DATA PRIVASI DALAM BIDANG KESEHATAN DI INDONESIA: ANTARA PERLINDUNGAN DAN IMPLEMENTASINYA

Oleh: Moody Rizqy Syailendra
Universitas Padjajaran
Jalan Dipati Ukur Nomor 35 Bandung

ABSTRAK

Kemajuan teknologi di era modern telah merambat ke segala bidang kehidupan. Kini, segala pekerjaan manusia menjadi lebih mudah akibat bantuan teknologi. Manusia meninggalkan metode konvensional yang kurang efektif dan efisien dan berpaling kepada sistem teknologi informasi dan komunikasi yang memudahkan pekerjaan mereka. Salah satu bidang yang terkena imbas perubahan ini adalah bidang pelayanan kesehatan. Kini, bidang tersebut menjadi lebih efektif dan efisien dalam melayani pasien dengan adanya teknologi *E-Health*. Akan tetapi dibalik segala kemudahan yang diberikan terdapat potensi gangguan yang dapat menimbulkan kerugian, baik kepada penyedia layanan kesehatan, maupun pasien sendiri. Ketentuan hukum yang spesifik dan komprehensif dibutuhkan untuk mengakomodasi segala kepentingan terkait dengan perlindungan data pribadi utamanya dalam bidang *E-Health*.

Kata Kunci: Perlindungan Data Pribadi.

ABSTRACT

Advances in technology in modern era has spread into all areas of life. This day, human doing their job easily due to the help of technology. Since then, human left conventional work methods which is less effective and efficient and turn into information and communication technology that provide them an easier work method. One of the field that has been affected by this change is the health care. With the advanced technology, E-Health, this field now has become more effective and efficient in serving patients. However, even with those advances provided by E-Health, there still potential thread that may cause harm, either to the healthcare provider, or the patients themselves. In order to establishing those threads, a specific and comprehend regulations is needed to accommodate all interest relating to the personal data protection, particularly in E-Health field.

Keywords: Personal Data Protection.

A. LATAR BELAKANG

Perkembangan Teknologi di era modern ini sangatlah pesat dan jauh berbeda dengan masa awal kehadirannya. Era globalisasi telah menempatkan teknologi informasi dan komunikasi kepada sebuah posisi yang strategis di mana ia dapat menciptakan suatu dunia tanpa ruang, batas, dan waktu serta mampu meningkatkan produktivitas dan efisiensi dalam bidang kehidupan manusia sehari-hari. Teknologi informasi dan komunikasi pula telah menyebabkan adanya perubahan di masyarakat yang juga mengakibatkan berubahnya sistem sosial budaya, ekonomi, dan kerangka hukum secara signifikan.

Perkembangan teknologi ini kini telah merambah ke berbagai bidang kehidupan. Berbagai macam teknologi baru dibuat guna menciptakan efisiensi dan efektivitas dalam membantu berbagai kegiatan manusia. Dengan adanya perkembangan teknologi, pekerjaan manusia yang dikerjakan dengan tangan, kini sudah tidak memerlukan lagi tenaga manusia yang digantikan oleh proses komputasi yang lebih efektif dan efisien.

Salah satu bidang kehidupan strategis yang tersentuh perkembangan teknologi adalah bidang kesehatan. Bidang ini merupakan salah satu yang paling penting dan sangat dibutuhkan bagi rakyat Indonesia, sehingga pemerintah perlu memberikan perhatian lebih dalam pengembangannya. Salah satu yang menjadi permasalahan besar adalah proses administrasi pasien yang memakan waktu lama. Hal ini menyebabkan pasien tidak mendapatkan penanganan secara cepat yang menyebabkan penumpukan pasien di rumah sakit dan fasilitas kesehatan lainnya. Pasien yang akan berobat akan diregistrasi ke dalam arsip rumah sakit. Kemudian pasien dibuatkan sebuah kartu yang menjadi bukti registrasi dan telah masuknya data pasien ke dalam arsip rumah sakit. Data registrasi ini lah yang selanjutnya dikenal dengan rekam medik. Rekam medis adalah berkas yang berisikan catatan dan dokumen tentang identitas pasien, pemeriksaan, pengobatan, tindakan dan pelayanan lain yang telah diberikan kepada pasien.[1] Dengan adanya ratusan, bahkan ribuan pasien yang berobat ke rumah sakit, dapat dibayangkan berapa banyak rekam medis yang masuk ke arsip rumah sakit. Apabila rumah sakit masih menggunakan metode konvesional berupa pencatatan dalam kartu, tentunya akan ada penumpukkan data pada arsip rumah sakit. Jelas hal ini tidak efisien dan membutuhkan banyak waktu untuk memproses data pasien. Di sisi lain, satu rekam medis dapat berisi berbagai macam rekam medis yang berbeda-beda. Tentunya keadaan seperti ini tidaklah efektif dan menghambat pelayanan kesehatan terhadap pasien yang pada waktu yang bersamaan membutuhkan penangan yang cepat. Hal ini juga diperparah dengan belum terintegrasinya koordinasi antara satu bagian dengan bagian lainnya (misalnya antara bagian administrasi dengan bagian pemeriksaan) di dalam rumah sakit. Sehingga, dapat dikatakan bahwa pelayanan medis masih belum efektif dan dilaksanakan dengan baik.

Untuk mengatasi masalah ini, dibuatlah suatu metode baru yang terintegerasi dengan TIK, yang dikenal sebagai *e-health*. *E-Health* merupakan suatu bentuk layanan kesehatan secara elektronis yang mempunyai tujuan mendukung kegiatan kesehatan secara umum dan meningkatkan kualitas layanan. Sistem ini merupakan perkembangan dari sistem CPR *(Computerized Patient Record)* atau catatan pasien berbasis komputer yang dikembangkan oleh *Institute of Medicine* (IOM) pada tahun 1991. Sistem ini dilatar belakangi oleh kebutuhan masyarakat akan akses layanan kesehatan yang praktis dan efisien. Salah satu program yang dimiliki *e-health* adalah registrasi dan rekam medis elektronik. Dengan adanya teknologi ini, tidak diperlukan waktu yang lama untuk meregistrasi dan memproses data-data milik pasien. Semua data yang masuk akan disimpan di dalam sebuah *server* yang teriintegrasi dengan seluruh bagian rumah sakit. Integrasi sistem informasi merupakan konsep utama dari penerapan manajemen sistem informasi, sehingga sistem yang ada pada setiap bagian saling terhubung dan saling mendukung satu sama lain untuk mengoptimalkan kinerja masing-masing bagian.[2] Dengan adanya sistem ini pelaksanaan kegiatan seperti registrasi pasien dapat berjalan dengan lebih efisien dan terjangkau.

Namun dibalik kemudahan yang diberikan, terdapat kekurangan dari sebuah sistem informasi. Di mana sistem tersebut dapat diekspolitasi sehingga dapat merugikan masyarakat, yang dalam hal ini adalah pasien-pasien dari rumah sakit yang telah mengadaptasi sistem ini. Terdapat kemungkinan data pribadi yang dimiliki oleh para pasien dalam bentuk rekam medis elektronik dapat diakses oleh orang

[1] Peraturan Menteri Kesehatan Republik Indonesia Nomor 269/MENKES/PER/III/2008.
[2] Pengenalan Produk MIRSA http://www.bvk.co.id/produk diakses pada 30 Januari 2016.

yang mampu melakukannya. Orang yang mampu melakukannya dalam hal ini, dikenal dengan sebutan *hacker* atau peretas. *Hacker* atau peretas adalah sebutan untuk orang atau sekelompok orang yang berkecimpung pada dunia jaringan dan sistem informasi. Terdapat banyak *hacker* yang memanfaatkan kelemahan suatu sistem dengan niat jahat untuk keuntungan pribadi. Perbuatan ini dikenal dengan *cybercrimes*. *Cybercrimes* adalah melaksanakan niat jahat melalui berbagai macam perbuatan.[3]

Berdasarkan fakta-fakta tersebut, dapat kita katakan bahwa *E-Health* merupakan sebuah solusi guna tercapainya pelayanan kesehatan yang optimal. Namun di sisi lain terdapat juga permasalahan di dalamnya. Permasalahan pertama adalah terkait dengan tanggung jawab penyedia layanan terhadap data pasien yang mereka simpan. Kemudian berkaitan dengan kewajiban terkait dengan pelanggaran privasi, adakah kewajiban yang harus dilakukan penyedia layanan, misalnya ganti rugi apabila terjadi pelanggaran privasi dan kebocoran data kepada para pasien. Selain itu adalah berkenaan dengan upaya yang dapat dilakukan apabila terjadi peretasan data pada pusat data.

Tentunya penyedia layanan akan mengupayakan berbagai hal untuk mencegah peretasan dan kebocoran data. Akan tetapi, apabila peretasan terjadi dan data pribadi milik para pasien bocor, dapatkah pasien menuntut ganti rugi kepada penyelenggara layanan? Permasalahan selanjutnya adalah terkait dengan akses yang dilakukan pihak ketiga. Penyedia layanan ini dapat memberikan beberapa hak istimewa kepada pihak lain (pihak ketiga), di mana pihak ketiga dapat mengakses kepada data yang dimiliki pasien yang berada di pusat data. Penyedia layanan haruslah mengungkapkan identitas dari pihak tersebut (apabila ada) kepada pasien atau pengguna layanannya. Pihak ketiga di sini dapat berupa otoritas hukum (penyidik kepolisian dan lainnya) atau karyawan dari penyedia layanan tersebut. Pengguna layanan harus diinformasikan terlebih dahulu mengenai hal ini sebelum pengguna menggunakan layanan ini. Terkait dengan masalah ini, penyedia layanan dapat lebih hati-hati dalam menjaga data pribadi dari pengguna layanannya.

Untuk itu, dalam pemanfaatan TIK, perlu diperhatikan lagi hal-hal yang berkaitan dengan keamanan dan kepastian hukum. Agar dapat mengatasi gangguan terkait dengan masalah keamanan dalam penyelenggaran sistem TIK, pendekatan hukum adalah mutlak karena tanpa adanya kepastian hukum, persoalan terkait dengan pemanfaatan TIK menjadi tidak optimal.[4]

Berkaitan dengan hal tersebut, Indonesia sendiri telah memiliki aturan yang tersirat mengenai perlindungan data pribadi di Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. Namun, yang perlu dijadikan kajian adalah mengenai kredibilitas undang-undang ini dalam mengakomodasi segala permasalahan terkait dengan perlindungan data pribadi, khususnya pada program *E Health*.

B. PEMBAHASAN

1. Tinjauan Terhadap Perlindungan Data

Dewasa ini, informasi adalah sebuah media yang sangat menentukan bagi perkembangan sebuah negara.[5] Informasi mengenai individu selalu dikelola oleh pemerintah dan swasta, namun dengan adanya kemajuan dalam bidang teknologi, munculah ancaman yang dapat menimbulkan kerugian dari individu tersebut sebagai akibat dari adanya ketidaktelitian dan kebocoran data yang memuat privasi seseorang. Era digital telah memicu

---

3 *Ibid*, hlm. 36

4 Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, Penjelasan Umum.

55 Shinta Dewi, *Perlindungan Privasi Atas Informasi Pribadi Dalam E-Commerce Menurut Hukum Internasional*, Bandung: Widya Padjajaran, 2009, hlm 53.

pertumbuhan data pribadi yang dibuat, disimpan dan ditransmisikan pada komputer dan perangkat *mobile*, *broadband* dan situs internet dan media.[6] Selain itu, kemajuan teknologi juga menyebabkan timbulnya ancaman serius bagi privasi pribadi dan keamanan informasi.

Pada konsep hukum telematika, data adalah representasi formal suatu konsep, fakta, atau instruksi. Dalam penggunaan sehari-hari data dapat berarti suatu pernyataan yang diterima secara apa adanya. Data adalah bentuk jamak *datum*, Bahasa latin yang berarti "sesuatu yang diberikan". Data adalah setiap informasi yang diproses melalui peralatan yang berfungsi secara otomatis menanggapi instruksi-instruksi yang diberikan bagi tujuannya dan disimpan dengan maksud untuk dapat diproses. Data merupakan bahan baku dari informasi yang selanjutnya informasi merupakan makna data itu bagi manusia.[7] Data merupakan sekumpulan fakta kasar yang masih perlu di olah agar memiliki makna, basisnya pada teknologi. Pasal 1 ayat (1) *Data Protection Act* Inggris mendefiniskan data sebagai informasi yang diproses melalui peralatan yang berfungsi secara otomatis menanggapi instruksi-instruksi dengan tujuan untuk disimpan dan dapat diproses.

Data, bahan baku informasi, didefinisikan sebagai kelompok teratur simbol-simbol yang mewakili kuantitas, tindakan, benda, dan sebagainya. Data terbentuk dari karakter yang dapat berupa alphabet, angka, maupun simbol khusus. Data disusun dan kemudian diolah menjadi bentuk struktur data, struktur *file*, dan *database.*[8] Sedangkan, data pribadi menurut Pasal 1 ayat (1) *Data Protection Act* Inggris adalah data yang berhubungan dengan seorang individu yang hidup dan dapat diidentifikasikan dari data atau dari data-data atau informasi yang dimiliki atau akan dimiliki oleh *data controller*.

Data pribadi terdiri dari fakta, komunikasi atau pendapat yang berkaitan dengan individunya. Sehingga dapat dikatakan data pribadi merupakan informasi yang sangat pribadi dan sensitif sehingga individu yang bersangkutan ingin menyimpan atau membatasi orang lain terhadap data tersebut untuk mengoleksi, menggunakan, atau menyebarkannya kepada pihak lain. Jerry Kang mengatakan bahwa data pribadi menggambarkan suatu informasi yang erat kaitannya dengan seseorang yang akan membedakan karakteristik masing-masing individu.[9] Sehingga pada dasaranya, bentuk perlindungan terhadap data dibagi menjadi dua kategori, yakni perlindungan data berupa pengamanan terhadap fisik data, baik data yang kasat mata dan tidak. Bentuk lainnya adalah adanya regulasi yang mengatur tentang penggunaan data oleh orang lain yang tidak berhak, penyalahgunaan data untuk kepentingan tertentu, dan perusakan terhadap data itu sendiri.

Keamanan Serta Kerahasiaan Data Dalam Teknologi Informasi

Dengan adanya perkembangan di bidang Teknologi Informasi, data menjadi sebuah komoditi yang eksklusif. Perlindungan terkait data menjadi viral, sehingga tindakan-tindakan pencegahan atas perusakan data dan informasi perlu mendapat pemikiran perlindungannya. Hal ini kemudian menjadi isu yang sangat penting dan berkembang terus seiring dengan pesatnya perkembangan di bidang Teknologi Informasi.

---

6 Cameron G. Shilling, "Privacy and Data Security: New Challenges of The Digital Age", *New Hampshire Bar Journal* (2011). hlm 1.

7 Purwanto, *Penelitian Tentang Perlindungan Hukum Data Digital*, Jakarta: Badan Pembinaan Hukum Nasional, 2007, hlm. 13.

8 Purwanto. *Ibid*. hlm 14.

9 Jerry Kang, "Information Privacy in Cyberspace Transaction", *Stanford Law ReviewVol 50*. (April 1998), hlm 5.

Berbagai permasalahan terkait dengan keamanan sistem menjadi suatu garapan yang membutuhkan biaya besar terkait penanganan dan pengamanannya. Sistem vital seperti, sistem pertahanan, perbankan, dan sistem lain setingkat itu membutuhkan tingkat keamanan yang tinggi, dan juga membutuhkan biaya yang sangat banyak. Hal ini disebabkan oleh konsep *open system* yang menyebabkan siapapun, di manapun, dan kapanpun memiliki kesempatan untuk mengakses hal-hal tersebut.

Dalam sistem komputer, untuk menjaga keamanan dan kerahasiaan data diperlukan bermacam jenis enkripsi[10] agar data tidak dapat dibaca atau dimengerti oleh sembarang orang kecuali orang yang berhak dan orang-orang yang memiliki kepentingan terkait dengan sistem tersebut. Pengamanan data tersebut selain bertujuan untuk meningkatkan keamanan data, juga berfungsi untuk melindungi data agar tidak dapat dibaca oleh orang yang tidak berhak dan mencegah agar orang-orang tersebut tidak menyisipkan atau menghapus data.[11]

Masalah keamanan dan kerahasiaan data merupakan salah satu aspek paling penting dari sebuah sistem informasi. Hal ini berkaitan erat dengan betapa pentingnya informasi tersebut dikirim dan diterima oleh orang yang berhak dan berkepentingan. Informasi menjadi tidak berguna apabila di tengah perjalanannya dibajak atau disadap oleh orang yang tidak bertanggung jawab. Oleh karenanya, pengamanan dalam sistem informasi menjadi sangat viral sejak pertama kali sebuah sistem diciptakan. Tanpa adanya keamanan yang baik, secanggih apapun sistem informasi akan menjadi tidak bermanfaat bagi manusia.[12]

Dengan adanya hubungan antara sebuah sistem informasi dengan internet, maka munculah peluang terjadinya kejahatan dan perilaku menyimpang yang dilakukan di dalam jaringan komputer. Hal ini merupakan tantangan bagi para penegak hukum di seluruh dunia untuk mencegah adanya kejahatan dalam dunia *cyber*. Saat ini, berbagai negara dari belahan dunia mulai memberikan perhatian lebih dalam bidang ini dengan membuat landasan hukum bagi internet. Terkait dengan masalah yang terjadi dan perlunya pengamanan terhadap data dalam sistem komputer, yang tidak hanya mencakup pengaturan mengenai keamanan fisik, tetapi juga berkaitan dengan keamanan akses, kemanan *file* dan data, keamanan jaringan, serta hal lainnya yang berkaitan dengan pengamanan di dalam dunia dan data, keamanan jaringan, serta hal lainnya yang berkaitan dengan pengamanan di dalam dunia *cyber*.[13] Ancaman yang paling signifikan di sini bukanlah ancaman yang berupa fisik, namun lebih ke dalam ancaman yang bersifat non-fisik, yaitu[14] *intruder* dan *malicious program.*[15]

---

[10] Enkripsi adalah sebuah proses yang melakukan perubahan sebuah kode dari yang bias dimengerti menjadi sebuah kode yang tidak bisa dimengerti atau tidak terbaca. Enkripsi dapat diartikan sebagai kode atau *chipper*. Enkripsi digunakan untuk menyandikan data-data atau informasi sehingga tidak dapat dibaca oleh orang yang tidak berhak. Dengan enkripsi data anda disandikan (*encrypted*) dengan menggunakan sebuah kunci (*key*). Untuk membuka (decrypt) data tersebut digunakan juga sebuah kunci yang dapat sama dengan kunci untuk mengenkripsi (untuk kasus *private key cryptography*) atau dengan kunci yang berbeda (untuk kasus *public key cryptography*).

[11] Purwanto, *Penelitian Tentang Perlindungan Hukum Data Digital*, Jakarta: Badan Pembinaan Hukum Nasional, 2007. *Op Cit*, hlm. 56.

[12] G.A Barger, *"Lost in Cyberspace: Inventors, Computer Piracy and Printed Publications under Section 102 (b) of the Patent Act of 1994",* (Detroit : Mercy L. Rev), hlm. 353.

[13] Purwanto*, Penelitian Tentang Perlindungan Hukum Data Digital*, Jakarta: Badan Pembinaan Hukum Nasional, 2007. *Op. Cit,* hlm. 49.

[14] *Ibid*, hlm 50.

[15] Malicious Program termasuk virus komputer, worm, trojan, spyware dan program lain yang dibuat secara khusus untuk memata-matai lalu lintas jaringan, merekam komunikasi pribadi menjalankan perintah yang

Tinjauan Mengenai *E-Health dan Permasalahannya*

E-Health merupakan sistem informasi yang memiliki susunan luas yang mengintegrasikan data dari berbagai sumber, mengumpulkan data pada titik pelayanan, mendukung pemberi pelayanan dalam pengambilan keputusan. Sebagai suatu sistem layanan kesehatan, di beberapa negara yang sedang dalam masa transisi dari *paper-based* menuju *computer+based record*, setiap praktik keperawatan per *shift* dilibatkan dalam dokumentasi *E-Health*. Melalui *E-Health*, perawat yang memberikan perawatan langsung pada pasien mempunyai akses yang baik dengan riwayat kesehatan pasien yang dihubungkan dengan *computeri-edstandard care plans.* Hal yang berkait dengan keperawatan secara khusus disebut *nursing informatics*, yang merupakan inti dari dokumentasi keperawatan berbasis komputer (Dahm M.F., et.al, Androwich dalam *Petrovskaya* et.al, 2009).

E-Health pada dasarnya merupakan sistem pelayanan kesehatan yang berbasis teknologi informasi dan telekomunikasi (TIK) dengan tujuan memberikan layanan kesehatan yang cepat dan efektif kepada pasien. Sebagai layanan aplikasi medis, manfaat e-*health* mencakup tiga aspek yang saling terkait, yaitu pasien, rumah sakit, dan dokter. Manfaat langsung bagi pasien adalah percepatan akses pasien ke pusat-pusat rujukan, mendapatkan pertolongan pertama sambil menunggu pertolongan langsung dari dokter pribadi, pasien merasakan tetap dekat dengan rumah di mana kerabat dapat memberikan dukungan, serta menyeleksi pasien yang perlu rawat inap dan yang tidak. Manfaat bagi rumah sakit adalah jaminan pelayanan berkualitas (*service quality assurance*) bagi publik dengan sistem operasional manajemen rumah sakit yang terotomasi. Sedangkan bagi dokter (atau paramedis) adalah percepatan transformasi informasi sehingga memudahkan dalam pengambilan keputusan serta kedekatan dengan pasien yang tak terbatas.

E-health diterapkan dalam aplikasi sektoral, regional, maupun nasional. Aplikasi sektoral hanya terbatas untuk satu subdisiplin ilmu kedokteran atau bidang layanan kesehatan. Aplikasi regional mencakup keseluruhan bidang layanan kesehatan terbatas pada wilayah tertentu dalam suatu negara. Sedangkan aplikasi nasional mencakup seluruh bidang layanan kesehatan di seluruh wilayah suatu negara.[16]

Permasalahan Keamanan Data Pada *E-Health*

Terdapat berbagai macam potensi ancaman yang dapat menimbulkan kerugian bagi pasien *E-Health* dan pihak penyedia layanan yang menyimpan data-data milik pasien, di antaranya: *hardware* atau komponen komputer yang dicuri atau rusak, program terkait dimodifikasi, data yang tersimpan di dalam server dihapus atau dicuri, serta jaringan komunikasi yang diputus atau dimodifikasi.

Selain itu terdapat pula ancaman lain yang sangat berbahaya dan tentunya merugikan bagi pasien dan penyedia layanan, seperti:

1. Data *Error* dan Kesalahan Data

   Dalam pengolahan data sering kali ditemukan adanya kesalahan dalam input atau memasukkan data. Hal ini bisa diakibatkan oleh berbagai faktor, di mana salah satunya adalah *Human Error.* Selain itu data yang terdapat di dalam server dapat mengalami *Error* atau *Corrupt* akibat dari virus atau malware yang baik sengaja ataupun tidak masuk dan menginfeksi server tersebut. Virus komputer adalah program komputer yang masuk ke dalam sistem untuk melakukan sesuatu, misalnya menginterupsi proses yang

tidak sah, mencuri dan mendistribusikan informasi pribadi dan rahasia, menonaktifkan komputer, menghapus file, dll.

[16] *Ibid,* hlm. 119.

sedang berjalan di CPU, memperlambat kinerja komputer, memenuhi memori komputer sehingga kegiatan CPU berhenti, memenuhi hard-disk, menghapus file-file, merusak sistem operasi, dan sebagainya.

Virus komputer juga merupakan hasil karya seorang programmer yang punya niat jahat atau hanya untuk memuaskan nafsu programmingnya yang berhasil menyusupkan virus ke dalam sistem komputer orang lain. Virus menyusup masuk ke dalam sistem komputer melalui berbagai cara, antara lain:

a. Pertukaran file, misalnya mengambil file *(copy & paste)* dari komputer lain yang telah tertular virus.
b. *E-mail*, membaca *e-mail* dari sumber yang tidak dikenal bisa berisiko tertular virus, karena virus telah ditambahkan *(attach)* ke file *e-mail*.
c. IRC, saluran *chatting* bisa dijadikan jalan bagi virus untuk masuk ke komputer

2. Pencurian Data

Dalam dunia jaringan baik yang bersifat lokal (intranet) maupun yang bersifat universal (internet) perlu kita sadari bahwa ada saja kemungkinan sistem komputer mendapat ancaman dari pihak yang tidak bertanggung jawab. Pihak yang dimasuksud di sini diklasifikasikan menjadi dua kelompok, yaitu: *Hacker,* merupakan orang-orang yang dapat dikategorikan sebagai programmer yang pandai dan senang mengutak-utik sesuatu yang dirasakan sebagai penghalang terhadap apa yang ingin dicapainya. Bagi seorang *hacker* perlindungan terhadap sistem komputer adalah tantangan, mereka akan mencari cara bagaimana bisa menembus *password*, *firewall*, *access-key* dan sebagainya. Walau demikian *hacker* bisa dibedakan atas dua golongan, golongan putih *(white hat)* dan golongan hitam *(black hat)*.[17]

Cracker, merupakan orang-orang yang menembus pertahanan keamanan sistem komputer hanya untuk merusak, mencari keuntungan pribadi dan merugikan pemilik sistem komputer. *Hacker* golongan hitam sebenarnya bisa dikategorikan sebagai *cracker*. *Hacker* dan *Cracker* keduanya tetap melakukan tindakan yang melanggar aturan yaitu menembus pertahanan keamanan sistem komputer karena tidak mendapat hak akses.

Secara praktis sistem *E-Health* memberikan berbagai macam keuntungan dalam pelayanan kesehatan. Namun tidak dapat dipungkiri jika dibalik segala kemudahan dan keuntungan yang diberikan sistem ini, tersimpan berbagai potensi ancaman yang dapat menimbulkan kerugian, baik terhadap pasien yang data pribadinya disimpan, maupun pihak yang menyediakan layanan. Oleh karenanya, penyedia layanan wajib memberikan proteksi dan jaminan terhadap keamanan data pasien. Pemerintah juga haruslah memberikan peranan dengan memberikan regulasi terkait dengan permasalahan ini.

Prinsip Perlindungan Data Pribadi

Abu Bakar Munir, mantan Dekan Universitas Malaya, mengungkapkan beberapa prinsip utama dalam perlindungan data pribadi,[18] di mana prinsip tersebut menjadi landasan dibentuknya *Personal Data Protection Act 2010* di Malaysia. Prinsip-prinsip itu adalah:

---

[17] *Hacker* dengan kategori *white hat* pada umumnya dipekerjakan oleh pembuat sistem/*programmer* informasi sebagai pemeriksa apabila sistem tersebut sudah memiliki pengamanan yang baik. Mereka bertugas memasuki dan mencari berbagai celah yang dapat dimasuki, yang kemudian melaporkannya kepada pembuat sistem informasi guna meningkatkan keamanan sistem tersebut.

[18] Abu Bakar Munir, 2002, *Privacy and Data Protection: A Comparative Analysis with Special Reference to Malaysian Proposed Law*, Sweet and Maxwell Asia, Malaysia.

1. *General Principle*, Data Pribadi seseorang tidak dapat diambil tanpa persetujuan orang yang bersangkutan. Pengumpulan data yang akan diproses harus memadai dan tidak berlebihan; untuk tujuan yang sah, dengan persetujuan dari individu yang terkait (Pemberian data kepada pihak lain harus berdasarkan persetujuan);
2. *Notice and Choice*, pemilik data harus mengetahui tujuan pengumpulan data pribadi miliknya;
3. *Disclosure*, Prinsip ini mengatur mengenai tujuan pengumpulan data. Pengumpulan data tersebut harus spesifik. Artinya, data yang diperoleh tidak boleh digunakan untuk tujuan lain, kecuali pemilik data menyetujui si pemegang data untuk menggunakannya ke pihak lain.
4. *Security*, pengguna data diharuskan mengambil langkah-langkah yang perlu guna menjaga keamanan data tersebut. Pihak penyimpan data wajib melindungi dengan metode apapun dari kehilangan, kepalsuan, serta akses ilegal, terhadap data yang disimpan;
5. *Retention*, Prinsip ini mengatur mengenai jangka waktu suatu data dapat dimusnahkan. Jika data tersebut sudah digunakan sesuai dengan tujuannya, data tersebut harus segera dimusnahkan.[19]
6. *Integrity*, data pribadi haruslah akurat, lengkap, terkini, dan tidak mem-bingungkan.
7. *Access,* pemilik data asli harus memberikan otoritas kepada pihak penyimpan data untuk memproses data pribadinya.

Latar belakang dirumuskannya prinsip-prinsip perlindungan data ini adalah faktor keamanan. Dengan adanya perkembangan di masyarakat, maka meningkat pula *awareness* (kesadaran) masyarakat akan keamanan data yang dimilikinya dari pihak-pihak yang tidak bertanggung jawab. Selain yang dirumuskan oleh Prof. Abu Bakar Munir tersebut, terdapat *General Principles* lain yang diterapkan pada perlindungan data pribadi di Inggris, *"Data Protection Act"*, yang mencakup:[20]

"The "Data Protection Act" controls how your personal information is used by organisations, businesses or the government. Everyone responsible for using data has to follow strict rules called "data protection principles". They must make sure the information is:

1. *used fairly, lawfully, and in particular, shall not be processed unless-*
   - *at least one of the conditions in Schedule 2 is met, and*
   - *in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.*
2. *used for limited, specifically stated purposes. Personal data shall be only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes;*
3. *used in a way that is adequate, relevant, and not exesive. Personal data shall be adequate, relevantm and not excesive in relation to the purpose or purposes for which they are processed;*
4. *accurate. Personal data shall be accurate and, where necessary, kept up to date;*
5. *kept no longer than is absolutely necessary. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purposes or those purposes;*
6. *handled according to people's data protection rights. Personal data shall be processed in accordance*

[19] Prinsip Perlindungan Data Pribadi ala Malaysia http://www.hukumonline.com/berita/baca/lt511644c55a2fc/enam-prinsip-perlindungan-data-pribadi-ala-malaysia Diakses 3 Juni 2016.

[20] Data Protection https://www.gov.uk/data-protection/the-data-protection-act Diakses 15 Juni 2016.

with the rights of data subjects under this act;

7. *kept safe and secure. Appropriate technical and organisational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage, to, personal data;*
8. *not transferred outside the European Economic Area without adequate protection. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subject in relation to the processing of personal data."*

Kasus Terkait Rekam Medis Bocor

1. Kasus Pembocoran Rekam Medis Pasien di Kragan

Bapak Hasyim merupakan pasien di Puskesmas Kragan II yang telah meninggal dunia setelah menerima perawatan dari Puskesmas tersebut. Saat masih hidup, bapak Hasyim sempat meminjam uang di Pemodalan Nasional Madani (PNM) Karangharjo, Kec. Kragan, sekaligus terdaftar dalam sebuah asuransi. Polis asuransi tersebut mengatakan jika peminjam uang meniggal dunia, maka asuransi yang akan melunasi hutangnya.[21]

Masalah timbul ketika putra almarhum, Nanghadi akan mengklaim asuransi milik ayahnya, pihak asuransi menolak membayarkan pelunasan hutang yang dimiliki ayahnya kepada PNM Karangharjo. Pihak asuransi berdalih bahwa ayah Nanghadi (bapak Hasyim) meninggal dunia akibat penyakit diabetes mellitus, sehingga polis asuransi tidak dapat diklaim. Pihak asuransi juga melampirkan rekam medis milik ayahnya sebagai bukti.

Sontak hal tersebut mengejutkan pihak keluarga, karena bagaimana mungkin rekam medis yang bersifat rahasia bisa dimiliki oleh pihak asuransi. Nanghadi mempertanyakan mengapa begitu mudahnya Puskesmas Kragan II menyerahkan rekam medis milik ayahnya kepada pihak asuransi. Padahal menurut ketentuan Pasal 47 ayat (2) Undang-Undang Nomor 29 tentang Praktik Kedokteran dikatakan bahwa:

> "Rekam medis sebagaimana dimaksud pada ayat (1) harus disimpan dan dijaga kerahasiannya oleh dokter atau dokter gigi dan pimpinan sarana pelayanan kesehatan."

Pihak Puskesmas dengan jelas telah melanggar ketentuan di dalam pasal ini apabila terbukti memberikan rekam medis milik pasiennya tanpa persetujuan pasien kepada pihak lain yang tidak memiliki kewenangan untuk mengakses data tersebut. Penyelidikan lebih lanjut masih dilakukan dikarenakan ada dugaan keterlibatan oknum yang sengaja membocorkan rekam medis milik pasien guna keuntungan pribadi. Jika terbukti, pihak penyedia sarana layanan kesehatan diancam dengan hukuman pidana Pasal 79 butir c Undang-Undang Praktik Kedokteran, yang berbunyi:

> "Dipidana dengan pidana kurungan paling lama 1 (satu) tahun atau denda paling banyak Rp 50.000.000,00 (lima puluh juta rupiah), setiap dokter atau dokter gigi yang:
> ….dengan sengaja tidak memenuhi kewajiban sebagaimana dimaksud dalam Pasal 51 huruf a, huruf b, huruf c, huruf d, atau huruf e."

Rekam Medis yang telah bocor tersebut telah menimbulkan kerugian bagi pihak keluarga Bapak Hasyim.

[21] Rekam Medik Diduga Bocor, Keluarga Pasien Protes http://radior2b.com/2016/03/08/rekam-medik-diduga-bocor-keluarga-pasien-protes/ Diakses 20 Mei 2016.

Pihak keluarga Bapak Hasyim dapat melakukan gugatan secara perdata untuk meminta penggaantian atas kerugian yang diderita terhadap penggunaan data pribadi/rekam medis tanpa persetujuan tersebut.

Terkait perlindungan data pribadi Pasal 26 ayat (1) UU ITE telah mengatur bahwa:

(1) Kecuali ditentukan lain oleh Peraturan Perundang-undangan, penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan Orang yang bersangkutan.

Terhadap pihak yang dirugikan atas dilanggarnya ketentuan tersebut, dapat mengajukan gugatan atas kerugian yang ditimbulkan berdasarkan ketentuan ayat (2) pasal tersebut.[22] Terkait dengan perlindungan rekam medis, Undang-Undang Nomor 29 Tahun 2004 tentang praktik kedokteran telah mengatur secara sekilas mengenai perlindungan rekam medis milik pasien. Pasal 47 ayat (2) undang-undang ini mengatakan:

"Rekam medis sebagaimana dimaksud pada ayat (1) harus disimpan dan dijaga kerahasiannya oleh dokter atau dokter gigi dan pimpinan sarana pelayanan kesehatan."

Dokter atau dokter gigi memiliki kewajiban untuk menyimpan, menjaga, dan melindungi segala informasi yang diketahuinya mengenai pasiennya. Hal ini seperti yang telah diatur di dalam Pasal 57 Huruf (c) undang-undang praktik kedokteran, yang berbunyi:

"Dokter atau dokter gigi dalam melaksanakan praktik kedokteran mempunyai kewajiban:

…. merahasiakan segala sesuatu yang diketahuinya tentang pasien, bahkan juga setelah pasien itu meninggal dunia."

Melalui pasal ini dapat kita lihat bahwa dokter dan pelaksana pelayanan kesehatan wajib melindungi dan menjaga kerahasiaan pasiennya. Pimpinan sarana pelayanan kesehatan memiliki arti bahwa penyelenggara program *E-Health* memiliki kewajiban untuk menjaga dan menyimpan rekam medis milik pasien. Kemudian pada Peraturan Menteri Kesehatan Nomor 269/MENKES/PER/III/2008 Pasal 14 dikatakan bahwa:

"Pimpinan sarana pelayanan kesehatan bertanggung jawab atas hilang, rusak, pemalsuan, dan/atau penggunaan oleh orang atau badan yang tidak berhak terhadap rekam medis."

Selanjutnya, apabila terjadi bocornya data pasien maka pihak yang bertanggung jawab dapat dikenakan Pasal 79 butir (c) undang-undang praktik kedokteran yang berbunyi:

"Dipidana dengan pidana kurungan paling lama 1 (satu) tahun atau denda paling banyak Rp 50.000.000,00 (lima puluh juta rupiah), setiap dokter atau dokter gigi yang:

…. dengan sengaja tidak memenuhi kewajiban sebagaimana dimaksud dalam Pasal 51 huruf a, huruf b, huruf c, huruf d, atau huruf e."

Penyedia layanan kesehatan/rumah sakit memiliki kewajiban-kewajiban yang harus dipenuhi sesuai dengan ketentuan di dalam Undang-Undang Nomor 44 Tahun 2009 tentang Rumah Sakit. Rumah Sakit memiliki fungsi utama untuk memberikan perawatan dan pengobatan yang sempurna kepada pasien baik pasien rawat inap, rawat

[22] Pasal 26 ayat (2) UU ITE: (2) Setiap Orang yang dilanggar haknya sebagaimana dimaksud pada ayat (1) dapat mengajukan gugatan atas kerugian yang ditimbulkan berdasarkan undang-undang ini.

jalan maupun pasien gawat darurat.[23] Pimpinan rumah sakit bertanggung jawab atas mutu pelayanan medik di rumah sakit yang diberikan kepada pasien. Rekam Medis sangat penting dalam mengemban mutu pelayanan medik yang diberikan oleh rumah sakit beserta staf mediknya. Rekam Medis merupakan milik rumah sakit yang harus dipelihara karena berfaedah bagi pasien, dokter maupun bagi rumah sakit.

Rumah Sakit bertanggung jawab untuk melindungi informasi yang ada di dalam rekam medis terhadap kemungkinan hilangnya keterangan ataupun memalsukan data yang ada di dalam rekam medis atau dipergunakan oleh orang yang semestinya tidak di beri izin.[24] Rekam Medis harus diberi data yang cukup terperinci, sehingga dokter lain dapat mengetahui bagaimana pengobatan dan perawatan kepada pasien dan konsulen dapat memberikan pendapat yang tepat setelah dia memeriksanya ataupun dokter yang bersangkutan dapat memperkirakan kembali keadaan pasien yang akan datang dari prosedur yang telah dilaksanakan.

C. KESIMPULAN

Dokter dan penyedia layanan kesehatan wajib menjaga dan melindungi serta memiliki tanggung jawab penuh terhadap rekam medis milik pasiennya dari akses dan penggunaan secara tidak bertanggung jawab oleh pihak lain yang tidak berhak dan tidak memiliki kepentingan akan hal tersebut. Hal ini seperti yang telah diatur di dalam Pasal 47 ayat (2) dan Pasal 57 huruf (c) undang-undang Nomor 29 Tahun 2004 tentang praktik kedokteran dan ketentuan di dalam Peraturan Menteri Kesehatan Nomor 269/PER/MENKES/III/2008 tentang Rekam Medis. Apabila terjadi kebocoran data milik pasien tersebut, dokter dapat dikenakan ketentuan pidana Pasal 79 butir (c) Peraturan Menteri Kesehatan Nomor 269/PER/III/2008, dengan ketentuan pidana kurungan maksimal satu tahun atau denda maksimal 50 juta rupiah. Pimpinan Rumah Sakit memiliki tanggung jawab atas segala kehilangan, kerusakan, pemalsuan, dan penggunaan oleh pihak lain terkait rekam medis adalah mutlak tanggung jawab pimpinan sarana pelayanan kesehatan sesuai dengan Pasal 14 Permenkes tersebut, namun tidak diatur secara spesifik mengenai sanksi dan bentuk tanggung jawab yang dapat diberikan kepada pihak yang dirugikan.

Prinsip-prinsip perlindungan data pribadi di Indonesia, nyatanya belum dilaksanakan sebagaimana seharusnya. Hal ini terbukti dengan masih adanya data pribadi/rekam medis milik pasien yang dapat dengan mudah diakses oleh pihak lain tanpa adanya persetujuan dengan pemilik data yang bersangkutan. Prinsip yang disampaikan oleh Prof. Abu Bakar Munir dan yang dicantumkan di dalam *Protectian Data Act* Inggris dapat dijadikan sebagai patokan oleh pemerintah dalam merumuskan regulasi yang lebih komprehensif terkait dengan perlindungan data pribadi. Perlindungan data pribadi telah diatur secara jelas di dalam Pasal 26 ayat (1) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). Namun peraturan yang khusus membahas mengenai privasi dan perlindungan data pribadi diperlukan agar dapat mengakomodasi segala kepentingan yang terkait dengan hal tersebut. Untuk dapat mengembangkan layanan *E-Helth* yang menghormati privasi dan melindungi data pribadi pasien *E-Health*, diperlukan regulasi yang lebih komprehensif.

---

[23] H. Syahrul Machmud, 2012, *Penegakan Hukum dan Perlindungan Bagi Dokter yang diduga Melakukan Medikal Malpraktek,* CV. Karya Putra Darwati, Bandung, hlm. 161.

[24] Budi Sampurna, 2008, *Pedoman Manajemen Informasi Kesehatan di Sarana Pelayanan Kesehatan*, Penerbit Universitas Indonesia, Jakarta., hlm.196.