PELINDUNGAN DATA PRIBADI DI INDONESIA: JALAN PANJANG MENUJU IMPLEMENTASI YANG EFEKTIF

RESEARCH NOTE

OPEN DATA LABS JAKARTA

WORLD WIDE WEB FOUNDATION

Penelitian ini ditulis oleh Dinita Andriani Putri, Project Manager di World Wide Web Foundation, Open Data Lab Jakarta

Kutipan yang Disarankan: Putri, Dinita A. (2019). *Pelindungan Data Pribadi di Indonesia: Jalan Panjang Menuju Implementasi yang Efektif. Jakarta: World Wide Web Foundation.*

Ucapan Terima Kasih: Penulis ingin berterima kasih kepada narasumber interview yang telah berkontribusi dan mendukung penelitian ini. Kepada Teddy Woodhouse, Carlos Iglesias, Dhanaraj Thakur, dan Glenn Maail dari Web Foundation untuk komentar dan saran yang diberikan, Sabine Matsheka dan Kara Nash sebagai penyunting, dan Miki Salman yang menerjemahkan penelitian ini ke dalam Bahasa Indonesia.

Ringkasan Eksekutif

Studi ini menyelidiki berbagai tantangan dalam pelaksanaan peraturan-peraturan yang sudah ada tentang pelindungan data pribadi dan mengidentifikasi berbagai strategi untuk penyusunan Undang-Undang Pelindungan Data Pribadi yang akan datang di Indonesia. Studi pustaka dan wawancara pakar digunakan untuk mendapatkan informasi mendalam tentang pokok bahasan ini. Studi ini dilakukan untuk memahami kerangka hukum pelindungan data pribadi di Indonesia dan tantangan-tantangan dalam implementasi kerangka hukum yang sudah ada.

Peraturan pelindungan data menjadi hal yang semakin penting di dunia berbasis data saat ini. Menerapkan peraturan pelindungan data adalah pekerjaan pelik, bahkan di mana peraturan komprehensif terkait hal ini sudah ada, seperti di Uni Eropa. Di Indonesia, peraturan pelindungan data yang tersebar di berbagai peraturan menghadapi tantang implementasi yang berbeda.

Studi ini melihat ada tiga tantangan utama dalam pelaksanaan peraturan pelindungan data di Indonesia. Pertama, tantangan regulasi. Studi ini mengonfirmasi bahwa peraturan -peraturan yang ada, meskipun banyak, masih kurang memadai untuk menjamin prinsip-prinsip privasi dan pelindungan yang menyeluruh. Kelompok-kelompok sasaran untuk peraturan yang ada pun cukup spesifik, di mana lebih banyak pasal dan mekanisme yang secara khusus ditetapkan untuk PSTE (Penyelenggara Sistem dan Transaksi Elektronik). Sedangkan terkait individu dan sektor publik sebagai subyek hukum, peraturannya cukup ambigu sehingga menciptakan pemahaman yang tidak jelas di kalangan pemangku kepentingan. Sektor swasta, khususnya perusahaan-perusahaan besar, termasuk para PSTE, memiliki kebijakan masing-masing terkait pelindungan data. Mereka umumnya merujuk pada GDPR (General Data Protection Regulation) Eropa atau PDPA (Personal Data Protection Act) Singapura karena keduanya merupakan undang-undang paling komprehensif yang ada secara global. Beberapa perusahaan perintis (*start-up*) juga memiliki kebijakan pelindungan data pribadi mereka sendiri, meskipun banyak dari mereka yang tampaknya membatasi lingkup pelindungan data pribadi hanya sejauh persetujuan untuk pengumpulan data.

Tantangan kedua adalah persoalan kelembagaan. Terlihat dari kasus-kasus yang dibahas bahwa pejabat pemerintah dan penegak hukum masih belum memiliki pengetahuan yang memadai tentang peraturan yang ada, apalagi dalam mengimplementasikannya. Tanpa adanya satu pun regulator untuk pelindungan data, penyelesaian dugaan kasus pelanggaran dan penyalahgunaan data juga tersebar di berbagai lembaga pemerintah. Bagi perusahaan-perusahaan besar, tidak ada tantangan kelembagaan yang signifikan terkait dengan peraturan-peraturan yang ada: hal ini sebagian karena mereka sudah mengikuti peraturan global yang lebih maju seperti GDPR. Untuk UU Pelindungan Data di masa

depan, perlu ditetapkan informasi terperinci mengenai kriteria Petugas Pelindungan Data (*Data Protection Officer*), dan tata kelembagaannya, baik di pemerintah maupun sektor swasta.

Ketiga adalah tantangan budaya. Perilaku budaya memiliki andil pada minimnya implementasi peraturan-peraturan yang ada. Masyarakat umum tidak melihat privasi dan keamanan data pribadi sebagai bagian yang melekat dari hak mereka sebagai warga negara. Oleh karena itu, sangat sedikit laporan terkait penyalahgunaan dan pelanggaran data pribadi walaupun mereka tahu bahwa data mereka diperdagangkan oleh pihak-pihak yang tidak bertanggung jawab. Peraturan-peraturan yang ada juga tidak dikomunikasikan secara menyeluruh, sehingga sulit bagi warga negara untuk memahami pentingnya hal ini dan bagaimana mereka dapat memperoleh manfaat dari pelindungan data pribadi. Ada kebutuhan mendesak untuk menyebarluaskan dan meningkatkan kesadaran dan pemahaman akan pentingnya data pribadi kepada warga. Pemerintah, sektor swasta, dan organisasi masyarakat sipil perlu terlibat dalam proses ini. Memahami latar belakang budaya juga penting untuk membangun strategi implementasi yang peka terhadap budaya untuk UU Pelindungan Data di masa depan.

Meski banyak tantangan, ada pula peluang untuk menerapkan peraturan pelindungan data yang lebih baik ke depannya. Dalam penyusunan UU Pelindungan Data yang akan datang, pemerintah melibatkan berbagai pemangku kepentingan dari sektor swasta, regulator lainnya, dan organisasi masyarakat sipil dalam prosesnya. Mereka membuka ruang untuk diskusi dan menyediakan waktu bagi para pemangku kepentingan untuk memberikan saran, masukan, dan umpan balik. Proses berkelanjutan ini tidak hanya dapat membawa pada suatu kerangka hukum pelindungan data yang komprehensif yang memberikan manfaat bagi seluruh pemangku kepentingan, namun juga mendidik pihak-pihak yang terlibat dalam proses tersebut.

Konteks

Pada 2018, jumlah pengguna Internet di Indonesia tercatat sebanyak 171,17 juta – artinya 64,8% dari total penduduk sudah *online* (APJII dan Polling Indonesia, 2019). Laporan yang sama menyoroti penetrasi internet tertinggi di kalangan anak muda usia 15-19 tahun (91%) dan orang dewasa muda usia 20-24 tahun (88,5%); sementara penetrasi terendah terdapat di antara orang lanjut usia 60-64 tahun (16,2%) dan di atas 65 tahun (8,5%).

Meskipun memiliki penetrasi internet tertinggi, kalangan muda masih tertinggal dalam hal kesadaran akan privasi dan pelindungan data. Sebuah kajian dari Web Foundation tentang kesadaran privasi di media sosial menemukan bahwa anak muda di Indonesia memiliki pandangan tertentu tentang privasi, dan kesadaran yang rendah akan pelindungan data pribadi (Canares, 2018). Dapat diasumsikan bahwa mereka yang kurang paham teknologi bahkan mungkin lebih rentan terhadap risiko privasi dan pelanggaran pelindungan data.

Wacana tentang privasi dan pelindungan data pribadi di Indonesia meningkat dalam dua tahun terakhir, khususnya sejak Facebook mengungkapkan bahwa informasi pribadi pengguna Facebook Indonesia bisa jadi telah diperoleh, dan disalahgunakan, oleh Cambridge Analytica[1]. Sejak saat itu, warga negara Indonesia mulai mempertanyakan pelindungan data pribadi mereka. Indonesia adalah salah satu dari hanya beberapa negara di Asia Tenggara yang tidak memiliki kerangka hukum pelindungan data yang memadai (World Wide Web Foundation, 2017; GSMA, 2018). Kurangnya pelindungan ini telah menyebabkan peningkatan kasus dugaan pelanggaran atau penyalahgunaan data pribadi; seperti perdagangan data nasabah bank dan pemegang kartu kredit[2], penyebaran identitas pelanggan dalam proses penagihan utang[3], hingga pesan teks harian tertarget yang diterima perorangan berisi penawaran produk-produk dan jasa seperti pinjaman dan kredit.

Saat ini peraturan pelindungan data di Indonesia bersifat sporadis dan terbatas pada sektor-sektor tertentu, di mana 30 peraturan didapatkan memiliki klausul terkait pelindungan data (Djafar et al., 2016). Ada tiga kerangka hukum utama yang dianggap sebagai peraturan inti yang ada terkait pelindungan data pribadi. Peraturan-peraturan tersebut adalah UU No. 11/2008 yang diamandemen oleh UU No. 19/2016 tentang Informasi dan Transaksi Elektronik, Peraturan Pemerintah No. 82/2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, dan Peraturan Menteri Komunikasi dan Informatika No. 20/2016 tentang Pelindungan Data Pribadi dalam Sistem Elektronik.

Tahun ini, pemerintah meneruskan proses pengesahan Rancangan Undang-Undang (RUU) Pelindungan Data Pribadi yang memberikan prinsip-prinsip yang lebih menyeluruh tentang pelindungan data pribadi yang dapat digunakan lintas sektor. RUU ini juga merinci tata kelola pelindungan data, seperti kewajiban seorang petugas pelindungan data, pengawas data, dan otoritas pelindungan data, serta menyinggung kebutuhan akan suatu organisasi independen yang menangani tata kelola pelindungan data. Meskipun terdapat beberapa kerangka hukum yang terkait dengan pelindungan data pribadi, prinsip-prinsip data pribadi di Indonesia masih jauh dari memadai. Selain itu, berbagai kasus dan berita pelanggaran data dan penyalahgunaan data pribadi terus meningkat.

[1] Untuk menyelesaikan kasus ini, pemerintah menerbitkan surat peringatan kepada Facebook Indonesia namun tidak ada tindak lanjut. Lihat https://www.thejakartapost.com/life/2018/04/06/facebook-faces-indonesian-police-investigation-over-data-breach.html

[2] Lihat https://www.thejakartapost.com/news/2019/05/14/bank-customers-personal-data-sold-to-credit-card-salespeople-kompas-investigation.html

[3] Lihat https://www.thejakartapost.com/news/2019/08/05/where-is-privacy-personal-data-on-spreading-spree-in-indonesia.html

Maka penting untuk memahami berbagai tantangan dalam proses implementasi peraturan-peraturan yang ada serta mengenali strategi-strategi yang dapat diperbaiki untuk implementasi UU Pelindungan Data Pribadi masa depan.

Tujuan dan Metodologi

Studi ini menyelidiki implementasi peraturan-peraturan yang ada tentang pelindungan data pribadi dan mengidentifikasi berbagai strategi dari pemerintah, sektor swasta, dan lembaga swadaya masyarakat dalam mematuhi peraturan yang ada.

Pertanyaan-pertanyaan yang kami ajukan adalah:

1. Apa saja tantangan dalam implementasi peraturan-peraturan yang ada tentang pelindungan data?
2. Apa saja strategi yang akan digunakan oleh publik untuk mematuhi UU pelindungan data pribadi ke depannya?

Studi ini memanfaatkan pendekatan-pendekatan kualitatif dengan studi pustaka dan wawancara pakar sebagai instrumen. Narasumber utama adalah pejabat-pejabat pemerintah, perwakilan dari organisasi masyarakat sipil yang melakukan advokasi dan pekerjaan terkait kasus-kasus pelindungan data pribadi, dan para pelaku sektor swasta yang secara aktif terlibat dalam diskusi soal isu-isu pelindungan data pribadi di Indonesia. Pendekatan *snowball sampling* juga diterapkan untuk mendapatkan lebih banyak sudut pandang dari berbagai narasumber. Pembicaraan dilakukan dengan 10 narasumber utama.

Salinan wawancara digunakan untuk melakukan analisis deskriptif, sementara hasil wawancara dikode untuk mengidentifikasi tema dan pola umum atas pertanyaan-pertanyaan penelitian. Bidang-bidang diskusi utama dalam wawancara adalah tantangan-tantangan dalam kerangka hukum yang ada terkait pelindungan data pribadi, strategi-strategi untuk mematuhi kerangka hukum yang ada, dan strategi-strategi untuk melaksanakan serta mematuhi kerangka hukum pelindungan data pribadi di Indonesia ke depannya dengan lebih baik.

Studi ini terbatas dalam cakupannya karena hanya fokus pada proses implementasi kerangka hukum pelindungan data yang sudah ada dan tidak memberikan pembahasan mendalam atas setiap pasal dalam peraturan-peraturan itu. Kerangka yang digunakan dalam penelitian ini didasarkan pada tiga variabel kerangka implementasi kebijakan (Material, Struktural, dan Kontekstual) dari Sabatier dan Mazmanian (1983). Ketiga variabel tersebut dipilih karena mewakili fokus analisis studi ini: kerangka hukum, pelaku pelaksana, dan kondisi sosial.

Variabel Material digunakan untuk menganalisis kerangka hukum dari kesulitan-kesulitan teknis, keragaman kelompok sasaran, dan sejauh mana perubahan perilaku yang dikehendaki oleh peraturan terkait. Variabel struktural mencakup fokus pada pelaku kelembagaan dan pelaksana dengan mengamati kesiapan organisasi-organisasi pelaksana,

ketersediaan dan kapasitas sumber daya pelaksana, serta proses mekanisme akuntabilitas. Variabel-variabel kontekstual memeriksa kondisi-kondisi sosial dengan memerhatikan kesadaran publik serta kesiapan dan dukungan mereka terhadap implementasi peraturan terkait pelindungan data pribadi.

Kerangka hukum pelindungan data pribadi di Indonesia

"Peraturan-peraturan yang ada sekarang itu fokusnya lebih ke kewajiban PSTE [penyelenggara sistem dan transaksi elektronik] yang mengumpulkan, memroses, dan menggunakan data pribadi; sedikit sekali merinci tentang hak-hak pemilik data dan siapa yang bertanggung jawab untuk melindungi hak-hak ini."

- aktivis hak asasi manusia, wawancara, Mei 2019

Terdapat tiga peraturan utama yang membahas data pribadi di Indonesia: UU Informasi Elektronik No. 11/2008 yang diubah dengan UU No. 19/2016, Peraturan Pemerintah No. 82/2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, dan Peraturan Menteri Komunikasi dan Informatika (Permenkominfo) No. 20/2016 sebagai peraturan pelaksana Peraturan Pemerintah No. 82/2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Menurut peraturan pemerintah ini, Penyelenggara Sistem dan Transaksi Elektronik (PSTE) adalah setiap orang, lembaga pemerintah, entitas bisnis, atau komunitas yang menyediakan, mengelola dan/atau menjalankan suatu sistem elektronik, baik secara perorangan maupun bersama, kepada pengguna sistem elektronik untuk kepentingannya sendiri atau pihak lainnya.

Permenkominfo No. 20/2016 adalah peraturan terbaru dan paling terperinci karena memberikan definisi tentang data pribadi, merinci kewajiban penyelenggara sistem dan transaksi elektronik terkait penggunaan dan pelindungan data pribadi, serta menyediakan rumusan untuk sanksi dan penyelesaian sengketa penyalahgunaan dan pelanggaran atas data pribadi.

UU/Peraturan	Pasal terkait data pribadi	Cakupan	Subyek Hukum	Mekanisme Pertanggungjawaban
UU No. 11/2008 yang diubah dengan UU No. 19/2016 tentang Informasi dan Transaksi Elektronik	Pasal 26 ayat (1) – (5): "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."	Pemrosesan, transmisi, dan berbagi data pribadi dalam sistem elektronik	Perseorangan, perusahaan	Setiap orang yang dilanggar haknya dapat mengajukan gugatan. Tersedia sanksi pidana dan finansial untuk penyalahgunaan data pribadi untuk tujuan pencemaran nama baik atau pemerasan dalam dokumen dan transaksi elektronik.
Peraturan Pemerintah No. 82/2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik	Pasal 1 ayat (27): "data pribadi adalah data perseorangan tertentu yang disimpan, dirawat, dan dijaga kebenaran serta dilindungi kerahasiaannya."	Menjamin perolehan, penggunaan, dan pemanfaatan data pribadi dalam sistem elektronik	Perseorangan, penyelenggara negara, badan usaha, masyarakat yang menyediakan, mengelola, dan/atau mengoperasikan Sistem Elektronik secara sendiri sendiri maupun bersama-sama kepada Pengguna Sistem Elektronik untuk keperluan dirinya	Mewajibkan PSTE untuk melindungi dan menjamin keamanan data pribadi, mendapatkan persetujuan untuk penggunaan apa pun atas data pribadi, dan untuk memberikan pemberitahuan jika terjadi kegagalan dalam pelindungan data pribadi

			dan/atau keperluan pihak lain	
Peraturan Menteri Komunikasi dan Informatika No. 20/2016	Pasal 1 ayat (1) - (3): "Data Pribadi adalah data perseorangan tertentu yang disimpan, dirawat, dan dijaga kebenaran serta dilindungi kerahasiaannya." "Data Perseorangan Tertentu adalah setiap keterangan yang benar dan nyata yang melekat dan dapat diidentifikasi, baik langsung maupun tidak langsung, pada masing-masing individu yang pemanfaatannya sesuai ketentuan peraturan perundang-undangan."	Perolehan, pengumpulan, pengolahan, penganalisisan, penyimpanan, penampilan, pengumuman, pengiriman, penyebarluasan, dan pemusnahan data pribadi dalam sistem elektronik	Perseorangan, lembaga negara, entitas bisnis, atau masyarakat sipil yang menyediakan, mengelola, dan/atau mengoperasikan Sistem Elektronik secara sendiri-sendiri maupun bersama-sama kepada Pengguna Sistem Elektronik untuk keperluan dirinya dan/atau keperluan pihak lain.	Tersedia sanksi administratif. Sengketa pertama-tama akan ditangani melalui penyelesaian tanpa proses pengadilan. Gugatan perdata dapat diajukan dalam hal terdapat kegagalan dalam penyelesaian tanpa proses pengadilan.

Table 1. Kerangka hukum yang ada terkait data pribadi

UU No. 11/2008 dan UU No. 19/2016 (perubahan) tentang Informasi dan Transaksi Elektronik

Pasal 26 UU No. 11/2018 tentang ITE, melarang penggunaan dan peralihan data pribadi tanpa persetujuan pemilik data. Pasal ini juga menyatakan bahwa seseorang dapat mengajukan gugatan dan kompensasi finansial jika mereka merasa bahwa data pribadi mereka dilanggar haknya. Perubahan terhadap UU ITE mewajibkan Penyelenggara Sistem dan Transaksi Elektronik (PSTE) untuk menghapus informasi atau dokumen elektronik yang tidak relevan berdasarkan permintaan pemilik data melalui keputusan pengadilan; dan untuk menyediakan suatu mekanisme untuk melakukannya. UU No. 19/2016 ini tidak membahas definisi dan cakupan data pribadi secara menyeluruh; dan tidak terdapat informasi tentang otoritas yang bertanggung jawab untuk melindungi hak-hak pemilik data.

Peraturan Pemerintah No. 82/2012 tentang Penyelenggara Sistem dan Transaksi Elektronik (PSTE)[4]

Peraturan ini fokus pada kewajiban PSTE, dan secara lebih khusus lagi dengan mengatur penggunaan dan lokasi pusat data. Klausul terkait data pribadi terdapat dalam salah satu kewajiban PSTE di mana mereka berkewajiban untuk melindungi data pribadi penggunanya. Peraturan ini juga mewajibkan PSTE untuk memberitahukan kepada penggunanya ketika terjadi kegagalan dalam pelindungan data pribadi. Seperti halnya UU ITE dan amandemennya, peraturan ini juga tidak memberikan definisi dan cakupan yang jelas tentang data pribadi.

Peraturan Menteri Komunikasi dan Informatika No. 20/2016 tentang Pelindungan Data Pribadi dalam Sistem Elektronik

Peraturan terbaru ini memberikan definisi yang lebih terperinci atas data pribadi. Ada dua lapisan dalam definisi data pribadi. Yang pertama dan umum menyatakan bahwa data pribadi adalah "data perseorangan tertentu yang disimpan, dirawat, dan dijaga kebenaran serta dilindungi kerahasiaannya". Peraturan ini selanjutnya memberikan definisi data perseorangan tertentu sebagai "keterangan yang benar dan nyata yang melekat dan dapat diidentifikasi, baik langsung maupun tidak langsung, pada masing-masing individu yang pemanfaatannya sesuai ketentuan peraturan perundang-undangan". Peraturan ini selanjutnya merinci ketentuan tentang kewajiban pemberitahuan dalam hal terjadi kegagalan pelindungan data pribadi oleh PSTE; klausul yang tidak terdapat dalam Peraturan Pemerintah No. 82/2012. Hak-hak pemilik data pribadi juga tersedia dalam peraturan ini, walaupun masih belum menyeluruh.

[4] Peraturan ini sedang direvisi.

Sintesis

Ketiga peraturan di atas fokus pada data pribadi yang diproses melalui sistem elektronik saja; sedangkan cara-cara lain dalam pengumpulan, pemrosesan, dan penggunaan data pribadi, masih mengacu pada peraturan di masing-masing sektor. Contohnya, pengumpulan, pemrosesan, dan transmisi data pribadi dalam sektor keuangan mengacu pada Peraturan Otoritas Jasa Keuangan No. 77/2016 tentang Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi dan Peraturan Otoritas Jasa Keuangan No. 13/2018 tentang Inovasi Keuangan Digital di Sektor Jasa Keuangan. Peraturan-peraturan ini tidak mengacu pada Peraturan Menteri Komunikasi dan Informatika, sehingga memiliki subyek dan ruang lingkup hukum sendiri.

Peraturan Menteri Komunikasi dan Informatika membatasi periode penyimpanan data pribadi hingga setidaknya lima tahun. Di lembaga-lembaga pemerintah, pengarsipan dan penyimpanan data, termasuk data pribadi, didasarkan pada UU Kearsipan No. 43/2009; sedangkan sektor swasta biasanya memiliki kebijakan mereka sendiri terkait periode penyimpanan data. Dalam hal pengalihan dan pembagian data, ketiga peraturan tersebut mengandalkan persetujuan tertulis yang harus diberikan dalam Bahasa Indonesia, namun tidak ada keterangan lebih lanjut tentang bagaimana persetujuan tersebut harus didapat.

Meskipun Peraturan Menteri Komunikasi dan Informatika merinci tentang pelindungan data pribadi, namun tingkat regulasinya tidak memadai untuk menghasilkan penegakan yang berdampak. Peraturan Menteri hanya memungkinkan untuk mengenakan sanksi administratif dalam hal terjadi penyalahgunaan atau kegagalan dalam pelindungan data. UU ITE memiliki sanksi-sanksi yang kuat bagi penyalahgunaan informasi elektronik (termasuk data pribadi), namun kembali lagi, UU ini tidak memiliki definisi yang jelas atas data pribadi dan karena itu sulit mendapatkan bukti memadai untuk membawa suatu kasus ke pengadilan (Greenleaf, 2017).

“kalau ditanya apakah kami mencoba mematuhi peraturan-peraturan yang ada, ya, kami berusaha [mematuhi]. Tapi apa kami menjadikannya [mematuhi peraturan] prioritas? rasanya nggak... karena peraturannya masih belum komprehensif. Kami memperlakukan peraturan Kominfo, misalnya, lebih ke pedoman; tapi kami merujuk sebagian besar kebijakan [pelindungan data pribadi] internal kami ke GDPR dan PDPA.”

- Staf hukum, sektor swasta, wawancara, Juni 2019

Tingkat peraturan menteri yang tidak memadai juga menyulitkan untuk dapat mengharapkan suatu perubahan perilaku yang diinginkan oleh peraturan tersebut. Lembaga-lembaga pemerintah masih berpegang pada peraturan sektoral mereka alih-alih Peraturan Menteri Komunikasi dan Informatika. Sektor swasta juga masih mengacu pada GDPR dan PDPA sebagai sumber utama untuk mengembangkan kebijakan-kebijakan pelindungan data mereka.

Tantangan kelembagaan dan proses akuntabilitas

Tantangan kelembagaan

"Pejabat pemerintah itu masih banyak yang nggak paham soal Permenkominfo [tentang Pelindungan Data Pribadi dalam Sistem Elektronik]... Mereka nggak sadar bahwa mereka adalah bagian dari subyek hukum peraturan tersebut, dan mereka juga bertanggung jawab untuk melindungi data pribadi warga [negara] yang mereka kumpulkan dan gunakan."

- Pejabat negara, Wawancara, Juli 2019

Dua tantangan kelembagaan utama dalam pelaksanaan peraturan-peraturan yang ada:

1. *Tumpang tindih tanggung jawab*. Karena tidak ada regulator khusus yang bertanggung jawab atas pelindungan dan tata kelola data pribadi, kasus-kasus terkait tata kelola data pribadi masih ditangani per sektor. Contohnya, untuk penanganan penyalahgunaan data pribadi oleh PSTE, ada regulator khusus di dalam Kemenkominfo yang bertanggung jawab, yang berbeda dengan regulator yang bertugas melakukan tata kelola data pribadi atau pengendalian aplikasi informatika. Penyalahgunaan data pribadi terkait sektor keuangan akan ditangani oleh Otoritas Jasa Keuangan, dan Kementerian Kesehatan bertanggung jawab atas penyalahgunaan data terkait rekam medis.
2. *Kurangnya pengetahuan, kapasitas, dan kapabilitas regulator*. Sebagian besar pejabat negara masih tidak menyadari bahwa mereka memproses data warga negara, dan tidak ada kebijakan internal khusus untuk mendapatkan persetujuan dalam pemrosesan data warga negara. Karena peraturan yang ada terutama fokus pada PSTE, pejabat negara masih merasa bahwa mereka tidak terikat oleh peraturan tersebut, meskipun dengan jelas dicantumkan dalam Peraturan Menteri Kominfo No. 20/2016 bahwa penyelenggara negara adalah bagian dari subyek hukum jika mereka memroses data pribadi dalam suatu sistem elektronik.

“Pendidikan dan pemahaman[tentang data pribadi] itu yang penting – nggak cuma untuk masyarakat atau pemilik data, tapi juga untuk penegak hukum, dan pegawai negara. Menurut saya hal ini [pelindungan data pribadi] masih belum jadi sesuatu yang mereka pahami betul.”

- Perwakilan dari Perusahaan Telekomunikasi, Wawancara, Mei 2019

Kementerian Komunikasi dan Informatika memiliki program-program peningkatan kapasitas tentang pelindungan data dan mereka secara berkala mengirim pejabat negara dari berbagai lembaga untuk berpartisipasi dalam lokakarya, pelatihan, dan program-program sertifikasi terkait pelindungan data. Upaya-upaya untuk meningkatkan kapasitas dan pengetahuan para pejabat negara sudah tersedia, namun masih sangat terbatas.

Sektor swasta memiliki kapasitas kelembagaan yang lebih maju. Tiga dari empat perusahaan yang diwawancarai mengakui bahwa mereka sudah mempunyai petugas khusus yang menangani pelindungan data pribadi. Petugas tersebut biasanya terintegrasi dengan Bagian Hukum dan Kepatuhan atau menjadi bagian dari Departemen IT (*Information Technology*). Seluruh pelaku usaha yang diwawancarai juga memiliki program-program peningkatan kapasitas internal untuk meningkatkan pengetahuan dan keterampilan para petugas dalam tata kelola data dan pelindungan data pribadi. Asosiasi bisnis juga membuat pedoman untuk pelindungan data pribadi. Sebagai contoh, Asosiasi Fintech Pendanaan Bersama Indonesia (AFPI) membuat pedoman yang membahas kewajiban untuk mematuhi peraturan yang ada tentang pelindungan data pribadi, dan etika prosedur penagihan utang untuk perusahaan-perusahaan peminjaman online.

Proses akuntabilitas

“Implementasi sanksi [atas pelanggaran atau penyalahgunaan data pribadi] itu masih sulit... Nggak jelas siapa yang berwenang memastikan dan melakukan konfirmasi [pelanggaran atau penyalahgunaan], menyelidiki, dan membuat keputusan atas insiden pelanggaran data; pemerintah kah? Siapa di pemerintah? Lembaga yang mana?... PSTE juga nggak pernah rasanya memberitahukan pengguna mereka kalau ada kegagalan

pelindungan data [seperti yang diamanatkan dalam Peraturan Pemerintah No. 82/2012]; masyarakat juga jarang sekali mengajukan pengaduan atas penyalahgunaan data pribadi... Sehingga hal ini [implementasi sanksi] belum bisa berjalan dengan baik."

- Pengacara Sipil, Wawancara, Juli 2019

Sanksi yang lemah, tidak adanya penyelidik independen, ketidakjelasan dan tumpang tindih otoritas dalam penanganan penyalahgunaan data pribadi mengarah pada sebuah proses akuntabilitas yang tak bergigi. Saat ini, laporan penyalahgunaan data pribadi juga diterima oleh Kementerian Komunikasi dan Informatika, tapi mereka tidak memiliki kewenangan untuk menjatuhkan sanksi dan hanya bertindak sebagai perantara. Kementerian ini kemudian meneruskan kasus tersebut kepada kejaksaan (untuk kasus-kasus terkait pencemaran nama baik) atau kepada kementerian sektoral terkait. Responden kami dari organisasi-organisasi hak asasi manusia, pejabat negara, dan perwakilan pelaku bisnis setuju bahwa selalu ada kesulitan untuk mendapatkan bukti yang memadai untuk memroses suatu gugatan terkait penyalahgunaan data pribadi. Sanksi yang lemah tersebut juga merupakan akibat dari kurangnya kapasitas sumber daya pelaksana, dalam hal ini, lembaga pemerintah dan aparat penegak hukum.

"Yang memprihatinkan itu kan ketika Negara sendiri yang melakukan pertukaran data [pribadi] dengan pihak-pihak ketiga. Ya... meskipun mungkin secara teknis tidak ada data pribadi yang dialihkan, tapi masalahnya kan bukan di situ. Masalahnya kan soal transparansi, akuntabilitas, dan hak-hak warga negara atas data pribadi mereka... Bagaimana mereka [negara] melindunginya [data warga]... Jadi ini bukan persoalan pelindungan data saja, tapi soal melindungi hak warga atas data pribadi mereka."

- Pegiat Literasi Digital, Wawancara, Juli 2019

Lembaga pemerintah yang mengumpulkan dan menggunakan data warga memperlakukan data pribadi serupa dengan data lainnya. Peraturan yang ada tidak merinci secara khusus mekanisme pengumpulan dan penggunaan data pribadi yang dilakukan oleh pemerintah, proses akuntabilitas penyimpanan data pribadi di instansi pemerintah, dan siapa yang memiliki akses terhadap data tersebut. Lebih lanjut, mekanisme berbagi data antar

Lembaga pemerintah maupun dengan pihak ketiga, jika pun ada, tidak pernah diungkapkan secara jelas.

Implikasi sosial dan budaya

"Di sini [Indonesia] itu, orang-orang dengan sengaja membagikan data-data mereka. Di Instagram, misalnya, menurut saya, di Instagram itu kita kan sharing data dan informasi pribadi, walau memang seharusnya [informasi] yang dibagi ya yang kita memang mau orang lain tahu. Walaupun sama-sama data pribadi, tapi beda pelindungannya dengan data pribadi yang ingin saya amankan seperti nomor telepon, nomor KTP, dan sebagainya. Tapi orang-orang masih banyak yang nggak bisa bedakan antara keduanya [jenis-jenis data pribadi]... Susah juga buat kami [pelaku usaha] melindungi data pribadi orang-orang [pengguna] yang bahkan tidak melindungi data pribadi mereka sendiri."

- Staff bagian hukum, perusahaan berbasis TIK, Wawancara, Juni 2019

Warga negara adalah kelompok yang paling rentan akibat tidak adanya peraturan pelindungan data yang komprehensif di Indonesia. Namun, sebagian besar warga masih belum terbiasa dengan konsep dasar privasi dan pelindungan data pribadi. Data pribadi masih belum dipandang sebagai bagian dari hak pribadi dan karenanya kurang dilindungi secara sadar. Kurangnya kesadaran ini berhubungan erat dengan latar budaya yang telah lama dipelajari sebagai bagian penting dari mekanisme pengaturan privasi (Altman, 1977; Li, 2011; Trepte et al., 2017). Indonesia tampaknya masih kurang memerhatikan karakteristik budaya warganya, baik dalam merumuskan maupun menerapkan peraturan-peraturan terkait data pribadi.

Mengomunikasikan privasi dan data pribadi kepada publik merupakan hal yang tidak mudah. Kebanyakan warga dan organisasi masih belum memandang privasi sebagai hak asasi, melainkan lebih dilihat dari perspektif "keamanan' – hal ini kemudian menyebabkan ketakutan akan kembali pada masa 'Orde Baru' di mana segala sesuatu harus tertutup/dilindungi oleh pemerintah. Dengan adanya peraturan pelindungan data, tampaknya masih ada ketakutakn bahwa pemerintah akan menutup informasi yang sekarang terbuka bagi publik. Kemudian, jika melihat perilaku *online* warga secara umum, hanya sebagian kecil warga yang menyadari risiko privasi, sedangkan sebagian besar warga

masih mengabaikan risiko privasi untuk memperoleh manfaat dari berbagai jenis jasa yang mereka dapatkan secara *online*. Contohnya, risiko adanya pelanggaran privasi dalam peminjaman online seringkali diabaikan, karena manfaat pinjaman *online* yang dirasa lebih besar dibandingkan risikonya.

"...Banyak perempuan dan Ibu-Ibu [pengguna pinjaman online] yang nggak terlalu peduli risikonya [dari pinjaman online]... yang penting sekarang mereka bisa mengajukan pinjaman sendiri, tanpa harus ada persetujuan dari suami atau pasangan mereka, menggunakan ponsel dan rekening mereka sendiri. Ini membuat mereka merasa lebih mandiri. Kita bisa saja bilang bahwa praktik ini [pinjaman online] berisiko tinggi jika nggak hati-hati. Tapi berisiko bagi siapa? Bagi mereka [pengguna perempuan dan Ibu-Ibu], risiko ini nggak seberapa dibanding manfaatnya."

- Perwakilan masyarakat sipil, Wawancara, Juli 2019

Walaupun terdapat banyak kasus dan cerita tentang pelanggaran privasi dan data pribadi di media massa, hal ini belum menjadi isu yang dipedulikan secara umum dan hanya menyentuh kelompok masyarakat tertentu saja. Perlu ada gerakan yang terstruktur dan menyentuh berbagai lapisan masyarkaat untuk menyebarkan pengetahuan melalui berbagai saluran, seperti kurikulum pendidikan dan praktik-praktik bisnis yang lebih baik. Dalam area di mana warga adalah yang paling rentan dan tidak memiliki pengetahuan yang memadai, pemerintah harus melakukan perannya dalam memberikan pelindungan yang menyeluruh.

Para narasumber penelitian ini mengharapkan UU Pelindungan Data Pribadi nantinya tidak hanya mengatur, tapi juga dapat mengedukasi warga tentang pentingnya pelindungan data. Namun, karena peraturan paling menyeluruh yang tersedia di dunia saat ini adalah GDPR, sebagian besar kerangka dalam RUU Pelindungan Data Pribadi mengacu pada peraturan tersebut.

"...pasal mengenai DPO [dalam RUU], misalnya, hanya seperti copy-paste dari GDPR. Ya memang.. keberadaan DPO menjadi salah satu indikator bahwa kita memiliki sebuah peraturan data pribadi yang memadai, tapi kita

juga harus memikirkan tentang prosesnya [penyusunan peraturan]. Mereka [Uni Eropa] itu jauh lebih maju dari kita, warganya memiliki pemahaman yang lebih baik [dari warga di Indonesia] akan privasi. Nggak semua hal yang berlaku di sana dapat juga dijalankan di sini."

- Pejabat Negara, Wawancara, Juli 2019

Karena adanya perbedaan dalam karakteristik budaya, merujuk pada GDPR belum tentu selalu menjadi pilihan terbaik. Sebagai contoh, GDPR memiliki pasal-pasal yang cukup mutakhir tentang privasi; dan lebih banyak berfokus pada kewajiban pengolah dan pengendali data. Ini karena warga Eropa memiliki tingkat pemahaman tentang privasi yang berbeda dengan di Indonesia (Trepte et al., 2017). Lebih lanjut, di Uni Eropa, Direktif tentang pelindungan data sudah ada sejak 1995; penduduk di sana sudah memiliki cukup banyak waktu untuk mempelajari tentang pelindungan data sebelum GDPR dibahas pada 2014 dan disahkan pada 2018. Meskipun waktu banyak tersebut tidak menjamin bahwa mereka benar-benar sudah memiliki kesadaran privasi, upaya untuk menjaga privasi sudah berlangsung sejak sebelum GDPR disahkan. Sementara itu, Indonesia masih harus berjuang antara meningkatkan kesadaran dan mengedukasi warganya tentang privasi dan pelindungan data, membangun prinsip-prinsip komprehensif tentang kerangka hukum pelindungan data pribadi, sekaligus mempertahankan pertumbuhan ekonomi digital. Selain GDPR, melihat praktik-praktik dari negara-negara tetangga yang telah memiliki kerangka hukum pelindungan data, seperti Filipina dan Singapura, mungkin dapat menjadi pembelajaran yang berguna mengingat kemiripan latar budaya dan karakteristik warganya.

Rekomendasi

"Diskusi dan narasi pelindungan data pribadi [di Indonesia] sekarang ini seperti direduksi menjadi [hanya] pelanggaran privasi, padahal ini kan seharusnya dipahami sebagai bagian penting dari hak-hak warga negara. Kita [sebagai warga negara] memiliki hak untuk dilindungi oleh negara, termasuk data pribadi kita."

- Staf Kementerian, Wawancara, Juli 2019

- Selama tidak ada peraturan pelindungan data yang komprehensif, pedoman yang jelas tentang pengumpulan dan penggunaan data pribadi harus ada. Kerangka hukum yang kaku mungkin akan kurang bermanfaat mengingat kurangnya pemahaman tentang privasi dan pelindungan data serta tingkat kesiapan pemangku kepentingan yang akan terdampak. Karenanya, memberikan serangkaian pedoman tentang bagaimana melindungi data pribadi dan bagaimana mengumpulkan dan

menggunakannya mungkin akan lebih bermanfaat. Pedoman ini dapat digunakan tidak hanya oleh lembaga pemerintah internal atau perusahaan-perusahaan besar, tapi juga oleh usaha mikro-kecil, perusahaan rintisan (*start-up*) yang sedang berkembang, organisasi masyarakat sipil, dan warga pada umumnya.

- Karena sifat sektoral yang begitu melekat di lembaga-lembaga pemerintah, diperlukan satu badan atau fungsi independen yang bertanggung jawab atas tata kelola pelindungan data pribadi. Bentuk badan ini perlu didiskusikan lebih lanjut mengingat faktor-faktor internal seperti susunan tugas dan fungsi, kemungkinan struktur, dan anggaran negara yang tersedia untuk membentuk badan atau fungsi semacam itu. Sebagai sebuah alternatif, badan atau fungsi independen ini dapat diusulkan melalui DPR sebagai salah satu amanat UU Pelindungan Data Pribadi yang akan datang. Proses pembentukan badan atau fungsi ini harus terbuka dan diawasi ketat oleh seluruh pemangku kepentingan.

- Dalam hal cakupan sanksi, jika sanksi administratif saja tidak efektif, kemungkinan menerapkan sanksi keuangan berjenjang dapat menjadi pilihan. Jenjang sanksi ini dapat didasarkan pada (i) apakah subyek hukum adalah perseorangan atau organisasi; (ii) ukuran perusahaan/organisasi; atau (iii) kuantitas data pribadi yang mereka proses. Selanjutnya, harus ada sebuah mekanisme pemulihan yang jelas bagi mereka yang terdampak oleh penyalahgunaan, pelanggaran, dan kegagalan pelindungan data pribadi.

- Model *sandbox* regulasi (*regulatory sandbox*) – sebuah mekanisme di mana peraturan dikembangkan seiring dengan model bisnis dan inovasi yang berkembang – dapat diterapkan untuk implementasi UU Pelindungan Data Pribadi nantinya. Diskusi lintas-pemangku kepentingan yang sedang berlangsung dalam proses penyusunan RUU dapat dilanjutkan menjadi sebuah *sandbox*, sambil menambahkan pelaku-pelaku penting lainnya. Manfaat praktik ini adalah dapat mengatasi dua ketidakpastian utama secara bersamaan (Centre for Information Policy Leadership, 2019); yaitu ketidakpastian inovasi digital yang sedang berkembang, dan ketidakpastian peraturan. Selain itu, model ini juga dapat menjadi sebuah proses pembelajaran untuk penegakan peraturan sembari mempertahankan ekosistem inovasi digital yang sedang berkembang.

- Memperkuat dan menyelaraskan gerakan warga tentang literasi privasi dan data pribadi dari tingkat akar rumput. Gerakan-gerakan ini kemudian akan menambahkan dimensi budaya dalam implementasi peraturan pelindungan data dan dapat menjadi sebuah solusi untuk mengatasi kesenjangan budaya dan pengetahuan tentang privasi di antara warga. Menambahkan dimensi budaya dalam pembuatan dan implementasi peraturan sangatlah penting agar peraturan yang dirumuskan maupun diterapkan lebih peka terhadap karakter dan budaya masyarakat.

Banyak penelitian yang mengeksplorasi prinsip-prinsip dan nilai-nilai privasi yang harus dimasukkan ke dalam kerangka hukum pelindungan data pribadi. Namun, tidak banyak yang membahas tantangan dalam mengimplementasikan kerangka hukum pelindungan data pribadi, khususnya dalam konteks di luar UE dan AS. Studi ini hanya mengamati sebagian kecil dari tantangan yang dihadapi dan masih diperlukan lebih banyak lagi studi untuk menghasilkan solusi yang tepat untuk mengatasi tantangan-tantangan dalam implementasi kerangka hukum pelindungan data pribadi di seluruh dunia.

Referensi

Altman, I. (1977) Privacy Regulation: Culturally Universal or Culturally Specific? *Journal of Social Issues*. [Online] 3366–84.

APJII & Polling Indonesia (2019) *Penetrasi & Profil Perilaku Pengguna Internet Indonesia: Survei 2018*.

Canares, M. (2018) *Online Privacy: Will they Care? Teenagers Use of Social media and their Understanding of Privacy Issues in Developing Countries*. [online]. Available from: https://webfoundation.org/docs/2018/08/WebFoundationSocialMediaPrivacyReport_Screen.pdf.

Centre for Information Policy Leadership (2019) *Regulatory Sandboxes in Data Protection: Constructive Engagement and Innovative Regulation in Practice*. [online]. Available from: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_on_regulatory_sandboxes_in_data_protection_-_constructive_engagement_and_innovative_regulation_in_practice__8_march_2019_.pdf.

Djafar, W. et al. (2016) *Protection of Personal Data in Indonesia: A Proposal for Policy Institutionalisation from the Human Rights Perspective*. [online]. Available from: https://elsam.or.id/protection-of-personal-data-in-indonesia-a-proposal-for-policy-institutionalisation-for-the-human-rights-perspective/.

Greenleaf, G. (2017) *Global Data Privacy Laws 2017: 120 National Data Privacy Laws, Including Indonesia and Turkey*. [online]. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2992986.

GSMA (2018) *Regional Privacy Framework and Cross-Border Data Flows: How ASEAN and APEC can Protect Data and Drive Innovation*. [online]. Available from: https://www.gsma.com/publicpolicy/wp-content/uploads/2018/09/GSMA-Regional-Privacy-Frameworks-and-Cross-Border-Data-Flows_Full-Report_Sept-2018.pdf.

Li, Y. (2011) Empirical Studies on Online Information Privacy Concerns: Literature Review and an Integrative Framework. *Communications of the Association for Information Systems*. [Online] 28 (28), . [online]. Available from: https://aisel.aisnet.org/cais/vol28/iss1/28.

Sabatier, P. A. & Mazmanian, D. A. (1983) *Implementation and public policy*. Scott, Foresman public policy analysis and management series. Glenview, Ill: Scott, Foresman.

Trepte, S. et al. (2017) A Cross-Cultural Perspective on the Privacy Calculus. *Social Media + Society*. [Online] (January-March), 1–13. [online]. Available from: journals.sagepub.com/home/sms.

World Wide Web Foundation (2017) *Personal Data: An overview of low and middle-income countries*. [online]. Available from: http://webfoundation.org/docs/2017/07/PersonalData_Report_WF.pdf.

Open Data Lab Jakarta

labs.webfoundation.org
@ODLabJkt
info@labs.webfoundation.org

World Wide Web Foundation

webfoundation.org
@webfoundation
contact@webfoundation.org