

UPAYA HUKUM TERHADAP PELANGGARAN IMPLEMENTASI *INTERNET OF THINGS* (IoT) DI BIDANG PELAYANAN KESEHATAN MENURUT KETENTUAN PERLINDUNGAN DATA PRIBADI

Andrea Sukmadilaga, Sinta Dewi Rosadi

Email: asukmadilaga@gmail.com

Fakultas Hukum, Magister Ilmu Hukum, Universitas Padjadjaran, Indonesia

Abstract

Implementation of Internet of Things (IoT) based applications in the health sector makes it easier for parties, both patients and doctors. In another hand the data collected is a person's health data, which belongs to the realm of privacy, it is necessary to pay close attention to the IoT security system as well as protection and legal remedies that patients can take in seeking justice if the data recorded in the IoT system is leaked and there is abuse. The method used in writing this article is normative juridical research with a statue approach and a conceptual approach. The results of the discussion show that the patient can take legal action by looking at the position and responsibility of each party as stated in the data processing contract so that the lawsuit against the law (Article 1365 of the Civil Code) or criminal charges (UU ITE jo. Law on Public Information Disclosure jo The Medical Practice Law) is not wrongly targeted and right in seeking justice for patients as consumers of health services. Supervision by the government, in this case in the field of technology, information and communication, is that the Ministry of Communication and Information Technology is still not maximal regarding the use of IoT in the health sector as evidenced by the lack of regulations related to IoT.

Keywords: *Internet of Things, Patients, Self Data Protections.*

Abstrak

Implementasi aplikasi berbasis *Internet of Things* (IoT) di bidang kesehatan memudahkan para pihak baik itu pihak pasien maupun dokter tetapi karena data yang dihimpun merupakan data kesehatan seseorang yang termasuk ranah privasi, maka perlu dicermati sistem keamanan IoT serta perlindungan dan upaya hukum yang dapat dilakukan pasien dalam mencari keadilan jika data yang terekam dalam sistem IoT tersebut bocor dan terjadi penyalahgunaan. Metode yang digunakan dalam penulisan artikel ini bersifat penelitian yuridis normatif dengan pendekatan perundang-undangan (*Statue Approach*) dan pendekatan konseptual (*Conceptual Approach*). Hasil pembahasan menunjukkan bahwa Pasien dapat melakukan upaya hukum dengan melihat terlebih dahulu kedudukan dan tanggung jawab masing-masing pihak yang tertuang dalam *data processing contract* sehingga gugatan perbuatan melawan hukum (Pasal 1365 KUHPperdata) ataupun tuntutan pidana (UU ITE jo. UU Keterbukaan Informasi Publik jo. UU Praktik Kedokteran) tidak menjadi salah sasaran dan tepat dalam mencari keadilan bagi Pasien sebagai konsumen jasa layanan kesehatan. Pengawasan oleh pemerintah dalam hal ini yang membidangi teknologi, informasi dan komunikasi adalah Kementerian Komunikasi dan Informatika masih belum maksimal terkait penggunaan IoT dalam sektor kesehatan dengan dibuktikan minimnya aturan-aturan terkait IoT.

Kata Kunci: *Internet of Things*, Pasien, Perlindungan Data Pribadi.

PENDAHULUAN

Perkembangan teknologi informasi di era Revolusi Industri 4.0. semakin menunjukkan kecanggihannya melalui sebuah sistem yang dirancang oleh manusia untuk memudahkan aktivitas dalam kehidupan sehari-hari. Internet yang saat ini digunakan juga merupakan hasil dari perkembangan teknologi yang bertujuan agar manusia dapat mempermudah mobilitas sehari-hari terkait informasi, komunikasi, wawasan, dan kreativitas. Contoh kecil saat ini banyak para Pelaku Usaha yang melakukan bisnisnya tidak lagi secara konvensional seperti memerlukan kantor, ruko dan sebagainya tetapi cukup membuat *website* penjualan secara mandiri tanpa harus mengeluarkan modal yang cukup besar untuk menyewa atau membeli lahan sebagai tempat usaha. Hal ini semakin mendorong gairah kreativitas pelaku usaha sehingga bermunculan *online marketplace* sebagai wadah yang memudahkan transaksi antara penjual dan pembeli tanpa harus tatap muka.

Awal mula internet hadir pada pertengahan abad 19 yang dikembangkan oleh Departemen Pertahanan Amerika ARPANET dalam rangka riset untuk keperluan militer. Saat itu internet hanya terdiri dari beberapa jaringan hingga sampai saat ini telah berkembang pesat menjadi ribuan jaringan yang dimana seluruh negara terhubung dalam internet untuk mempermudah

mobilitas dalam berbagai aspek, salah satunya kesehatan. Perkembangan inilah yang melahirkan teknologi *Internet of Things (IoT)* yang menjadi isu hangat saat ini.

IoT merupakan sebuah konsep untuk memperluas manfaat dari konektivitas internet yang tersambung secara terus menerus. Adapun kemampuan seperti berbagi data, *remote control*, dan sebagainya, termasuk juga pada benda di dunia nyata (Sri Ariyanti, et. al. 2016. hlm. 2). Implementasi IoT dalam kehidupan sehari-hari telah nampak terutama dalam bidang pelayanan kesehatan. Dalam bidang pelayanan kesehatan, keberadaan IoT menjadi sangat penting dalam rangka mempercepat pelayanan kesehatan sehingga menjadi lebih efisien terutama dalam pemantauan kondisi kesehatan pasien. Dinamika yang terjadi inilah menimbulkan perubahan dan kebiasaan baru pada masyarakat sehingga diperlukan formulasi yang membatasi hal tersebut agar masyarakat tetap dalam koridor tanpa keluar dari norma yang berlaku yakni hukum.

Implementasi IoT dalam pelayanan di bidang kesehatan memang memudahkan para pihak baik itu pihak pasien maupun dokter tetapi karena data yang dihimpun merupakan data kesehatan seseorang, maka perlu dicermati sistem keamanan IoT dan perlindungan bagi data pasien ataupun seseorang yang telah terekam data kesehatannya oleh

fitur IoT karena data yang berhubungan dengan kesehatan seseorang dikatakan ‘sensitif’ bilamana merujuk pada Uni Eropa *Directive* yang membedakan antara data ‘sensitif’ dan ‘non-sensitif’ berdasarkan tingkat bahaya yang akan dirasakan kepada individu jika terjadi akses oleh pihak yang tidak bertanggungjawab sistem dari IoT tersebut harus sesuai dengan standarisasi yang telah ditetapkan demi mencegah terjadinya kebocoran ataupun pemrosesan data secara illegal sehingga hal ini tentu merugikan pihak yang datanya terekam dalam IoT.

Privasi dan data pribadi menjadi sebuah hal yang penting karena pengguna dalam jaringan tidak akan melakukan sebuah transaksi digital apabila merasa keamanan akan privasi dan data pribadinya terancam. Salah satu perlindungan privasi dan data pribadi tersebut berkenaan bagaimana data pribadi tersebut akan diproses termasuk data sensitif dari pengguna yang apabila disebarkan ke pihak yang tidak bertanggung jawab akan berpotensi menimbulkan kerugian finansial, bahkan mengancam keamanan dan keselamatan pemiliknya (Sinta Dewi Rosadi, et. al. 2018).

Dalam Pasal 57 ayat (1) Undang-Undang Nomor 36 Tahun 2009 Tentang Kesehatan jo. Pasal 17 huruf h angka 2 Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik yang

pada intinya mengatur bahwa setiap orang berhak atas rahasia kondisi kesehatan pribadinya yang telah dikemukakan kepada penyelenggara pelayanan kesehatan dan setiap badan publik wajib membuka akses bagi setiap pemohon informasi publik untuk mendapatkan informasi publik, kecuali, salah satunya, mengenai riwayat, kondisi dan perawatan, pengobatan kesehatan fisik, dan psikis seseorang, karena bila dibuka dan diberikan kepada pemohon informasi publik dapat mengungkapkan rahasia pribadi.

Berdasarkan Pasal 38 ayat (1) dan (2) Undang-Undang Nomor 44 Tahun 2009 Tentang Rumah Sakit bahwa setiap rumah sakit harus menyimpan rahasia kedokteran, yang hanya dapat dibuka untuk kepentingan kesehatan pasien, untuk pemenuhan permintaan aparat penegak hukum dalam rangka penegakan hukum, atas persetujuan pasien sendiri, atau berdasarkan ketentuan peraturan perundang-undangan.

Tanggung jawab hukum jika terjadi kegagalan sistem pada IoT ataupun terdapat penyalahgunaan Data pasien masih dikatakan belum jelas sehingga memerlukan kajian yang komprehensif untuk menelaah siapa saja pihak yang dapat dimintai pertanggungjawaban secara hukum. Dalam peraturan perundang-undangan terkait layanan kesehatan, memang telah tegas tercantum sanksi-sanksi bagi siapa saja yang

melakukan penyalahgunaan data Pasien tetapi karena lahirnya IoT sebagai hasil dari perkembangan teknologi informasi, menjadi sebuah tantangan bagaimana jika terjadi permasalahan hukum dan mendapatkan preskripsi yang dapat dinilai adil oleh para pihak jika di kemudian hari merasa dirugikan.

Dalam hal ini, tentu menjadi tugas baru bagi pemerintah bagaimana memberikan jaminan keamanan terhadap pelaksanaan dan keamanan IoT dalam bidang kesehatan mengingat Data tersebut sangat sensitif sebagaimana dalam Undang-Undang Dasar Negara Republik Indonesia pada Pasal 28 G ayat (1) Undang-Undang Dasar Tahun 1945 yang menyatakan bahwa setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang dibawah kekuasaannya, serta berhak atas rasa aman dan perlindungan diri dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi.

Berdasarkan pada latar belakang tersebut, permasalahan hukum yang akan dibahas dalam artikel ini adalah sebagai berikut:

1. Bagaimana upaya hukum yang dapat dilakukan terhadap penyalahgunaan dan pelanggaran data pasien yang terekam dalam sistem IoT (*Internet of Things*)?
2. Bagaimana seharusnya peran pemerintah dalam pengawasan penggunaan *Internet of Things* (IoT)

dalam jasa layanan kesehatan dikaitkan dengan ketentuan perlindungan data pribadi?

METODE PENELITIAN

Penulisan artikel ini akan membahas tanggung jawab hukum jika terjadi penyalahgunaan dan pelanggaran data pasien yang terekam dalam sistem IoT (*Internet of Things*) dan peran pemerintah dalam pengawasan penggunaan IoT dalam jasa layanan kesehatan dikaitkan dengan ketentuan Perlindungan Data Pribadi demi meminimalisir risiko dalam penggunaan IoT pada bidang kesehatan. Metode yang digunakan penulis dalam penelitian ini adalah penelitian yuridis normatif.. Penelitian yuridis normatif adalah penelitian yang dilakukan dengan mengacu pada norma hukum yang terdapat pada peraturan perundang-undangan dan putusan pengadilan serta norma-norma yang berlaku di masyarakat atau juga yang menyangkut kebiasaan yang berlaku di masyarakat (Soerjono Soekanto, et. al. 1979. hlm. 18). Mengingat pada penelitian ini menggunakan tipe penelitian normatif dengan menggunakan pendekatan Yuridis Normatif, maka pendekatan yang digunakan dalam penelitian ini adalah pendekatan perundang-undangan (*Statue Approach*) dan pendekatan konseptual (*Conceptual Approach*). Pendekatan ini digunakan untuk memberikan konklusi hasil penelitian.

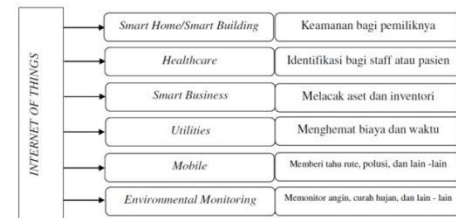
HASIL PENELITIAN DAN PEMBAHASAN

A. *Internet of Things* (IoT) di Bidang Layanan Kesehatan: Tinjauan Teoritis dan Yuridis Berdasarkan Ketentuan Perlindungan Data Pribadi di Indonesia dan EU GDPR

Mendefinisikan *Internet of Things* (IoT) dapat menjadi tantangan karena kompleksitas teknis dan konseptualnya. Pada dasarnya, IoT adalah fenomena yang ditemukan di jaringan objek, dihubungkan oleh *tag* atau *microchip*, yang mengirim data ke sistem penerima. IoT mencakup setiap koneksi di antara objek; oleh karena itu IoT memiliki sistem mesin-ke-mesin (M2M) yang mengkomunikasikan data dan informasi *real-time* (Nicola Fabiano. hlm. 201).

Internet of Things (IoT) adalah sebuah konsep yang menggunakan internet sebagai jaringan infrastruktur utama yang mengkoneksikan objek-objek tertentu (Daniele Miorandi, et. al. 2012. hlm. 1497). Dalam hal ini IoT juga bisa diartikan internet yang menghubungkan antar *things*, dimana *things* disini berarti informasi seperti meta data (Bari, Mani, & Berkovich, 2013). Pengaplikasian dari IoT bisa diklasifikasikan menjadi berbagai macam kegunaan yang bisa dilihat di gambar 1.1 (Mohsen Hallaj Asghar, et. al. 2015).

Gambar 1.1 Contoh pengaplikasian IoT



Sumber: Principle Application and Vision in Internet of Things (Hallaj Asghar, Mohammadzadeh, & Negi, 2015)

Sensor dalam IoT dapat mengumpulkan informasi yang bahkan lebih sensitif, seperti: langkah-langkah yang diambil, kualitas tidur, suhu kulit, pola pernapasan, dan detak jantung, hanya untuk beberapa nama. karena perangkat ini mengandung sensor pengukuran multi-segi yang rumit seperti giroskop dan akselerometer, bahkan informasi yang lebih sensitif dapat diambil dari kombinasi output data mentah melalui sensor-fusion. Sebagai contoh, para peneliti telah menemukan bahwa keadaan emosi atau mental dapat diturunkan dari data tersebut. Data tersebut bahkan dapat digunakan untuk memprediksi perilaku dan menyimpulkan kebiasaan pribadi (Lidiya Mishchenko. 2016. hlm. 96). Suatu data adalah data pribadi apabila data tersebut berhubungan dengan seseorang, sehingga dapat digunakan untuk mengidentifikasi orang tersebut, yaitu pemilik data (European Union Agency for Fundamental Rights and Council of Europe. 2014. hlm. 36).

Dalam sektor kesehatan bila dilihat dari kecanggihannya dan kegunaannya, sistem IoT sangat bermanfaat bagi petugas medis maupun pasien rumah sakit itu sendiri dalam rangka pemberian preskripsi pengobatan ataupun langkah preventif agar penyakit dari pasien tersebut tidak semakin parah dengan merekam data dari pasien tersebut. Adapun model komunikasi IoT terdiri dari (Karen Rose, et. al. 2015. hlm. 18-23):

1. *Device to Device Communications*

Merupakan dua atau lebih perangkat yang terhubung secara langsung dan berkomunikasi antara yang satu dengan yang lain, bukan melalui server aplikasi sementara. Perangkat ini berkomunikasi melalui berbagai jenis jaringan, termasuk jaringan IP atau internet.

2. *Device to Cloud Communications*

Perangkat IoT terhubung secara langsung ke layanan cloud pada internet seperti penyedia layanan aplikasi untuk bertukar data dan mengontrol trafik.

3. *Device to Gateway Model / Device to Application Layer Gateway*

Menghubungkan perangkat IoT ke layanan ALG sebagai saluran untuk mencapai cloud. Dalam istilah sederhana, ada aplikasi

software yang beroperasi pada perangkat *gateway local*.

4. *Back to End Data Sharing Model*
Merupakan arsitektur komunikasi yang memungkinkan pengguna untuk mengirimkan dan menganalisis objek data dari layanan *cloud* yang terkombinasi dengan data sumber lain.

IoT untuk sektor kesehatan di Indonesia saat ini sudah diterapkan oleh Kementerian Kesehatan, yaitu *telemedicine* sejak tahun 2012 dengan tujuan meningkatkan akses dan layanan kesehatan masyarakat khususnya daerah rural, dimana akses antara puskesmas atau Rumah Sakit kelas D jauh dari Rumah Sakit rujukan. *Telemedicine* ini menggunakan model *Device to Application Layer Gateway* dalam memantau atau merekam kondisi kesehatan Pasien (Sri Ariyanti, et. al. 2016. hlm. 7-9).

Dalam *General Data Protection Regulation* (GDPR), Semua data pribadi didefinisikan sebagai setiap informasi yang berkaitan dengan orang yang diidentifikasi atau dapat diidentifikasi, harus dikumpulkan sesuai dengan Pasal 5 GDPR, yang berarti data harus:

1. Dikumpulkan untuk tujuan yang ditentukan, sah dan eksplisit dan tidak diproses dengan cara yang tidak sesuai dengannya.
2. Diproses secara sah, adil dan transparan.

3. Diproses untuk memastikan keamanan data yang tepat, adil, relevan dan terbatas pada apa yang diperlukan dalam kaitannya dengan tujuan yang diproses.
4. Akurat dan *up to date*.
5. Disimpan dalam bentuk yang memungkinkan identifikasi subyek data tidak lebih lama dari yang diperlukan untuk tujuan yang diproses.
6. Dikendalikan oleh pengontrol yang bertanggung jawab atas data dan mampu menunjukkan kepatuhan.

Mengingat data kesehatan seseorang dikategorikan sebagai data yang sensitif, tentu perlindungan dan kepastian hukum terhadap data tersebut harus secara jelas dan tegas siapa saja yang harus bertanggung jawab bilamana terjadi kegagalan sistem dari IoT tersebut entah karena adanya tindakan illegal ataupun kelalaian dari pengontrol. Jangan sampai perkembangan teknologi dengan adanya *Internet of Things* yang telah diciptakan dan digunakan menjadi bumerang bagi masyarakat sendiri dan menimbulkan banyak kerugian akibat tidak dilandaskan dengan ketentuan Hukum yang jelas dan tegas agar dapat mengatur, mengawasi, dan melindungi hak-hak terkait data pribadi dan privasi masyarakat.

Hal ini sejalan dengan Teori Hukum Pembangunan yang diungkapkan Prof. Mochtar Kusumaatmadja bahwa Hukum yakni

segenap asas dan kaidah yang berfungsi mengatur anggota masyarakat dalam pergaulan hidupnya serta memelihara ketertiban dalam kelompok masyarakat tersebut. Hukum juga meliputi berbagai proses serta lembaga yang diberdayakan untuk mewujudkan keberlakuan kaidah sebagai sebuah fakta yang tidak dapat dibantah dalam masyarakat (Mochtar Kusumaatmadja. 2002. hlm. 14).

Pasien dalam hal ini dapat dikategorikan sebagai konsumen dari jasa layanan yang disediakan oleh Rumah Sakit sehingga Undang-Undang Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen (UUPK) dapat dijadikan sebagai *umbrella act* sebagai upaya pemenuhan hak-hak yang harus didapatkan oleh Pasien dan kewajiban Rumah Sakit sebagai Penyelenggara Jasa Layanan Kesehatan bagi masyarakat. Pasal 4 UUPK hak-hak konsumen yakni:

1. Hak atas kenyamanan, keamanan, dan keselamatan dalam mengonsumsi barang dan/atau jasa.
2. Hak untuk memilih barang dan/atau jasa serta mendapatkan barang dan/atau jasa tersebut sesuai dengan nilai tukar dan kondisi jaminan yang dijanjikan.
3. Hak atas informasi yang benar, jelas, dan jujur mengenai kondisi dan jaminan barang dan/atau jasa.
4. Hak untuk didengar pendapat dan keluhannya atas barang dan/atau jasa yang digunakan.

5. Hak untuk mendapatkan advokasi, perlindungan konsumen, dan upaya penyelesaian sengketa perlindungan konsumen secara patut.
6. Hak untuk mendapat pembinaan dan pendidikan konsumen.
7. Hak untuk diperlakukan atau dilayani secara benar dan jujur serta tidak diskriminatif.
8. Hak untuk mendapatkan kompensasi, ganti rugi, dan/atau penggantian jika barang dan/atau jasa yang diterima tidak sesuai dengan perjanjian dan tidak sebagaimana mestinya.

Secara umum, perlindungan data pasien telah diatur dalam Undang-Undang Nomor 44 Tahun 2009 Tentang Rumah Sakit pada Pasal 32 pada butir (i) yang berisi hak-hak pasien termasuk hak mendapatkan privasi dan kerahasiaan penyakit yang diderita beserta data-data medisnya. Dinyatakan pula di dalam Undang-Undang Nomor 29 Tahun 2004 Tentang Praktik Kedokteran pada Pasal 48, yaitu :

1. Setiap dokter atau dokter gigi dalam melaksanakan praktik kedokteran wajib menyimpan rahasia kedokteran;
2. Rahasia kedokteran dapat dibuka hanya untuk kepentingan kesehatan pasien, memenuhi permintaan aparaturnya penegak hukum dalam rangka penegakkan hukum, permintaan pasien sendiri, atau berdasarkan ketentuan perundang-undangan.

Data kesehatan pasien hanya diperuntukkan dan diperbolehkan dibuka hanya kepada seseorang yang berlaku sebagai pasien itu sendiri ataupun penanggung jawab pasien dalam rangka upaya medis lanjutan yang akan dilakukan. Prof. Veronica Komalawati mengungkapkan terkait persetujuan tindakan kedokteran yaitu suatu kesepakatan/persetujuan pasien atas upaya medis yang akan dilakukan terhadap dirinya, setelah mendapat informasi dari dokter mengenai upaya medis yang dapat menolong dirinya disertai informasi mengenai segala risiko yang mungkin terjadi (Indah Susilowati, et. al. 2018).

Kewajiban kerahasiaan data Pasien juga dituangkan dalam bentuk Peraturan Menteri Kesehatan Nomor 36 Tahun 2012 Tentang Rahasia Kedokteran pada Pasal 3 yang menyatakan bahwa informasi identitas pasien, informasi hasil anamnesis, pemeriksaan fisik atau tindakan kedokteran lainnya merupakan informasi medis yang harus dijaga.

B. Upaya Hukum Terhadap Penyalahgunaan dan Pelanggaran Data Pasien yang Terekam Dalam Sistem IoT (*Internet Of Things*)

Dalam Undang-Undang Undang-Undang Nomor 44 Tahun 2009 Tentang Rumah Sakit pada Pasal 32 huruf i dan q bahwa pasien berhak mendapatkan privasi dan kerahasiaan penyakit yang diderita termasuk data-data medisnya serta pasien

mempunyai hak untuk menggugat dan/atau menuntut Rumah Sakit apabila Rumah Sakit diduga memberikan pelayanan yang tidak sesuai dengan standar baik secara perdata ataupun pidana. Pendapat Warren dan Brandeis dalam karyanya yang berjudul “The Right to Privacy” menyatakan bahwa privasi adalah hak untuk menikmati kehidupan dan hak untuk dihargai perasaan dan pikirannya. Lebih lanjut, dalam Pasal 46 menyatakan bahwa Rumah Sakit bertanggung jawab secara hukum terhadap semua kerugian yang ditimbulkan atas kelalaian yang dilakukan oleh tenaga kesehatan di Rumah Sakit (Sinta Dewi Rosadi. 2015. hlm. 12).

Walaupun sudah diatur secara jelas, tetapi dalam konteks penggunaan aplikasi berbasis IoT, ada pihak lain yang sesungguhnya dapat dimintai pertanggung jawaban sehingga tidak hanya Rumah Sakit semata yang bertanggung jawab secara penuh karena mengingat masalah ini ada kaitannya dengan pemanfaatan teknologi. Dalam rangka melakukan upaya hukum terhadap penyalahgunaan dan pelanggaran data pasien yang terekam dalam sistem IoT untuk meminta pertanggung jawaban secara hukum demi mencari keadilan bagi pasien atau pihak yang merasa dirugikan, harus terlebih dahulu mencermati apakah pihak yang diduga melakukan penyalahgunaan dan pelanggaran data dapat dikatakan sebagai subjek

hukum yang harus bertanggung jawab atas tindakan ataupun kelalaian yang mengakibatkan sistem keamanan dalam IoT menjadi lemah sehingga Data pasien dalam hal ini mudah dan berpotensi menyebar atau tidak.

Dalam GDPR, subjek hukum yang harus di atur terbagi menjadi 2 (dua) yakni Pengontrol Data Pribadi/ *Controller* dan Pemroses Data Pribadi/ *Processor*. *Controller* adalah orang atau badan hukum, otoritas publik, swasta atau badan lain yang secara mandiri atau bersama-sama dengan orang lain, menentukan tujuan dan sarana pengolahan data. Sedangkan *processor* adalah orang atau badan hukum, otoritas publik, swasta atau badan lain yang memproses data pribadi atas nama pengontrol. Dengan demikian, keberadaan *processor* tergantung pada keputusan yang diambil oleh *controller* yang dapat memproses data dalam organisasinya (misal melalui karyawan sendiri) atau mendelegasikan semua atau sebagian dari kegiatan pemrosesan ke organisasi eksternal.

Dikaitkan dengan penggunaan aplikasi pemantauan kesehatan berbasis IoT, Rumah Sakit dalam hal ini merupakan pengontrol data yang merupakan penentu arah kebijakan dalam menentukan tujuan dan sarana pengolahan data, tetapi Rumah Sakit belum tentu berlaku sebagai Pemroses data karena bisa saja Rumah Sakit sebagai pengontrol

mendelegasikan pemrosesan data tersebut kepada pihak eksternal bukan internal Rumah sakit itu sendiri (misal kepada suatu Divisi Penyimpanan dan Pengolahan Data) atau dalam hal ini perusahaan swasta yang bergerak dalam teknologi informasi yang telah bekerja sama dengan Rumah Sakit.

Oleh karena dalam GDPR dan peraturan perundang-undangan di Indonesia yang tidak mengatur secara eksplisit mengenai perbadaan dan tanggung jawab hukum antara *controller* dengan *processor*, penulis lebih mencermati dan mengarahkan upaya hukum dengan terlebih dahulu memperhatikan atau mengetahui isi dari perjanjian atau yang dikenal dengan *data processing contract* yang telah disepakati antara *controller* dengan *processor* untuk dapat melakukan langkah dan upaya hukum yang tepat.

Ketika sudah mengetahui bagaimana kedudukan dan tanggung jawab para pihak dalam perjanjian tersebut, maka mekanisme yang dapat dilakukan yaitu dengan gugatan perbuatan melawan hukum (*onrechtmatige daad*) atau dengan tuntutan pidana dengan pembuktian yang meyakinkan bahwa terjadinya penyalahgunaan data, kegagalan sistem yang mengakibatkan kebocoran data tidak terjadi karena keadaan memaksa/*force majeure*, kesalahan dan atau kelalaian pihak pengguna sistem elektronik sebagaimana dalam Pasal 15 ayat (3)

Undang-Undang Nomor. Nomor 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik (UU ITE).

Pasal 1365 Kitab Undang-Undang Hukum Perdata (KUHPerdata) jo. Pasal 26 UU ITE menyatakan bahwa setiap perbuatan yang melanggar hukum dan membawa kerugian kepada orang lain, mewajibkan orang yang menimbulkan kerugian itu karena kesalahannya untuk menggantikan kerugian tersebut. maka jelas siapapun baik *naturalijk persoon* atau *rechtspersoon* dapat dimintai pertanggung jawaban berupa ganti kerugian yang sesuai atas kesalahan dan kelalaian dalam menjaga dan mengelola data kesehatan pasien melalui gugatan melawan hukum melalui jalur litigasi ataupun non-litigasi.

Terkait perlindungan data kesehatan pasien dalam bentuk Dokumen Elektronik atau Informasi Elektronik, Pasal 32 UU ITE mengatur tentang larangan bagi setiap Orang untuk melakukan interferensi (mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan) terhadap bentuk Dokumen Elektronik atau Informasi Elektronik tanpa hak dan dengan cara melawan hukum. Ancaman hukuman atas perbuatan tersebut diatur dalam Pasal 48 UU ITE yang berbunyi:

- (1) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32 ayat (1) dipidana dengan pidana penjara paling

lama 8 (delapan) tahun dan/atau denda paling banyak Rp2.000.000.000,00 (dua miliar rupiah).

(2) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32 ayat (2) dipidana dengan pidana penjara paling lama 9 (sembilan) tahun dan/atau denda paling banyak Rp3.000.000.000,00 (tiga miliar rupiah).

(3) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32 ayat (3) dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp5.000.000.000,00 (lima miliar rupiah).

Dari kedua upaya hukum yang dapat dilakukan oleh pasien, penyelesaian secara perdata melalui gugatan perbuatan melawan hukum lebih tepat digunakan terlebih dahulu dalam perkara penyalahgunaan data yang terekam dalam aplikasi atau sarana berbasis IoT karena melibatkan Rumah Sakit sebagai badan usaha yang menyelenggarakan pelayanan kesehatan perorangan secara paripurna yang menyediakan pelayanan rawat inap, rawat jalan, dan gawat darurat karena didalamnya terdapat struktur organisasi yang sama dengan perusahaan sebagaimana yang tersirat dalam Pasal 2 Peraturan Presiden Republik Indonesia Nomor 77 Tahun 2015

Tentang Pedoman Organisasi Rumah Sakit dan adanya kemungkinan keterlibatan perusahaan swasta yang bekerja sama yang tertuang dalam *data processing contract*.

C. Peran Pemerintah Dalam Pengawasan Penggunaan *Internet Of Things* (Iot) Dalam Jasa Layanan Kesehatan Dikaitkan Dengan Ketentuan Perlindungan Data Pribadi

Perkembangan teknologi dan informasi yang terjadi baik itu dalam pengembangan aplikasi berbasis IoT ataupun kecanggihan teknologi lainnya harus diikuti dengan pengaturan dan pengawasan yang ketat dari pemerintah. Dalam tingkat ekonomi global, Indonesia dinilai sebagai negara dengan posisi strategis dalam perdagangan internasional, termasuk transaksi elektronik yang memungkinkan terjadinya persebaran data pribadi yang semakin luas (Heppy Endah Palupy. 2011. hlm. 35). Namun pada kenyataannya, Indonesia merupakan salah satu negara di ASEAN yang masih belum memiliki kebijakan atau regulasi yang secara khusus mengenai perlindungan data pribadi (Yoga Hastyadi Widiartanto. 2015).

Meskipun Indonesia belum memiliki peraturan *lex specialis* yang mengatur tentang perlindungan data pribadi, tetapi jaminan perlindungan akan hak privasi termuat dalam konstitusi Indonesia, yaitu Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 (UUD 1945),

khususnya Pasal 28 G yang menyatakan bahwa setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang dibawah kekuasaannya, serta berhak atas rasa aman dan perlindungan diri dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi (Wahyudi Djafar, et. al. 2016. hlm. 29). Rancangan Undang-Undang Perlindungan Data Pribadi (RUU PDP) yang diharapkan menjadi *umbrella act* terkait perlindungan data pribadi sampai saat ini pun belum disahkan.

Penggunaan IoT pada sektor layanan kesehatan tidak hanya berdampak positif tetapi juga memiliki potensi negatif bilamana tidak memperhatikan aspek perlindungan hukum bagi pasien dan langkah preventif guna meminimalisir kejahatan terhadap data ataupun kebocoran data sehingga melanggar privasi seseorang dari pemerintah. Berdasarkan JRC *Conference and Workshop Reports* oleh *European Commission*, telah mengidentifikasi 4 (empat) tantangan utama yang akan muncul bagi pemerintah dari penerapan IoT yaitu (Marisa Ponti, et. al. 2019. hlm. 4-5):

1. IoT dapat secara radikal mengubah hubungan antara manusia dan perangkat yang saling berhubungan, memberikan otonomi objek kepada manusia. Untuk mencegah terwujudnya dari risiko ini,

intervensi pemerintah diperlukan untuk mengatasi dan mengatur IoT dengan pengaturan standarisasi dan etika dalam penggunaannya.

2. Regulasi yang dikeluarkan harus memperhatikan aspek keadilan antara hak dan kewajiban konsumen, berorientasi pada perkembangan teknologi, dan menghasilkan nilai publik. Jangan sampai adanya regulasi tersebut menghambat bisnis atau layanan berbasis IoT dari Perusahaan ataupun Institusi yang berdampak pada perekonomian.

3. Regulasi yang dikeluarkan tidak boleh menghambat inovasi-inovasi yang dilakukan oleh perusahaan yang mengembangkan aplikasi berbasis IoT dikemudian hari.

4. Faktanya, walaupun tingginya potensi kebocoran dan penyalahgunaan data pribadi tetapi penggunaan IoT merupakan hal yang sangat positif untuk memecahkan masalah sosial terutama dalam bidang kesehatan. Maka diperlukan sosialisasi untuk mendapatkan aspirasi baik dari kalangan intelektual ataupun rakyat biasa demi penyempurnaan aturan yang dapat diimplementasikan dengan baik.

Pengaturan standarisasi teknis alat dan perangkat untuk IoT telah diatur dalam Peraturan Menteri Kominfo Nomor 35 Tahun 2015 Tentang Persyaratan Teknis Alat dan Perangkat Telekomunikasi Jarak Dekat, tetapi hanya berupa penjelasan komponen-komponen apa saja yang

diwajibkan untuk digunakan, yang artinya belum adanya regulasi yang cukup jelas terkait implementasi IoT baik itu dalam bidang kesehatan ataupun bidang lainnya.

Disamping dipercepatnya pengesahan Rancangan Undang-Undang Perlindungan Data Pribadi (RUU PDP), diperlukan suatu politik hukum yang komprehensif disertai kajian-kajian yang masif untuk mengeluarkan produk hukum berkualitas yang mencakup persyaratan standarisasi komponen-komponen dari penggunaan IoT secara jelas sebagai langkah preventif yang dapat dilakukan mengingat kecanggihan IoT jika tidak diatur secara komprehensif dikhawatirkan menjadi bumerang bagi masyarakat.

Pengawasan oleh Pemerintah dalam hal ini yang membidangi teknologi informasi dan komunikasi yakni Kementerian Komunikasi dan Informatika harus lebih diperketat terkait penggunaan aplikasi berbasis IoT disektor kesehatan dengan mengeluarkan peraturan menteri kominfo terkait hal tersebut ataupun melalui Undang-Undang agar lebih mempertegas urgensi daripada penggunaan IoT. Legislatur dalam hal ini bertindak sebagai seorang seniman yang diamanatkan oleh rakyat untuk membuat Undang-Undang harus melakukan pendekatan secara futuristik yang memiliki kandungan nilai progresif dalam proses pembuatannya sehingga

Undang-Undang yang lahir dapat selalu mengikuti perkembangan teknologi informasi dan komunikasi.

PENUTUP

A. Kesimpulan

a. Upaya hukum yang dilakukan yaitu melihat terlebih dahulu perjanjian antara *controller* dengan *processor* yang tertuang dalam *data processing contract* yang telah disepakati untuk mengetahui kedudukan dan tanggung jawab masing-masing pihak dalam perjanjian tersebut sehingga gugatan perbuatan melawan hukum (Pasal 1365 KUHPerdara) ataupun tuntutan pidana (UU ITE jo. UU Keterbukaan Informasi Publik jo. UU Praktik Kedokteran) tidak menjadi salah sasaran dan tepat dalam mencari keadilan bagi Pasien sebagai konsumen jasa layanan kesehatan.

b. Pengawasan oleh pemerintah dalam hal ini yang membidangi teknologi, informasi dan komunikasi adalah Kementerian Komunikasi dan Informatika masih belum maksimal terkait penggunaan IoT dalam sektor kesehatan dengan dibuktikan minimnya aturan-aturan terkait IoT.

B. Saran

a. Dari kedua upaya hukum yang dapat dilakukan oleh pasien, penyelesaian secara perdata melalui gugatan perbuatan melawan hukum lebih tepat digunakan terlebih dahulu

dalam perkara penyalahgunaan data yang terekam dalam aplikasi atau sarana berbasis IoT karena melibatkan Rumah Sakit sebagai badan usaha dan kemungkinan keterlibatan perusahaan swasta yang bekerja sama yang tertuang dalam *data processing contract*.

b. Peran Pemerintah dalam pengawasan penggunaan IoT dalam sektor kesehatan perlu ditingkatkan dengan mengeluarkan peraturan yang terkait hal tersebut ataupun legislator dapat membuat undang-undang yang memperhatikan aspek pendekatan futuristik sehingga produk hukum yang dihasilkan berkualitas dan progresif. Mendorong untuk segera melakukan pengesahan RUU PDP agar menjadi *umbrella act* ataupun *lex specialis* dalam upaya perlindungan data pribadi tetapi jika dimungkinkan dengan mempertimbangkan perkembangan IoT, dapat dilakukan evaluasi kembali terhadap RUU PDP untuk memperjelas pengawasan dan standarisasi dari penggunaan IoT. Menetapkan standarisasi dan legalitas *Data Protection Officer* untuk ditempatkan disetiap Rumah Sakit yang menggunakan aplikasi berbasis IoT melalui peraturan perundang-undangan.

DAFTAR PUSTAKA

Peraturan Perundang-Undangan:

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.

Kitab Undang-Undang Hukum Perdata.

Undang-Undang Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen.

Undang-Undang Nomor 29 Tahun 2004 Tentang Praktik Kedokteran.

Undang-Undang Nomor 14 Tahun 2008 Tentang Keterbukaan Informasi Publik.

Undang-Undang Nomor 36 Tahun 2009 Tentang Kesehatan.

Undang-Undang Nomor 44 Tahun 2009 Tentang Rumah Sakit.

Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik.

Peraturan Menteri Kesehatan Nomor 36 Tahun 2012 Tentang Rahasia Kedokteran.

Peraturan Menteri Kominfo Nomor 35 Tahun 2015 Tentang Persyaratan Teknis Alat dan Perangkat Telekomunikasi Jarak Dekat.

Peraturan Presiden Republik Indonesia Nomor 77 Tahun 2015 Tentang Pedoman Organisasi Rumah Sakit.

Peraturan Pemerintah (PP) Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

Buku:

- Ariyanti, Sri *et al.* 2016. *Implementasi Internet of Things Untuk Sektor Kesehatan*. Jakarta. Badan Penelitian dan Pengembangan Sumber Daya Manusia Kementerian Komunikasi dan Informatika Republik Indonesia.
- Djafar, Wahyudi. *et al.* 2016. *Perlindungan Data Pribadi di Indonesia (Usulan Pelembagaan Kebijakan dari Perspektif Hak Asasi Manusia)*. ELSAM.
- European Union Agency for Fundamental Rights and Council of Europe. 2014. *Handbook on European Data Protection Law*. Belgium.
- Kusumaatmadja, Mochtar. 2002. *Konsep-Konsep Hukum Dalam Pembangunan (Kumpulan Karya Tulis)*. Bandung. Alumni.
- Rosadi, Sinta Dewi. 2015. *Aspek Perlindungan Data Pribadi Menurut Hukum Internasional, Regional dan Nasional*. Bandung. Refika.
- Rose, Karen. *et al.* 2015. *The Internet Of Things: An Overview Understanding The Issues And Challenges Of A More Connected World*. Internet Society.
- Soekanto, Soerjono *et al.* 1979. *Peranan dan Penggunaan Kepustakaan di Dalam Penelitian Hukum*. Jakarta. Pusat Dokumen Universitas Indonesia.
- Voigt, Paul, *et al.* 2017. *The EU General Data Protection Regulation (GDPR) A Practical Guide*. Cham. Springer International.
- Jurnal atau Artikel Ilmiah:**
- Fabiano, Nicola. "Internet of Things and the Legal Issues related to the Data Protection Law according to the new European General Data Protection Regulation". *Athens Journal of Law*. Volume 3. Issue 3. 2017.
- Miorandi, Daniele *et al.* "Internet of Things: Vision, Applications and Research Challenges". *Elsevier Journal*. Volume 10. Issue 7. September 2012.
- Mishchenko, Lidiya. "The Internet of Things: Where Privacy and Copyright Collide". *Santa Clara High Technology Journal*. Volume 33. Issue 1. Juni 2016.
- Rosadi, Sinta Dewi Rosadi, *et al.* "Perlindungan Privasi Dan Data Pribadi Dalam Era Ekonomi Digital Di Indonesia". *Jurnal Veritas et Justitia*. Volume 4. Nomor 1. 24 Juni 2018.
- Susilowati, Indah, *et al.* "Perlindungan Hukum Terhadap Hak Privasi dan Data Medis Pasien di Rumah

Sakit X Surabaya”. *Jurnal Wiyata*. Volume 5. Nomor 1. Tahun 2018.

Widiartanto, Yoga Hastyadi
Widiartanto. “Indonesia Belum
Punya UU Perlindungan
Data Pribadi”. *Kompas*. 17
Februari 2015.

Hasil Penelitian atau Tugas Akhir:

Palupy, Heppy Endah. *Privacy and
Data Protection: Indonesia
Legal Framework*. Tesis
Program Master Law and
Technology di Universiteit van
Tilburg, Tilburg 2011.

Makalah:

Asghar, Mohsen Hallaj, *et al.*
“Principle Application and
Vision in Internet of
Things (IoT)”. *International
Conference Reports*. Noida,
India 2015.

Ponti, Marisa, *et al.* “Internet of
Things: Implications for
Governance”. *JRC Conference
and Workshop Reports*.,
Ljubljana, Slovenia., May 13th
and 14th, 2019.

Artikel Majalah atau Koran:

Widiartanto, Yoga Hastyadi
Widiartanto. “Indonesia Belum
Punya UU Perlindungan Data
Pribadi”. *Kompas*. 17 Februari
2015