

# URGENSI PERATURAN PERLINDUNGAN DATA PRIBADI DALAM ERA BISNIS *FINTECH*

Ana Sofa Yuking S.H., M.H<sup>1</sup>

## I. Pendahuluan

### A. Perkembangan *Fintech* Saat Ini

Pergerakan *startup* di Indonesia dapat dikatakan terus mengalami perkembangan yang pesat. Jenis *start-up* dibedakan menjadi dua, yaitu *e-commerce* dan *financial technology (fintech)*. *E-commerce* merupakan perusahaan yang menyediakan *platform* jual beli *online*, sementara *fintech* lebih berpusat pada perusahaan yang melakukan inovasi di bidang jasa keuangan dengan sentuhan teknologi modern.

Jenis *fintech* cukup beragam, mulai dari pengelolaan aset, penggalangan dana (*crowdfunding*), *e-money*, *Peer to Peer (P2P) Lending*, *payment gateway*, *remittance*, saham, hingga meliputi bidang asuransi. Dengan perkembangan *start-up* yang ada, banyak pula investor, baik dari individu maupun institusi yang melirik perusahaan *startup* sebagai lahan untuk berinvestasi.

Saat ini perusahaan *e-commerce* pun sudah banyak yang melakukan pengembangan bisnis *fintech* seperti *payment gateway* untuk memudahkan sistem pembayaran di situs web atau aplikasi *e-commerce* tersebut, seperti Go-Jek yang kemudian membuat Go-Pay sebagai *payment gateway*. Bahkan perusahaan *e-commerce* seperti Bukalapak juga telah mengeluarkan produk *fintech* Bukareksa yang memungkinkan masyarakat membeli reksadana melalui situs atau aplikasi Bukalapak. Perkembangan *e-commerce* yang merambah ke *fintech* semakin banyak dan tidak terbendung. Pemerintah mendukung perkembangan model bisnis baru ini dengan mengeluarkan berbagai regulasi untuk mengakomodir bisnis *fintech* serta untuk memberi perlindungan kepada masyarakat selaku konsumen sebagai pengguna.<sup>2</sup>

---

<sup>1</sup> Managing Partner Yuking & Co Attorneys at Law

<sup>2</sup> Sebagaimana diamankan oleh Peraturan Anggota Dewan Gubernur Bank Indonesia No. 19/14/PADG/2017 tentang Ruang Uji Coba Terbatas (*Regulatory Sandbox*) Teknologi Finansial Pasal 16 ayat (2) huruf b.

## 1. Definisi *Fintech*

Sebelum membahas *fintech* lebih jauh, perlu lebih dahulu mengetahui apa itu *fintech*. *Financial Technology (Fintech)* adalah salah satu bentuk penerapan teknologi informasi di bidang keuangan. Meskipun tidak terdapat definisi yang baku, pada dasarnya *fintech* adalah sebuah segmen dari dunia *start-up* yang memiliki fokus untuk memaksimalkan penggunaan teknologi guna mengubah, mempercepat atau mempertajam berbagai aspek dari layanan keuangan yang tersedia saat ini. Mulai dari metode pembayaran, transfer dana, pinjaman, pengumpulan dana, hingga pengelolaan aset.<sup>3</sup>

Secara yuridis, pengertian *Fintech* ditemukan pada Peraturan Bank Indonesia (PBI) *Fintech*. Berdasarkan Pasal 1 ayat (1) PBI No. 19/12/PBI/2017 Tentang Penyelenggaraan Teknologi Finansial (selanjutnya disebut PBI *Fintech*):

*“Teknologi Finansial adalah penggunaan teknologi dalam sistem keuangan yang menghasilkan produk, layanan, teknologi, dan/atau model bisnis baru serta dapat berdampak pada stabilitas moneter, stabilitas sistem keuangan, dan/atau efisiensi, kelancaran, keamanan, dan keandalan sistem pembayaran.”*

## 2. Klasifikasi *Fintech*

Dalam PBI *Fintech* Penyelenggaraan Teknologi Finansial dikategorikan ke dalam: sistem pembayaran; pendukung pasar; manajemen investasi dan manajemen risiko; pinjaman, pembiayaan, dan penyediaan modal; dan jasa finansial lainnya.

Penyelenggaraan Teknologi Finansial pada kategori sistem pembayaran antara lain penggunaan teknologi *blockchain* atau *distributed ledger* untuk penyelenggaraan transfer dana, uang elektronik, dompet elektronik, dan *mobile payments*. Contohnya seperti OVO, Doku, Go-Pay, E-Money, dan sebagainya. Kategori *fintech* selanjutnya adalah pendukung pasar. Yang dimaksud dengan pendukung pasar adalah teknologi finansial yang menggunakan teknologi informasi dan/atau teknologi elektronik untuk memfasilitasi pemberian informasi yang lebih cepat dan lebih murah terkait dengan produk dan/atau layanan jasa keuangan kepada masyarakat. Contoh Teknologi Finansial kategori pendukung

---

<sup>3</sup> Adhi, “Apa itu Finansial Technology (Fintech)”, 2017, <<https://www.money.id/digital/apa-itu-finansial-technology-fintech-160219n.html>>, 14 Februari 2018.

pasar antara lain penyediaan data perbandingan informasi produk atau layanan jasa keuangan seperti Cermati, CekAja.com, HeloMoney.com.

Kategori *fintech* yang ketiga ialah penyelenggaraan manajemen investasi dan manajemen risiko antara lain penyediaan produk investasi *online* dan asuransi *online* contohnya seperti DompetSehat dan NgaturDuit. Kemudian penyelenggaraan *Fintech* pada kategori pinjaman (*lending*), pembiayaan (*financing* atau *funding*), dan penyediaan modal (*capital raising*) antara lain layanan pinjam meminjam uang berbasis teknologi informasi (*Peer to peer lending*) serta pembiayaan atau penggalangan dana berbasis teknologi informasi (*crowd-funding*). *Peer to peer lending* saat ini sedang marak seperti Amarta, Investree, dan Kredivo. Sementara itu *crowd-funding* yang sedang *booming* yakni kitabisa.com yang melakukan penggalangan dana untuk donasi. Sementara itu, yang dimaksud dengan “jasa finansial lainnya” adalah Teknologi Finansial selain kategori sistem pembayaran, pendukung pasar, manajemen investasi dan manajemen risiko, serta pinjaman, pembiayaan, dan penyediaan modal.

Sementara itu, berdasarkan klasifikasi *fintech* oleh Otoritas Jasa Keuangan (OJK), terdapat dua golongan *fintech* yang akan masuk ke dalam ranah pengawasan OJK.<sup>4</sup> Mereka adalah *Fintech 2.0 Digital LJK* dan *Digital Banking* dan *Fintech 3.0-3.5 Start-up Companies*. Kedua kategori tersebut nantinya harus mematuhi segala aturan yang dibuat oleh OJK. Kategori *Fintech 2.0* melingkupi tiga ranah sektor industri diantaranya perbankan, pasar modal, dan industri keuangan non-bank (IKNB). Untuk perbankan, ranah bisnis yang akan diatur mulai dari *E-banking*, Layanan Keuangan Tanpa Kantor dalam Rangka Keuangan Inklusif (Laku Pandai), *Digital Branch*, dan *Banking Anywhere (Omnichannel)*. Sementara, untuk pasar modal yakni *E-stocks*, *Bonds*, *Mutual Funds*, dan *Trading*. Terakhir, dalam IKNB yang akan diatur adalah E-Gadai, E-LKM, E-Penjaminan, dan E-Asuransi. Kategori berikutnya, *Fintech 3.0-3.5* khusus mengatur perusahaan startup *fintech* non-lembaga jasa keuangan (LJK), dengan ranah bisnis yang akan diatur adalah koperasi, bursa berjangka, dan *loan-based crowdfunding (P2P Lending)*.

Di sisi lain, Bank Indonesia menaungi dan mengatur Alat Pembayaran dengan menggunakan kartu (APMK), *E-Money*, *Telco Money*, *Blockchain (Bitcoin)*, dan

---

<sup>4</sup> Marsya Nabila, “Berikut ini Klasifikasi Fintech yang Akan Diatur OJK”, <<https://dailysocial.id/post/berikut-ini-klasifikasi-fintech-yang-akan-diatur-ojk>>, diakses pada tanggal 4 Februari 2018.

*National Payment Gateway* (NPG) sebagaimana yang telah disebutkan dalam PBI *Fintech*.

### **3. Peraturan Perundang-undangan Yang Berkaitan Dengan *Fintech***

Perkembangan *fintech* yang sangat pesat perlu diatur oleh hukum untuk pengembangan industri itu sendiri juga untuk melindungi masyarakat selaku pengguna. Pemerintah melalui BI dan OJK sebagai badan yang berwenang mengatur *fintech* sesuai dengan kategorinya, telah mengeluarkan peraturan teknis dalam regulasi terkait *fintech*, diantaranya yakni POJK No. 77/POJK.01/2016 tentang Layanan Pinjam Meminjam Uang Berbasis Teknologi Finansial (POJK *Fintech*), PBI No. 19/12/PBI/2017 Tentang Penyelenggaraan Teknologi Finansial (selanjutnya disebut PBI *Fintech*), PBI No. 18/40/PBI/2016 Tentang Penyelenggaraan Pemrosesan Transaksi Pembayaran, PBI No. 11/12/PBI/2009 Tentang Uang Elektronik yang telah diubah dalam PBI No. 16/8/PBI/2014.

### **4. Kebutuhan Regulasi Pendukung Pelaksanaan *Fintech* Dalam Hal Perlindungan Data Pribadi**

Untuk mendukung perkembangan bisnis *fintech* di Indonesia, selain didukung oleh peraturan yang diterangkan pada bagian sebelumnya, perlu juga didukung dengan peraturan pendukung pelaksanaan *fintech* yang diantaranya berkaitan dengan perlindungan data penggunaan data pribadi. Penggunaan teknologi informasi dalam bisnis *fintech* sangat berkaitan erat dengan data atau informasi. Dalam hal ini masyarakat selaku konsumen *fintech* perlu mendapatkan perlindungan kerahasiaan informasi konsumen. Data konsumen terutama yang menyangkut informasi pribadi pengguna sangat rawan disalahgunakan oleh pihak yang tidak bertanggungjawab. Saat ini regulasi terkait perlindungan data pribadi di Indonesia masih tersebar dalam beberapa peraturan. Oleh karena itu, regulasi perlindungan data pribadi yang komprehensif dirasa sangat dibutuhkan keberadaannya karena saat ini belum terdapat peraturan perundang-undangan yang menjadi *lex specialis* mengenai perlindungan data pribadi khususnya dalam bisnis *fintech*.<sup>5</sup>

---

<sup>5</sup> Naskah Akademik RUU PDP hlm. 7.

Saat ini Indonesia belum memiliki Undang-undang yang komprehensif mengenai perlindungan data pribadi. Undang-Undang Dasar Republik Indonesia Tahun 1945 (UUD 1945) sebagai konstitusi Indonesia tidak secara eksplisit mengatur mengenai perlindungan data sebagai salah satu bentuk penghormatan atau pengakuan, perlindungan dan pemenuhan HAM dalam bentuk perlindungan privasi. Meskipun UUD 1945 menyatakan dengan tegas adanya perlindungan terhadap hak asasi manusia. Dalam UUD 1945 ketentuan mengenai perlindungan data, secara implisit bisa ditemukan dalam pasal 28F dan 28G (1), mengenai kebebasan untuk menyimpan informasi dan perlindungan atas data dan informasi yang melekat kepadanya. Hal ini juga yang mendasari semua peraturan perundang-undangan selaku aturan yang mengatur tentang privasi sebagai HAM, selain untuk kepastian hukum (sebagai salah satu syarat suatu negara hukum),<sup>6</sup> termasuk Undang-Undang Perlindungan Data Pribadi yang nantinya akan terbentuk.<sup>7</sup>

Saat ini, pengaturan perlindungan data pribadi secara implisit masih tersebar di berbagai jenjang peraturan perundang-undangan yang ada di Indonesia. Peraturan terkait perlindungan data pribadi masih terpisah dan terpecah-pecah tergantung masing-masing sektor, diantaranya yakni sebagai berikut:<sup>8</sup>

No	Produk Hukum	Jumlah Pasal
1	Rancangan Undang-Undang Tentang Perlindungan Data dan Informasi Pribadi	48 Pasal
2	Peraturan Menteri Komunikasi dan Informasi Nomor 20 Tahun 2016 Tentang Perlindungan Data Pribadi Dalam Sistem Elektronik	37 Pasal
3	Peraturan Pemerintah Nomor 37 Tahun 2007 Tentang Pelaksanaan Undang-Undang Nomor 23 Tahun 2006 Tentang Administrasi Kependudukan	13 Pasal
4	Undang-Undang Nomor 23 Tahun 2006 Tentang Administrasi Kependudukan	8 Pasal
5	Peraturan Pemerintah Nomor 82 Tahun 2012 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik	6 Pasal
6	Peraturan Pemerintah Nomor 83 Tahun 2012 Tentang Perubahan Atas Peraturan Pemerintah Nomor 5 Tahun 2009 Tentang Bantuan Keuangan Kepada Partai Politik	6 Pasal

<sup>6</sup> Naskah Akademik RUU PDP hlm. 36.

<sup>7</sup> Naskah Akademik RUU PDP hlm. 10-11,16, .

<sup>8</sup> KlikLegal.com, "Ini Berbagai Peraturan Perlindungan Data Pribadi di Indonesia", <<https://kliklegal.com/ini-berbagai-peraturan-perlindungan-data-pribadi-di-indonesia/>>, diakses pada tanggal 11 Januari 2018.

7	Undang-Undang Nomor 24 Tahun 2013 Tentang Revisi Administrasi Kependudukan	4 Pasal
8	Peraturan Menteri Komunikasi dan Informasi Nomor 11 Tahun 2016 Tentang Klasifikasi Permainan Interaktif Elektronik	3 Pasal
9	Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik	3 Pasal
10	Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik	2 Pasal
11	Undang-Undang Nomor 43 Tahun 2009 Tentang Kearsipan	2 Pasal
12	Undang-Undang Nomor 56 Tahun 1999 Tentang Rakyat Terlatih	2 Pasal
13	Peraturan Menteri Komunikasi dan Informasi Nomor 4 Tahun 2016 Tentang Sistem Manajemen Pengaman Informasi	1 Pasal
14	Peraturan Menteri Komunikasi dan Informasi Nomor 36 Tahun 2014 Tentang Tata Cara Pendaftaran Penyelenggara Sistem Elektronik	1 Pasal
15	Peraturan Menteri Komunikasi dan Informasi Nomor 11 Tahun 2010 Tentang Penyelenggaraan Layanan Televisi Protokol Internet (Internet Protocol Television / IPTV)	1 Pasal
16	Undang-Undang Nomor 36 Tahun 2009 Tentang Kesehatan	1 Pasal
17	Undang-Undang Nomor 11 Tahun 2012 Tentang Sistem Peradilan Pidana Anak	1 Pasal
18	Undang-Undang Nomor 3 Tahun 1997 Tentang Pengadilan Anak	1 Pasal
19	Undang-Undang Nomor 10 Tahun 2011 Tentang Perubahan Atas Undang-Undang Nomor 32 Tahun 2007 Tentang Perdagangan Berjangka Komoditi	1 Pasal
20	Undang-Undang Nomor 32 Tahun 2007 Tentang Perdagangan Berjangka Komoditi	1 Pasal

Meskipun telah ada Permenkominfo No. 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik untuk memberikan perlindungan terhadap industri *fintech*, tetapi produk hukum tersebut masih lemah. Belum ada ketentuan mengenai sanksi yang kuat dalam hal terjadi pelanggaran data pribadi konsumen. Untuk itu, diperlukan Undang-Undang Perlindungan Data Pribadi sebagai payung hukum perlindungan data pribadi untuk semua sektor khususnya dalam pemanfaatan sistem elektronik.

## II. Urgensi Perlindungan Data Pribadi Pada *Fintech*

### A. Kebutuhan Peraturan Perlindungan Data Pribadi Dalam Bisnis *Fintech*

Penggunaan teknologi informasi merupakan *core* bisnis *fintech*, dan dalam penggunaan teknologi informasi, terdapat resiko yang dengan erat berhubungan dengan penggunaan teknologi informasi itu sendiri serta telah terbukti tidak dapat dieliminir.<sup>9</sup> Oleh karena itu, DPR selaku badan legislatif yang berwenang membuat undang-undang maupun pemerintah perlu segera menerbitkan peraturan perundang-undangan mengenai perlindungan data pribadi (sebagai tolok ukur) bagi penyelenggara jasa, bukan hanya bagi konsumen.<sup>10</sup> Sampai saat ini produk hukum tersebut masih berupa *ius constituendum* (hukum yang dicita-citakan) berupa rancangan Undang-undang Perlindungan Data Pribadi (RUU PDP). Peraturan perundang-undangan yang nantinya ada haruslah menjamin perlindungan data pribadi dari pengguna jasa baik perlindungan data konvensional maupun data *digital* pada penggunaan secara *offline* maupun penggunaannya pada ruang lingkup *cyberspace*. Peraturan perundang-undangan tersebut haruslah memuat sanksi yang jelas bagi pelanggar dan tidak membuat *overlapping* dengan ketentuan lain.

Sebelum membahas lebih lanjut mengenai perlindungan data pribadi, perlu diketahui lebih dahulu apa yang dimaksud data pribadi. Berangkat dari pengertiannya, data pribadi adalah data yang berupa identitas, kode, simbol, huruf atau angka penanda personal seseorang yang bersifat pribadi. Setiap negara menggunakan peristilahan yang berbeda antara informasi pribadi dan data pribadi. Akan tetapi secara substantif kedua istilah tersebut mempunyai pengertian yang hampir sama sehingga kedua istilah tersebut sering digunakan bergantian. Amerika Serikat, Kanada, dan Australia menggunakan istilah informasi pribadi sedangkan negara-negara Uni Eropa dan Indonesia sendiri dalam UU ITE menggunakan istilah data pribadi.

Pengertian data pribadi dapat ditemui dalam Pasal 1 angka 1 Permenkominfo No. 20 Tahun 2016 Tentang Perlindungan Data Pribadi Dalam Sistem Elektronik. Data pribadi diartikan sebagai "... data perseorangan tertentu yang disimpan, dirawat, dan dijaga kebenaran serta dilindungi kerahasiaannya". Dengan demikian, dapat disimpulkan bahwa data pribadi merupakan data perseorangan tertentu

---

<sup>9</sup> Steven R. Chabinsky, "Fintech: Cybersecurity Risk Management for Financial Institutions and Technology Vendors", 2017, <<https://www.lexology.com/library/detail.aspx?g=3acc8886-d0bb-4e86-8521-1b4445e79ad9>>, 22 Februari 2018.

<sup>10</sup> *Ibid.*

berupa identitas, kode, simbol, huruf atau angka penanda personal seseorang yang bersifat pribadi yang dijaga dan dilindungi kerahasiannya.

Maraknya perkembangan industri berbasis teknologi informasi menyadarkan masyarakat akan pentingnya menjaga kerahasiaan data pribadi miliknya dari berbagai ancaman penyalahgunaan data. Di Indonesia terdapat kekhawatiran mengenai pelanggaran privasi dan perlindungan data pribadi. Hal ini disebabkan karena secara sosiologis, pada mulanya sebagian besar negara di Asia termasuk Indonesia tidak mengenal privasi. Hal tersebut didasarkan pada sejarah masyarakat Asia yang secara tradisional hidup dalam masyarakat komunal yang mana tidak memberi perhatian untuk privasi. Istilah privasi sebagai hak asasi manusia pada dasarnya memang berasal dari bangsa Barat (atau bukan dari Indonesia).<sup>11</sup> Privasi kemudian menjadi penting dalam era teknologi informasi dan komunikasi, sehingga kebutuhan akan undang-undang mengenai perlindungan privasi dan perlindungan data pribadi menjadi agenda mendesak.

Kembali lagi ke industri *Fintech* yang pada dasarnya memanfaatkan teknologi informasi dalam sistem keuangan yang menghasilkan produk, layanan, teknologi, dan/atau model bisnis baru. Bisnis modal baru ini perlu didukung oleh pemerintah karena sangat menguntungkan untuk peningkatan ekonomi Indonesia baik dari segi dunia usaha maupun masyarakat selaku konsumen. Akan tetapi, perlu diperhatikan pula bahwa penggunaan teknologi informasi bagi pisau bermata dua. Teknologi jika dimanfaatkan dengan baik dapat membantu kehidupan manusia, namun teknologi juga dapat menjadi sangat berbahaya apabila tidak dibatasi penggunaannya, seperti dalam hal tidak dilindunginya data pribadi karena tidak terdapat kewajiban dalam hukum positif yang secara rinci mengatur dan memberikan sanksi terhadap pelanggaran.

Bahaya tersebut dapat timbul dari adanya pencurian data pribadi, kerusakan *system* yang dapat memungkinkan terjadinya pembobolan data (termasuk data pribadi), penyalahgunaan data pribadi yang telah dikuasai oleh pelaku usaha itu sendiri<sup>12</sup> ataupun pihak-pihak lainnya yang dapat mengakses data pribadi konsumen (seperti pemerintah).<sup>13</sup> Kebutuhan pengaturan akan hal ini dinilai

---

<sup>11</sup> Naskah Akademik RUU PDP hlm. 126.

<sup>12</sup> Lihat kebijakan privasi *google* yang di dalamnya tertera kewenangan untuk mengubah data mendistribusikan data pribadi tanpa harus meminta izin terlebih dahulu dari si pemilik data.

<sup>13</sup> Seperti yang terjadi pada kasus pembobolan *iCloud*; Naskah Akademik RUU PDP hlm. 44.



penting karena data pribadi merupakan hak privasi seseorang, selain juga secara fundamental dapat bernilai ekonomis bagi pihak ketiga yang hendak memanfaatkannya.

Bahaya dari adanya kekosongan hukum pada rezim perlindungan data pribadi akan sangat merugikan konsumen, dikarenakan banyak sekali ancaman dari pembobolan disamping kelalaian yang dapat disebabkan karena kurang matangnya *system* perlindungan data pribadi yang digagas pelaku usaha sektor *fintech* maupun ancaman dari adanya kesengajaan pelaku bisnis atau tenaga kerja pada sektor bisnis *fintech* yang berniat membobol data pribadi untuk kepentingan tertentu. Resiko tersebut dapat menjadikan *fintech* di Indonesia mendapat predikat buruk dari negara yang telah memiliki peraturan perlindungan data pribadi yang lebih mumpuni maupun dari konsumen dan calon konsumen jasa *fintech*.

## **B. Pemanfaatan *Big Data* Yang Belum Memiliki Rezim Pengaturan Perlindungan Konsumen**

Di era digital saat ini, informasi merupakan komoditas yang paling dicari dan sangat menguntungkan bagi pihak yang dapat mengolahnya. Hal itu terbukti dari *big data* yang sangat menguntungkan bagi pebisnis maupun pemerintah. *Big data* dimanfaatkan oleh pelaku usaha *e-commerce* seperti Go-Jek, Grab, Tokopedia, dan sebagainya. *Big data* yang dalam hal ini merupakan sekumpulan data hasil olahan data pribadi yang didapatkan dari kegiatan konsumen sehari-hari. Dari situ dapat terlihat kebiasaan konsumen seperti tempat yang biasa dikunjungi setiap harinya, kebiasaan tertentu (*cookies*, kebiasaan belanja, dan lain sebagainya), *browsing history*, likes, dan lain-lain.

*Big Data* sendiri oleh *Joint Committee of the European Supervisory Authorities* didefinisikan sebagai situasi di mana data yang beragam, dalam tingkat *volume* tinggi, diproduksi dalam kecepatan tinggi dari berbagai sumber, diproses secara *real time* oleh perangkat *IT*, dengan serangkaian teknologi seperti *processor*, piranti lunak, dan algoritma.<sup>14</sup> Dalam kaitannya dengan perlindungan konsumen, maka isu yang harus diangkat adalah permasalahan hukum yang berkaitan dengan privasi, perlindungan data, penegakan hukum dan HAM.

---

<sup>14</sup> BIPAR, "Digitalisation and Fintech", 2018, <<http://www.bipar.eu/en/page/digitalisation-and-fintech>>, 21 Februari 2018.

Resiko datang ketika konsumen tidak harus mengeluarkan biaya untuk menggunakan jasa sebuah *fintech* melalui aplikasi, namun, dibalik skema yang ada, terdapat penjualan data pribadi oleh penyelenggara jasa kepada pihak ketiga tanpa menghargai privasi seseorang.<sup>15</sup> Data pribadi yang paling rentan dimanfaatkan secara ilegal adalah identitas seseorang yang terekspos secara tidak sengaja atau dicuri. Terbukti dari data yang dibuat oleh perusahaan *anti-virus* Symantec yang menyebutkan bahwa telah terjadi pencurian atau pembukaan data terhadap sebanyak 500 juta identitas *digital* sepanjang tahun 2015 saja.<sup>16</sup>

Penggunaan *Big Data* memuat data pribadi yang bernilai ekonomis (memiliki nilai tinggi untuk kepentingan bisnis).<sup>17</sup> Penggunaan data yang tidak sesuai dengan peruntukan dan kesepakatan, akan berujung pada pelanggaran privasi maupun pelanggaran ketentuan dalam kaidah-kaidah yang membatasi persaingan usaha. Sebagai contoh adalah adanya data mengenai riwayat penyakit, database penggunaan *GPS* (Untuk melacak lokasi seseorang)<sup>18</sup> dari ponsel seseorang, jejak penggunaan jejaring sosial, data yang terlacak dari penggunaan *IoT*, dan lain sebagainya, yang diantara data-data tersebut ada yang bersifat sensitif, seperti riwayat penyakit seorang pasien.<sup>19</sup> Dan akan mencederai hak seorang konsumen apabila data tersebut jatuh ke pihak lain dan dimanfaatkan secara melawan hukum.

Bocornya data merupakan resiko yang paling ditakuti atau dengan istilah lain menjadi *significant concern* bagi pelaku usaha maupun konsumen. Sayangnya, tatanan hukum di Indonesia masih belum memiliki mekanisme penindakan yang secara khusus dapat memberikan wewenang khusus bagi sebuah instansi penegakan hukum dalam ranah perlindungan konsumen untuk mengambil tindakan tertentu dan memproses pelanggaran hukum tersebut, serta memberikan sanksi bagi pihak-pihak yang terlibat dan juga diuntungkan oleh adanya kebocoran data (*data breach*). Dari hal-hal seperti inilah pemanfaatan *big data* dinilai riskan karena

---

<sup>15</sup> EDPS, Privacy and Competitiveness in the Age of Big Data”, 2018, < [https://edps.europa.eu/press-publications/press-news/press-releases/2014/privacy-and-competitiveness-age-big-data\\_en](https://edps.europa.eu/press-publications/press-news/press-releases/2014/privacy-and-competitiveness-age-big-data_en)>, diakses pada tanggal 22 Februari 2018; Dasar hukum bagi wewenang EDPS ada pada *Regulation (EC) No. 45/2001*; Naskah Akademik RUU PDP hlm. 5.

<sup>16</sup> Louis de Koker, *Op Cit.*, note 5, hlm. 6.

<sup>17</sup> Naskah Akademik RUU PDP hlm. 44.

<sup>18</sup> Pernah terjadi skema *location-based messaging* untuk mempromosikan produk dari lokasi tertentu bagi konsumen yang sedang berada pada lokasi tersebut; Naskah Akademik RUU PDP hlm. 6.

<sup>19</sup>John S. Pruitt *et al*, “Big Data and Cybersecurity: The Federal Insurance Office Explores New Frontiers for Consumer Protection”, 2017 ,<<https://www.lexology.com/library/detail.aspx?g=b2663a0a-6603-4ca4-831e-5c94ca42a296>>, diakses pada tanggal 22 Februari 2018;

memang belum memiliki rezim perlindungan konsumen karena belum diatur secara khusus.

### **III. Review RUU Perlindungan Data Pribadi**

#### **A. Materi Muatan Yang Diatur di Dalam RUU Perlindungan Data Pribadi**

Beberapa poin penting yang menurut penulis ada pada materi muatan di dalam RUU perlindungan data pribadi diantaranya sebagai berikut:

##### **1. Dimuatnya Asas-asas di Bidang Hukum Perlindungan Data Pribadi Dalam Pertimbangan dan Pasal-pasalny**

Asas Perlindungan sebagai dasar dari dilindunginya data pribadi, asas kepentingan umum sebagai pengecualian boleh diterobosnya data pribadi, asas keseimbangan yang mengatur batasan antara hak individu dan hak negara, dan asas pertanggungjawaban sebagai landasarn bagi pelaku usaha untuk menyelenggarakan *system* pemrosesan, penyebarluasam, pengelolaan, dan pengawasan data pribadi yang bertanggung jawab harus menjadi dasar bagi adanya pasal-pasal lainnya yang akan merinci perlindungan data pribadi.<sup>20</sup>

##### **2. Kesepakatan Dari Konsumen Untuk Menyerahkan Data Pribadi Pada Pelaku Usaha dan Keterbukaan Informasi Terhadap Penyimpanan dan Pengolahan Data Oleh Pelaku Usaha**

Perbuatan yang paling utama dan terlebih dahulu harus diatur adalah kesepakatan (*consent*) para pihak berkaitan dengan penyerahan data. Untuk memenuhi asas konsensualitas dalam segala perikatan diperlukan pengaturan tentang hal ini sebagai materi muatan yang paling fundamental.

Harus ditentukan bahwa data pribadi yang telah diambil dari konsumen harus terlebih dahulu didahului oleh kesepakatan yang sebaiknya dibuat dalam bentuk tertulis, dinyatakan secara eksplisit, dan dibubuhi tanda tangan atau tanda tangan digital sebagai alat bukti bahwa konsumen telah secara sadar menyetujui data pribadinya utuk diproses oleh pelaku usaha. Penulis menilai hal tersebut akan mempermudah pembuktian apabila nantinya terjadi sengketa.

Kesepakatan tersebut juga harus secara jelas menentukan tujuan penggunaan data pribadi yang telah diberikan agar hanya dapat digunakan atau diperbolehkan

---

<sup>20</sup> Naskah Akademik RUU PDP hlm. 37.

sebatas untuk tujuan yang telah disepakati bersama dan bukan untuk tujuan lainnya. Atau dengan kata lain penggunaannya semata-mata hanya untuk tujuan yang secara langsung berhubungan dengan fungsi dari pengumpulan dan pengolahan data tersebut saja. Kesepakatan tersebut juga haruslah memuat klausul yang menyatakan dan mengikat pelaku usaha untuk tidak memberikan atau menjual data pribadi konsumen *fintech* pada pelaku usaha lain atau pihak ketiga lainnya lagi, apabila tidak diperkenankan.

### 3. Hak-hak Pemilik Data Pribadi

Hak dari pemilik data perlu dijabarkan satu persatu, karena tidak hanya meliputi perlindungan data semata. Sekalipun tujuan utama dari RUU PDP adalah perlindungan yang layak terhadap kepentingan privasi, namun, banyak juga persyaratan pendukung yang perlu diikuti agar tujuan utama dapat dipenuhi dengan optimal, diantaranya adalah sebagai berikut:

- a) Hak untuk mengajukan akses yang memadai
- b) Hak atas salinan data pribadi dari pengelola data pribadi
- c) Hak meminta pengelola data untuk memperbaiki kesalahan yang terdapat pada data pribadi yang sebelumnya telah diberikan dan tersimpan
- d) Hak untuk memperbaharui data pribadi yang berada pada pengelola data
- e) Hak untuk melengkapi data dan pribadi sebelum data pribadi tersebut dikelola oleh pengelola
- f) Hak untuk meminta pada pengelola data pribadi untuk memusnahkan data pribadi konsumen
- g) Hak untuk menuntut dan menerima ganti rugi atas pelanggaran terhadap hak-hak konsumen
- h) Hak untuk dapat setiap saat menarik kembali persetujuan pengelolaan data yang telah diberikan
- i) Hak untuk dapat setiap saat menarik kembali persetujuan pengelolaan data yang telah diberikan pada pengelola data dengan pemberitahuan.<sup>21</sup>

Akses terhadap data dan penyimpanan data memang sudah seharusnya dijamin agar seseorang dapat menjalankan hak untuk mendapatkan pengamanan data miliknya dan untuk mengoreksi data ketika didapati bahwa terdapat kesalahan pada data yang disimpan, pun untuk menarik kembali penyerahan data pribadi.<sup>22</sup> Sebagai catatan juga bahwa konsumen berhak menyerahkan data pribadinya ke hadapan publik apabila disetujui oleh Individu pemilik data pribadi tersebut.<sup>23</sup> Karena hak tersebut juga adalah hak konsumen, maka terpenuhinya penyerahan

---

<sup>21</sup> Naskah Akademik RUU PDP hlm. 139&140.

<sup>22</sup> Naskah Akademik RUU PDP hlm. 32 & 64.

<sup>23</sup> Naskah Akademik RUU Perlindungan Data Pribadi hlm. 27.

data pribadi untuk konsumsi publik juga harus dapat ditarik kembali atau pada awalnya harus dengan segera dapat dipenuhi oleh pengelola data.

#### **4. Perbedaan Antara Data Pribadi dan Data Pribadi Sensitif**

Dalam RUU Perlindungan data pribadi (tahun 2015), pengertian data pribadi adalah:

*“... setiap data tentang kehidupan seseorang baik yang teridentifikasi dan/atau diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik dan/atau non elektronik.”*

Terdapat perbedaan dari pengertian data pribadi dalam Permenkominfo dengan RUU Perlindungan data pribadi. Perbedaannya adalah, bahwa dalam RUU PDP dibedakan antara data pribadi dan data pribadi sensitif.<sup>24</sup> Meskipun demikian, secara substansi produk hukum tersebut pada dasarnya mengatur materi muatan yang sama, yakni keamanan data pribadi yang dikumpulkan, dikendalikan atau dikuasai, dan diproses oleh pelaku bisnis *fintech* terlepas dari perbedaan jenis data pribadi yang diatur (data pribadi sensitif atau bukan data pribadi sensitif). Barulah nanti di dalamnya terdapat perbedaan tingkat perlindungan pada data pribadi sensitif dengan perlindungan tingkat tinggi. Semakin sensitif suatu informasi maka penjagaannya harus dilakukan dengan perlindungan tinggi.<sup>25</sup>

#### **5. Kewajiban Pelaku Usaha Bagi Aktivitas Yang Berkaitan Dengan Pengumpulan, Pengendalian, Pemrosesan, dan Penggunaan Data Pribadi**

Pengelola data pribadi dalam kenyataannya merupakan badan hukum. Oleh karena itu, selaku subjek hukum, perlu juga diatur mengenai kewajiban apa saja yang menjadi beban tanggung jawab pelaku usaha dalam menyelenggarakan jasa *fintech* dan mengumpulkan serta memproses data. Dalam Naskah Akademik RUU PDP, selain mendapatkan persetujuan pengumpulan data seperti yang sudah dijelaskan pada sub-bab sebelumnya, kewajiban-kewajiban lain tersebut diantaranya adalah sebagai berikut:

- a) Legalitas dari pengelola data pribadi
- b) Kejelasan tujuan pengelolaan data pribadi
- c) Jenis-jenis data pribadi harus diklasifikasikan
- d) Perincian periode retensi dokumen yang memuat data pribadi termasuk jangka waktu pengelolaan dan pemusnahan data
- e) Perincian keterangan data pribadi yang dikumpulkan

---

<sup>24</sup> Sebagai contoh data pribadi sensitif atau *sensitive personal data* menurut UK *Data Protection Act* 1998 adalah agama, riwayat penyakit, keterangan mengenai ras/etnis, pendapat politik, kehidupan seks, dan lain-lain seperti tercantum dalam Naskah Akademik RUU PDP hlm. 62; Sedangkan data pribadi diantaranya adalah nama, tanggal lahir, fotografer, rekaman video, alamat *e-mail*, nomor telepon, *IP addresses*, dan *communication content*.

<sup>25</sup> Naskah Akademik RUU PDP hlm. 24.

- f) Kewajiban untuk tidak mencegah atau mempersulit pemilik data untuk merubah, menghapus, dan menarik kembali data pribadinya untuk dikelola penyelenggara jasa
- g) Kewajiban untuk menunda proses pengelolaan data pribadi sebagian atau seluruhnya apabila dimintakan penundaan oleh pemilik data
- h) Pengumuman kebijakan penggunaan privasi bagi konsumen dan/atau calon konsumen
- i) Pemenuhan hak yang berkaitan dengan *habeas data*<sup>26</sup> pada bagian sebelumnya selaku kewajiban penyelenggara jasa
- j) Memastikan pengawasan optimal terhadap tenaga kerja yang terlibat dalam pengelolaan data pribadi
- k) Memastikan bahwa data pribadi adalah akurat dan lengkap apabila data tersebut akan dimintakan untuk membuat suatu keputusan yang mempengaruhi pemilik data pribadi (contoh riwayat penyakit atau catatan medis dalam bentuk lainnya)
- l) Memastikan keamanan *system* agar tidak terbobol dan terjadi pencurian data
- m) Beranggunggungjawab atas segala kelalaian atau kesengajaan yang menimbulkan tidak terpenuhinya perlindungan data pribadi konsumen
- n) Kewajiban untuk memusnahkan data pribadi apabila: Telah mencapai periode retensi; Tujuan pengelolaan data pribadi telah tercapai; atau terdapat permintaan dari pemilik data
- o) Kewajiban untuk melakukan pemberitahuan pada pemilik data yang dirugikan tanpa penundaan fakta bahwa data pribadi miliknya terungkap.
- p) Kewajiban untuk menginformasikan pemasangan alat pemroses data visual ke masyarakat dan menjamin keamanan data pribadi yang diperolehnya dari alat pemroses data visual (seperti perekaman biometrik).<sup>27</sup>

Bahwa apabila nantinya terdapat pembobolan data atau *data breach*, keterlibatan pengelola data dalam perbuatan tindak pidana korupsi, analisa konsumen tanpa persetujuan konsumen, penipuan, pencucian uang, pendanaan terorisme, dan penggelapan dan lain sebagainya, serta hal tersebut diketahui dan secara sengaja terjadi pembiaran dari pelaku usaha, maka nantinya pelaku usaha akan dapat dijerat oleh Undang-undang ini. Termasuk pula dalam hal terdapat *data breach* yang diketahui dan tidak dicegah atau ditanggulangi, maka hal pertanggungjawabannya juga dapat dibebankan pada pelaku usaha. Oleh karena itu, perluasan dan penambahan kewajiban juga perlu dilakukan untuk memastikan bahwa pengelola data apabila terlibat tindak pidana tersebut dapat dimintakan pertanggungjawabannya.

---

<sup>26</sup> '*habeas data*' yakni hak seseorang untuk mendapatkan pengamanan terhadap datanya dan untuk membenarkan ketika ditemukan kesalahan terhadap datanya dalam Naskah Akademik RUU PDP hlm. 32.

<sup>27</sup> Naskah Akademik RUU PDP bagian kewajiban pengelola data pribadi hlm. 151.

Kejelasan mengenai tujuan pengumpulan data yang harus berkaitan erat dengan sektor bisnis yang dijalankan pun harus diberi batasan, agar kegiatan pengumpulan data tidaklah dilakukan secara serampangan. Sebagai contoh apabila penyedia jasa *fintech* yang tidak bergerak pada bidang asuransi kesehatan hendak mengambil data pribadi konsumen yang berkaitan dengan riwayat penyakit,<sup>28</sup> maka hal tersebut patut dipertanyakan karena berada di luar batasan yang ditentukan yang mengatur hal-hal teknis yang berkaitan dengan kaidah tujuan pengumpulan data yang mewajibkan agar pelaku usaha hanya diperbolehkan untuk mengumpulkan data pribadi konsumen sebatas pada data pribadi yang berkaitan dengan jasa atau bisnis yang akan digunakan atau dilakukannya secara spesifik.

Sebagai perbandingan, dalam Pasal 6 *Ethics Standard for Data Controllers EU Data Protection Directive* menyebutkan bahwa data-data tersebut harus diproses secara adil dan berdasarkan hukum, pengumpulan data haruslah spesifik penggunaannya dan jelas peruntukannya, serta tujuannya dapat dilegitimasi oleh hukum. Apabila hal tersebut dilanggar, maka seseorang dapat memintakan pertanggungjawaban dan ganti kerugian pada negara. Karena pengumpulan data yang tidak berkaitan dengan keperluan konsumen pada penyelenggara jasa cenderung berpotensi dan mengarah pada penyalahgunaan data pribadi. Oleh karena itu, nantinya peraturan perundang-undangan yang ada haruslah memuat aturan tentang kejelasan hubungan antara data pribadi yang dikumpulkan, dengan sektor bisnis yang dijalankan *fintech* tersebut (atau jasa yang akan ditawarkan) demi kejelasan tujuan pengumpulan data pribadi.

## **6. Pendaftaran *Fintech* dan Standarisasi Teknologi Perlindungan Data Pribadi Bagi Para Penyelenggara Jasa *Fintech***

Kemenkominfo dapat memberikan *assessment* bagi penyelenggara jasa untuk memastikan penyedia jasa *fintech* dapat berperan mengikuti standar yang telah ditetapkan atau tidak. Tentunya segalanya harus sesuai dengan kriteria dan standar yang ditetapkan oleh RUU. Seperti keterbukaan dari penyedia jasa tentang pemanfaatan data pribadi yang dikumpulkannya, kredibilitas *system* yang dibangun pelaku usaha agar dapat menangkal bahaya dan resiko yang berkaitan dengan *cybersecurity*, berapa banyak salinan data pribadi yang disimpan, pengaturan

---

<sup>28</sup> Naskah Akademik RUU Perlindungan Data Pribadi hlm. 1.

tentang di mana data tersebut disimpan, siapa sajakah yang dapat mengakses data tersebut, penggunaan *encryption* bagi mekanisme pengaksesan data, dan lain-lain.<sup>29</sup> Serta hal-hal teknis dan prosedural lainnya yang diatur dan wajib dipatuhi oleh pelaku usaha. Untuk memudahkan pengawasan dalam hal ini, maka penyelenggara teknologi finansial wajib mendaftarkan diri pada Bank Indonesia dan/atau Otoritas Jasa Keuangan.

## 7. Pemenuhan Privasi dan Perlindungan Data Pribadi Sebagai HAM

Secara filosofis, penekanan bahwa perlindungan data pribadi juga merupakan bentuk pengakuan, perlindungan, dan pemenuhan HAM juga perlu diterangkan di dalam RUU.<sup>30</sup> Bahwa hukum positif yang nantinya ada haruslah memberikan perlindungan terhadap hidup dan barang milik seseorang. Hal tersebut dikarenakan data pribadi ini dapat dinilai sebagai barang berharga tidak berwujud milik seseorang, selain juga sebagai pemenuhan privasi seseorang sebagai HAM, maka apabila terdapat pelanggaran hukum terhadap data pribadi, seseorang dapat juga menuntut ganti kerugian pada pelanggar yang melanggar kebebasan, hak atas benda dan hak-hak lainnya yang melekat kepada seorang individu.

Interferensi dalam bentuk penggeledahan, penyitaan, penyadapan, dan bentuk-bentuk interferensi lainnya hanya diperbolehkan apabila terdapat *probable cause* dengan berdasar pada hukum yang ada atau adanya ancaman pada keamanan nasional, kepentingan publik, kepentingan ekonomi sebuah negara, pencegahan tindak pidana, perlindungan moral dan kesehatan atau perlindungan bagi hak dan kebebasan orang lain.<sup>31</sup> Bentuk-bentuk interferensi lainnya, seperti *hacking* atau *data breach* berarti juga pelanggaran HAM apabila hal tersebut dilakukan oleh Pemerintah sendiri tanpa adanya *probable cause* atau dilakukan dengan kolusi bersamaan dengan pelaku usaha demi keuntungan materil, adalah pelanggaran hukum sekaligus melanggar prinsip “*the right to enjoy life and the right to be left alone*” sebagai konsep paling dasar dari perlindungan privasi. Sekalipun pada umumnya, memang ada batasan terhadap interferensi yang diperbolehkan ini yang akan dijelaskan oleh peneliti pada bagian berikutnya.

---

<sup>29</sup> Seperti diamanatkan oleh Pasal 25 dan 32 – 34 *GDPR* yang mana akan berlaku juga bagi penyelenggara jasa *fintech* dengan konsumen dari Uni Eropa.

<sup>30</sup> Naskah Akademik RUU Perlindungan Data Pribadi hlm. 2 & 121.

<sup>31</sup> *Ibid*, hlm. 6.



Dalam Undang-undang PDP juga nantinya perlu dibuat penggolongan / pengklasifikasian terhadap privasi yang dilindungi oleh Undang-undang ini, seperti misalnya privasi atas informasi untuk melindungi data pribadi tentang informasi kredit dan kesehatan, privasi anggota badan untuk perlindungan data pribadi yang berkaitan dengan penggunaan obat bius dan pengambilan data biometrik, privasi atas komunikasi, dan privasi atas teritorial.<sup>32</sup> Mengingat pemanfaatan teknologi yang seiringan dengan pemenuhan hak privasi pun telah diwacanakan di dalam Rencana Pembangunan Jangka Panjang 2005-2025.<sup>33</sup>

## **8. Penerobosan dan Batasan Interferensi Pemerintah Terhadap Data Pribadi Atau Bab Pengecualian Terhadap Perlindungan Data Pribadi**

Perlindungan Data Pribadi melalui ketentuan ini tidaklah dipandang sebagai rezim yang absolut. Karena dalam keadaan tertentu dan alasan yang diperbolehkan oleh hukum, Data Pribadi dapat dibukakan untuk kepentingan sebagai berikut.<sup>34</sup>

- a) keamanan nasional
- b) Kepentingan proses penegakan hukum
- c) Kepentingan pers Sepanjang data pribadi tersebut diperoleh dari informasi yang sudah dipublikasikan
- d) Kepentingan penelitian ilmiah dan statistik
- e) Untuk kepentingan perpajakan
- f) Urusan piutang bank
- g) Untuk kepentingan lembaga peradilan dalam perkara pidana (dengan wewenang pada polisi, jaksa, dan hakim atas izin pimpinan bank Indonesia. Atau dalam perkara antara bank dan nasabahnya.
- h) Dalam rangka pertukaran informasi antar bank
- i) Atas persetujuan permintaan, dan kuasa pemilik data sendiri, ahli waris, atau orang yang dikuasakan

Pada tatanan hukum *anglo-saxon* dikenal juga doktrin *probable cause* sebagai keadaan awal yang menyebabkan pembatasan pemenuhan hak suatu subjek hukum dapat dikecualikan atau dibatasi. Seperti keperluan penyidikan dugaan tindak pidana, pun dalam keadaan yang menimbulkan batasan perlindungan data pribadi seperti di atas, batasan dan penerobosan dapat dibenarkan asalkan untuk memenuhi keperluan-keperluan tertentu seperti yang dicantumkan pada poin-poin di atas.

---

<sup>32</sup> Naskah Akademik RUU PDP hlm. 31.

<sup>33</sup> Rencana Pembangunan Jangka Panjang 2005-2025, hlm. 41.

<sup>34</sup> Beberapa syarat sudah diatur juga di dalam legislasi lain seperti, Undang-undang No. 10/1998 Bab VII tentang Rahasia Bank Pasal 41 – 44.

## 9. Transparansi dan Standarisasi Sistem Dalam Penyelenggaraan *Fintech* Sebagai Kewajiban Tambahan Selain Perlindungan Data Pribadi Sebagai Kewajiban Utama

Sebagai salah satu bentuk kewajiban yang dapat disyaratkan pada pelaku usaha *fintech* yang memiliki dan memanfaatkan *big data* secara bertanggung jawab dapat dimulai dari pemberian kewajiban mekanisme / sistem transparansi pengolahan data yang terkumpul dalam *big data* miliknya untuk dibukakan (dilakukan *disclosure*) kepada komisi khusus demi kepentingan perlindungan konsumen.<sup>35</sup> Karena tanpa adanya transparansi, pengumpulan dan pengolahan data dapat berujung pada *data breach*. Dengan adanya transparansi, diharapkan resiko dapat dimitigasi dan diminimalisir oleh pelaku usaha dengan bantuan dan pengawasan dari komisi.

Resiko pelanggaran akan semakin tinggi apabila data yang ada pada penguasaan penyedia jasa, dikelola oleh sistem yang tidak mumpuni dan transparan (dengan penilaian yang mengacu pada kriteria/standarisasi kelayakan dan transparansi yang disediakan oleh komisi khusus).<sup>36</sup>

Dalam RUU, sebagai bagian dari standarisasi pelayanan jasa, perlu juga diatur substansi mengenai pengaturan teknis yang berkaitan dengan penyelenggaraan, pemrosesan transaksi pembayaran, jasa sistem pembayaran, *Switching*, *Payment Gateway*, *Dompot Elektronik*, *Proprietary Channel*, dan segala jenis sektor usaha yang dapat digolongkan ke dalam sektor *fintech* karena kesemuanya memiliki kekhususan sistem masing-masing yang membutuhkan standar baku yang khusus. RUU PDP juga perlu disertai dan didukung dengan regulasi yang mengatur hal teknis akan mekanisme transparansi ini.

Sebelumnya, sistem dan aturan teknis untuk *fintech* BI juga telah diatur di dalam PBI No. 18/40/PBI/2016 dan untuk P2P Lending diatur dalam POJK No. 77/POJK.01/2016. Undang-Undang Perlindungan Data Pribadi yang nantinya ada harus menjadi payung hukum dan memiliki ‘pasal jembatan’ bagi regulasi yang

---

<sup>35</sup> Seperti yang ada pada *Personal Data Privacy Ordinance of 1995* Hong Kong atau *Data Protection Commission and Administration* serta *Advisory Committees* sebagai lembaga tambahan di Singapura, *Personal Information Protection Act* di Korea Selatan & *Personal Data Protection Commissioner* di Malaysia; Naskah Akademik RUU PDP hlm. 68.

<sup>36</sup> Sinta Dewi, “Konsep Perlindungan Hukum Atas Privasi dan Data Pribadi Dikaitkan Dengan Penggunaan *Cloud Computing* di Indonesia”, *Yustisia*, Vol. 5 No. 1, hlm. 24, 2016.

berada di bawahnya agar dapat selaras dan secara rinci mengatur ketentuan teknis segala materi muatan yang mana secara garis besar, telah diatur pula oleh Undang-Undang Perlindungan Data Pribadi.

#### **10. Pendefinisian *Consumer Harm* dan *Non-discrimination***

Bagi kasus tertentu, pemanfaatan data pribadi dapat merugikan konsumen apabila timbul diskriminasi terhadap konsumen, tanpa keharusan akan adanya *data breach*. Dirugikannya konsumen *fintech* akibat dari pemanfaatan data pribadi tidak saja hanya karena adanya *data breach*, atau kerugian pada konsumen yang timbul karena jatuhnya data pribadi konsumen pada pelaku usaha lain yang dapat memanfaatkan data tersebut secara substansial sehingga konsumen dirugikan. Diperlukan pula perluasan *consumer harm* yang tidak hanya disebabkan oleh adanya *data breach*. Sebagai contoh kasus adalah sebagai berikut, diketahuinya nominal pendapatan bulanan seorang konsumen yang menyerahkan data pribadi berisi nominal gaji untuk kepentingan pelayanan jasa *fintech* berupa *P2P lending* atau *fintech* sektor asuransi, yang mana selanjutnya data pribadi tersebut diperjualbelikan atau dibocorkan pada pelaku usaha lainnya di sektor keuangan. *Consumer harm* timbul apabila terjadi diskriminasi karena nominal gaji seseorang dinilai sebagai faktor utama seorang konsumen untuk mendapatkan *rating* pinjaman atau untuk mendapatkan jasa lainnya pada penyelenggara jasa *fintech* yang berbeda dan bukan terlebih dahulu dinilai melalui *assessment 5C* sebagai kelayakan calon debitur.<sup>37</sup>

Lain lagi dengan kasus dimana terjadi diskriminasi konsumen akibat dari data pribadi yang menjelaskan status *gender*, ras, etnis, dan agama seseorang oleh pelaku usaha dipakai secara melawan hukum atau bocor pada pihak lain dan menimbulkan diskriminasi. Dalam perumpamaan, dapat diibaratkan sebagai berikut, apabila konsumen A memiliki data pribadi tentang ras/etnis pada pelaku usaha X, lantas ia mendapatkan perlakuan diskriminatif oleh pelaku usaha *fintech* Y setelah adanya *data breach*. Keadaan-keadaan seperti diterangkan di atas merupakan *consumer harm* sebagai akibat tidak langsung dari adanya pengumpulan, pengolahan dan pemanfaatan data pribadi yang tidak sesuai dengan hukum yang berlaku.

---

<sup>37</sup> Kim Law Firm, “The Growth of Big Data and Consumer Protection”, 2017, <<https://www.thekimlawfirmllc.com/the-growth-of-big-data-and-consumer-protection/>>, diakses pada tanggal 22 Februari 2018.

Kecenderungan pelanggaran ke arah kasus yang dicontohkan akan semakin tinggi kemungkinan terjadinya apabila RUU PDP tidak mengatur hal tersebut.

## 11. Pembentukan Komisi Pengawas

Pembentukan komisi diperlukan untuk memastikan efektifitas berlakunya undang-undang PDP. Nantinya komisi yang ada bertugas untuk memantau kepatuhan seluruh pihak yang terkait dengan pengumpulan data pribadi. Komisi juga akan berperan dalam mengarahkan para penyelenggara jasa untuk memenuhi standar minimum dalam PDP, menerima pengaduan, memfasilitasi penyelesaian sengketa, dan melakukan pendampingan terhadap pemilik data dalam hal terjadi pelanggaran terhadap undang-undang ini. Apabila disandingkan, maka komisi ini juga dapat mengemban tugas pokok dan tanggung jawab sebuah lembaga perlindungan konsumen, karena akan bertindak sebagai penengah diantara penyelenggara jasa dengan konsumen ataupun antara penyelenggara jasa dengan pemerintah / kementerian. Dibentuknya sebuah panitia khusus atau sebuah komisi yang mengkhususkan diri untuk mengkaji lebih lanjut arah strategi dan kebijakan yang nantinya dapat menjadi acuan pembentukan peraturan perundang-undangan yang memberikan perlindungan bagi konsumen dari pelaku usaha yang memanfaatkan *Big Data*.

Komisi pengawas juga dituntut untuk mampu merumuskan dan melaksanakan rencana dan kebijakan memperkuat perlindungan data pribadi, mempublikasikan secara teratur panduan langkah-langkah perlindungan data pribadi memberi rekomendasi pada aparat penegak hukum dalam hal adanya penuntutan yang berkaitan dengan PDP, melakukan penelitian,<sup>38</sup> memberikan surat teguran pada pengeola data pribadi, melakukan penelitian, memberikan saran dan pendapat bagi penerapan peraturan yang berkaitan dengan PDP, melakukan kerja sama dengan otoritas negara lain, membentuk sekretariat untuk mempermudah pelaksanaan UU PDP, dan lain-lainnya. Komisi yang nantinya dibentuk dapat berupa komisi baru atau dilekatkan pada tugas pokok dan fungsi Komisi Informasi<sup>39</sup> yang memiliki fungsi melindungi privasi dan data pribadi (demi penghematan keuangan negara).

---

<sup>38</sup> Hasil dari kajian panitia khusus atau komisi tersebut dapat menjadi acuan bagi legislator dan regulator dalam merancang peraturan perundang-undangan yang memberikan perlindungan konsumen dalam memanfaatkan *big data*.

<sup>39</sup> Sebagaimana diatur dalam Pasal 17 huruf g, huruf h, dan huruf j Undang-Undang Nomor 14 Tahun 2008 Tentang Keterbukaan Informasi Publik.

## **12. Pemberian Sanksi Bagi Pelanggar**

Pelanggaran yang berkaitan dengan hak atas data pribadi harus diberikan untuk memberikan kepatuhan, edukasi, dan efek jera. Dalam kajian komparatif penulis, hukuman penjara dan denda untuk kasus pencurian data telah diterapkan oleh Negara seperti Korea Selatan, Hongkong, Singapura, dan Malaysia.<sup>40</sup> Hukuman haruslah proporsional dengan pelanggaran yang dilakukan. Sanksi dapat berupa pidana dan sanksi perdata berupa ganti rugi. Penetapan sanksi perlu dilengkapi dengan mekanisme penegakan hukumnya yang disesuaikan dengan ketentuan peraturan perundang-undangan yang berlaku.<sup>41</sup>

## **13. Pengaturan *Transfer Data***

Perpindahan data pribadi antar negara harus diatur di dalam RUU PDP demi diperhatikannya kepentingan nasional dan juga (secara bersamaan) kepentingan bersama dengan negara lain. Pengaturan tentang pemindahan data pribadi antar yurisdiksi juga harus memenuhi standar yang berlaku baku secara internasional. Pengadopsian instrumen hukum dari negara lain untuk *transfer data* dengan negara yang telah mengatur pengaturan perpindahan data maka dapat dimungkinkan pengadopsian aturan-aturan dari *OECD Guidelines*, *EC Directives*, maupun *AFTA Privacy Framework* untuk mempermudah formulasi Undang-undang.

## **14. Penyelesaian Sengketa**

Alternatif penyelesaian sengketa lebih diutamakan. Negosiasi, mediasi, atau konsiliasi secara sukarela dapat dipimpin oleh anggota komisi khusus. Litigasi menurut penulis, dapat ditempuh setelah negosiasi dan mediasi dapat diselesaikan terlebih dahulu. Litigasi dapat diganti juga dengan arbitrase apabila para pihak menghendaki untuk memberikan kewenangan adjudikasi pada lembaga arbitrase dan bukan lembaga peradilan demi untuk menghindari pertentangan kompetensi antar lembaga.

## **15. Penghentian Pemasaran Langsung (*Direct Marketing*)**

Kegiatan pemasaran langsung dari pihak-pihak yang mengelola data pribadi sesuai kesepakatan haruslah dapat dihentikan oleh pemilik data pribadi yang merasa

---

<sup>40</sup> Naskah Akademik RUU PRP hlm. 73 – 74.

<sup>41</sup> Naskah Akademik RUU PDP hlm. 150.

dirugikan atas hal ini. Apabila pemasaran langsung tersebut datang dari pihak ketiga, patut diduga bahwa telah terjadi pelanggaran PDP dan konsumen selaku pemilik data dapat memintakan penghentian dan penindakan dugaan pelanggaran tersebut.

#### **16. Pembentukan Pedoman Perilaku Pengelola Data Pribadi,**

Kode Etik bagi para pelaku usaha dapat diupayakan melalui asosiasi pelaku usaha. Apabila asosiasi tersebut telah terbentuk, maka komisi dapat memberikan saran mengenai pembentukan kode etik yang nantinya akan memberikan batasan etis bagi para pelaku usaha melalui sanksi administratif yang ada dalam kode etik tersebut.

#### **17. Kerja Sama Internasional**

Perumusan dan penetapan undang-undang PDP dan regulasi yang berkaitan juga perlu diiringi dengan kerja sama internasional demi meningkatnya standar perlindungan data pribadi.

#### **18. Partisipasi Masyarakat Sebagai Unsur Pendukung Pelaksanaan Perlindungan Data Pribadi**

Untuk memudahkan penyelenggaraan PDP juga, pendidikan dan/atau pelatihan, advokasi, bimbingan teknis, dan sosialisasi dengan menggunakan berbagai media.

### **B. Penutup**

#### **A. Kesimpulan**

1. Di era *Digital Economy* saat ini, kebutuhan undang-undang perlindungan data pribadi tidak dapat dielakan lagi. Perlindungan data pribadi bagi konsumen sangat dibutuhkan untuk mencegah dan menanggulangi resiko kebocoran data (*data breach*) dan pelanggaran lainnya terkait perlindungan data pribadi. Rancangan Undang-Undang Perlindungan Data Pribadi dikarenakan adanya kebutuhan untuk memberikan perlindungan terhadap individu sehubungan dengan pengumpulan, pemrosesan, dan pengelolaan data pribadi. Oleh karena itu, dibutuhkan peraturan perundang-undangan yang akan mengantisipasi agar hal tersebut tidak lagi menjadi resiko yang akan menghambat perkembangan sektor usaha ini. Melalui regulasi yang tepat, resiko dapat dimitigasi. Dengan adanya undang-undang

mengenai perlindungan data pribadi, diharapkan adanya transformasi dan harmonisasi antar peraturan (yang sebelumnya telah mengatur privasi dan perlindungan data secara terpisah) apabila nanti RUU PDP ini sah diundangkan.

2. Secara umum Materi mutan yang diatur dalam RUU PDP harus berasal dari studi komparasi peraturan terkait perlindungan data pribadi di beberapa negara yang telah mengatur perlindungan data pribadi lebih dalam. Saat ini ketentuan tentang perlindungan data pribadi telah diatur di dalam peraturan perundang-undangan. Maka dengan adanya Undang-undang baru mengenai perlindungan data pribadi, diharapkan juga ke depannya terjadi transformasi dan harmonisasi antar peraturan (yang sebelumnya telah mengatur privasi dan perlindungan data secara terpisah) apabila nanti RUU PDP ini akan sah diundangkan. Upaya perancangan peraturan perundang-undangan yang baik tentang PDP apabila berhasil diundangkan maka secara langsung juga telah memberikan keberhasilan bagi para ahli hukum untuk mewujudkan perlindungan data pribadi dalam era bisnis *fintech* selaku cita hukum (*rechtsidee*), sehingga nantinya tidak terdapat kekosongan hukum dan meningkatkan kepastian hukum dalam tatanan hukum nasional.

## **B. Saran**

1. Resiko yang berhubungan dengan penggunaan *fintech* harus dapat diminimalisir dengan metode perancangan peraturan perundang-undangan yang sebaik mungkin oleh para pihak yang terkait. Perancangan UU PDP harus matang agar selalu aktual dan tidak memiliki celah yang dapat menimbulkan kekosongan hukum antara perkembangan teknologi dan keterlambatan dari regulasi yang mengaturnya. Selain melalui upaya internal seperti mitigasi resiko oleh pelaku usaha, pendekatan perbandingan hukum dapat juga dipakai untuk menentukan kaidah-kaidah hukum apa sajakah yang menjadi unsur-unsur umum dalam pengaturan PDP di berbagai Negara. Nantinya, hasil kajian komparatif tersebut dapat dipakai guna melengkapi ataupun mengubah kaidah-kaidah yang sebelumnya telah ada dan berlaku juga pada beberapa peraturan perundang-undangan yang mengatur konsumen secara umum, maupun perlindungan konsumen yang secara khusus berbicara tentang perlindungan data pribadi.
2. Banyak instrumen hukum yang dapat dicontoh untuk membandingkan rezim perlindungan PDP di era bisnis *fintech*. Salah satunya adalah pencapaian Uni

Eropa yang telah mengeluarkan regulasi *The General Data Protection (GDPR)* yang akan berlaku efektif pada bulan Mei 2018 yang muatannya mewajibkan pengelola dan pengendali data untuk mengimplementasikan tindakan teknis dan keorganisasian yang dinilai layak untuk memastikan adanya kesebandingan antara keamanan dan resiko yang dihadapi pelaku usaha dan konsumen.

Apabila *model* Eropa kembali dikaji dan ditiru, maka perlu pula dilihat dan dibahas bahwa selain melalui *GDPR*, lembaga lain juga memiliki wewenang untuk meningkatkan *cybersecurity* yang secara tidak langsung akan turut serta melindungi keamanan data pribadi. Lembaga tersebut adalah *European Union's Network and Information Security (NIS)* yang berwenang memberikan persyaratan keamanan terhadap pelaku usaha yang diantaranya adalah jasa perbankan dan finansial lainnya. Lembaga-lembaga lainnya yang berada di Eropa dengan peran serupa adalah *the Payment Services Directive 2 (PSD2)* dan *the Bank of England's CBEST Program*. Inti dari peran semua lembaga tersebut adalah memastikan keamanan pada transaksi dan sistem finansial yang jangkauannya semakin meluas dan tatanan pengawasan serta pengaturannya sekalipun memiliki resiko *overlapping* tetapi perlindungan data pribadi akan diatur oleh rezim perlindungan yang rangkap, sehingga celah dan resiko *data breach* maupun pelanggaran lainnya dari sebuah *legal loophole* dapat diminimalisir.

Bagi Indonesia, langkah tersebut dapat pula ditiru dan diterapkan pada tingkat regional dengan secara bersama-sama dengan negara-negara ASEAN lainnya, menerapkan hukum serupa pada tingkat regional seperti Uni Eropa. Dengan cara tersebut, Indonesia merancang sebuah standar keamanan perlindungan data yang akan berlaku secara serempak melalui pengadopsian standar tersebut menjadi sebuah peraturan-perundang-undangan yang akan berlaku secara seragam di setiap yurisdiksi negara anggota ASEAN (melalui proses ratifikasi), tidak hanya pada tingkat nasional saja. Sehingga, *market* dari pelaku usaha *fintech* di Indonesia dapat lebih diperbanyak, diperluas, dan menjangkau pangsa pasar masyarakat ASEAN. Apabila *fintech company* yang didirikan di Indonesia telah dapat menjangkau konsumen asing di luar ASEAN, maka bukan tidak mungkin para pengguna jasa yang berasal dari berbagai negara tersebut akan menginginkan pelaku bisnis dari Indonesia untuk bisa mengikuti



perkembangan standarisasi perlindungan data pribadi yang ditetapkan oleh negara-negara yang kini telah mengaturnya dengan lebih baik. Maka dari itu, urgensi untuk segera mengatur perlindungan data pribadi bagi konsumen dengan peraturan perundang-undangan yang *up-to-date* dan didapat dari hasil kajian komparatif dirasa semakin diperlukan urgensinya dan harus sesegera mungkin dilaksanakan.

## DAFTAR PUSTAKA

### **Peraturan Perundang-undangan**

Undang-Undang Nomor 14 Tahun 2008 Tentang Keterbukaan Informasi Publik

Peraturan Menteri Komunikasi dan Informatika No. 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik

Peraturan Bank Indonesia No. 19/12/PBI/2017 Tentang Penyelenggaraan Teknologi Finansial

Peraturan Bank Indonesia No. 18/40/PBI/2016 Tentang Penyelenggaraan Pemrosesan Transaksi Pembayaran

Peraturan Bank Indonesia No. 11/12/PBI/2009 Tentang Uang Elektronik yang telah diubah dalam PBI No. 16/8/PBI/2014.

Peraturan Anggota Dewan Gubernur Bank Indonesia No. 19/14/PADG/2017 tentang Ruang Uji Coba Terbatas (*Regulatory Sandbox*) Teknologi Finansial

Rancangan Undang-Undang Perlindungan Data Pribadi

Naskah Akademik RUU Perlindungan Data Pribadi

## **Jurnal & Makalah**

Departemen Kebijakan dan Pengawasan Sistem Pembayaran Bank Indonesia, “Analisa Peluang Indonesia Dalam” *Temu Ilmiah Nasional Peneliti*, Bogor, 2016.

Sinta Dewi, “Konsep Perlindungan Hukum Atas Privasi dan Data Pribadi Dikaitkan Dengan Penggunaan *Cloud Computing* di Indonesia”, *Yustisia*, Vol. 5 No. 1, 2016.

## **Internet**

Adhi, “Apa itu Finansial Technology (Fintech)”, 2017, <<https://www.money.id/digital/apa-itu-finansial-technology-fintech-160219n.html>>, 14 Februari 2018.

Marsya Nabila, “Berikut ini Klasifikasi Fintech yang Akan Diatur OJK”, <<https://dailysocial.id/post/berikut-ini-klasifikasi-fintech-yang-akan-diatur-ojk>>, diakses pada tanggal 4 Februari 2018.

KlikLegal.com, “Ini Berbagai Peraturan Perlindungan Data Pribadi di Indonesia”, <<https://kliklegal.com/ini-berbagai-peraturan-perlindungan-data-pribadi-di-indonesia/>>, diakses pada tanggal 11 Januari 2018.

Steven R. Chabinsky, “Fintech: Cybersecurity Risk Management for Financial Institutions and Technology Vendors”, 2017, <<https://www.lexology.com/library/detail.aspx?g=3acc8886-d0bb-4e86-8521-1b4445e79ad9>>.

BIPAR, “Digitalisation and Fintech”, 2018, <<http://www.bipar.eu/en/page/digitalisation-and-fintech>>, 21 Februari 2018.

EDPS, “Privacy and Competitiveness in the Age of Big Data”, 2018, <[https://edps.europa.eu/press-publications/press-news/press-releases/2014/privacy-and-competitiveness-age-big-data\\_en](https://edps.europa.eu/press-publications/press-news/press-releases/2014/privacy-and-competitiveness-age-big-data_en)>, diakses pada tanggal 22 Februari 2018

John S. Pruitt *et al*, “Big Data and Cybersecurity: The Federal Insurance Office Explores New Frontiers for Consumer Protection”, 2017, <<https://www.lexology.com/library/detail.aspx?g=b2663a0a-6603-4ca4-831e-5c94ca42a296>>, diakses pada tanggal 22 Februari 2018.

Kim Law Firm, “The Growth of Big Data and Consumer Protection”, 2017, <<https://www.thekimlawfirmllc.com/the-growth-of-big-data-and-consumer-protection/>>, diakses pada tanggal 22 Februari 2018.

John Villasenor, “Ensuring Cybersecurity In Fintech: Key Tren and Solution”, 2016, <<https://www.forbes.com/sites/johnvillasenor/2016/08/25/ensuring-cybersecurity-in-fintech-key-trends-and-solutions/#11930e435fd9>>, diakses pada tanggal 21 Februari 2018.

EDPS, “Big Data & Digital Clearinghouse”, 2018, <[https://edps.europa.eu/data-protection/our-work/subjects/big-data-digital-clearinghouse\\_en](https://edps.europa.eu/data-protection/our-work/subjects/big-data-digital-clearinghouse_en)>, diakses pada tanggal 22 Februari 2018.

Loreta Andziulyte, “Data Protection in FinTech Companies – Time to Prepair For the New Generation”, 2018, <<http://ecovis.lt/2017/04/20/data-protection-in-fintech-companies-time-to-prepair-for-the-new-regulation/>>, diakses pada tanggal 21 Februari 2018.