

DigiTimes #22
MEI 2019

PERLINDUNGAN DATA PRIBADI DI INDONESIA: PERSPEKTIF HUKUM DAN SOSIAL



cfDS
CENTER FOR DIGITAL SOCIETY

Room BC 201 - 202
Faculty of Social and Political Sciences
Universitas Gadjah Mada
Jalan Sosio Yustisia 1, Bulaksumur, Yogyakarta
(0274) 563362, Ext. 116 | cfds.fisipol@ugm.ac.id



Researchers

Faiz Rahman
Anggika Rahmadiani

Editor

Anisa Pratita Kirana Mantovani

Cover Design and Layout

Masgustian

May 2019

■ DAFTAR ISI

2	PENDAHULUAN
3	Pengaturan mengenai Perlindungan Data Pribadi di Indonesia
10	Perlindungan Data Pribadi Ditilik dari Perspektif Sosial
12	Tantangan Era Keterbukaan Data: Tanggung Jawab Pemerintah Indonesia
13	Administrasi Publik: E-KTP dan Pendaftaran Kartu SIM Prabayar
14	Bisnis: <i>Direct Marketing</i>
15	Bisnis: <i>Skimming</i> ATM dan Keamanan Perbankan Indonesia
15	Bisnis: Data Pribadi Penumpang Transportasi Online
16	Kesimpulan





■ PENDAHULUAN

Tidak dapat dipungkiri bahwa di era digital seperti sekarang ini, keamanan siber menjadi aspek yang selalu menjadi diskursus tersendiri dalam pembahasan mengenai dunia digital. Lebih lanjut, salah satu isu terkait keamanan siber yang belakangan kerap diperbincangkan oleh publik berkaitan dengan isu privasi atau perlindungan terhadap data pribadi. Apalagi, dengan semakin berkembangnya teknologi-teknologi seperti *big data*, *Internet of Things*, maupun *Artificial Intelligence*, data pribadi memiliki posisi yang cukup signifikan. Salah satu hal yang menjadi perhatian adalah adanya tendensi penyalahgunaan dalam pemanfaatan data pribadi masyarakat yang dikumpulkan secara masif, baik oleh pemerintah maupun oleh pihak swasta, dengan memanfaatkan berbagai teknologi sebagaimana disebutkan di atas.

Dapat dilihat dari beberapa contoh kasus yang terjadi selama setahun ke belakang, seperti misalnya isu kebocoran NIK dan KK dalam proses registrasi kartu SIM di Indonesia¹, serta insiden kebocoran data pengguna Facebook Indonesia pada kasus Cambridge Analytica², membuat atensi terhadap perlindungan data pribadi semakin meningkat. Bahkan, pasca insiden Cambridge Analytica yang juga berdampak pada pengguna dari Indonesia, dorongan berbagai kalangan masyarakat kepada DPR dan Pemerintah untuk segera mengesahkan RUU Perlindungan Data Pribadi (RUU PDP) juga semakin kuat. Hal ini direspons dengan usulan dimasukkannya RUU PDP ke dalam program legislasi nasional pada tahun 2019³. Padahal, Naskah Akademik dan RUU PDP sendiri telah dibuat sejak tahun 2015.⁴

Apabila melihat dari konteks regulasi, Indonesia hingga saat ini belum memiliki undang-undang yang secara komprehensif mengatur mengenai perlindungan data pribadi, akan tetapi cenderung sporadis tersebar di berbagai undang-undang yang sifatnya sektoral. Pengaturan yang secara eksplisit mengatur tentang perlindungan data pribadi justru berada pada level peraturan menteri, yakni melalui Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik (Permenkominfo PDPSE), yang merupakan amanat dari Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE). Pengaturan tersebut pun

dinilai oleh masyarakat masih belum cukup dalam memberikan perlindungan hukum atas data pribadi mereka.

Tulisan ini mencoba memberikan gambaran mengenai *status quo* perlindungan data pribadi di Indonesia dengan melihat dari dua aspek, yakni aspek yuridis dan aspek sosial. Pendekatan dari aspek yuridis dilakukan untuk melihat bagaimana kondisi pengaturan mengenai perlindungan data pribadi di Indonesia saat ini, sedangkan pendekatan dari aspek sosial diperlukan untuk melihat bagaimana dan seberapa besar dampak sosial yang mungkin terjadi dengan tidak adanya pengaturan tentang perlindungan data pribadi yang memadai.



■ PENGATURAN MENGENAI PERLINDUNGAN DATA PRIBADI DI INDONESIA

Berbicara mengenai perlindungan data pribadi, tentu tidak terlepas dari konstruksi perlindungan hak atas privasi. Hal ini dapat dilihat salah satunya melalui penjelasan Pasal 26 ayat (1) Undang-Undang Nomor 11 Tahun 2008 *jo.* Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE), yang menyebutkan bahwa perlindungan data pribadi merupakan salah satu bagian dari hak pribadi (*privacy rights*).⁵ Kendati demikian, dalam Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 (UUD NRI Tahun 1945) sebagai Konstitusi Indonesia, hak pribadi tidak disebutkan secara eksplisit sebagai salah satu hak asasi manusia yang secara konstitusional

dilindungi. Hak pribadi ditafsirkan oleh beberapa pihak sebagai bagian dari “hak atas perlindungan diri pribadi” sebagaimana diatur dalam Pasal 28G ayat (1) UUD NRI Tahun 1945.⁶

Dalam konteks internasional, hak atas privasi merupakan salah satu hak yang dilindungi oleh beberapa konvensi internasional seperti *Universal Declaration of Human Rights* (UDHR) dan *International Covenant on Civil and Political Rights* (ICCPR), atau *European Convention of Human Rights* (ECHR) pada tingkat regional. Lebih lanjut, McDermott menyatakan bahwa adanya pengaturan mengenai perlindungan data pribadi dapat menegakkan empat prinsip HAM



yakni *privacy* (privasi), *transparency* (transparansi), *autonomy* (otonomi), dan *non-discrimination*.⁷ Berbagai negara juga telah mengundang undang-undang mengenai data pribadi, seperti misalnya di *General Data Protection Regulation* di tingkat Uni Eropa, *Data Protection Act 2018* di Inggris, *Personal Data Protection Act 2012* di Singapura, *the Malaysian Personal Data Protection Act 2010* di Malaysia, maupun *Personal Information Protection Act 2011* di Korea Selatan.

Apabila melihat pada beberapa negara di atas, Indonesia dapat dikatakan cukup tertinggal dalam hal pengaturan mengenai perlindungan data pribadi secara menyeluruh, khususnya pada level undang-undang. Kendati demikian, perlindungan terhadap data pribadi sudah menjadi perhatian sejak lama, meskipun hanya terhadap data pribadi pada sektor-sektor tertentu. Sebagai contoh, dalam Undang-Undang Nomor 7 Tahun 1992 *jo.* Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan (UU Perbankan), diatur mengenai kewajiban Bank untuk merahasiakan data pribadi nasabah, meskipun terdapat pengecualian-kecualian pada hal-hal tertentu.⁸ Pada sektor lain, misalnya sektor kesehatan, dijelaskan mengenai perlindungan pasien, yang secara spesifik salah satunya

mengatur hak pasien atas rahasia kondisi kesehatan pribadinya,⁹ meskipun tidak dijelaskan bagaimana kemudian pelaksanaan dari perlindungan terhadap hak tersebut. Dalam Undang-Undang Nomor 43 Tahun 2009 tentang Kearsipan (UU Kearsipan) juga disebutkan bahwa pencipta arsip dapat menutup akses atas arsip dengan alasan apabila akses arsip tersebut dibuka dapat mengungkapkan rahasia atau data pribadi.¹⁰

Lebih lanjut, berdasarkan penelusuran, frasa “data pribadi” didefinisikan secara yuridis pertama kali dalam Undang-Undang No. 23 Tahun 2006 tentang Administrasi Kependudukan (UU Adminkuk), yakni data perseorangan tertentu yang disimpan, dirawat, dan dijaga kebenaran serta dilindungi kerahasiaannya.¹¹ Apabila merujuk pada definisi tersebut, maka segala informasi yang dirahasiakan, khususnya berdasarkan amanat dari peraturan perundang-undangan, dapat diklasifikasikan sebagai data pribadi, termasuk informasi nasabah dan data kesehatan pasien sebagaimana telah dipaparkan di atas.

Dalam UU Adminkuk sendiri, terdapat satu Bab, yakni Bab IX yang secara spesifik mengatur mengenai perlindungan data pribadi penduduk (khusus terkait dengan data kependudukan). Dalam Bab tersebut diatur mengenai jenis data pribadi yang dilindungi, sedangkan terkait dengan penyimpanan dan perlindungannya diatur lebih lanjut dalam Peraturan Pemerintah.¹² Jenis data pribadi yang dilindungi dalam UU Adminkuk pun juga mengalami perkembangan. Untuk lebih jelasnya dapat dilihat pada tabel berikut:

Tabel 1. Perbandingan Jenis Data Pribadi dalam UU Adminduk 2006 dan UU Adminduk 2013¹³

UU Adminduk 2006	UU Adminduk 2013
Pasal 84 (1) Data Pribadi Penduduk yang harus dilindungi memuat: a. nomor KK; b. NIK; c. tanggal / bulan / tahun lahir; d. keterangan tentang kecacatan fisik dan/atau mental; e. NIK ibu kandung; f. NIK ayah; dan Beberapa isi catatan peristiwa Penting (catatan mengenai data yang bersifat pribadi dan berkaitan dengan peristiwa penting yang perlu dilindungi;	Pasal 84 (1) Data Pribadi Penduduk yang harus dilindungi memuat: a. keterangan tentang cacat fisik dan/atau mental; b. sidik jari; c. iris mata; d. tanda tangan; dan e. elemen data lainnya yang merupakan aib seseorang

Berdasarkan tabel di atas, dapat terlihat bahwa ada perhatian yang lebih khusus diberikan terhadap data-data pribadi yang lebih khusus, seperti sidik jari, iris mata, dan tanda tangan. Hal ini menjadi logis apabila dilihat secara historis bahwa hal-hal tersebut merupakan data pribadi yang dikumpulkan dalam proses pembuatan KTP elektronik sejak tahun 2010.¹⁴

Dalam undang-undang lain, misalnya Undang-Undang No. 14 Tahun 2008 tentang Keterbukaan Informasi Publik (UU KIP), memberikan jenis-jenis “informasi yang berkaitan dengan hak-hak pribadi”, yakni:¹⁵

- a. riwayat dan kondisi anggota keluarga;
- b. riwayat, kondisi dan perawatan, pengobatan kesehatan fisik, dan psikis seseorang;
- c. kondisi keuangan, aset, pendapatan, dan rekening bank seseorang;
- d. hasil-hasil evaluasi sehubungan dengan kapabilitas, intelektualitas, dan rekomendasi kemampuan seseorang; dan/atau
- e. catatan yang menyangkut pribadi seseorang yang berkaitan dengan kegiatan satuan pendidikan formal dan satuan pendidikan non-formal.



Jenis informasi yang berkaitan dengan hak-hak pribadi sebagaimana disebutkan di atas telah menunjukkan adanya akomodasi dari beberapa jenis data pribadi, riwayat kesehatan (poin b), kondisi keuangan (poin c), serta hal-hal yang sifatnya personal lainnya (poin a, d, dan e). Tentunya, jenis-jenis informasi tersebut berkaitan dengan informasi publik, yakni informasi yang dihasilkan, disimpan, dikelola, dikirim, dan/atau diterima oleh suatu badan publik yang berkaitan dengan penyelenggara dan penyelenggaraan negara, serta informasi lain terkait kepentingan publik.¹⁶

Dalam konteks digital, pengaturan terkait dengan data pribadi dipayungi oleh UU ITE. Kendati demikian, pengaturan mengenai data pribadi dalam UU ITE hanya terdapat dalam 1 pasal, yakni Pasal 26, yang menyatakan bahwa penggunaan informasi melalui media elektronik yang menyangkut data pribadi harus dilakukan atas persetujuan orang yang bersangkutan.¹⁷ Apabila terdapat pelanggaran terhadap hal tersebut, maka orang yang bersangkutan dapat mengajukan gugatan atas kerugian yang ditimbulkan.¹⁸ Meskipun terdapat pengaturan mengenai data pribadi, akan tetapi dalam UU ITE tidak dapat ditemukan definisi mengenai apa yang disebut sebagai data pribadi. Definisi data pribadi baru ditemui pada level Peraturan Pemerintah, yang mana definisi tersebut sama seperti definisi data pribadi dalam UU Adminduk sebagaimana



telah dipaparkan di atas.

Perlindungan terhadap data pribadi dalam ketentuan PP PSTE merupakan salah satu kewajiban dari Penyelenggara Sistem Elektronik, yang mencakup pula pemerintah dan pihak swasta yang menyelenggarakan sebuah sistem elektronik. Dalam PP PSTE, dinyatakan bahwa Penyelenggara Sistem Elektronik wajib:¹⁹

- a. menjaga rahasia, keutuhan, dan ketersediaan Data Pribadi yang dikelolanya;
- b. menjamin bahwa perolehan, penggunaan, dan pemanfaatan Data Pribadi berdasarkan persetujuan pemilik Data Pribadi, kecuali ditentukan lain oleh peraturan perundang-undangan; dan
- c. menjamin penggunaan atau pengungkapan data dilakukan berdasarkan persetujuan dari pemilik Data Pribadi tersebut dan sesuai dengan tujuan yang disampaikan kepada pemilik Data Pribadi pada saat perolehan data.



Dalam rangka menegakkan kewajiban tersebut, diamanatkan adanya pengaturan lebih lanjut mengenai pedoman perlindungan data pribadi dalam sistem elektronik, yang kemudian diatur dalam Peraturan Menteri Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik (Permenkominfo PDPSE).

Pengaturan mengenai perlindungan data pribadi dalam Permenkominfo PDPSE dapat dikatakan sudah memuat beberapa hal yang krusial seperti misalnya cakupan perlindungan data pribadi (misalnya dalam proses perolehan, pengolahan, penyimpanan, pengiriman, dan pembukaan akses), hak pemilik data pribadi, kewajiban pengguna data pribadi, kewajiban penyelenggara sistem elektronik, penyelesaian sengketa terkait data pribadi, pengawasan, dan sanksi administratif. Apabila membandingkan dengan beberapa UU di negara lain seperti UU PDP di Malaysia, UU PIP di Korea Selatan, dan juga GDPR di Uni Eropa, maka Permenkominfo PDPSE belum menunjukkan adanya klasifikasi terhadap data pribadi itu sendiri, baik data pribadi umum maupun data pribadi yang khusus.

Kendati beberapa substansi penting dalam konteks perlindungan data pribadi telah diakomodir dalam Permenkominfo PDPSE, pengaturan dalam level peraturan menteri dirasa masih belum cukup, utamanya dalam konteks penegakan hukum dalam hal terjadi permasalahan hukum terkait dengan

penyalahgunaan data pribadi. Adanya ketentuan sanksi yang lebih kuat dirasa perlu dalam rangka perlindungan terhadap data pribadi. Hal ini mengingat bahwa pada level peraturan menteri, tidak memungkinkan adanya pengaturan mengenai ketentuan pidana, mengingat ketentuan pidana hanya dapat diatur pada level undang-undang dan secara terbatas pada peraturan daerah.²⁰

Sebagaimana telah disampaikan di atas, sejak tahun 2015, Badan Pembinaan Hukum Nasional telah mempublikasikan Naskah Akademik dan Rancangan Undang-Undang Perlindungan Data Pribadi.²¹ Pengaturan terhadap perlindungan data pribadi dalam RUU tersebut dapat dikatakan cukup komprehensif. Untuk lebih lengkapnya dapat dilihat pada tabel berikut:



**Tabel 2. Materi Muatan Rancangan Undang-Undang
Perlindungan Data Pribadi Indonesia**

Materi Muatan RUU PDP Versi 2015

1. Ketentuan Umum
2. Asas dan Tujuan, Ruang Lingkup, Prinsip-Prinsip Perlindungan Data Pribadi
3. Penyelenggaraan Data Pribadi (jenis data pribadi, penyelenggara Data Pribadi dan Pemroses Data Pribadi, Penyelenggaraan Data Pribadi)
4. Hak Pemilik Data Pribadi
5. Kewajiban Penyelenggara Data Pribadi (persetujuan penyelenggara data pribadi, keamanan data pribadi, akses dan perbaikan data pribadi, pengawasan, akurasi, perlindungan dan pemusnahan data pribadi, alat pemroses/pengolah data visual/CCTV, data pribadi yang terungkap)
6. Pengecualian terhadap Perlindungan Data Pribadi
7. Komisi (fungsi, tugas dan wewenang)
8. Transfer Data Pribadi (kepada pihak ketiga dalam wilayah NKRI; dalam penggabungan, pemisahan, peleburan perusahaan atau transaksi bisnis lainnya; yang sifatnya lintas batas nasional)
9. Pemasaran Langsung
10. Pembentukan Pedoman Perilaku Penyelenggara Data Pribadi
11. Kerjasama Internasional
12. Partisipasi Masyarakat
13. Penyelesaian Sengketa
14. Ketentuan Pidana
15. Hukum Acara Komisi (mediasi, adjudikasi, melalui Komisi Informasi, pemeriksaan, putusan Komisi Informasi)
16. Aturan Peralihan
17. Ketentuan Penutup

Jumlah Pasal: 55 Pasal

Materi muatan dalam RUU PDP tersebut memiliki kemiripan dengan UU Perlindungan Data Pribadi Malaysia dan Singapura. Hal tersebut salah satunya dikarenakan kedua UU PDP di kedua negara tersebut dijadikan sebagai salah satu acuan dalam perancangan RUU PDP Indonesia. Selain itu, dalam perancangan NA dan RUU tersebut, telah dilakukan pula analisis terhadap beberapa undang-undang yang terkait dengan data pribadi, seperti misalnya UU Perbankan, UU Telekomunikasi, UU Perlindungan Konsumen, UU Adminduk, UU KIP, dan UU ITE. Hal ini menjadi penting untuk melihat bagaimana keterkaitan antara berbagai peraturan perundang-undangan, khususnya berbagai undang-undang yang mengatur terkait dengan data pribadi.

Harmonisasi pengaturan juga diperlukan untuk mencegah adanya tumpang tindih pengaturan yang justru dapat menghambat pelaksanaan perlindungan data pribadi di Indonesia. Terlepas dari hal tersebut, keinginan politik dan perhatian DPR terhadap isu perlindungan data pribadi menjadi hal yang krusial, sehingga pembahasan terhadap draf RUU PDP dapat segera dilakukan, untuk kemudian RUU

tersebut dapat segera diselesaikan dan pada akhirnya dapat diimplementasikan.

Lebih lanjut, mengingat salah satu sifat dari dunia digital yang tanpa batas (*borderless*), maka risiko pelanggaran terhadap data pribadi juga dapat dilakukan oleh pihak asing, tidak hanya warga negara Indonesia. Sebagai contoh, kasus Cambridge Analytica beberapa waktu silam yang juga berdampak pada data pengguna Indonesia. Maka dari itu, kehadiran pengaturan yang lebih kuat, terutama pada level undang-undang, dirasa diperlukan dalam rangka perlindungan terhadap data pribadi, sehingga dapat lebih memberikan jaminan kepastian hukum dalam pelaksanaan dan penegakannya. Hal ini juga berkaitan dengan konstruksi hukum perlindungan data pribadi, yang pada dasarnya dapat dikatakan sebagai bentuk manifestasi perlindungan hak atas diri pribadi yang dilindungi oleh UUD NRI Tahun 1945. Kehadiran pengaturan yang lebih kuat dan komprehensif tentang perlindungan data pribadi, didukung dengan mekanisme penegakan hukum yang jelas dan tegas, menjadi hal yang penting, terutama di era digital seperti sekarang ini. Dengan demikian, diharapkan hal tersebut dapat meminimalisir terjadinya penyalahgunaan terhadap data pribadi, baik yang dikumpulkan, disimpan, dan diproses oleh pemerintah atau oleh pihak-pihak yang lainnya.



■ PERLINDUNGAN DATA PRIBADI DITILIK DARI PERSPEKTIF SOSIAL

Semenjak masyarakat mengenal *world wide web*, terdapat perubahan pola konsumsi dan produksi di masyarakat yang juga dipengaruhi dari munculnya ekonomi digital. Digitalisasi pun menyebar di berbagai lini, pada pemerintahan mulai diperkenalkan *e-government*, sedangkan interaksi sosial masyarakat mulai beralih ke media sosial. Jejak digital atas data pribadi di laman daring menjadi langkah awal pengguna untuk melakukan aktifitas digital. Transformasi ini menyebabkan adanya perubahan perspektif dalam memandang data pribadi yang awalnya hanya sekedar pemenuhan administratif menjadi salah satu jenis aset yang strategis, baik untuk individu maupun publik.

Data pribadi menjadi aset strategis ketika digitalisasi telah masuk ke ranah sosial, ekonomi dan administrasi publik dengan meningkatnya penggunaan teknologi seperti komputasi awan, *big data* dan *internet of things*. Transformasi digital ini menyebabkan keterhubungan tak terbatas dan munculnya isu terkait penyimpanan dan penggunaan data pribadi. Masyarakat mulai mempertanyakan bagaimana data pribadinya dikelola, hal ini mencuat karena mulai maraknya kebocoran data pribadi akhir-akhir ini. Hal ini disebabkan proses pengumpulan data pribadi tidak selalu transparan dan membutuhkan persetujuan dari pemilik data pribadi tersebut. Misalnya, model bisnis di era digital, contohnya adalah *Infomediary* dan *Advertising Model* sangat tergantung pada pendaftaran, penggunaan

dan penyebaran data pribadi pengguna dalam sebuah platform digital agar pengguna memiliki akses untuk konten dan jasa.²³

Sementara itu, diskusi mengenai data pribadi akan berkaitan secara langsung dengan privasi. Sejauh ini, privasi dilindungi sebagai salah satu hak asasi manusia dalam Pasal 12 Deklarasi Universal Hak Asasi Manusia. Sedangkan perlindungan Data Pribadi membutuhkan sebuah mekanisme yang lebih spesifik dan ditujukan kepada mekanisme bagaimana pihak ketiga yang mengelola data individu mengelola informasi dalam pengumpulan, pemrosesan, penyimpanan, penggunaan dan penyebaran data pribadi.²⁴

Secara teknis, definisi atas data pribadi adalah segala macam informasi yang bisa mengidentifikasi seorang individu, yang dapat diakses dan diproses. Pemerintah Indonesia



telah mendefinisikan batasan dari Data Pribadi dalam Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Pasal 1 yaitu: *"Data Pribadi adalah data perseorangan tertentu yang disimpan, dirawat, dan dijaga kebenaran serta dilindungi kerahasiaannya. Pemilik Data Pribadi adalah individu yang padanya melekat Data Perseorangan Tertentu, Persetujuan Pemilik Data Pribadi yang selanjutnya adalah pernyataan secara tertulis baik secara manual dan/atau elektronik yang diberikan oleh Pemilik Data Pribadi setelah mendapat penjelasan secara lengkap mengenai tindakan perolehan, pengumpulan, pengolahan, penganalisisan, penyimpanan, penampilan, pengumuman, pengiriman, dan penyebarluasan serta kerahasiaan atau ketidakrahasiaan Data Pribadi."* Menurut UNCTAD *Global Cyber Law Tracker*, sebanyak 60 negara-negara berkembang belum memiliki landasan dasar hukum bagi perlindungan data pribadi dan 35 negara masih menggodok draft regulasi perlindungan data pribadi. Indonesia termasuk dalam 95 negara berkembang tersebut.

Uni Eropa pada Mei 2018 telah resmi menerapkan regulasi perlindungan data yaitu General Data Protection Regulation (GDPR). GDPR menjadi rezim perlindungan data pribadi regional yang berlaku di negara Uni Eropa, namun secara bersamaan juga menuntut

negara-negara lain untuk memiliki regulasi perlindungan data pribadi yang serupa dalam konteks pertukaran data pribadi yang terjadi dalam transaksi perdagangan internasional di platform-platform e-commerce.²⁵

Dalam konteks negara Indonesia, regulasi mengenai perlindungan data pribadi akan membutuhkan upaya dua arah, baik dari pemerintah sebagai regulator dan pihak swasta sebagai pengelola akses data pribadi serta masyarakat sebagai pemilik data pribadi tersebut. Perlindungan data pribadi akan berhasil dengan memperhatikan tiga faktor yang bekerja yaitu (1) regulasi terpusat pemerintah (2) kesadaran masyarakat akan keamanan data pribadi (3) kerjasama teknis yang berkelanjutan antar pengelola akses data pribadi, pemilik data, dan pemerintah.



TANTANGAN ERA KETERBUKAAN DATA: TANGGUNG JAWAB PEMERINTAH INDONESIA

Sensitifitas data pribadi dan kalkulasi risikonya tidak termanifestasikan dalam mekanisme perlindungan data di Indonesia. Pemerintah Indonesia telah mengatur mengenai tertib administrasi kependudukan dalam UU No. 23 Tahun 2006, dimana secara jelas juga disebutkan bahwa Negara yang bertanggungjawab atas perlindungan kerahasiaan data pribadi penduduknya. Pemaknaan 'ketidaktertiban administrasi' bergeser dari yang awalnya sekedar ketidaklengkapan data menjadi buruknya sistem perlindungan data pribadi oleh pengelola data. Individu menjadi subjek utama yang paling dirugikan dari absennya regulasi tentang perlindungan data pribadi. Regulasi perlindungan data pribadi yang masih bersifat sektoral belum cukup menangani karakteristik cepatnya persebaran data pribadi di era digital ini. Diperlukan sistem perlindungan data pribadi yang terintegrasi untuk menjawab tantangan ini.

Absennya regulasi tentang perlindungan data pribadi membawa berbagai konsekuensi sosial permasalahan penyalahgunaan data pribadi akhir-akhir ini di Indonesia. Berikut adalah kasus-kasus prominen yang bisa dijadikan pembelajaran antisipatif atas konsekuensi yang mungkin muncul bagi para pengampu kebijakan untuk merumuskan regulasi perlindungan data pribadi berdasarkan permasalahan empiris di lapangan. Studi kasus ini akan dibagi menjadi permasalahan dalam dua sektor, yaitu pemerintah dan pelaku bisnis selaku aktor yang akan menjadi pengelola data pribadi.





ADMINISTRASI PUBLIK: E-KTP DAN PENDAFTARAN KARTU SIM PRABAYAR

Selain dari perlindungan konsumen, konsekuensi tidak dimilikinya regulasi perlindungan data pribadi adalah tidak terjaminnya kerahasiaan dan keamanan data pribadi masyarakat oleh Pemerintah. Pemerintah Indonesia memiliki polemik dengan adanya adaptasi digital di lini pemerintahan, khususnya di catatan sipil dan kependudukan dengan diberlakukannya E-KTP. Polemik muncul ketika NIK E-KTP digunakan untuk registrasi kartu SIM prabayar yang hanya boleh maksimal dipakai untuk tiga nomor. Terdapat dugaan penyalahgunaan data pribadi dengan ditemukannya perbedaan jumlah penduduk sekitar 45 juta NIK, sementara data pemerintah menyebutkan jumlah lain, sebesar 350,7 juta dengan data operator seluler sebagai pihak ketiga yang mengelola data yang hanya sebesar 304 juta.²⁶ Fakta lain yang mendukung adalah, ditemukannya pencurian data NIK untuk mendaftarkan 11 nomor kartu prabayar.²⁷

Dugaan kebocoran data pengguna layanan kartu SIM prabayar ini bukan yang pertama kalinya. Di tahun 2011, Indonesia juga dikejutkan dengan bocornya data 25 juta pelanggan kartu SIM prabayar kepada para penyedia Kredit Tanpa Agunan (KTA) yang menyebarkan pesan penawaran *spam*. Yayasan Lembaga Konsumen Indonesia menduga adanya peran operator seluler dalam kebocoran data yang meresahkan para pengguna.²⁸

Konsekuensi bocornya data NIK E-KTP akan sangat berbahaya bagi masyarakat Indonesia. Bukan hanya transaksi digital, tetapi transaksi administrasi lainnya di segala lini yang menggunakan data KTP akan rentan terhadap pencurian data pribadi, seperti keuangan dan asuransi kesehatan. Arsitektur keamanan data pribadi di Pemerintah Indonesia belum mumpuni untuk memiliki ketahanan terhadap ancaman-ancaman siber. Apabila dalam waktu mendatang Pemerintah akan menggunakan sistem e-vote dalam pemilihan umum, data NIK dalam E-KTP ini akan sangat rentan untuk dicuri apabila tidak memiliki regulasi keamanan data pribadi.



■ BISNIS: DIRECT MARKETING

Menurut hasil survey tim perumus Rancangan Undang-Undang Perlindungan Data Pribadi pada tahun 2017, kasus penyalahgunaan data pribadi di Indonesia paling banyak adalah spamming sebagai teknik direct marketing, dengan 83% responden menyatakan pernah menjadi target *direct marketing* dari hotel, asuransi maupun iklan produk.²⁹

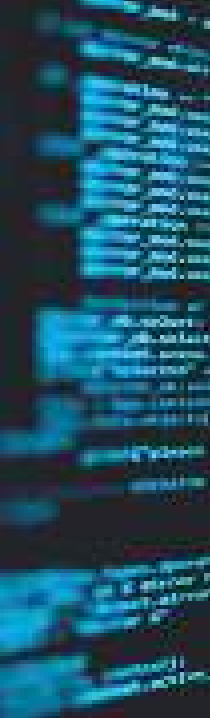
Statistik ini juga serupa dengan pengaduan konsumen pada Yayasan Lembaga Konsumen Indonesia dimana aduan penawaran kartu kredit dan asuransi lewat *direct marketing* menempati posisi paling atas. Lebih lanjut, YLKI dan Direktorat Tindak Pidana Ekonomi dan Khusus Bareskrim Polri menyelidiki bahwa terdapat praktik jual-beli data nasabah secara online sejak tahun 2010.³⁰ Menurut Return Path Q3 Email Intelligence Report, *direct marketing* melalui surat elektronik di Amerika Serikat mendapatkan komplain sebanyak 70% dari total keseluruhan komplain mengenai *spam*.³¹

Selain dari surat elektronik, kerap masyarakat mendapatkan panggilan telepon dari pihak perusahaan yang berisi tentang promosi produk. Pola ini sudah lumrah terjadi, seperti Pemerintah Inggris yang mendapatkan temuan bahwa setengah dari komplain tentang pelanggaran perlindungan data pribadi datang dari *spam phone calls*.³²

Apabila Indonesia telah memiliki rezim regulasi yang mumpuni di bidang perlindungan data pribadi, Pemerintah dapat menindak tegas penyalahgunaan data pribadi konsumen yang dilakukan oleh para pelaku bisnis. Seperti Pemerintah Britania Raya melalui *Information Commissioner's Office* yang sejak tahun 2015 telah memberlakukan anti-spamming and data protection law dan mengenakan sanksi bagi perusahaan-perusahaan yang melanggar regulasi tersebut, dengan total denda sebanyak 8,7 juta poundsterling sampai tahun 2018.³³

Dalam kasus Direct Marketing ini, perlu adanya panduan dan skema perlindungan data pribadi konsumen yang lebih komprehensif mengenai hak-hak perlindungan data konsumen serta *privacy policy* dari perusahaan terkait.





■ BISNIS: SKIMMING ATM DAN KEAMANAN PERBANKAN INDONESIA

Pada bulan Maret 2018, terdapat rentetan kasus skimming ATM di berbagai kota di Indonesia. Skimming dilakukan dengan menggunakan alat yang bisa membaca kode PIN ATM nasabah ketika transaksi berlangsung dan mengambil sejumlah uang yang ada di rekening tersebut. Pelaku tertangkap adalah sindikat kriminal terorganisir transnasional dari Rumania dan Bulgaria.³⁴

Dengan adanya kasus ini, informasi data pribadi yang lebih tinggi tingkatannya, yaitu kode rahasia sudah bisa dibobol oleh sindikat kriminal. Perlindungan data pribadi dalam kasus ini sudah semakin urgen karena telah mampu menyebabkan kerugian secara materiil yang signifikan. Setelah kejadian ini, OJK dan asosiasi bank se-Indonesia telah memiliki mekanisme perlindungan data pribadi dengan mengganti kartu ATM dengan yang sudah dilengkapi oleh microchip untuk peningkatan keamanan.³⁵ Meskipun begitu, perlindungan sektoral ini masih dirasa belum cukup melihat meningkatnya jumlah transaksi perbankan setiap tahunnya dan kerentanan nasabah yang semakin meningkat.

■ BISNIS: DATA PRIBADI PENUMPANG TRANSPORTASI ONLINE

Maraknya perkembangan startup di Indonesia tidak lepas dari gelombang digitalisasi dan *gigs economy*. Salah satu *startup* yang prominen adalah Gojek dengan inovasi transportasi onlinenya, namun sayangnya *startup* juga tidak kebal dari permasalahan perlindungan data pribadi konsumennya. Pada tahun 2016, seorang *programmer* membeberkan beberapa *bug* yang menjadi celah keamanan data pribadi pengguna Gojek dimana data pribadi pengguna seperti nomor telepon, email, rute perjalanan sampai menu makanan yang dipesan masih bisa diakses lewat API Point.³⁶

Tidak hanya itu, terdapat juga insiden teror oleh *driver* Gojek kepada penumpangnya yang memberi *review* buruk.³⁷ Kejadian ini merupakan bukti bahwa Gojek belum memiliki sistem anonimitas pengguna untuk melindungi konsumennya dalam mekanisme *review*nya sehingga *driver* masih bisa mengontak penumpang yang memberi *review* buruk. Permasalahan entitas bisnis ini pun masih serupa, yaitu perihal *privacy policy* yang belum berpihak kepada konsumen. Namun, Gojek dan entitas bisnis sebelumnya seperti perbankan memiliki perbedaan jenis pengumpulan data dimana Gojek telah mampu menganalisis data



yang sifatnya *user behaviour* seperti rute perjalanan, destinasi yang paling sering didatang, jenis makanan yang dipesan.

Dalam statistik global yang dilaporkan dalam laporan United Nations Conference on Trade and Development (UNCTAD) tahun 2013 menunjukkan bahwa pelaku pelanggaran data pribadi sekitar 53% berasal dari sektor bisnis, dan jenis data pribadi yang dikumpulkan bukan data yang bersifat umum lagi, namun spesifik seperti password akun dan detil nama akun.³⁸



■ KESIMPULAN ●



Dari studi-studi kasus diatas, dapat disimpulkan bahwa Indonesia telah mencapai titik urgen untuk memiliki regulasi perlindungan data pribadi karena secara prospektif dapat dianalisis bahwa absennya payung hukum yang mengatur telah mampu mengakibatkan kerugian dalam skala besar yang bisa mengancam bukan lagi kepentingan material individu, seperti kasus dalam stakeholder bisnis dan perbankan, namun perputaran roda pemerintahan. Hal ini mengingat bagaimana *e-government* dan integrasi digital data kependudukan telah menunjukkan adanya gejala kerentanan siber. Sebagai kesimpulan dari analisis studi kasus ini, dapat dilihat sektor-sektor yang sekiranya akan sangat strategis dalam menjadi aktor pengelola data pribadi di Indonesia, yaitu: (1) Perbankan (2) Asuransi (3) Operator Seluler (4) Media Sosial (5) Startup Aplikasi Digital (6) *E-commerce* dan (7) Penyedia Layanan Kesehatan.



¹Kuwado, F J. (2018). 1 Juta Data Pengguna Asal Indonesia Bocor, Menkominfo Panggil Facebook [daring] *Kompas*. Tersedia di: <https://nasional.kompas.com/read/2018/04/05/17361101/1-juta-data-pengguna-asal-indonesia-bocor-menkominfo-panggil-facebook> [diakses 2 Mar. 2019].

²Hutabarat, D. (2018). Masuk prolegnas, Kemkominfo targetkan RUU Perlindungan Data Pribadi selesai 2019 [daring] *Kominfo*. Tersedia di: https://kominfo.go.id/content/detail/15730/masuk-prolegnas-kemkominfo-targetkan-ruu-perlindungan-data-pribadi-selesai-2019/0/sorotan_media [diakses 2 Mar. 2019].

³Kurnia, D. (2015). Kemkominfo Siapkan RUU Perlindungan Data Pribadi [daring] *Kementerian Komunikasi dan Informatika Republik Indonesia*. Tersedia di: https://kominfo.go.id/index.php/content/detail/6142/Kemkominfo+Siapkan+RUU+Perlindungan+Data+Pribadi/0/sorotan_media [diakses 2 Mar. 2018]. Lihat juga Naskah Akademik dan Rancangan Undang-Undang tentang Perlindungan Data Pribadi. Tersedia di: <http://peraturan.go.id/rancangan-undang-undang-tentang-perlindungan-data-pribadi.html> [diakses 2 Mar. 2019].

⁴Lihat Penjelasan Pasal 26 ayat (1) Undang-Undang Nomor 11 Tahun 2008 jo. Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik.

⁵Selengkapnya: Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi. (Pasal 28G ayat (1) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945. Lihat juga pertimbangan hukum Mahkamah Konstitusi dalam Putusan Mahkamah Konstitusi Nomor 5/PUU-VIII/2010 perihal Pengujian Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, hlm. 60-72.

⁶McDermott, Y. (2017). Conceptualizing the Right to Data Protection in an Era of Big Data. *Big Data & Society*, hlm. 2-3.

⁷Selengkapnya: Bank **wajib merahasiakan keterangan mengenai Nasabah Penyimpan dan simpanannya**, kecuali dalam hal sebagaimana dimaksud dalam Pasal 41, Pasal 41A, Pasal 42, Pasal 43, Pasal 44, dan Pasal 44A. (Pasal 40 ayat (1) Undang-Undang Nomor 7 Tahun 1992 jo. Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan).

⁸Selengkapnya: Setiap orang **berhak atas rahasia kondisi kesehatan pribadinya** yang telah dikemukakan kepada penyelenggara pelayanan kesehatan. (Pasal 57 ayat (1) Undang-Undang Nomor 36 Tahun 2009 tentang Kesehatan).

⁹Lihat Pasal 44 ayat (1) huruf h Undang-Undang Nomor 43 Tahun 2009 tentang Kearsipan.

¹⁰Lihat Pasal 1 angka 22 Undang-Undang No. 23 Tahun 2006 jo. Undang-Undang No. 24 Tahun 2013 tentang Administrasi Kependudukan.

¹¹Lihat Pasal 85 ayat (2) Undang-Undang No. 23 Tahun 2006 jo. Undang-Undang

No. 24 Tahun 2013 tentang Administrasi Kependudukan.

¹²Lihat Pasal 84 ayat (1) Undang-Undang No. 23 Tahun 2006 jo. Undang-Undang No. 24 Tahun 2013 tentang Administrasi Kependudukan.

¹³Nugroho, B.P. (2017). Perjalanan Megaprojek e-KTP Sejak 2010 hingga akan Disidangkan [daring] *Detik News*. Tersedia di: <https://news.detik.com/berita/d-3442091/perjalanan-megaprojek-e-ktp-sejak-2010-hingga-akan-disidangkan> [diakses 29 Juli 2018].

¹⁴Pasal 6 ayat (3) huruf c dan Pasal 17 huruf h Undang-Undang No. 14 Tahun 2008 tentang Keterbukaan Informasi Publik.

¹⁵Pasal 1 angka 1 Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik.

¹⁶Lihat Pasal 26 ayat (1) Undang-Undang Nomor 11 Tahun 2008 jo. Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik.

¹⁷Pasal 26 ayat (2) Undang-Undang Nomor 11 Tahun 2008 jo. Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik.

¹⁸Pasal 15 ayat (1) Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

¹⁹Pasal 15 ayat (1) Undang-Undang No. 12 Tahun 2011 tentang Pembentukan Peraturan Perundang-undangan.

²⁰Naskah Akademik dan Rancangan Undang-Undang tentang Perlindungan Data Pribadi. Tersedia di: <http://peraturan.go.id/rancangan-undang-undang-tentang-perlindungan-data-pribadi.html> [diakses 2 Mar. 2019].

²¹*Ibid*, hlm. 90-120.

²²Rappa. (2001). *Business models on the web: Managing the digital enterprise*. [Online]. Tersedia di digitalenterprise.org/models/models.html. [Diakses pada 4 Maret 2019]

²³Berger, et al. (2016). *Privacy and Data Protection*. [Online]. How to Engage in Cyber Policy. Diperoleh dari <https://www.youtube.com/watch?v=ZNEPaGFAPx4> [Diakses pada 3 Maret 2019]

²⁴Setyowati, D. (2018). Pemerintah Perlu Batasi Swasta Mengakses Data Pribadi. [online] kata data . Tersedia di : <https://katadata.co.id/berita/2018/04/10/pemerintah-perlu-batasi-swasta-mengakses-data-pribadi> [Diakses pada 3 Maret 2019]

²⁵Witjaksono (2018) *Misteri Bocor Data e-KTP* [Online] *kompas.com* Diperoleh dari <https://nasional.kompas.com/read/2018/03/26/08101681/misteri-bocor-data-e-ktp> [Diakses pada 3 Maret 2019]

²⁶*Ibid*

²⁷Detik. Inet. (2011). *Ada Andil Operator Dalam Bocornya Data Pelanggan?* [Online] *detik.com* Diperoleh dari <https://inet.detik.com/telecommunication/1552903/ada-andil-operator-dalam-bocornya-data-pelanggan> [Diakses pada 4 Maret 2019]

²⁸Maryani. (2017). *Perlindungan Data Pribadi di Indonesia* [Online] *combine.or.id* Diperoleh dari https://www.combine.or.id/article/Perlindungan-Data-Pribadi-di-Indonesia_%23_194 [Diakses pada 3 Maret 2019]

²⁹Manalu et al.(2017). *Kasus jual beli informasi nasabah: Lindungi data pribadi*. [Online] kalimantan.bisnis.com Diperoleh dari <https://kalimantan.bisnis.com/read/20170824/244/683631/kasus-jual-beli-informasi-nasabah-lindungi-data-pribadi>- [Diakses pada 4 Maret 2019]

³⁰Urbanski. (2012). *Biggest Spammers? Marketers* [Online] dmnews.com Diperoleh dari <https://www.dmnews.com/channel-marketing/email/news/13059396/biggest-spammers-marketers>. [Diakses pada 2 Maret 2019]

³¹The SMS Works (2018) *58% Rise in Fines for Spam and Data Breaches* [Online] digit.fyi Diperoleh dari <https://digit.fyi/rise-in-fines-for-spam-data-breaches/> Diakses pada 2 Maret 2019.

³²*Ibid*

³³Zaenudin. (2018). *Polisi: Pelaku Skimming Sudah Siap Bobol 1.200 Kartu ATM Indonesia*. [Online] Tirto.id. Diperoleh dari <https://tirto.id/polisi-pelaku-skimming-sudah-siap-bobol-1200-kartu-atm-indonesia-cGwo> [Diakses pada 4 Maret 2019]

³⁴Mamduh. (2018). *Pengamat Desak Migrasi Kartu Debit Pakai Chip Dipercepat*. [Online] tirto.id. Diperoleh dari <https://tirto.id/pengamat-desak-migrasi-kartu-debit-pakai-chip-dipercepat-cHyF>. [Diakses pada 4 Maret 2019]

³⁵Nistanto. (2016). *Programmer Temukan "Kutu" Berbahaya di Aplikasi Gojek*. [Online] tekno.kompas.com Diperoleh dari <https://tekno.kompas.com/read/2016/01/10/20510327/zProgrammer.Temuan.Kutu.Berbahaya.di.Aplikasi.GoJek>. [Diakses pada 4 Maret 2019]

³⁶Gunawan. (2015). *Pengguna Go-Jek Diteror Setelah Memberikan Bad Review!*. [Online] id.techinasia.com Diperoleh dari <https://id.techinasia.com/talk/pengguna-go-jek-diteror-setelah-memberikan-bad-review> [Diakses pada 4 Maret 2019]

³⁷Nistanto. (2016) *Kebocoran Go-Jek Memuncak, Rute Sehari-hari Pengguna Bisa Dilacak* [Online] tekno.kompas.com Diperoleh dari <https://tekno.kompas.com/read/2016/01/20/16031307/Kebocoran.Go-Jek.Memuncak.Rute.Sehari-hari.Pengguna.Bisa.Dilacak>. [Diakses pada 4 Maret 2019]

³⁸Ayuwuragil, K. (2018). *Kominfo Akui 'Pencurian' NIK dan KK Saat Registrasi Kartu SIM* [daring] CNN Indonesia. Tersedia di: <https://www.cnnindonesia.com/teknologi/20180305204703-213-280691/kominfo-akui-pencurian-nik-dan-kk-saat-registrasi-kartu-sim> [diakses 2 Mar. 2019].

ABOUT CfDS

Center for Digital Society (CfDS) is the research center established by the Faculty of Social and Political Sciences, Universitas Gadjah Mada. The institution is created under the concern over the contemporary dynamics of socio-political condition of the world that is accentuated by the impeccable influence of information technology. The phenomenon triggers the new patterns and complexities in the society, and thus requires new approaches in managing such complexities.

CfDS pledged to delve more on the study of contemporary digital society, including related issues surrounding the topic; such as the issues of smart city and urban development. The emphasis is then put on the utilization of technology to shape the society in becoming digitalized, as well as to bring solvency to social issues.

Vision

Solving Social Problem and Accelerating Prosperity through Indonesia Digital Society

Activities

1. Research and Development
2. Dissemination and Publication
3. Education and Policy Advocacy

Research Scopes

1. Digital Governance
2. Digital Economy
3. Future Technology



facebook.com/cfdsugm



@cfds_ugm



Center for Digital Society (CfDS)



@cfds_ugm



cfds.fisipol.ugm.ac.id



cfds_ugm



CfDS UGM

