhan) pengaturan yang mengatur terkait hal tersebut.

Akibatnya, keresahan masyarakat tidak terakomodir mengingat pengaturan yang dimiliki saat ini tidak tegas dan tidak komprehensif mengatur terkait perlindungan data pribadi. Seiring dengan perkembangan zaman, data pribadi merupakan komoditi yang mempunyai nilai ekonomi tinggi, sehingga terhadap kegiatan pemrosesan data harus mendapat pengawasan dan keamanan optimal karena data pribadi merupakan privasi seseorang yang wajib dijaga kerahasiaannya.[8]

Kasus peretasan data pribadi di Indonesia akhir-akhiri ini semakin marak dalam segala lapisan masyarakat. Terutama pada kondisi pandemi saat ini yaitu banyak data kesehatan pasien di retas dan diperdagangkan dalam situs *dark web* oleh pihak ketiga. Data kesehatan tersebut meliputi nama, status kewarganegaraan, tanggal lahir, alamat, rekam medis dan lain sebagainya. Kemudian, hasil tes Covid-19 (*CoronaVirus Disease 19*) juga diungkapkan secara tanpa hak dengan terperinci yaitu gejala pasien, tanggal mulai sakit dan tanggal pemeriksaan.

Insiden peretasan data pribadi di bidang kesehatan lainnya yaitu terdapat pada aplikasi layanan kesehatan berbasis internet yang bernama *Electronic Health Alert Card* (e-HAC). E-HAC di dalamnya memuat sejumlah informasi terkait status kesehatan, informasi keberangkatan, rekam medis dan lain sebagainya. Berdasarkan amanat dari Pasal 28G Ayat (1) UUD 1945, perlindungan data pribadi sebagai bagian dari privasi yang merupakan hak asasi manusia. Sehingga, dalam kegiatan pengumpulan data pribadi pasien telah memberikan tanggung jawab bagi penyelenggara sistem elektronik untuk menyimpan data secara aman dan hanya digunakan untuk tujuan tertentu.

Melihat dari berbagai insiden data pribadi masyarakat yang diretas, hal tersebut tentunya sangatlah bertentangan dengan hak asasi terkait dengan privasi seseorang. Di Indonesia, UUD 1945 memang tidak menegaskan secara eksplisit terhadap hak pribadi. Namun, dalam deklarasi umum hak asasi manusia Internasional, yakni :

[8]Edmon Makarim, *Kompilasi Hukum Telematika*, (Jakarta: PT. Raja Grafindo Persada, 2003), Hal.3

The Universal Declaration of Human Rights[9] menegaskan bahwa setiap orang memiliki hak untuk hidup, kebebasan, dan keamanan keluarga dan kehormatan pribadi.

Selain amanah dari UUD 1945 dan literatur *international*. Permenkominfo 20/2016 juga telah menguraikan pengertian perlindungan data pribadi dalam sistem elektronik, bahwa data pribadi berisikan fakta-fakta terkait individu yang merupakan informasi bersifat rahasia menyangkut privasi seseorang. Dijelaskan bahwa, data pribadi merupakan bagian dari hak pribadi (*privacy rights*) yakni hak untuk menikmati hidup pribadi dan bebas dari segala macam gangguan dan ancaman ketakutan; hak untuk kebebasan dalam komunikasi dengan orang tanpa tindakan memata-mata; hak untuk mengawasi akses informasi tentang kehidupan pribadi dan informasi seseorang dan hal tersebut merupakan amanah di dalam Pasal 28 huruf G UUD 1945.

Ruang lingkup dari hak pribadi itu sendiri, yaitu; (1) gangguan terhadap tindakan seseorang sehingga membuat orang tersebut mengasingkan diri, (2) pengungkapan fakta-fakta pribadi yang memalukan pada publik, (3) publisitas yang membuat seseorang secara keliru di hadapan publik.[10] Dalam pelaksanaannya, melihat dari perkembangan dari suatu inovasi dalam bidang teknologi informasi dan komunikasi diperlukan sinkronisasi antara suatu inovasi dan ketentuan pengaturan yang dapat memberikan perlindungan secara optimal pada masyarakat.

Dengan diberikannya kemudahan dalam pemanfaatan teknologi salah satunya penggunaan aplikasi berbasis internet sehingga informasi yang terdaftar di dalamnya tidak terjamin keamanannya. Kemudian, hal tersebut dapat menimbulkan kekhawatiran orang tersebut mengenai informasi pribadi miliknya yang telah terdaftar dalam *platform* terkait. Sehingga di Indonesia sudah menjadi urgensi terkait pengesahan Rancangan Undang-Undang Perlindungan Data Pribadi (RUU Perlindungan Data Pribadi) yang perlu segera di akselerasi demi meminimalisir terjadinya pelanggaran hak dalam masyarakat.

[9]Selanjutnya Disebut *UDHR*. *UDHR* Ini Berisikan Suatu Daftar Hak-Hak Dasar Manusia, Sebagai Suatu Standar Bersama Bagi Semua Orang Dan Semua Bangsa.

[10]William L. Prosser, *Privacy: A Legal Analysis*, (California : Law Review 48, 1960), Hal. : 338-423.

Menurut literatur dan data yang telah dikumpulkan, telah terjadi insiden kebocoran data pasien Covid-19 sebanyak 231.636 (dua ratus tiga puluh satu ribu enam ratus tiga puluh enam) yang diretas dan diperdagangkan secara bebas dalam situs *dark web* melalui *Rapid Forums* dengan akun bernama *Database Shopping*. Data pasien Covid-19 tersebut dijual secara lengkap yakni nama, status kewarganegaraan, tanggal lahir, alamat, rekam medis dan lain sebagainya. Bentuk pelanggaran lainnya juga terdapat pada data pribadi dalam platform lainnya dengan berbagai bidang yang salah satunya dalam *platform electronic commerce* (*E-Commerce*).

Contoh kasus lainnya yang terjadi adalah data pribadi nasabah BRI Life berhasil diretas oleh pihak ketiga secara tanpa hak. Kegiatan tersebut ditujukan untuk memperoleh keuntungan dari transaksi dalam situs tertentu. Data nasabah berjumlah lebih dari 2.000.000 (dua juta) data pribadi yang meliputi informasi lengkap mengenai nasabah, total manfaat yang diperoleh dan total periode. Terlebih lagi, terdapat juga informasi pribadi yang bersifat sensitif dapat mendeskripsikan seseorang yakni nama, tanggal lahir, alamat, jenis kelamin, nomor identitas pajak, foto buku rekening bank dan lain sebagainya. Oleh karena itu, RUU Perlindungan Data Pribadi dapat dijadikan hukum positif atau payung hukum dalam perlindungan data pribadi di Indonesia dengan pengaturan yang secara spesifik dan komprehensif mengatur yang diharapkan dapat memberikan kepastian hukum bagi masyarakat dan menjawab tantangan praktik yang terjadi selama ini. Dalam hal ini, Penulis tertarik untuk mengadakan penelitian lebih lanjut ke dalam tulisan ini dengan judul **"Perlindungan Hukum Terhadap Data Kesehatan Melalui Pengesahan Rancangan Undang-Undang Perlindungan Data Pribadi"** dengan menggunakan contoh kasus yang telah Penulis uraikan di atas.

B. Permasalahan

Berdasarkan latar belakang yang telah diuraikan di atas, permasalahan dalam penelitian ini adalah:

1. Bagaimana Perlindungan Hukum Terhadap Data Kesehatan Dalam Hukum Positif Saat Ini?

2. Bagaimana Perlindungan Hukum Terhadap Data Kesehatan Dalam RUU Perlindungan Data Pribadi?

C. Metode Penelitian

1. Jenis Penelitian

Jenis penelitian yang digunakan ialah penelitian normatif yang bersifat deskriptif analisis dengan tujuan memberikan data secara sistematis dan terperinci berdasarkan materi yang berkaitan dengan perlindungan data pribadi.[11] Pemilihan bahan pustaka meliputi data dasar pada suatu ilmu penelitian digolongkan sebagai data sekunder merupakan data yang diperoleh oleh Penulis dari sumber yang ada antara lain mencakup dokumen-dokumen resmi, buku-buku, hasil-hasil penelitian yang berwujud laporan, buku harian, dan seterusnya. Dalam penelitian hukum, data sekunder mencakup;

a. Bahan Hukum Primer, yaitu bahan hukum yang mengikat yang terdiri dari peraturan perundang-undangan;
   1) Undang-Undang Dasar Negara Republik Indonesia Nomor 1945.
   2) Rancangan Undang-Undang Perlindungan Data Pribadi.
   3) Undang-Undang Nomor 36 Tahun 2009 tentang Kesehatan.
   4) Undang-Undang Nomor 29 Tahun 2004 tentang Praktik Kedokteran.
   5) Undang-Undang Nomor 44 Tahun 2009 tentang Rumah Sakit.
   6) Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
   7) Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.
   8) Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik.

b. Bahan Hukum Sekunder, yaitu berupa publikasi tentang hukum meliputi buku teks, kamus hukum dan jurnal hukum, komentar atas putusan pengadilan dan wawancara yang dituangkan dalam bentuk tulisan.

II. Pembahasan

[11]Bambang Sunggono, *Metodologi Penelitian Hukum*, (Jakarta: PT RajaGrafindo Persada, 2008), Hal.86

A. Perlindungan Data Pribadi Menurut Hukum Positif Indonesia

Perlindungan data pribadi khususnya data kesehatan di tanah air masih rentan terhadap kebocoran dan tidak terakomodir sepenuhnya. Mengingat di Indonesia belum memiliki pengaturan yang mengatur secara khusus dan spesifik mengenai perlindungan data pribadi dan masih ditemukan sejumlah kasus penyalahgunaan data pribadi masyarakat dalam berbagai *platform.* Perlindungan Data Pribadi tercipta karena maraknya akan pelanggaran terhadap data pribadi seseorang maupun badan hukum. Penyalahgunaan data pribadi dapat menimbulkan kerugian yang tidak hanya pada materiil saja, tetapi moral juga dirugikan terkait hal ini yakni nama baik dan kehormatan seseorang atau lembaga terlecehkan. Apabila kita melihat akhir-akhir ini, banyak kasus yang menimpa masyarakat terhadap peretasan data pribadi mereka oleh pihak yang tidak bertanggung jawab. Terlebih lagi, dengan semakin canggihnya teknologi yang memudahkan masyarakat untuk melaksanakan aktivitas sehari-hari melalui daring dengan koneksi internet. Sehingga, penyalahgunaan data pribadi semakin berpotensi dan menyebar dengan cepat.

Pengaturan berkenaan mengenai Perlindungan Data Pribadi di Indonesia masih bersifat umum dan tidak mengakomodir berbagai isu permasalahan yang sering terjadi pada masyarakat serta terletak secara terpisah dalam berbagai peraturan perundang-undangan. Dengan tersedianya pengaturan yang secara khusus dan komprehensif, dirasakan Indonesia dapat lebih siap menghadapi tantangan mengenai persoalan data pribadi dan juga dapat memberikan jaminan keamanan terhadap data setiap individu serta dapat menjerat pelaku penyalahgunaan data pribadi dengan sanksi yang tegas.

Dalam hal ini, sudah menjadi suatu kewajiban dan sejatinya negara hukum sebagaimana tercantum dalam Pasal 1 ayat (3) UUD 1945 bahwa negara Indonesia adalah negara hukum. Artinya bahwa Indonesia adalah sebuah negara yang berlandaskan hukum dan juga demokratis yang harus memberikan perlindungan hukum terhadap warga negaranya dalam konteks persoalan perlindungan data pribadi. Data merupakan suatu bahan baku yang terkandung dalam informasi yang dapat memberikan makna atau keterangan pribadi bagi

manusia. Data adalah segala informasi yang mengandung identitas seseorang yang dapat diproses dengan suatu alat yang bertujuan untuk disimpan atau dengan tujuan tertentu.

Data pribadi di bidang kesehatan juga sering mengalami kebocoran, akan semakin fatal apabila data yang berhasil bocor merupakan rekam medis yang bersifat sangat rahasia. Istilah data pribadi dalam bidang kesehatan yaitu rekam medis yang merupakan keterangan yang tertulis dan terekam tentang identitas laboratorium, diagnosa pelayanan, tindakan dan pengobatan yang diberikan kepada pasien baik yang dirawat inap maupun rawat jalan dan yang sedang mendapatkan perawatan dalam keadaan darurat.

Dalam Peraturan Menteri Kesehatan Nomor 269 Tahun 2008 tentang Rekam Medis ("Permenkes 269/2008") disebutkan bahwa informasi mengenai identitas dan riwayat medis pasien yang harus dijaga kerahasiaannya oleh pihak penyelenggara sistem elektronik dalam hal ini rumah sakit antara lain petugas, pengelola dan pimpinan.[12] Tetapi, untuk kepentingan pasien, permintaan dari aparat penegak hukum dalam rangka penegakan hukum dan berdasarkan ketentuan peraturan perundang-undangan, informasi tersebut dapat dibuka. Permintaan tersebut harus disampaikan dengan permohonan secara tertulis yang diserahkan kepada pihak Rumah Sakit.

Peraturan yang mengatur mengenai perlindungan data pribadi khususnya pada bidang kesehatan diatur dalam Undang-Undang Nomor 29 Tahun 2004 tentang Praktik Kedokteran (UUPK) dalam Pasal 47 ayat (2) yang berbunyi "Rekam medis harus disimpan dan dijaga kerahasiaannya oleh dokter atau dokter gigi dan pimpinan sarana pelayanan kesehatan". Kemudian setiap pasien juga mempunyai hak atas rahasia kondisi kesehatan pribadinya yang diatur dalam Undang-Undang Nomor 36 Tahun 2009 tentang Kesehatan (UUK) Pasal 57 ayat (1) berbunyi "Setiap orang berhak atas rahasia kondisi kesehatan pribadinya yang telah dikemukakan kepada penyelenggara pelayanan kesehatan".

[12] Indonesia, Peraturan Menteri Kesehatan Republik Indonesia Nomor 269/MENKES/PER/III/2008 tentang Rekam Medis, Pasal 10 Ayat (1)

Sejatinya setiap pasien yang dirawat dalam rumah sakit berhak atas kerahasiaan privasinya seperti rekam medis yang dialami pasien yang terdapat pengaturannya dalam Undang-Undang Nomor 44 Tahun 2009 tentang Rumah Sakit (UURS) Pasal 32 huruf i yang berbunyi "Setiap pasien mempunyai hak untuk mendapatkan privasi dan kerahasiaan atas penyakit yang dialami beserta data medis pasien". Peraturan berikutnya yang bersangkutan bahwa setiap penyelenggara data pribadi pada bidang kesehatan dalam hal ini Rumah Sakit mempunyai kewajiban terhadap pasien yang tertuang dalam UU RS Pasal 29 ayat (1) huruf m yang berbunyi "Setiap rumah sakit mempunyai kewajiban untuk menghormati dan melindungi hak-hak pasien". Bahwa setiap rekam medis yang terdapat dan/atau dikemukakan dalam penyelenggara pelayanan kesehatan merupakan bagian dari privasi pasien yang sejatinya harus dijaga kerahasiaannya.

Terlebih lagi, dengan kecanggihan teknologi memberikan kemudahan dalam menghubungkan antara 1 (satu) pihak dengan pihak lainnya, seperti halnya Rumah Sakit menghubungkan dengan Pusat Kesehatan Masyarakat atau instansi terkait lainnya menggunakan aplikasi *e-Health* yang berpotensi timbul persoalan di kemudian hari. Proses pelayanan yang dilakukan dalam *e-Health* akan mengumpulkan sejumlah data pribadi pasien yang dikategorikan sebagai data sensitif. Kekhawatiran yang muncul adalah, rentan akan menimbulkan permasalahan hukum yaitu sejauh mana bentuk perlindungan penyelenggara jasa kesehatan dalam hal ini Rumah Sakit pada data pribadi pasien yang diakses dengan mudah melalui kemajuan teknologi.

Sebelumnya, setiap aktivitas yang berhubungan dengan identitas pasien dilakukan secara konvensional. Metode tersebut sudah tidak relevan mengingat perkembangan teknologi yang sangat pesat dan jelas tidak praktis dan efisien untuk dilakukan pemrosesan data pasien. Hal ini dapat mengakibatkan penumpukan data pada arsip Rumah Sakit yang dapat menghambat pelayanan kesehatan terhadap pasien dalam waktu yang bersamaan, karena tentu penyimpanan data pasien secara konvensional akan memberi dampak pada penumpukan data.

Sebagai solusi terhadap pernyataan diatas, hadirlah bentuk pelayanan kesehatan yang bernama *e-Health*. Dengan adanya *e-Health*, akan secara mudah menunjang aktivitas seperti pemindahan, pemrosesan dan penyimpanan data pasien secara elektronik yang bertujuan untuk mendukung kegiatan pelayanan kesehatan secara efektif dan meningkatkan kualitas layanan. Akan tetapi, tentu semua hal terdapat kelebihan dan kekurangan. Dibalik kemudahan solusi tersebut, terdapat kekurangan pada *e-Health* itu sendiri. Sebagaimana kita ketahui, *e-Health* berbasis sistem informasi dimana pada sistem tersebut rentan di eksplotasi dan kerentanan pada keamanan sistem,[13] karena data yang terdapat pada suatu sistem merupakan aset berharga yang dapat diperdagangkan. Sehingga, jika data tersebut berhasil diretas maka, akan menimbulkan kerugian atas penyalahgunaan data pribadi.

Data pribadi dengan privasi memiliki hubungan erat yang semakin kesini dianggap hal yang sama. Padahal privasi dan data pribadi merupakan 2 (dua) hal yang berbeda. Perlindungan privasi dan perlindungan data pribadi secara teori memiliki ruang lingkup yang berbeda. Privasi memiliki pengertian dan ruang lingkup yang lebih abstrak dan luas antara lain hak untuk tidak diganggu atau memiliki kendali atas informasi pribadi, apabila perlindungan data pribadi lebih menuju kepada perlindungan secara khusus tentang bagaimana Undang-Undang melindungi dan bagaimana data pribadi tersebut dipergunakan seperti dikumpulkan, diserahkan, disebarluaskan dan lain sebagainya.

Keterkaitan data dengan privasi juga dikarenakan isi yang terdapat di dalam privasi yaitu informasi data pribadi yang rentan disalahgunakan sehingga bersifat sensitif. Karena apabila suatu data mengalami peretasan, maka akan timbul kekhawatiran dan ketakutan bagi pemilik data pribadi atas tersebarnya informasi mereka. Sehingga juga dapat mempengaruhi kebebasan pemilik data pribadi dalam melakukan tindakan tertentu. Perlindungan data pribadi sangat penting dalam menjamin kebebasan dan terhadap penggunaan informasi pribadi seseorang.

[13] Josua Sitompul, *Cyberspace, Cybercrime, Cyberlaw*, (Jakarta: Tatanusa, 2012), Hal.33

Apabila terjadi pelanggaran terhadap data pribadi, berdasarkan hukum positif saat ini dapat mengacu pada Undang-Undang Nomor 11 Tahun 2008 jo. Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE) yang mengatur jika setiap orang yang dilanggar haknya pada penggunaan informasi tentang dirinya melalui media elektronik yang berhubungan dengan data pribadi dapat mengajukan gugatan atas kerugian yang ditimbulkan kepada pihak yang menyelenggarakan sistem elektronik atau teknologi informasi. Pada pengaturan ini sifatnya melarang seseorang dengan memerintahkan agar tidak dilakukan tindakan tersebut.

Korban yang mengalami kerugian atas tindakan peretasan yang tanpa seizin dari korban, dapat dimintakan ganti rugi yang termuat dalam Pasal 26 ayat (1) UU ITE, yaitu setiap penggunaan informasi yang menyangkut data pribadi melalui sistem media elektronik, harus mendapatkan persetujuan dari orang yang tersebut.[14] Kemudian pada Pasal 26 ayat (2) UU ITE juga dijelaskan bagi korban yang haknya dilanggar dapat mengajukan gugatan atas kerugian yang ditimbulkan. Melalui Pasal tersebut sebagai bentuk upaya dalam melindungi penyalahgunaan data pribadi elektronik.

Indikator penggunaan informasi yang berhubungan dengan data pribadi yaitu jika seseorang dengan sengaja dan tanpa hak mengakses informasi dan dokumen elektronik yang bersifat rahasia melalui suatu komputer atau perangkat elektronik miliki orang lain baik yang menyebabkan perubahan atau tidak, menghilangkan, dan menghambat proses transmisi informasi dan dokumen elektronik.

Namun pada UU ITE tersebut, hanya mengupayakan dan memfokuskan melindungi penyalahgunaan data elektronik dan data pribadi elektronik yang bersifat umum. Data pribadi pada sistem non elektronik dan data sensitif tidak tercantum pada UU tersebut. Pengaturan yang lain juga terdapat pada Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan

[14)] Indonesia, *Undang-Undang Nomor 11 Tahun 2008 jo. Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik, (Tambahan Lembaran Negara Republik Indonesia Nomor 5952)*, Pasal 26 ayat (1)

Transaksi Elektronik (PSTE) dan Permenkominfo Nomor 20/2016. Pada kedua aturan tersebut hanya menyangkut data pribadi dalam sistem elektronik saja, dan PSTE merupakan pengaturan lebih lanjut dari beberapa ketentuan dalam UU ITE, serta tidak mengatur secara khusus mengenai perlindungan data pribadi yang bersifat sensitif mengingat kemajuan teknologi yang sangat pesat. Sehingga, hukum positif yang dimiliki saat ini tidak relevan dengan permasalahan dan keresahan masyarakat atas persoalan penyalahgunaan data pribadi.

B. Perlindungan Data Kesehatan Berdasarkan Rancangan Undang-Undang Perlindungan Data Pribadi

Melihat hukum positif yang mengatur terkait Perlindungan Data Pribadi di Indonesia sangat tidak signifikan diatur dan hanya merupakan ketentuan umum serta tidak mampu menjawab persoalan yang banyak terjadi saat ini. Sehingga dapat dikatakan bahwa, pengaturan berkenaan mengenai Perlindungan Data Pribadi di Indonesia masih bersifat umum dan tersebar dalam beberapa peraturan perundang-undangan.

Negara Indonesia sampai saat ini belum mempunyai undang-undang khusus yang mengatur mengenai Perlindungan Data Pribadi secara komprehensif terhadap banyaknya kasus kebocoran data pada masyarakat. Jika ditelaah dari seluruh regulasi atau peraturan perundang-undangan positif yang berlaku di Indonesia, pengaturan terkait Perlindungan Data Pribadi sudah ada, namun tidak komprehensif karena hal ini dapat terlihat dari 30-an (tiga puluhan) peraturan yang secara substansi hanya sedikit menyinggung mengenai perlindungan data pribadi.

Akhir-akhir ini timbul banyak permasalahan di masyarakat terkait penyalahgunaan data pribadi dari tidak adanya payung hukum dan/atau kekosongan hukum yang secara komprehensif mengatur mengenai Perlindungan Data Pribadi. Salah satu masalah yang terjadi, terdapat penyalahgunaan data pribadi masyarakat khususnya konsumen karena ada perpindahan data pribadi kepada pihak ketiga tanpa sepengetahuan dan persetujuan terlebih dahulu.

Dalam hal ini, regulasi atau peraturan perundang-undangan terkait Perlindungan Data Pribadi di Tanah Air dirasa belum cukup menjawab tantangan terhadap Perlindungan Data Pribadi yang begitu besar. Kemudian masyarakat mendesak agar dibentuknya peraturan dalam bentuk Undang-Undang mengenai Perlindungan terhadap Data Pribadi. Sehingga, membuat Pemerintah mulai menyusun RUU Perlindungan Data Pribadi pada tahun 2016 (dua ribu enam belas). Tetapi, hingga saat ini RUU Perlindungan Data Pribadi belum disahkan.

Apabila kita menelaah substansi atau materi dari RUU Perlindungan Data Pribadi, terdapat banyak pengaturan yang baru dan ruang lingkupnya lebih luas jika dibandingkan dengan peraturan yang sudah ada saat ini. Misalnya, pada Pasal 3 RUU Perlindungan Data Pribadi membagi data pribadi menjadi 2 (dua) kategori, yaitu data pribadi yang bersifat umum dan data pribadi yang bersifat spesifik. Pengkategorian seperti ini tidak ditemukan dalam regulasi yang ada saat ini.

Dalam hal ini, kategori data pribadi yang bersifat umum merupakan data yang dapat diperoleh secara umum yang tercantum dalam identitas resmi yang pengungkapannya secara tanpa hak dapat merugikan Pemilik Data Pribadi, misalnya adalah nama lengkap, jenis kelamin, alamat tempat tinggal dan lain sebagainya.[15] Sedangkan, data pribadi yang bersifat spesifik merupakan data pribadi sensitif terhadap kenyamanan dan berpengaruh pada keamanan kehidupan Pemilik Data Pribadi yang dapat diperoleh hanya atas persetujuan Pemilik Data kecuali ditentukan lain dalam Undang-Undang, dan apabila terjadi pengungkapan data ini secara tanpa hak dapat melanggar privasi Pemilik Data Pribadi, misalnya data dan informasi kesehatan, data biometrik, data genetika, dan lain sebagainya.[16]

Jika dikaitkan dengan peraturan yang berlaku di Indonesia saat ini, data pribadi yang bersifat umum yaitu data yang memuat identitas warga negara (nama, tempat tanggal lahir, alamat, jenis kelamin dan lain sebagainya) yang

[15)] Indonesia, *Rancangan Undang-Undang Perlindungan Data Pribadi*, Penjelasan Pasal 3 ayat (2)
[16)] Indonesia, *Rancangan Undang-Undang Perlindungan Data Pribadi*, Penjelasan Pasal 3 ayat (3)

diejawantahkan dalam bentuk KTP. Sedangkan, data pribadi yang bersifat spesifik yaitu data yang dimaksud dalam UUPK, UUK dan UURS yaitu rekam medis seseorang dan segala hal yang diketahui oleh dokter mengenai kesehatan pasiennya. Kemudian, data keuangan milik pribadi yang disimpan dan dirahasiakan oleh Lembaga Perbankan sebagaimana amanat Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan ("UU Perbankan") juga merupakan data pribadi bersifat spesifik.

Munculnya istilah baru dalam RUU Perlindungan Data Pribadi adalah terdapat istilah pengendali data pribadi dan prosesor data pribadi. Pengendali data pribadi adalah pihak yang menentukan tujuan dan melakukan kendali pemrosesan data pribadi. Sedangkan, prosesor data pribadi adalah pihak yang melakukan pemrosesan data pribadi atas nama pengendali data pribadi. Apabila dibandingkan dengan pengaturan dalam Permenkominfo 20/2016, pihak yang melakukan pemrosesan dinamakan dengan istilah Pengguna dan dalam konteks UU Perbankan, pihak yang melakukan pemrosesan adalah lembaga perbankan. Ruang lingkup dalam pemrosesan data pribadi dalam RUU Perlindungan Data Pribadi juga berbeda dibandingkan dalam Permenkominfo 20/2016.

Hal yang ditambah dalam ruang lingkup pemrosesan data pribadi menurut RUU Perlindungan Data Pribadi yaitu perbaikan, pembaruan, transfer, pengungkapan, dan penghapusan. Sedangkan, yang dihilangkan yaitu pengiriman dan pembukaan akses. Penggunaan istilah "transfer" pada RUU Perlindungan Data Pribadi memiliki ruang lingkup yang lebih luas dibandingkan dengan istilah "pengiriman". Dalam penjelasan RUU Perlindungan Data Pribadi dinyatakan transfer adalah perpindahan, pengiriman, dan/atau penggandaan data pribadi baik secara manual maupun elektronik dari pengendali data pribadi kepada pihak lain.

Dengan memperluas istilah "pengiriman" menjadi "transfer" dalam ruang lingkup pemrosesan data, akan memberi dampak baik dan buruk terhadap Perlindungan Data Pribadi, tergantung dari penggunaan atau peruntukannya. Dengan kurangnya "pembukaan akses" dalam ruang lingkup pemrosesan data dalam RUU Perlindungan Data Pribadi, tidak akan berdampak buruk terhadap

Perlindungan Data Pribadi, karena "pembukaan akses" sudah diakui sebagai hak dari Pemilik Data Pribadi sebagaimana tercantum dalam Pasal 6 RUU Perlindungan Data Pribadi yang menyatakan bahwa Pemilik Data Pribadi berhak "mengakses" dan memperoleh salinan data pribadi miliknya.

Pengendali dan prosesor data pribadi meliputi Setiap Orang, Badan Hukum, dan organisasi/institusi. Kewajiban yang dimiliki oleh Pengendali dan prosesor data pribadi lebih luas dibandingkan kewajiban yang dimiliki oleh Pengguna. Kewajiban pengendali data diatur dalam Pasal 23 (dua puluh tiga) sampai dengan Pasal 40 (empat puluh) RUU Perlindungan Data Pribadi. Kewajiban prosesor data pribadi diatur dalam Pasal 41 (empat puluh satu) dan Pasal 42 (empat puluh dua) RUU Perlindungan Data Pribadi. Sedangkan, pada Permenkominfo 20/2016 kewenangan yang dimiliki oleh Pengguna hanya diatur dalam Pasal 27 (dua puluh tujuh).

Dalam hal ini, pihak rumah sakit sebagai pengendali data pribadi dalam melakukan pemrosesan data kesehatan wajib memperoleh persetujuan dari pasien sebagai pemilik data kesehatan, kecuali terdapat pengecualian seperti pemrosesan tersebut dilakukan untuk melindungi pasien dari ancaman terhadap keselamatan nyawa, untuk proses peradilan, diperlukan untuk pelaksanaan perjanjian dengan pasien dan lain sebagainya.

Apabila terdapat perubahan informasi pada saat pemrosesan data kesehatan, maka pihak rumah sakit wajib memberitahukan kepada pasien paling lambat 7 (tujuh) hari setelah terjadinya perubahan informasi. Jika pasien menarik kembali persetujuan pemrosesan data kesehatan, pihak rumah sakit wajib menghentikan pemrosesan dan penghentian pemrosesan data kesehatan dilakukan paling lambat 3 x 24 (tiga kali dua puluh empat) jam terhitung sejak rumah sakit menerima permintaan penarikan kembali persetujuan pemrosesan data kesehatan.

Rumah sakit wajib melakukan penundaan dan pembatasan pemrosesan data kesehatan baik sebagian atau seluruhnya paling lambat 2 x 24 (dua kali dua puluh empat) jam terhitung sejak pihak rumah sakit menerima permintaan

penundaan pembatasan pemrosesan data kesehatan, pembatasan dan penundaan tersebut dikecualikan dalam hal dapat membahayakan keselamatan pihak lain, pasien terikat perjanjian tertulis tidak memungkinkan untuk melakukan pembatasan dan penundaan, dan/atau terdapat peraturan yang tidak memungkinkan untuk dilakukannya pembatasan dan penundaan.

Pihak rumah sakit wajib melindungi dan memastikan keamanan data kesehatan yang diprosesnya. Rumah sakit wajib melakukan pengawasan terhadap setiap pihak yang terlibat dalam pemrosesan data kesehatan di bawah kendali pihak rumah sakit. Rumah sakit juga wajib memastikan perlindungan data kesehatan dari pemrosesan data kesehatan yang tidak sah. Rumah sakit juga berkewajiban untuk mencegah data kesehatan yang diakses secara tidak sah dengan menggunakan sistem keamanan terhadap data kesehatan yang diprosesnya. Selain itu, Pihak rumah sakit juga wajib melakukan perekaman terhadap seluruh kegiatan pemrosesan data kesehatan. Rumah sakit wajib memberikan akses kepada pasien terhadap data kesehatan yang diproses serta rekam jejak pemrosesan data kesehatan paling lambat 3 x 24 (tiga kali dua puluh empat) jam terhitung sejak tanggal diterimanya permintaan akses sesuai dengan jangka waktu penyimpanan data kesehatan.

Disamping pengaturan yang baru, banyak juga ditemukan ketentuan dalam RUU Perlindungan Data Pribadi sejalan dengan peraturan perundang-undangan yang ada saat ini, misalnya seperti pengecualian dalam menjaga kerahasiaan data milik pribadi, pentingnya persetujuan pemilik data pribadi dalam pemrosesan data milik pribadi dan lain sebagainya. Ketentuan pidana yang diatur dalam RUU Perlindungan Data Pribadi juga telah menjangkau praktik-praktik yang selama ini dianggap tidak dapat diakomodir oleh peraturan perundang-undangan pidana yang ada di Indonesia, misalnya jual beli data milik pribadi. Berkaca pada negara lain seperti, Singapura, Malaysia, Amerika dan Eropa sudah memiliki pengaturan khusus yang mengatur terkait perlindungan data pribadi.

Dengan dipositifkannya ketentuan di atas, diharapkan pemberantasan terhadap tindak pidana yang belum dijangkau oleh peraturan hukum pidana Indonesia saat ini dapat terwujud. Kemudian, sebelum RUU Perlindungan Data Pribadi disahkan, akan lebih baik dilakukan sinkronisasi agar Negara Indonesia dapat memiliki peraturan sekelas Undang-Undang yang mengatur secara komprehensif dan khusus terkait perlindungan data pribadi.

III. PENUTUP

A. Kesimpulan

1. Berdasarkan penelitian Penulis, Penulis memberikan kesimpulan bahwa ketiadaan hukum mengenai Perlindungan Data Pribadi menjadi suatu kelemahan dibandingkan negara lain yang sudah memiliki pengaturan khusus terkait Perlindungan Data Pribadi. Sebagai salah satu anggota masyarakat internasional, Indonesia harus menyesuaikan dengan perkembangan negara lain yang sudah lama mengatur masalah mengenai perlindungan data pribadi. Pengaturan terkait perlindungan data pribadi di Indonesia saat ini masih terpisah-pisah dalam berbagai peraturan perundang-undangan dan hanya sedikit substansi yang mengatur terkait hal tersebut. Hingga saat ini, Indonesia belum memiliki Undang-Undang mengenai Perlindungan Data Pribadi secara khusus, dengan berbagai permasalahan dan keresahan masyarakat terkait penyalahgunaan data pribadi oleh pihak ketiga yang tidak bertanggung jawab.
2. Pemerintah Indonesia dituntut untuk melindungi masyarakat dari permasalahan tersebut dengan segera mengesahkan RUU Perlindungan Data Pribadi. Sehingga, harmonisasi dan sinkronisasi pengaturan antara Indonesia dengan negara lain sangat diperlukan demi tercipta suatu kepastian hukum bagi masyarakat yang akan memicu perkembangan dan kemajuan berbagai bidang di Indonesia dan dapat menjawab keresahan masyarakat terhadap praktik-praktik yang ada dalam masyarakat. RUU

Perlindungan Data Pribadi ini jadikan sebagai payung hukum dalam hal Perlindungan Data Pribadi di Indonesia.

B. Saran

Berdasarkan kesimpulan di atas, penulis memberikan saran terkait hal tersebut yakni, sudah sejatinya dokter dan penyedia layanan kesehatan wajib menjaga, melindungi dan bertanggung jawab terhadap data kesehatan milik pasien dari pengungkapan, akses dan penggunaan tanpa persetujuan pasien oleh pihak lain yang tidak berhak atas data tersebut. Penerapan prinsip perlindungan data pribadi belum dilaksanakan secara optimal di Indonesia dan di butuhkan pengaturan yang lebih spesifik dan komprehensif mengatur terkait perlindungan data pribadi guna mengakomodasi segala kebutuhan dan menjawab keresahan masyarakat selama ini pada kasus kebocoran data. Diterapkan kewajiban pengendali dan prosesor data pribadi agar tercipta praktik pemrosesan data yang sebagaimana mestinya.

IV. DAFTAR PUSTAKA

A. Buku

Djafar, Wahyudi dan Asep Komarudin. *Perlindungan Hak Atas Privasi di Internet Beberapa Penjelasan Kunci*. (Jakarta: Elsam, 2014.)

Makarim, Edmond. *Pengantar Hukum Telematika (Suatu Kompilasi Kajian)*. (Jakarta: RajaGrafindo Persada, 2005.)

Makarim, Edmond. *Kompilasi Hukum Telematika*. (Jakarta: PT. Raja Grafindo Persada, 2003.)

RE, Latumahina. *Aspek Hukum Perlindungan Data Pribadi di Dunia Maya*. (Jakarta: Gema Aktualita Vol.3 No.2, 2014.)

Sunggono, Bambang. *Metodologi Penelitian Hukum*. (Jakarta: PT. Raja Grafindo Persada, 2008.)

Sitompul, Josua. *Cyberspace, Cybercrime, Cyberlaw*. (Jakarta: Tatanusa, 2012.)

B. Peraturan Perundang-Undangan

Indonesia. Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.

_____. *Peraturan Menteri Kesehatan Republik Indonesia Nomor 269/MENKES/PER/III/2008 tentang Rekam Medis).*

Indonesia. Undang-Undang Nomor 11 Tahun 2008 jo. Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (Tambahan Lembaran Negara Republik Indonesia Nomor 5952)

Indonesia. Rancangan Undang-Undang Perlindungan Data Pribadi

C. Artikel Jurnal *Online*

Anonim. UDHR ini Berisikan Suatu Daftar Hak-Hak Dasar Manusia Sebagai Suatu Standar Bagi Semua Orang Dan Semua Bangsa.

Greenleaf, Graham. "76 Global Data Protection Laws, Privacy Laws & Business Special Report". Law Article. 2011

H, Cynthia. "Registrasi Data Pribadi Melalui Kartu Prabayar Dalam Perspektif Hak Asasi Manusia". Jurnal HAM. Volume 9 Nomor 2 Tahun 2018

Prosser, William L. "Privacy: A Legal Analysis". California: Law Review 48. 1960

D. Internet

Elnizar, Normand Edwin. "Ini 4 Perbedaan GDPR dan Perlindungan Data Pribadi di Indonesia". Hukumonline Berita. 20 Agustus 2021