

URGENSI UNDANG-UNDANG PERLINDUNGAN DATA PRIBADI DI INDONESIA; STUDI PERBANDINGAN HUKUM INGGRIS DAN MALAYSIA

URGENCY OF PERSONAL DATA PROTECTION LAW IN INDONESIA; COMPARATIVE STUDY OF ENGLISH AND MALAYSIA LAW

Lia Sautunnida

Fakultas Hukum Universitas Syiah Kuala
Jalan Putroe Phang No. 1 Darussalam, Banda Aceh 23111
E-mail: liasautunnida@unsyiah.ac.id

Diterima: 02/07/2018; Revisi: 17/07/2018; Disetujui: 31/07/2018

DOI: <https://doi.org/10.24815/kanun.v20i2.11159>

ABSTRAK

Artikel ini ingin menjawab pentingnya penetapan aturan hukum yang tegas dan komprehensif yang dapat memberikan perlindungan terhadap data pribadi yang berlangsung melalui media elektronik di Indonesia. Permasalahan ini muncul dengan perkembangan teknologi informasi saat ini telah menimbulkan persoalan hukum baru, yaitu mengenai perlindungan keamanan atas data pribadi yang berlangsung melalui media elektronik. Banyaknya pihak yang menggunakan media elektronik tersebut sebagai alat komunikasi dan transaksi mengakibatkan terjadinya penyalahgunaan data pribadi. Sejumlah negara seperti Uni Eropa, Amerika, Inggris, Hongkong, Singapura, dan Malaysia, telah memiliki aturan yang tegas dan komprehensif berkenaan dengan data pribadi. Akan tetapi sampai sejauh ini Indonesia belum punya undang-undang khusus yang mengatur perlindungan data pribadi. Di Indonesia aturan mengenai hal tersebut terdapat dalam Pasal 26 UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dan juga tercantum dalam beberapa aturan hukum lainnya yang terpisah. Meskipun demikian, Pasal tersebut dianggap umum. Hal ini dipandang perlu segera disahkan dalam bentuk undang-undang tersendiri untuk memberikan jaminan keamanan dan perlindungan data pribadi serta dapat memberikan sanksi baik dalam bentuk pidana ataupun perdata bagi yang menyalahgunakan data pribadi tersebut.

Kata Kunci: Data Pribadi, Perlindungan, Aturan Hukum.

ABSTRACT

This article aims to answer the importance of enactments assertive and comprehensive legal rules in Indonesia that can provide personal data protection on electronic media. This problem emerges with the recent development of information technology which has led to new legal issues. The issues are about security and protection towards personal data that occurred through electronic media. There are people who use electronic media as a tool of communication and transaction which may lead to the abuse of personal data. Some countries such as the European Union, the United States, the United Kingdom, Hongkong, Singapore and Malaysia already have assertive and comprehensive law regarding the protection of personal data; however, so far there is no specific law in Indonesia that regulates personal data protection. In Indonesia, the regulation about personal data protection is stated in Article 26 of Law Number 11 Year 2008 on Information and Electronic Transactions and also this personal data

protection regulation listed in several separate legal rules. Nevertheless, it's Article is considered general. Therefore, it is deemed necessary to be immediately ratified in the form of law to provide security and protection and may impose sanctions in both criminal and civil forms for those who misuse the personal data.

Key Words: Personal Data, Protection, Regulation.

PENDAHULUAN

Dalam perkembangan teknologi informasi saat ini, berbagai macam kegiatan baik dalam konteks pemerintahan, transaksi bisnis, komersil ataupun komunikasi berlangsung melalui media elektronik (*online*). Data atau informasi yang disampaikan melalui media elektronik itu sesungguhnya merupakan hal yang berharga. Selain itu, kegiatan yang berlangsung *online* tersebut juga memiliki risiko karena dapat menimbulkan masalah apabila data atau informasi tersebut bocor sehingga bisa disalahgunakan oleh pihak yang tidak bertanggung jawab.

Data-data pribadi berkenaan dengan kependudukan dan demografis di Indonesia seperti NIK, E-KTP dan KK sangat penting dilindungi agar tidak mudah dieksploitasi. Ada beberapa bentuk penyalahgunaan data seperti penjualan data, data profiling, tujuan pemasaran, penelitian, bahkan termasuk pemantauan/spionase. lebih parah lagi penyalahgunaan data pribadi untuk tindak kriminal seperti pembuatan akun palsu, penipuan dalam jaringan, pencucian uang, pasar palsu dan juga transaksi ilegal. Oleh karena itu, diperlukan rangkaian pengamanan dan aturan yang komprehensif berkenaan dengan data pribadi.

Kegiatan yang berlangsung melalui media elektronik tersebut banyak memberikan manfaat dan kemudahan. Akan tetapi berdasarkan penelusuran dan pengamatan, banyak juga ditemukan kasus dan permasalahan berkenaan dengan penyalahgunaan data dan informasi tersebut. Salah satu kasus yang berkaitan dengan penyalahgunaan data dan informasi adalah kasus *skimming* atau penyalinan data dan informasi kartu ATM BRI nasabah yang kemudian pelaku *skimming* melakukan penarikan dana dari tempat lain. Pelaku *skimming* ini beberapa dari mereka berasal dari

luar negeri.¹ Kamera pengintai sudah jarang digunakan seiring dengan semakin canggihnya alat *skimmer* yang digunakan para pelaku.²

Selain kasus *Skimming* diatas tantangan serta ancaman terhadap penyalahgunaan data pribadi di Indonesia semakin populer yaitu sejak pemerintah Indonesia mensosialisasikan program KTP elektronik (e-KTP) yang merupakan program perekaman data pribadi oleh pemerintah dimana seluruh warga negara Indonesia diwajibkan untuk melakukan perekaman tersebut di masing-masing domisilinya. Data pribadi yang terekam dalam e-KTP memiliki risiko mengalami kebocoran data sehingga rentan untuk disalahgunakan oleh pihak-pihak yang tidak bertanggung jawab, terutama apabila kurang pengamanannya.³

Kasus lainnya yaitu dengan perkembangan moda transportasi *online* seperti saat ini seperti Gojek dan Grab juga telah menimbulkan permasalahan berkenaan dengan data pribadi dimana terjadinya kebocoran data pengguna, dimana rute sehari-hari pengguna bisa dilacak. Data sensitif milik pelanggan dan pengemudi Gojek, seperti nama, alamat, nomor telepon, koordinat, dan tujuan, masih bisa diakses dari API *endpoint* yang dimiliki Gojek.⁴

Berdasarkan beberapa kasus di atas, diperlukan perlindungan dan pembentukan hukum yang tegas dan komprehensif berkenaan dengan penggunaan data dan informasi agar perkembangan dan pemanfaatannya dapat berjalan dengan baik. Undang-undang yang jelas dan komprehensif, sangat

¹ Hadi Maulana, "BRI Batam Akui 4 Nasabahnya Jadi Korban Skimming", diambil dari <https://regional.kompas.com/read/2018/03/27/17434581/bri-batam-akui-4-nasabahnya-jadi-korban-skimming>, edisi 27/03/2018, 17:43 WIB, diakses 29 Maret 2018. *Card skimming* adalah aktivitas menggandakan informasi yang terdapat dalam pita magnetik (*magnetic stripe*) yang terdapat pada kartu kredit maupun ATM/debit secara tidak sah/ilegal. *magnetic stripe* adalah garis lebar hitam yang berada dibagian belakang kartu ATM. Fungsinya kurang lebih seperti tape kaset, material Ferromagnetic yang dapat dipakai untuk menyimpan data (suara, gambar, atau bit biner).

² Liputan6, "Begini Cara Kerja Skimming Kartu ATM", diambil dari <http://www.liputan6.com/tekno/read/2049670/begini-cara-kerja-iskimmingi-kartu-atm>, diakses 29 Maret 2018.

³ Rosalinda Elsin Latumahina, *Aspek Hukum Perlindungan Data Pribadi di Dunia Maya*, Jurnal GEMA AKTUALITA, Vol. 3 No. 2, Desember 2014, hlm. 2. Program e-KTP pertama kali diluncurkan pada awal tahun 2011, yang menghendaki adanya *single identity* bagi setiap penduduk Indonesia, yang berlaku seumur hidup. Perekaman data penduduk dilakukan pemerintah dalam rangka merekam informasi pribadi, termasuk identitas dan ciri-ciri fisiknya.

⁴ Reska K. Nistanto, "Kebocoran Go-Jek Memuncak, Rute Sehari-hari Pengguna Bisa Dilacak", diambil dari <https://tekno.kompas.com/read/2016/01/20/16031307/Kebocoran.GoJek.Memuncak.Rute.Seharihari.Pengguna.Bisa.Dilacak>, diakses 9 Mei 2018.

dibutuhkan untuk menentukan langkah-langkah yang pasti dalam proses pengamanan. Selain itu aturan perundangan memiliki efek memaksa agar data dan informasi dilindungi sebagaimana mestinya.

Atas dasar itulah, artikel ini ingin menjawab pentingnya Undang-Undang tentang Perlindungan Data Pribadi di Indonesia, dengan disertai studi perbandingan dengan Inggris dan Malaysia.

METODOLOGI PENELITIAN

Penelitian yang dilakukan ini adalah yuridis normatif. Pendekatan yang digunakan dalam penelitian adalah *statute approach* dengan mendeskripsikan peraturan perundang-undangan yang relevan dengan permasalahan yang diteliti, terutama substansi yang berkaitan dengan perlindungan data pribadi. Pendekatan lain yang digunakan adalah *comparative approach*, yakni perbandingan peraturan perundang-undangan berkaitan dengan perlindungan data pribadi di Inggris dan Malaysia.

HASIL PENELITIAN DAN PEMBAHASAN

1) Konsep Data Pribadi dan Privasi

Data pribadi adalah data yang berkenaan dengan ciri seseorang, nama, umur, jenis kelamin, pendidikan, pekerjaan, alamat, dan kedudukan dalam keluarga.⁵ Pengertian lain dari “data pribadi” adalah data yang berupa identitas, kode, simbol, huruf atau angka penanda personal seseorang yang bersifat pribadi dan rahasia.⁶

Berdasarkan penelusuran dapat diketahui bahwa sejarah penggunaan istilah perlindungan data pertama kali digunakan di Jerman dan Swedia pada tahun 1970-an yang mengatur tentang

⁵ <http://kamusbahasaindonesia.org/data%20pribadi/miripKamusBahasaIndonesia.org>. Diakses 28 Februari 2018 Jam 11.55.

⁶ Rosalinda Elsina Latumahina, *Aspek Hukum Perlindungan Data Pribadi di Dunia Maya*, Jurnal GEMA AKTUALITA, Vol. 3 No. 2, Desember 2014, hlm. 16. Berdasarkan Pasal 1 Peraturan Menteri Komunikasi dan

perlindungan data pribadi dengan diberlakukannya aturan berkenaan dengan perlindungan data pribadi tersebut ke dalam sebuah aturan perundang-undangan yang bersifat sistematis.⁷ Pemberlakuan aturan berkaitan dengan data pribadi tersebut karena pada masa itu alat yang digunakan untuk menyimpan data penduduk adalah komputer untuk keperluan pendataan sensus penduduk. Akan tetapi pada praktiknya sering terjadi banyak penyalahgunaan yang dilakukan oleh pihak pemerintah maupun pihak swasta. Oleh sebab itu diperlukan adanya aturan perundang-undangan yang akomodatif dan yang bisa memberikan jaminan dan keamanan terhadap data pribadi sehingga penggunaan data pribadi tersebut tidak dapat disalahgunakan. Masing-masing negara menggunakan terminologi yang berbeda antara informasi pribadi dan data pribadi. Akan tetapi secara substantif kedua istilah tersebut mempunyai definisi yang hampir sama sehingga kedua istilah tersebut sering digunakan secara bergantian. Seperti misalnya Amerika Serikat, Kanada, dan Australia menggunakan istilah informasi pribadi sedangkan negara-negara Uni Eropa, Malaysia dan Indonesia sendiri dalam UU ITE menggunakan istilah data pribadi.⁸

Di dalam data pribadi mencakup fakta-fakta, komunikasi atau pendapat yang berkaitan dengan individu yang merupakan informasi yang sifatnya rahasia, pribadi atau sensitif sehingga pribadi yang bersangkutan ingin menyimpan atau membatasi orang lain untuk mengoleksi, menggunakan atau menyebarkannya kepada pihak lain.

Informatika No. 20 Tahun 2016, data pribadi adalah data perseorangan tertentu yang disimpan, dirawat, dan dijaga kebenaran serta dilindungi kerahasiaannya.

⁷ Shinta Dewi, sebagaimana dikutip Rosalinda Elsin Latumahina. Lihat juga, Wafiya, *Perlindungan Hukum Bagi Nasabah yang Mengalami Kerugian dalam Transaksi Perbankan Melalui Internet*, Kanun Jurnal Ilmu Hukum, Vol. 14 No. 1, 2012.

⁸ *Ibid*, hlm. 17. Beberapa pengertian mengenai pengaturan perlindungan data berdasarkan *Data Protection Act* 1998, antara lain: (1) 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 juga termasuk informasi yang merupakan bagian tertentu dari catatan-catatan kesehatan, kerja sosial, pendidikan atau yang disimpan sebagai bagian dari suatu sistem penyimpanan yang relevan (Pasal 1 ayat (1)); (2) Data pribadi adalah data yang berhubungan dengan seseorang individu yang hidup yang dapat diidentifikasi dari data atau dari data-data atau informasi yang dimiliki atau akan dimiliki oleh data controller (Pasal 1 ayat (1)); (3) Data sensitif adalah data pribadi yang terdiri dari informasi yang berhubungan dengan ras, etnis, dari seseorang individu, pendapat politiknya, keyakinan keagamaan, keanggotaan serikat pekerja, kesehatan fisik dan mental, kehidupan seksual, keberatan-keberatan oleh atau terhadap dirinya, proses peradilan dan hukuman akibat keberatan-keberatan tersebut.

Menurut Jerry Kang, data pribadi mendeskripsikan suatu informasi yang erat kaitannya dengan seseorang yang dapat membedakan karakteristik masing-masing pribadi.⁹ Pada prinsipnya bentuk perlindungan terhadap data pribadi dibagi dalam dua bentuk, yaitu bentuk perlindungan data berupa pengamanan terhadap fisik data itu, baik data yang kasat mata maupun data yang tidak kasat mata. Bentuk perlindungan data yang kedua adalah adanya sisi regulasi yang mengatur tentang penggunaan data oleh orang lain yang tidak berhak, penyalahgunaan data untuk kepentingan tertentu, dan pengrusakan terhadap data itu sendiri.¹⁰

Berkenaan dengan data pribadi, di negara maju, terminologi lain yang kerap kali digunakan adalah *privacy*/privasi sebagai hak yang harus dilindungi, yaitu hak seseorang untuk tidak diganggu kehidupan pribadinya.¹¹ Menurut Yuwinanto, privasi merupakan konsep abstrak yang mengandung banyak makna. Penggambaran populer mengenai privasi antara lain adalah hak individu untuk menentukan apakah dan sejauh mana seseorang bersedia membuka dirinya kepada orang lain atau privasi adalah hak untuk tidak diganggu. Privasi merujuk padanan dari Bahasa Inggris *privacy* adalah kemampuan satu atau sekelompok individu untuk mempertahankan kehidupan dan urusan personalnya dari publik, atau untuk mengontrol arus informasi mengenai diri mereka.¹² Menurut Kamus Besar Bahasa Indonesia, definisi dari privasi adalah bebas, kebebasan atau keleluasaan. Hak atas privasi ini juga dimuat dalam Deklarasi Universal Hak Asasi Manusia (DUHAM) / *Universal Declaration of Human Rights* (UDHR) Pasal 12, yang menyatakan: “*No one shall be subjected to*

⁹ Radian Adi Nugraha, *Analisis Yuridis Mengenai Perlindungan Data Pribadi dalam Cloud Computing System Ditinjau dari Undang-Undang Informasi dan Transaksi Elektronik*, Universitas Indonesia, 2012, hlm.. 31.

¹⁰ *Ibid*, hlm. 32.

¹¹ Rosalinda Elsin Latumahina, *Op.Cit*, hlm. 17. Konsep privasi untuk pertama kalinya dikembangkan oleh Warren dan Brandeis yang menulis sebuah artikel di dalam jurnal ilmiah Sekolah Hukum Universitas Harvard yang berjudul “*The Right to Privacy*”. Warren dan Brandeis dalam Jurnal tersebut memberikan pendapat bahwa dengan adanya perkembangan dan kemajuan teknologi telah melahirkan kesadaran masyarakat bahwa ada hak individu untuk menikmati hidup yang artinya terdapat hak seseorang untuk tidak diganggu kehidupan pribadinya oleh siapapun. Oleh karena itu dalam hal ini hukum harus mengakui dan melindungi hak privasi tersebut. Konsep privasi itu sendiri sangatlah sulit untuk didefinisikan karena setiap orang akan memberi pemahaman yang berbeda tergantung dari sudut pandang masing-masing dalam memberikan penilaiannya

¹² Helmy Prasetyo Yuwinanto, *Privasi Online dan Keamanan Data*.

arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks.”

Berdasarkan beberapa definisi dan istilah berkenaan dengan data dan informasi juga privasi tersebut diatas dapat dipahami bahwa data dan informasi itu berkenaan dengan kehidupan individu dan juga dekat kaitannya dengan konsep kerahasiaan atau hak privasi seseorang yang harus dijaga dan dilindungi oleh aturan perundang-undangan.

2) Hukum Inggris

Sampai saat ini kurang lebih 25 negara di dunia mempunyai undang-undang mengenai perlindungan data pribadi.¹³ Edmon Makarim menjelaskan bahwa Inggris bukanlah negara pertama yang mempunyai aturan berkenaan dengan perlindungan data pribadi. Berdasarkan penelusuran diketahui bahwa sejarah mencatat negara yang pertama kali mengatur mengenai perlindungan data pribadi adalah negara bagian Hesse di Jerman pada tahun 1970 kemudian diikuti oleh Swedia pada tahun 1973 dan Amerika Serikat pada tahun 1974 dan Inggris pada tahun 1984.¹⁴

Di Inggris aturan berkaitan dengan perlindungan data pribadi terdapat di dalam undang-undang perlindungan data 1998 (*The Data Protection Act 1998*). Dalam undang-undang tersebut disebutkan adanya suatu badan pelaksana yaitu *The Data Protection Commisioner* yang berwenang untuk mengawasi semua pengguna data yang menguasai data pribadi. Sementara di Indonesia badan

¹³ Radian Adi Nugraha, *Op. Cit*, hlm.. 45.

¹⁴ Edmon Makarim, *Pengantar Hukum Telematika (Suatu Kompilasi Kajian)*, dalam Radian Adi Nugraha, *Analisis Yuridis Mengenai Perlindungan Data Pribadi dalam Cloud Computing System Ditinjau dari Undang-Undang Informasi dan Transaksi Elektronik*, Universitas Indonesia, 2012, hlm 50. Isu berkenaan dengan perlindungan data pribadi di beberapa negara maju sudah dianggap sebagai bagian dari hak asasi manusia (*Individual Rights*) yang bersifat fundamental dan wajib mendapatkan perlindungan dan oleh karena itu telah dituangkan dalam peraturan perundang-undangan tersendiri. Inggris mengatur tentang perlindungan data pribadi dalam *Data Protection Act 1998* yang mulai berlaku sejak tahun 2000. *Act* ini merupakan pengganti dari peraturan sebelumnya (*Data Protection Act 1984*). Undang-undang ini lahir disebabkan oleh perkembangan penggunaan komputer yang semakin meningkat yang menimbulkan kekhawatiran terhadap data dan informasi tentang seseorang yang diproses tanpa sepengetahuan mereka serta tanpa adanya kemampuan untuk mengakses informasi tersebut atau memperbaikinya jika salah.

komisioner ini tidak disebutkan dalam aturan manapun. Badan komisiner ini dianggap penting sebagai pihak yang melakukan pengawasan terhadap data atau informasi yang digunakan dalam berbagai transaksi yang berlangsung di media *online*. Selain itu, perlindungan terhadap hak privasi individual juga disebutkan dalam ketentuan *Data Protection Act* 1998 yang memungkinkan subjek data untuk mendapatkan informasi tentang pengolahan data pribadinya dan untuk mencegah beberapa jenis pengolahan data yang berlangsung bila dianggap akan membahayakan kepentingannya.¹⁵ Perlindungan terhadap data pribadi di Inggris bersifat kuat dan tegas, *Act* ini bahkan melarang data pribadi ditransfer ke negara di luar Eropa kecuali apabila negara yang bersangkutan dapat menjamin perlindungan data yang sama. Berkaitan dengan hal ini pemerintah Indonesia juga belum menjadikan poin transfer data ke negara lain menjadi salah satu hal yang penting untuk dibicarakan, padahal hal tersebut sangat penting dalam menjawab tantangan dan kesempatan dalam era ekonomi digital saat ini yang cakupannya bahkan luas sampai pada level transaksi internasional. Para pihak yang diatur dalam ketentuan *Data Protection Act* 1998, adalah meliputi :

a. *The Data Protection Commisioner*

Semua pengguna data yang menguasai data pribadi harus mendaftar pada badan ini.

b. *Data Subject*/subjek data.

Artinya setiap individu yang menjadi subjek dari data pribadi tersebut.

c. *Data Controller* (pengguna data)

Artinya setiap orang yang menentukan tujuan dan cara mengolah data pribadi.

d. *Data Processor*

Artinya yang dipersamakan dengan *computer bureau* (biro komputer), yaitu orang (di luar pegawai *data controller*) yang memproses data atas nama *data controller*.

Beberapa prinsip penting dari *Data Protection Act* adalah sebagai berikut:

¹⁵ *Ibid*, hlm. 50.

- [1] *Personal data shall be obtained 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.* (Data Pribadi harus diperoleh hanya untuk satu atau lebih tujuan yang spesifik dan sah dan tidak boleh di proses lebih lanjut dengan cara apapun yang tidak sesuai dengan tujuan-tujuan tersebut).
- [2] *Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.* (Data pribadi yang diproses untuk tujuan apapun tidak boleh disimpan lebih lama dari yang diperlukan untuk tujuan-tujuan tersebut).
- [3] *Personal data shall be processed in accordance with the rights of data subjects under this Act.* (Data pribadi harus diproses sesuai dengan hak dari subjek data berdasarkan aturan undang-undang).
- [4] *Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to personal data.* (Tindakan teknis dan organisasi yang sesuai harus diambil terhadap pihak yang tidak berwenang dan tidak sah untuk memproses data pribadi dan terhadap kerugian dan kerusakan yang tidak terduga atau kerusakan terhadap data pribadi).
- [5] *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 subjects in relation to the processing of personal data.* (Data pribadi tidak boleh di transfer ke negara atau ke wilayah luar area ekonomi Eropa kecuali negara atau wilayah itu menjamin adanya perlindungan yang sama terhadap hak dan kebebasan dari subjek data berkaitan dengan proses data pribadi).

Berdasarkan Pasal 14 dari *Data Protection Act 1998* menjelaskan bahwa apabila pengadilan menemukan bahwa data pribadi diproses oleh pengontrol data tidak akurat, pengadilan dapat memerintahkan perbaikan, menghalangi, penghapusan atau kerusakan dari data tersebut. Bagi

mereka sedang terkena dampak langsung dari pengolahan data pribadi dapat meminta Badan Komisariss untuk mengevaluasi proses untuk menentukan jika memenuhi ketentuan *Data Protection Act 1998*. Data subyek berhak untuk mengklaim kompensasi untuk setiap kerugian yang diderita sebagai akibat dari pelanggaran *Data Protection Act* oleh pengontrol data dan mungkin juga mengklaim kompensasi untuk bahaya yang ditimbulkan.

3) Hukum Malaysia

Negara tetangga Malaysia sudah terlebih dahulu daripada Indonesia mengatur mengenai perlindungan data pribadi dalam bentuk undang-undang tersendiri.¹⁶ Malaysia mengaturnya dalam *Personal Data Protection Act* (PDPA) 2010. *Malaysia Personal Data Protection Act* (PDPA) 2010 akhirnya disahkan oleh parlemen Malaysia pada awal Mei 2010. Dengan berlakunya Undang-undang ini, maka Malaysia untuk pertama kalinya memiliki Undang-undang yang mengatur secara spesifik mengenai privasi dan memberikan perlindungan terkait data pribadi.¹⁷ Aturan dari PDPA ini bertujuan untuk mengatur pengolahan data pribadi oleh pengguna data dalam konteks transaksi komersial, dengan maksud menjaga kepentingan subjek data itu. Hal ini dicapai dengan memastikan bahwa persetujuan dari subjek data diperoleh sebelum pengolahan data pribadi serta memberikan data dengan subjek hak untuk mengakses, benar dan juga kontrol pengolahan data pribadi mereka. Hal tersebut sama halnya dengan apa yang disebutkan di dalam Pasal 26 UU ITE Indonesia. Selain PDPA, aturan lain berkaitan dengan perlindungan data pribadi yang berlaku di Malaysia yaitu: *a. Communication and Multimedia Act 1998*, *b. Computer Crimes Act 1997*, *c. Copyright Act 1987*, *d.*

¹⁶ Zuryati Mohamed Yusoff, *The Malaysian Personal Data Protection Act 2010: A Legislation Note*, New Zealand Journal of Public and International Law, Vol. 9, No. 1, 2011, hlm. 6. Lebih dari 10 tahun lalu, inisiasi berlakunya Undang-Undang tersebut dari Proyek Multimedia Super Corridor Malaysia (MSC) yang telah di formulasikan dengan dukungan penuh dari pemerintah Malaysia untuk mengubah negara menjadi negara yang berpengetahuan berdasarkan ekonomi. Sebagai bagian dari program kala itu, undang-undang perlindungan data pribadi telah dihadirkan untuk menciptakan kerangka hukum dan aturan untuk proyek yang dijalankan.

¹⁷ [NewDataPrivacyLawinMalaysia.http://www.bakermckenzie.com/RRSingaporeNewDataPrivacyLawAug10/](http://www.bakermckenzie.com/RRSingaporeNewDataPrivacyLawAug10/) Diakses pada 12 Mei 2018. Aturan tersebut mengacu pada aturan tentang perlindungan data pribadi yang dianut di

Digital Signature Act 1997, e. Electronic Commerce Act 2006, f. Electronic Government Activities Act 2007, g. Payment System Act 2003, h. Credit Reporting Agencies Act 2010, i. Telemedicine Act 1997, j. Penal Code dan k. Communication and Multimedia Content Code. PDPA 2010 ini dirancang sebagai undang-undang untuk melindungi data pribadi dengan mematuhi beberapa prinsip perlindungan data pribadi dengan beberapa modifikasi dan perubahan yang kemudian disesuaikan dengan kebutuhan dan keadaan lokal di Malaysia.¹⁸

Dengan berlakunya PDPA 2010 tersebut, setiap individu akan mendapat hak-hak baru seperti hak untuk diinformasikan mengenai data pribadinya serta hak untuk mengakses, mengkoreksi dan juga mengontrol pengolahan atau penggunaan data pribadi mereka oleh pihak lain. Transfer data pribadi lintas batas (*cross-border transfer*) juga diatur dalam PDPA. Sama halnya dengan Inggris yang juga mengatur tentang transfer data antar negara. PDPA menetapkan bahwa tidak ada transfer data pribadi di luar Malaysia dapat terjadi kecuali pada tempat yang telah ditetapkan oleh Menteri Informasi, Kebudayaan dan Komunikasi. Kemudian negara tujuan tempat data pribadi ditransfer wajib memiliki tingkat perlindungan yang memadai yang setidaknya setara dengan tingkat perlindungan yang diberikan oleh PDPA Malaysia.¹⁹

Berkaitan dengan hal tersebut, Indonesia belum mengatur tentang transfer data antar negara. Sebenarnya hal tersebut sangat penting untuk segera diatur sehingga Indonesia bisa bersaing di level internasional dalam kegiatan ekonomi dan bisnis digital dengan memiliki aturan yang akomodatif berkaitan dengan data pribadi.

PDPA 2010 memuat tujuh prinsip hukum setiap pengguna data dan mengharuskan bagi pengguna data untuk menyesuaikan dengan beberapa prinsip antara lain; prinsip umum, justifikasi untuk pemrosesan data seperti persetujuan, prinsip pemberitahuan dan pilihan. Hak untuk

Eropa (*European Data Protective Directive*). PDPA 2010 ini juga dominan sekali terpengaruh oleh Undang-Undang Perlindungan Data Pribadi (privasi) dari Hongkong 1995 dan Undang-Undang Perlindungan Data Pribadi UK 1998.

¹⁸ Op. Cit, Hal. 6

¹⁹ Gupinder Assi, Op. cit, Hal. 6

mendapatkan informasi tentang tujuan pemrosesan data; prinsip keterbukaan. Tidak bersifat tertutup kecuali berkaitan dengan tujuan; prinsip keamanan. Menjamin data tersebut akurat dan update; prinsip akses, hak individu untuk mengakses ke data pribadinya). Kewajiban untuk mengambil langkah yang praktis untuk perlindungan data; prinsip retensi. Tidak menyimpan data lebih lama dari yang diperlukan; prinsip integritas data.²⁰ Ketujuh prinsip ini mengatur secara komprehensif mengenai perlindungan data pribadi. Contohnya dalam *Retention Principle*, data pribadi yang diproses untuk tujuan apapun harus tidak disimpan lebih lama dari yang diperlukan untuk pemenuhan tujuan perlindungan data pribadi. Dalam hal ini akan menjadi tugas dari pengguna data untuk mengambil semua langkah-langkah yang wajar untuk memastikan bahwa semua data pribadi dihancurkan atau dihapus secara permanen. Dengan adanya PDPA 2010 ini, jaminan keamanan bagi data pribadi pengguna media elektronik di Malaysia pun meningkat.

4) Hukum Indonesia

Aturan berkaitan dengan Perlindungan data pribadi di Indonesia masih lemah dan bersifat umum karena aturannya termaktub dalam beberapa peraturan perundang-undangan yang terpisah dan hanya menggambarkan konsep perlindungan data pribadi secara general dan aturan yang hanya dituangkan dalam bentuk Peraturan Menteri Komunikasi dan Informatika Republik Indonesia. Beberapa aturan Undang-undang yang terpisah tersebut antara lain terdapat dalam Undang-Undang Informasi dan Transaksi Elektronik (ITE) No. 11 Tahun 2008, Undang-Undang Nomor 43 Tahun 2009, tentang Kearsipan, Undang-Undang Nomor 8 Tahun 1997 tentang Dokumen Perusahaan, Undang-Undang Nomor 10 Tahun 1998 tentang Perubahan atas Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan, Undang-Undang Nomor 36 Tahun 2009 tentang Kesehatan, Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi (UU Telekomunikasi), dan Undang-

²⁰ Abu Bakar Munir, "The Malaysian Personal Data Protection Bill", <http://profabm.blogspot.com/2009/12/malaysian-personal-data-protection-bill.html> Diakses pada 12 Mei 2018.

Undang Nomor 24 Tahun 2013 tentang Perubahan Atas Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan (UU Adminduk).

Selain beberapa aturan tersebut diatas secara implisit, Konstitusi Indonesia (UUD NKRI 1945) memuat norma tentang Perlindungan data pribadi. Pasal 28 G ayat (1) memuat “Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang dibawah kekuasaannya,...”.²¹

Pengaturan mengenai perlindungan data pribadi diatur dalam beberapa Pasal di UU ITE. UU ini memang belum memuat aturan perlindungan data pribadi secara tegas dan komprehensif. Meskipun demikian, secara tidak langsung UU ini melahirkan pemahaman baru mengenai perlindungan terhadap keberadaan suatu data atau informasi elektronik baik yang bersifat umum maupun pribadi. Penjelasan tentang data elektronik pribadi diamanatkan lebih lanjut oleh UU ITE dalam PP Penyelenggaraan Sistem dan Transaksi Elektronik (PSTE). Perlindungan data pribadi dalam sebuah sistem elektronik di UU ITE meliputi perlindungan dari penggunaan tanpa izin, perlindungan oleh penyelenggara sistem elektronik, dan perlindungan dari akses dan interferensi ilegal.

Terkait dengan perlindungan data pribadi dari penggunaan tanpa izin, Pasal 26 UU ITE menyebutkan bahwa penggunaan setiap data pribadi dalam sebuah media elektronik harus mendapat persetujuan pemilik data bersangkutan. Setiap orang yang melanggar ketentuan ini dapat digugat atas kerugian yang ditimbulkan.²² Dalam penjelasannya, Pasal 26 UU ITE juga menyatakan

²¹ Daniar Supriadi, *Data Pribadi dan Dua Dasar Legalitas Pemanfaatannya*, September 2017. <http://www.hukumonline.com/berita/baca/lt59cb4b3feba88/data-pribadi-dan-dua-dasar-legalitas-pemanfaatannya-oleh--daniar-supriyadi>

²² Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Pasal 26 ayat (1). Bunyi Pasal 26 UU ITE adalah sebagai berikut: 1) Penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan orang yang bersangkutan. 2) Setiap Orang yang melanggar haknya sebagaimana dimaksud pada ayat (1) dapat mengajukan gugatan atas kerugian yang ditimbulkan berdasarkan Undang-Undang ini. Penjelasan/tafsir resmi dari pasal ini tertulis bahwa perlindungan data pribadi adalah bagian dari *privacy rights* dengan pengertian (i) hak untuk menikmati kehidupan pribadi dan bebas dari segala macam gangguan; (ii) hak untuk dapat berkomunikasi dengan orang lain (perseorangan dan/atau badan hukum) tanpa tindakan memata-matai; (iii) hak untuk mengawasi akses tentang kehidupan pribadi dan data seseorang. Selain itu, tanggung

bahwa data pribadi merupakan salah satu bagian dari hak pribadi seseorang. UU ITE (11/2008 yo. 19/2016) sebagai UU generik memuat norma perlindungan data pribadi pada Pasal 26, yang pada intinya, penggunaan setiap data dan informasi di media elektronik yang terkait dengan data pribadi seseorang harus dilakukan atas persetujuan orang yang bersangkutan atau berdasarkan hukum positif (peraturan perundang-undangan). Pada dasarnya ketentuan ini memuat dua dasar legitimasi pemrosesan data pribadi yaitu (a) *consent*/persetujuan; dan (b) norma hukum positif. Kedua prinsip ini adalah dasar *lawful data processing*.

Akan tetapi menurut Sonny Zulhuda, dari International Islamic University Malaysia mengatakan bahwasanya Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik masih sangat tidak signifikan dalam mengatur penggunaan data pribadi karena Pasal yang ada dalam UU ITE tersebut hanya merupakan ketentuan umum dan tidak menjelaskan berbagai isu masalah yang banyak di bicarakan di level internasional saat ini.²³ Jadi dapat dipahami berdasarkan deskripsi diatas bahwa aturan berkenaan dengan Perlindungan Data Pribadi Indonesia masih bersifat umum dan terletak terpisah-pisah dalam beberapa aturan undang-undang. Selain itu juga diharapkan pemerintah dan parlemen Indonesia untuk segera membahas RUU Perlindungan Data Pribadi sehingga Indonesia akan lebih siap menghadapi tantangan ekonomi digital juga dapat

jawab dan kewajiban perlindungan data pribadi lebih utama diupayakan/wujudkan kepada setiap pengguna data pribadi di media elektronik (*the users of data, either data controller or data processor*). Penjelasan pasal 26 ayat (1) UU ITE juga menjabarkan lebih lanjut tentang pengertian hak pribadi. Isi penjelasan itu adalah sebagai berikut: Dalam pemanfaatan Teknologi Informasi, perlindungan data pribadi merupakan salah satu bagian dari hak pribadi (*privacy rights*). Hak pribadi mengandung pengertian sebagai berikut: a. Hak pribadi merupakan hak untuk menikmati kehidupan pribadi dan bebas dari segala macam gangguan, b. Hak pribadi merupakan hak untuk dapat berkomunikasi dengan Orang lain tanpa tindakan memata-matai, c. Hak pribadi merupakan hak untuk mengawasi akses informasi tentang kehidupan pribadi dan data seseorang. Berdasarkan penafsiran secara umum dapat dipahami bahwa perlindungan data pribadi sebenarnya telah diatur ke dalam beberapa pasal di UU ITE, yaitu pada Pasal 30 sampai Pasal 33 dan Pasal 35 yang masuk ke dalam Bab VII mengenai perbuatan yang dilarang. Dalam UU ITE melarang adanya akses secara melawan hukum kepada data milik orang lain melalui sistem elektronik untuk memperoleh informasi dengan cara menerobos sistem pengaman. Selain itu juga UU ITE secara tegas menyatakan bahwa penyadapan (*interception*) adalah termasuk perbuatan yang dilarang kecuali dilakukan oleh pihak yang memiliki kewenangan untuk itu dalam hal keperluan upaya hukum.

²³ Syarpani, *Tinjauan Yuridis Terhadap Perlindungan Data Pribadi di Media Elektronik (Berdasarkan Pasal 25 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*, Jurnal Beraja Niti, Volume 3 Nomor 6 2014, hlm. 7

memberikan jaminan keamanan terhadap data pribadi pengguna serta dapat memberikan sanksi yang tegas terhadap pihak yang menyalahgunakan data pribadi pihak lain.

SIMPULAN

Ada kecemasan tentang perlindungan data pribadi di Indonesia karena hingga saat ini belum ada undang-undang yang spesifik mengatur hal tersebut. Hal tersebut bisa dilihat dari beberapa kasus yang terus terjadi seperti yang telah diuraikan diatas, dimana pelanggaran terhadap data pribadi terus berkembang akan tetapi aturan yang ada di Indonesia saat ini yang berkenaan dengan perlindungan data pribadi tersebut belum bisa mengakomodasi bahkan belum bisa memberikan jaminan terhadap keamanan data pribadi dalam melakukan kegiatan dengan menggunakan media elektronik.

Meskipun telah diatur secara umum dalam UU ITE dan secara khusus dalam PM KI dan juga dalam beberapa peraturan perundangan lainnya, namun Indonesia dirasa sangat perlu untuk segera diberlakukan aturan khusus mengenai perlindungan data pribadi yang disahkan dalam bentuk Undang-Undang. Diharapkan dengan adanya peraturan yang tegas dan memadai dapat memberikan keamanan bagi pengguna teknologi informasi dan juga dapat meningkatkan kegiatan ekonomi digital dan dapat bersaing dalam kegiatan bisnis pada taraf internasional.

DAFTAR PUSTAKA

- Abu Bakar Munir, “The Malaysian Persona lData Protection Bill”, <http://profabm.blogspot.com/20-09/12/malaysian-personal-data-protection-bill.html> Diakses pada 12 Mei 2018.
- Daniar Supriadi, *Data Pribadi dan Dua Dasar Legalitas Pemanfaatannya*, September 2017.
<http://www.hukumonline.com/berita/baca/lt59cb4b3feba88/data-pribadi-dan-dua-dasar-legalitas-pemanfaatannya-oleh--daniar-supriadi>.

Hadi Maulana, “BRI Batam Akui 4 Nasabahnya Jadi Korban Skimming”, diambil dari <https://regional.kompas.com/read/2018/03/27/17434581/bri-batam-akui-4-nasabahnya-jadi-korban-skimming>, edisi 27/03/2018, 17:43 WIB, diakses 29 Maret 2018.

<http://kamusbahasaindonesia.org/data%20pribadi/miripKamusBahasaIndonesia.org>. Diakses 28 Februari 2018 Jam 11.55.

Liputan6, “Begini Cara Kerja Skimming Kartu ATM”, diambil dari <http://www.liputan6.com/tekno/read/2049670/begini-cara-kerja-iskimmingi-kartu-atm>, diakses 29 Maret 2018.

Radian Adi Nugraha, 2012, *Analisis Yuridis Mengenai Perlindungan Data Pribadi dalam Cloud Computing System Ditinjau dari Undang-Undang Informasi dan Transaksi Elektronik*, Universitas Indonesia, Jakarta.

Reska K. Nistanto, “Kebocoran Go-Jek Memuncak, Rute Sehari-hari Pengguna Bisa Dilacak”, diambil dari <https://tekno.kompas.com/read/2016/01/20/16031307/Kebocoran.GoJek.Memuncak.Rute.Seharihari.Pengguna.Bisa.Dilacak>, diakses 9 Mei 2018.

Rosalinda Elsin Latumahina, 2014, *Aspek Hukum Perlindungan Data Pribadi di Dunia Maya*, Jurnal GEMA AKTUALITA, Vol. 3 No. 2.

Syarpani, 2014, *Tinjauan Yuridis Terhadap Perlindungan Data Pribadi di Media Elektronik (Berdasarkan Pasal 25 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*, Jurnal Beraja Niti, Volume 3 Nomor 6.

Wafiya, 2012, *Perlindungan Hukum Bagi Nasabah yang Mengalami Kerugian dalam Transaksi Perbankan Melalui Internet*, Kanun Jurnal Ilmu Hukum, Vol. 14 No. 1.

Zuryati Mohamed Yusoff, 2011, *The Malaysian Personal Data Protection Act 2010: A Legislation Note*, New Zealand Journal of Public and International Law, Vol. 9, No. 1.