BAB III

HASIL PENELITIAN DAN PEMBAHASAN

A. Perbandingan Hukum Tindak Pidana Pencurian Data (*Data Theft*) di Indonesia dan di Singapura

Ada beberapa faktor yang menjadi pembeda antara Hukum Tindak Pidana Pencurian Data (*Data Theft*) yang ada di Indonesia dan Hukum Tindak Pidana Pencurian Data (*Data Theft*) yang ada di Singapura, mulai dari subyek tindak pidananya hingga sanksi yang akan dijatuhkan kepada para pelakunya.

Saat ini Indonesia masih belum memiliki kebijakan atau regulasi mengenai perlindungan data pribadi dalam satu undang-undang khusus. Pengaturan tersebut masih berupa rancangan undang-undang perlindungan data pribadi. Aturan yang berlaku saat ini mengenai hal tersebut masih termuat terpisah dan tersebar di beberapa undang-undang dan hanya mencerminkan aspek perlindungan data pribadi secara umum. Lalu, dalam peraturan tingkat menteri, Menteri Komunikasi dan Informatika telah mengeluarkan Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 Perlindungan Data Pribadi Dalam Sistem Elektronik. Ada juga Undang-Undang yang memuat penjelasan tentang Data Pribadi yang nantinya akan menjadi dasar atas pengaturan pidana tentang pencurian data.

Sedangkan di Singapura, Undang-Undang perlindungan data komprehensif Singapura, *Personal Data Protection Act 2012* (PDPA) telah berlaku selama delapan tahun. Pada 14 Mei 2020, makalah konsultasi publik dan RUU Perlindungan Data Pribadi atau *Personal Data Protection (Amendment) Bill* (RUU Amandemen atau *Amendment Bill*) yang menyertai diterbitkan, untuk meminta umpan balik atas beberapa usulan revisi pada PDPA.

Di Indonesia yang menjadi subyek hukum tindak pidana pencurian data adalah perorangan, belum ada Undang-Undang yang mengatur aturan untuk pelanggaran yang dilakukan oleh koorporasi, berbeda dengan di Singapura yang sudah mencakup keduanya sekaligus.

Sanksi yang akan diterima oleh para pelaku tindak pidana pencurian data pada Indonesia dan Singapura, keduanya hampir sama yaitu denda atau pidana penjara. Namun ada sanksi lainnya yang berlaku di Singapura yaitu pelaku dituntut untuk menjadi relawan sukarela, yang nantinya akan membantu tugas-tugas dalam masyarakat.

Berikut ini merupakan Daftar Inventarisasi Masalah atau DIM yang menjadi pembeda antara Hukum Tindak Pidana Pencurian Data (*Data Theft*) di Indonesia dan di Singapura:

Tabel 3.1. Perbandingan Pengaturan Perlindungan Data Pribadi di Indonesia dan Singapura

No.	Objek yang diatur	Indonesia		Singapura	Keterangan
1.	Pengertian Data Pribadi	1. Pasal 1 Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik. 2. Pasal 58 Ayat (2) Undang-Undang Nomor 24 Tahun 2013 tentang Perubahan atas Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan. 3. Pasal 1 Rancangan Undang Undang tentang Perlindungan Data Pribadi Tahun 2020.		*Personal Data Protection (Amendment) Bill Amendment of section 2 (b)*	Di Indonesia, peraturan yang mengatur tentang data pribadi tersebar diberbagai Undang-Undang, sedangkan di Singapura sudah dijelaskan dalam satu Undang-Undang khusus yang membahas tentang data pribadi.
2.	Pengaturan Tindak Pidana (Pengaturan atau Undang-Undang yang mengatur tentang Tindak Pidana Pencurian Data) dalam Hukum Positif.	Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan sebagaimana telah diubah dengan Undang-Undang Nomor 10 Tahun 1998 tentang Perubahan atas Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan;	Pasal 49: Anggota Dewan Komisaris, Direksi, atau pegawai bank yang dengan sengaja merusak data akan dikenai pidana atau denda.	1. *Personal Data Protection Act 2012* (PDPA). 2. *Personal Data Protection (Amendment) Bill* (RUU Amandemen atau *Amendment Bill*).	Dalam hal ini, Singapura sudah memiliki persiapan dan rencana atas Tindak Pidana Pencurian Data, berbeda dengan Indonesia yang masih belum dapat melengkapi Undang-Undangnya.
		Undang-Undang Nomor 8 Tahun 1997 tentang Dokumen Perusahaan;	Pasal 11: Kewajiban penyimpanan adalah tidak menghilangkan		

			fungsi dokumen yang bersangkutan sebagai alat bukti sesuai dengan kebutuhan sebagaimana ditentukan dalam ketentuan mengenai daluwarsa suatu tuntutan yang diatur dala Peraturan Perundang-Undangan yang berlaku, atau untuk kepentingan hukum lainnya.		
		Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi;	Pasal 39: Penyelenggara telekomunikasi wajib melakukan pengamanan dan perlindungan terhadap instalasi dalam jaringan telekomunikasi yang digunakan untuk penyelenggaraan telekomunikasi. Pasal 40: Setiap orang dilarang		

			melakukan kegiatan penyadapan atas informasi yang disalurkan melaiui jaringan telekomunikasi dalam bentuk apapun. dan Pasal 42: Penyelenggara jasa telekomunikasi wajib merahasiakan informasi yang dikirim dan atau diterima oleh pelanggan jasa telekomunikasi melalui jaringan telekomunikasi dan atau jasa telekomunikasi yang diselenggarakannya.		
		Undang-Undang Nomor 24 Tahun 2013 tentang Perubahan Atas Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan;	Pasal 79: Data Perseorangan dan dokumen kependudukan wajib disimpan dan dilindungi kerahasiaannya oleh Negara.		

			Pasal 84: Data Pribadi Penduduk yang harus dilindungi memuat mulai dari sidik jari hingga elemen data lainnya yang merupakan aib seseorang. dan Pasal 86: Menteri sebagai penanggung jawab memberikan hak akses Data Pribadi kepada petugas provinsi dan petugas Instansi Pelaksana, dan petugas dilarang menyebarluaskan Data Pribadi yang tidak sesuai dengan kewenangannya.		
		Undang-Undang Nomor 36 Tahun 2009 tentang Kesehatan;	Pasal 57: Setiap orang berhak atas rahasia kondisi kesehatan pribadinya yang telah dikemukakan kepada penyelenggara pelayanan		

			kesehatan.		
		Undang-Undang Nomor 43 Tahun 2009 tentang Kearsipan;	Pasal 44: Pencipta arsip wajib menjaga kerahasiaan arsip tertutup, dan dapat menutup akses arsip terbuka apabila memenuhi beberapa syarat.		
		Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 Perlindungan Data Pribadi Dalam Sistem Elektronik;			
		Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik;	a. Pasal 26 ayat (1); Penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan Orang yang bersangkutan. b. Pasal 30 ayat (3);		

			Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apapun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan. c. Pasal 32; Setiap orang dilarang untuk mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu data orang lain atau public secara sengaja maupun tidak sengaja.		

			d. Pasal 45; Setiap Orang yang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan sebagaimana dimaksud dalam Pasal 27 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).		
		Rancangan Undang Undang Pelindungan Data Pribadi Tahun			

		2020.			
3.	Subjek Tindak Pidana (Subjek yang dapat dijatuhi hukuman apabila melakukan Tindak Pidana Pencurian Data)	Undang-Undang Nomor 10 Tahun 1998 tentang Perubahan atas Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan;	Orang dan Koorporasi.	Orang dan Koorporasi.	Dalam Pengaturan Hukum Singapura, semua yang memenuhi syarat hukum (orang maupun koorporasi) dapat terkena sanksi apabila melanggar Tindak Pidana Pencurian Data, hukum di Indonesia lebih condong kepada pihak perseorangan sebagai subyek Tindak Pidana Pencurian Data, daripada kepada pihak koorporasi.
		Undang-Undang Nomor 8 Tahun 1997 tentang Dokumen Perusahaan;	Koorporasi.		
		Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi;	Orang dan Koorporasi.		
		Undang-Undang Nomor 24 Tahun 2013 tentang Perubahan Atas Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan;	Orang dan Koorporasi.		
		Undang-Undang Nomor 36 Tahun 2009 tentang Kesehatan;	Orang.		
		Undang-Undang Nomor 43 Tahun 2009 tentang Kearsipan;	Orang.		
		Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 Perlindungan Data Pribadi Dalam	Orang.		

		Sistem Elektronik;			
		Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik;	Orang dan Koorporasi.		
		Rancangan Undang Undang Pelindungan Data Pribadi Tahun 2020.	Orang perseorangan atau Koorporasi.		
4.	Pidana (Sanksi yang akan dijatuhkan kepada para pelaku)	Undang-Undang Nomor 10 Tahun 1998 tentang Perubahan atas Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan;	Sanksi Administratif, pidana penjara sekurang-kurangnya 5 tahun dan paling lama 15 tahun serta denda sekurang-kurangnya Rp 10.000.000.000,00 (sepuluh miliar rupiah) dan paling banyak Rp 200.000.000.000,00 (dua ratus miliar rupiah).	1. *Voluntary undertakings* atau relawan sukarela; 2. *Financial penalties* atau denda, dan; 3. *Imprisonment* atau pidana penjara.	Hukuman yang akan diberikan kepada pelaku oleh Singapura beragam, itu juga karena budaya yang ada disana, sebagai contohnya menjadi relawan sukarela. Hukuman yang ada di Indonesia sudah cukup untuk menghukum para pihak yang melanggar.
		Undang-Undang Nomor 8 Tahun 1997 tentang Dokumen Perusahaan;	-		

		Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi;	Dipidana dengan pidana penjara paling lama 15tahun, dipidana dengan pidana penjara paling lama 2 tahun dan atau denda paling banyak Rp 200.000.000,00 (dua ratus juta rupiah).		
		Undang-Undang Nomor 24 Tahun 2013 tentang Perubahan Atas Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan;	Dipidana dengan pidana penjara paling lama 2 tahun dan/atau denda paling banyak Rp 25.000.000,00 (dua puluh lima juta rupiah).		
		Undang-Undang Nomor 36 Tahun 2009 tentang Kesehatan;	-		
		Undang-Undang Nomor 43 Tahun 2009 tentang Kearsipan;	Dipidana dengan pidana penjara paling lama 5 tahun atau denda paling banyak Rp 250.000.000,00 (dua ratus lima puluh juta rupiah).		
		Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 Perlindungan Data Pribadi Dalam	Sanksi Administratif.		

		Sistem Elektronik;			
		Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik;	dipidana dengan pidana penjara paling lama 6 tahun dan/atau denda paling banyak Rp 1.000.000.000,00 (satu miliar rupiah).		
		Rancangan Undang Undang Pelindungan Data Pribadi Tahun 2020.	Sanksi Administratif.		
5.	Tindak Pidana (Merupakan tindakan-tindakan yang melanggar dan dapat dijerat oleh UU Pencurian Data)	Undang-Undang Nomor 10 Tahun 1998 tentang Perubahan atas Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan;	mengubah, mengaburkan, menyembunyikan, menghapus, atau menghilangkan adanya suatu pencatatan dalam pembukuan atau dalam laporan, maupun dalam dokumen atau laporan kegiatan usaha, laporan transaksi atau rekening suatu bank, atau dengan sengaja mengubah, mengaburkan, menghilangkan, menyembunyikan atau	*An organisation shall not provide an individual with the individual's personal data or other information under subsection:* *a. threaten the safety or physical or mental health of an individual other than the individual who made the request;* *b. cause immediate or grave harm to the safety or to the*	Di Singapura secara garis besar, pencurian Data Pribadi akan dibebankan pada organisasi yang menyimpan data pribadi seseorang tersebut, namun apabila di Indonesia yang akan dibebani hukuman adalah pihak yang menyebarluaskan data pribadi korban.

			merusak catatan pembukuan tersebut.	*physical or mental health of the individual who made the request;* *c. reveal personal data about another individual;* *d. reveal the identity of an individual who has provided personal data about another individual and the individual providing the personal data does not consent to the disclosure of his identity; or* *e. be contrary to the national interest.*	
		Undang-Undang Nomor 8 Tahun 1997 tentang Dokumen Perusahaan;	-		
		Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi;	Setiap orang dilarang melakukan kegiatan penyadapan atas informasi yang disalurkan melalui jaringan telekomunikasi dalam bentuk apapun.		
		Undang-Undang Nomor 24 Tahun 2013 tentang Perubahan Atas Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan;	dilarang menyebarluaskan Data Kependudukan yang tidak sesuai dengan kewenangannya, dilarang menyebarluaskan Data Pribadi yang tidak sesuai dengan kewenangannya.		
		Undang-Undang Nomor 36 Tahun 2009 tentang Kesehatan;	-		
		Undang-Undang Nomor 43 Tahun 2009 tentang Kearsipan;	dilarang mengungkapkan rahasia atau data pribadi, dengan sengaja tidak menjaga		

			kerahasiaan arsip tertutup.		
		Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 Perlindungan Data Pribadi Dalam Sistem Elektronik;	dilarang melakukan tindakan apa pun yang dapat mengakibatkan berubah atau hilangnya Data Pribadi tersebut dan tetap wajib menjaga keamanan atau memberikan perlindungan rahasia Data Pribadi dalam Sistem Elektronik yang dikelolanya, memperoleh, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarluaskan Data Pribadi tanpa hak atau tidak sesuai dengan ketentuan dalam Peraturan Menteri ini atau peraturan perundang-undangan lainnya.		
		Undang-Undang Nomor 19 Tahun	dengan sengaja dan tanpa hak		

		2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik;	mengirimkan Informasi Elektronik dan/atau Dokumen Elektronik.		
		Rancangan Undang Undang Pelindungan Data Pribadi Tahun 2020:	a. dilarang memperoleh atau mengumpulkan Data Pribadi yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum atau dapat mengakibatkan kerugian Pemilik Data Pribadi. b. dilarang secara melawan hukum mengungkapkan Data Pribadi yang bukan miliknya. c. dilarang secara melawan hukum menggunakan Data Pribadi yang bukan miliknya.		

			d. dilarang secara melawan hukum memasang dan/atau mengoperasikan alat pemroses atau pengolah data visual di tempat umum atau fasilitas pelayanan publik yang dapat mengancam dan/atau melanggar pelindungan Data Pribadi. e. dilarang secara melawan hukum menggunakan alat pemroses atau pengolah data visual yang dipasang di tempat umum dan/atau fasilitas pelayanan publik yang digunakan untuk mengidentifikasi seseorang. f. dilarang memalsukan Data Pribadi dengan maksud untuk		

			menguntungkan diri sendiri atau orang lain atau yang dapat mengakibatkan kerugian bagi orang lain. g. dilarang menjual atau membeli Data Pribadi.		

1. Hukum Tindak Pidana Pencurian Data (*Data Theft*) di Indonesia

Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik menjelaskan bahwa:

Pasal 1 angka (1), berbunyi:

"Data Pribadi adalah data perseorangan tertentu yang disimpan, dirawat, dan dijaga kebenaran serta dilindungi kerahasiaannya."

Hal-hal yang dianggap sebagai data perseorangan di Indonesia sesuai dengan Pasal 58 ayat (2) Undang-Undang Nomor 24 Tahun 2013 tentang Perubahan atas Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan, meliputi:

1. Nomor KK;
2. NIK;
3. Nama lengkap;
4. Jenis kelamin;
5. Tempat lahir;
6. Tanggal/bulan/tahun lahir;
7. Golongan darah;
8. Agama/kepercayaan;
9. Status perkawinan;
10. Status hubungan dalam keluarga;
11. Cacat fisik dan/atau mental;
12. Pendidikan terakhir;

13. Jenis pekerjaan;

14. NIK Ibu kandung;

15. Nama Ibu kandung;

16. NIK Ayah;

17. Nama Ayah;

18. Alamat sebelumnya;

19. Alamat sekarang;

20. Kepemilikan akta kelahiran/Surat kenal lahir;

21. Nomor akta kelahiran/Nomor surat kenal lahir;

22. Kepemilikan akta perkawinan/Buku nikah;

23. Nomor akta perkawinan/Buku nikah;

24. Tanggal perkawinan;

25. Kepemilikan akta perceraian;

26. Nomor akta perceraian/Surat cerai;

27. Tanggal perceraian;

28. Sidik jari;

29. Iris mata;

30. Tanda tangan; dan

31. Elemen data lainnya yang merupakan aib seseorang.

Berdasarkan hasil wawancara mengenai pemahaman tentang Data Pribadi dengan Hakim, beliau menyatakan bahwa:

> "Mengenai data pribadi kaitannya adalah dengan data individu perseorangan, inti poinnya adalah sang pemilik data pribadi harus masuk dalam sistem penyelenggara yang mempunyai kaitan dengan elektronik: data pribadi itu perseorangan, tapi baru akan

diakui sebagai data pribadi apabila sudah diverifikasi keakuratannya dan harus bisa dicek akurasinya oleh penyelenggara elektronik tersebut. Data pribadi itu sifatnya terlalu individual, poin pentingnya adalah harus sudah terenskripsi yang keakuratannya sudah diverifikasi. Data pribadi mengacu pada penyelenggara elektronik, supaya bisa dienskripsi[41].”

Adapun pemahaman beliau tentang Tindak Pidana Pencurian Data adalah sebagai berikut:

“Kalau mengenai pencurian itu tindak pidana, UU yang menentukan dan tidak bisa berdiri sendiri. Hakim kalau akan menjatuhi hukuman itu butuh 2 faktor, yaitu terbukti secara sah dan meyakinkan (mengacu ke KUHAP, minimal alat bukti). Kalau tidak ada salah satunya, tidak bisa dijatuhi hukuman. Peraturan Perundangan itu bersanksi, kalau tidak berarti hakim tidak bisa memakainya. Tapi kalau Pencurian Data biasanya diatur dalam UU ITE (Pasal 30, 32, 43, 48) yang akan dijadikan hakim sebagai unsur apakah memenuhi atau tidak[42].”

Lalu mengenai penentuan tersangka (perorangan atau koorporasi), Hakim menyebutkan bahwa:

”Kalau Hakim akan menentukan tersangka, harus melihat unsur terlebih dahulu, seperti: apakah di dalam UU tertulis hukuman sebagai penyebar atau kelalaian atau kesengajaan. Seseorang untuk dapat diklasifikasi sebagai tersangka, harus memenuhi unsur-unsur sebagaimana dalam UU dan pasal-pasal yang bersanksi. Tapi, untuk sebagai terpidana dan terdakwa, Hakim harus melihat alat buktinya (contoh: saksi, surat, ahli, petunjuk). Semuanya bisa kena sanksi apabila memenuhi unsur yang sudah tertulis dalam pasal yang bersanksi[43].”

Mengenai Pemerintah sebagai payung hukum dalam melindungi data pribadi, Hakim menyatakan:

“Pemerintah sebagai pelaku penyelenggara sistem elektronik, contoh: berkaitan dengan KTP yang bersifat nasional. Induk semuanya adalah pemerintah, karena pemerintahlah yang

[41] Wawancara dengan Yogi Arsono, S.H., K.N., M.H, Hakim Pengadilan Negeri Semarang, pada hari Selasa, tanggal 2 Maret 2021.
[42] ibid.
[43] ibid.

> memberikan perlindungan atau memayungi. UU yang sudah disahkan juga merupakan salah satu contoh perlindungan hukum untuk masyarakat, agar semuanya terakomodasi dan tidak menyebar ke segala arah[44]."

Melihat dari Undang-Undang perlindungan data yang masih tersebar dalam beberapa pengaturan yang bersifat sektoral, pengaturan mengenai perlindungan data yang ada di Indonesia menurut Jaksa:

> "Belum menjadi UU, dan RUU belum disahkan, apalagi belum ada efek atau reaksi yang ditimbulkan dari UU tersebut. Jadi, masyarakat di Indonesia belum mendapat perlindungan hukum yang seutuhnya karena RUU belum disahkan[45]."

Pendapat Penulis mengenai hasil wawancara dengan Hakim dan Jaksa, Penulis merasa kurang setuju apabila dikatakan bahwa peraturan-peraturan yang ada saat ini sudah dapat menjadi payung hukum yang melindungi warga Indonesia, karena faktanya di Indonesia sendiri belum ada satu hukum yang pasti dan khusus untuk mengatur tentang Tindak Pidana Pencurian Data, bahkan dalam Undang-Undang yang bersifat sektoral atau tersebar yang sudah disebutkan di atas pun, belum ada pengaturan khusus yang mengatur tentang Tindak Pidana Pencurian Data Pribadi. Peraturan yang ada kebanyakan hanya menyinggung sedikit mengenai Pencurian Data.

Tindak Pidana Pencurian Data merupakan suatu Tindak Pidana yang bisa dilakukan dengan menggunakan perangkat komputer, dan juga bisa dilakukan dengan melalui komputer. Berbeda dengan *cybercrime* yang lainnya, yang kebanyakan hanya memenuhi satu syarat dari dua

[44] ibid.

[45] Wawancara dengan Ibu Lilis, Jaksa Kejaksaan Negeri Semarang, pada hari Rabu, tanggal 3 Maret 2021.

syarat tadi saja. Dapat disimpulkan bahwa Tindak Pidana Pencurian Data ini benar-benar suatu Tindak Pidana yang ganas dan harus diwaspadai.

Apabila di Indonesia belum ada satu peraturan yang khusus untuk mengatur hal ini, maka perlindungan hukum bagi Warga Indonesia menurut Penulis masih belum sempurna.

Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik menegaskan sebagai berikut:

> Pasal 26 ayat (1), berbunyi:
>
> "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."
>
> Pasal 26 ayat (2), berbunyi:
>
> "Setiap Orang yang dilanggar haknya sebagaimana dimaksud pada ayat (1) dapat mengajukan gugatan atas kerugian yang ditimbulkan berdasarkan Undang-Undang ini."

Yang berarti bahwa setiap orang bertanggung jawab atas data pribadinya masing-masing, dan apabila ada orang yang tidak bertanggung jawab dan menyebabkan hak orang lain dilanggar, maka gugatan dapat diajukan.

Salah satu tindak kejahatan yang kerap kali terjadi menyangkut dengan tindak pidana pencurian data adalah *cracking*. *Cracking* dapat berarti sebagai peretasan dengan cara merusak sebuah sistem elektronik. Selain merusak, *cracking* juga bisa mencakup tentang pembajakan data pribadi maupun akun pribadi seseorang, sehingga mengakibatkan data

pribadi maupun akun pribadi seseorang tadi hilang atau berubah dan digunakan tanpa persetujuan dari pemiliknya, bahkan merugikan pemilik data pribadi tersebut. Oleh karena itu, penggunaan data pribadi oleh *cracker* dengan tujuan sebagaimana dimaksud di atas dapat dikategorikan sebagai bentuk pelanggaran Pasal 26 ayat (1) Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Tindakan *cracking* ini dapat dikatakan termasuk perbuatan yang melanggar dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, yaitu:

Pasal 30 ayat (3), berbunyi:

"Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apapun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan."

Pasal 32, berbunyi:

(1) "Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik publik.

(2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun memindahkan atau mentransfer Informasi Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik Orang lain yang tidak berhak.

(3) Terhadap perbuatan sebagaimana dimaksud pada ayat (1) yang mengakibatkan terbukanya suatu Informasi Elektronik dan/atau Dokumen Elektronik yang bersifat rahasia menjadi dapat diakses oleh publik dengan keutuhan data yang tidak sebagaimana mestinya."

Sistem Elektronik tidak selamanya sempurna, pasti ada kerusakan ataupun kegagalan yang bisa terjadi dalam sistemnya. Lalu, apabila jika terjadi kerusakan ataupun kegagalan dalam pelindungan terhadap data pribadi yang dikelolanya, Penyelenggara Sistem Elektronik (PSE) wajib memberitahukannya secara tertulis kepada pemilik data pribadi tersebut. Kegagalan yang dimaksud adalah terhentinya sebagian atau seluruh fungsi sistem elektronik sehingga sistem elektronik yang menyimpan data menjadi tidak dapat berfungsi sebagaimana mestinya. Lalu, dari sini pemilik data pribadi tersebut dapat mengajukan gugatan apabila data pribadinya disalahgunakan.

Kegagalan sistem dapat disebabkan oleh faktor internal dan faktor eksternal. Salah satu faktor eksternal yang sering terjadi adalah adanya *cybercrime*. Sedangkan faktor internal yang terjadi kebanyakan dipicu oleh *human error*, atau kesalahan dari PSE tersebut. Dilihat dari jenis aktivitasnya, *cybercrime* itu sendiri dapat berupa *hacking, cracking, phising, identity theft, data theft*, dan lain-lain. Dampak kerugian yang timbul antara lain adalah kebocoran data pribadi, manipulasi data, pelanggaran privasi, kerusakan sistem, bahkan kerugian materiil dan sebagainya.

2. Hukum Tindak Pidana Pencurian Data (Data Theft) di Singapura

Menurut Personal Data Proctection Act 2021, Undang-undang ini memiliki tujuan yaitu sebagai pengatur pengumpulan, penggunaan, dan pengungkapan data pribadi yang dilakukan oleh organisasi dengan

mengakui hak individu guna melindungi data pribadi dan kebutuhan organisasi untuk mengumpulkan, menggunakan atau mengungkapkan data pribadi guna anggapan yang tepat bagi orang berakal sehat dalam keadaan tersebut.

Pihak-pihak yang dapat dikenai hukuman apabila melanggar Undang-Undang ini, antara lain:

1. Setiap individu yang bertindak dalam kapasitas pribadi atau domestik;
2. Setiap karyawan yang bertindak selama masa kerjanya di suatu organisasi;
3. Badan publik atau organisasi apa pun yang sedang bertindak atas nama badan publik terkait dengan pengumpulan, penggunaan, atau pengungkapan data pribadi; atau
4. Organisasi atau data pribadi lainnya, atau kelas organisasi atau data pribadi, yang ditentukan untuk tujuan ketentuan ini.

Undang-undang ini tidak akan berlaku sehubungan dengan;

1. Data pribadi tentang individu yang terkandung dalam catatan yang telah ada setidaknya selama 100 tahun; atau
2. Data pribadi tentang individu yang telah meninggal, kecuali bahwa ketentuan yang berkaitan dengan pengungkapan data pribadi dan pasal 24 (perlindungan data pribadi) akan berlaku sehubungan dengan data pribadi tentang seseorang yang telah meninggal selama 10 tahun atau kurang.

Menurut *Personal Data Protection Act 2012* Access to personal data atau akses ke data pribadi harus sesuai dengan hal-hal berikut ini:

"(1) Subject to subsections (2), (3) and (4), on request of an individual, an organisation shall, as soon as reasonably possible, provide the individual with;

(a) personal data about the individual that is in the possession or under the control of the organisation; and

(b) information about the ways in which the personal data referred to in paragraph (a) has been or may have been used or disclosed by the organisation within a year before the date of the request.

(2) An organisation is not required to provide an individual with the individual's personal data or other information under subsection (1) in respect of the matters specified in the Fifth Schedule.

(3) An organisation shall not provide an individual with the individual's personal data or other information under subsection (1) if the provision of that personal data or other information, as the case may be, could reasonably be expected to —

(a) threaten the safety or physical or mental health of an individual other than the individual who made the request;

(b) cause immediate or grave harm to the safety or to the physical or mental health of the individual who made the request;

(c) reveal personal data about another individual;

(d) reveal the identity of an individual who has provided personal data about another individual and the individual providing the personal data does not consent to the disclosure of his identity; or

(e) be contrary to the national interest.

(4) An organisation shall not inform any individual under subsection (1) that it has disclosed personal data to a prescribed law enforcement agency if the disclosure was made without the consent of the individual pursuant to paragraph 1(f) or (n) of the Fourth Schedule or under any other written law.

(5) If an organisation is able to provide the individual with the individual's personal data and other information requested under subsection (1) without the personal data or other information excluded under subsections (2), (3) and (4), the organisation shall provide the individual with access to the personal data and other information without the personal data or other information excluded under subsections (2), (3) and (4)."

Apabila diterjemahkan ke dalam Bahasa Indonesia, esensi dari ketentuan diatas adalah setiap organisasi yang menyimpan data pribadi seseorang bertanggung jawab sepenuhnya dan harus dapat menjaga data tersebut dengan sebaik-baiknya, karena sebagian besar hukuman atau sanksi di Singapura menitikberatkan pada organisasi-organisasi yang ada.

B. Sumbangan Pengaturan atau Formulasi Tindak Pidana Pencurian Data (*Data Theft*) dalam Hukum Pidana Singapura yang dapat diformulasikan dalam Hukum Pidana Indonesia

Menurut Penulis, beberapa hal dalam Hukum Pidana Indonesia dapat dilakukan formulasi setelah melakukan perbandingan kedua Pengaturan atau Formulasi Tindak Pidana Pencurian Data (Data Theft) pada kedua negara yaitu Indonesia dan Singapura. Pertama, sampai saat ini Indonesia belum memiliki satu hukum yang spesifik mengatur Pencurian Data yang pasti untuk difungsikan sebagai perlindungan hukum bagi Warga Indonesia, sedangkan pengaturan yang mengatur Hukum Pidana mengenai Pencurian Data tersebut umumnya memiliki sifat sektoral dan tersebar, selain itu terdapat pula pengaturan mengenai Pencurian Data yang belum memadai dan tidak membahas Pencurian Data secara rinci.

Dengan demikian, Penulis merasa bahwa perlu mengambil contoh dari Singapura dengan segera mengesahkan Rancangan Undang-Undang mengenai Tindak Pidana Pencurian Data, karena problematika tersebut kerap terjadi di Indonesia meskipun banyak Warga Indonesia yang tidak menyadarinya. Pada realitanya, Warga Indonesia kerap kali menjadi

korban Pencurian Data namun banyak yang tidak menyadarinya, karena kurangnya pemahaman masyarakat terhadap penyalahgunaan *privacy*. Menurut Penulis, melalui pengesahan Rancangan Undang-Undang mengenai Tindak Pidana Pencurian Data, data-data pribadi masyarakat di Indonesia akan lebih terlindungi dibandingkan dengan sebelumnya, dan di kemudian hari hal tersebut akan berdampak pada pengurangan Tindak Pidana Kejahatan Melalui dan Menggunakan Media Internet.

Dalam menyusun penelitian ini, Penulis mewawancarai Ibu Jaksa selaku Ahli Hukum, yang menyuarakan pendapat serupa. Beliau mengungkapkan perlunya suatu payung hukum untuk melindungi Warga Negara Indonesia terkait dengan data pribadi, sehingga merupakan hal baik apabila semua Undang-Undang yang mengatur mengenai data pribadi dikodifikasikan, dijadikan sebagai satu Undang-Undang khusus, seperti yang terdapat pada Singapura, yaitu *Personal Data Protection Act.*

Setiap orang memiliki pendapat yang berbeda-beda, dan semua orang mempunyai hak untuk mengungkapkan pendapatnya. Selain Ibu Jaksa, dalam menyusun penelitian ini, Penulis juga melakukan wawancara dengan Hakim yang mengungkapkan pendapat yang berbeda. Beliau berpendapat bahwa Undang-Undang di Indonesia sudah cukup memadai untuk melindungi para Warga Negaranya dalam cakupan Tindak Pidana Pencurian Data. Beliau juga mengutarakan bahwa Undang-Undang yang sudah disahkan merupakan salah satu contoh perlindungan hukum untuk

masyarakat Indonesia, agar semuanya terakomodasi dan tidak menyebar ke segala arah.

Menurut Penulis, apabila Undang-Undang yang mengatur tentang Tindak Pidana Pencurian Data Pribadi hanya sedikit menyinggung saja tanpa ada Undang-Undang khusus yang berlaku, itu nantinya akan menyebabkan kerugian besar bagi para korban yang datanya dicuri, dan akan menimbulkan kejahatan-kejahatan yang serupa di masa yang akan datang karena tiadanya Undang-Undang yang menjadi payung hukum bagi masyarakat.

Seiring dengan perkembangan zaman, pergerakan digital juga maju dengan pesat, dan begitu pula dengan kejahatan-kejahatan, otak-otak kriminal yang akan selalu dengan liciknya mengikuti perkembangan jaman. Maka dari itu, sangat dibutuhkan perlindungan hukum untuk kategori Informasi dan Transaksi Elektronik (ITE) untuk melindungi masyarakat Indonesia dari kejahatan-kejahatan tersebut, mengingat kerugian yang dapat timbul cukup besar apabila sampai menjadi salah satu korban. Penulis berharap supaya Rancangan Undang-Undang tentang Perlindungan Data Pribadi segera disahkan oleh para anggota DPR untuk menanggulangi kerugian-kerugian yang disebabkan oleh Tindak Pidana Pencurian Data Pribadi.

Kedua, Penulis merasa bahwa terdapat kemungkinan sanksi-sanksi yang diterapkan di Singapura dapat diformulasikan ke Indonesia. Contohnya adalah menjadi sukarelawan, disamping sanksi ini sangat

membantu masyarakat sekitar yang membutuhkan, Penulis merasa bahwa sanksi ini juga dapat meningkatkan rasa kemanusiaan dalam diri para pelaku kejahatan. Selain dididik untuk menjadi jera, akan lebih baik juga apabila dididik untuk menjadi pribadi yang lebih baik.

Sanksi-sanksi lain yang dapat dijatuhkan kepada pelaku Tindak Pidana Pencurian Data di Singapura sebagian besar sudah sama dengan yang ada di Indonesia, yaitu ada pidana penjara dan denda. Sanksi untuk menjadi Pekerja Sukarela atau biasa disebut dengan *Voluntary Undertakings* jarang terdengar di Indonesia. Hal ini dapat diformulasikan sebagai sebuah pembinaan untuk para pelaku Tindak Pidana Pencurian Data.

Setiap penjatuhan pidana kepada pelaku kejahatan haruslah berhati-hati karena masalah pemberian pidana apapun bentuknya berkaitan erat dengan karakter dan sifat orang yang dijatuhkan sanksi pidana. Sanksi pidana bukan semata-mata sebagai pembalasan tetapi pidana harus bersifat prospektif dan berorientasi kedepan. Oleh karena itu, antara pemberian sanksi pidana dengan pelaku tindak pidana harus terdapat kesesuaian, sehingga (antara) tujuan diberikannya dalam menjatuhkan sanksi pidana harus memperhatikan sifat-sifat atau karakter dari sifat pelaku tindak pidana[46].

Namun, itu semua harus disesuaikan terlebih dahulu, contohnya dengan cara memilih peserta yang dianggap mampu mematuhi ketentuan-

[46] Hamja, 2015, *Mimbar Hukum Volume 27, Nomor 3: Model Pembinaan Narapidana Berbasis Masyarakat (Community Based Corrections) Dalam Sistem Peradilan Pidana*, Yogyakarta: Fakultas Hukum Universitas Gadjah Mada, hlm. 445.

ketentuan yang ada. Pemilihan peserta tersebut dapat dipertimbangkan berdasarkan faktor-faktor yang ada, yaitu faktor wilayah, apabila wilayahnya tidak memadai maka tidak dapat dilaksanakan hukuman pekerjaan sukarela tersebut, faktor usia, apabila usianya terlalu muda ada kemungkinan akan mengalami kesulitan memasuki dunia kerja, sedangkan narapidana yang usianya terlalu tua akan mengalami kesulitan pada jenis pekerjaan yang sesuai dengan narapidananya yang luas ada di masyarakat. Lalu, faktor jenis kelamin, karena narapidana perempuan masih relative sedikit, dan faktor narapidana yang membahayakan, mungkin akan ada narapidana dengan kasus-kasus tertentu yang dianggap sebagai kasus yang berbahaya, dan lain sebagainya, supaya hukuman pekerjaan sukarela tadi yang bertujuan baik tidak menjadi sebuah *boomerang* yang bisa saja malah mencelakai orang lain.

Prinsip pertama, narapidana harus memiliki kemauan dan kesempatan untuk pekerjaan sukarela, prinsip kedua yang harus diterapkan adalah pelaku Tindak Pidana harus diseleksi terlebih dahulu, lalu prinsip yang ketiga adalah narapidana tidak boleh dieksploitasi.

Apabila itu semua dapat dilaksanakan dengan baik dan para pelaku Tindak Kejahatan dapat berkoorperasi dengan maksimal, menurut Penulis akan ada terobosan dalam pelaksanaan Hukum di Indonesia. Para pelaku Tindak Kejahatan akan menjadi pribadi yang lebih baik dari sebelumnya, dan tentunya akan tetap menimbulkan efek jera karena telah melakukan kejahatan yang telah merugikan orang lain.