



## ***Consumer Protection System (CPS): Sistem Perlindungan Data Pribadi Konsumen Melalui Collaboration Concept***

**Dararida Fandra Mahira<sup>1</sup>, Emilda Yofita<sup>2</sup>, Lisa Nur Azizah<sup>3</sup>**

<sup>1</sup> *Fakultas Hukum Universitas Brawijaya. E-mail: adararida@gmail.com*

<sup>2</sup> *Fakultas Hukum Universitas Brawijaya. E-mail: emildayofita2@gmail.com*

<sup>3</sup> *Fakultas Hukum Universitas Brawijaya. E-mail: lisanurazizah2406@gmail.com*

### ***Abstract***

*Increasingly massive Internet technology has become the basis for trading transactions and money-lending transactions online. Its existence is characterized by more trading electronics commerce (e-commerce) and the presence of fintech. On the other hand, the use of e-commerce and fintech also has a variety of problems that one of them related to user personal data. Often when a person commits a transaction or registration, he/she must submit certain personal data that is often misused. Therefore, the protection of consumer personal data becomes very important. On the other hand, Indonesia has a wide range of consumer protection institutions but it is not maximally caused by many people who feel confused with various functions of these institutions that are felt to have the same function, from that end many people do not report the Problematics encountered. Problems related to regulation also become the cause of the protection of consumers in Indonesia is not maximized. This is because the legislation regarding the protection of personal data of existing consumers is still not able to cope with the problems that exist. Therefore, the authors provide effective solutions with the concept of Consumer Protection System (CPS): online consumer personal Data protection system through the Collaboration Concept. The research method used is a type of normative juridical study, with the approach and Conceptual approach. The authors are based on online consumer protection problems in Indonesia and then visualized in the framework of thinking. This concept is expected to optimize consumer protection in Indonesia.*

**Keywords:** *e-commerce; Fintech; Personal Data; Online consumer protection;*

### ***Abstrak***

Teknologi internet yang semakin masif telah menjadi basis bagi transaksi perdagangan dan transaksi pinjaman uang secara online. Keberadaannya ditandai dengan semakin banyak perdagangan elektronik/*electronic commerce (e-commerce)* dan hadirnya *fintech*. Selain menyuguhkan kemudahan, disisi lain, penggunaan *e-commerce* dan *fintech* juga memiliki berbagai permasalahan yang salah satunya terkait data pribadi pengguna. Seringkali apabila seseorang melakukan transaksi atau pendaftaran, maka ia harus mengirimkan data-data pribadi tertentu yang seringkali disalahgunakan. Oleh karena itu, perlindungan terhadap data pribadi konsumen menjadi sangat penting. Disisi lain Indonesia



memiliki berbagai macam lembaga perlindungan konsumen namun dirasa belum maksimal yang disebabkan banyak masyarakat yang merasa bingung dengan berbagai macam fungsi lembaga tersebut yang dirasa memiliki fungsi yang sama, dari hal tersebut yang akhirnya banyak masyarakat tidak melaporkan problematika yang dihadapi. Permasalahan terkait regulasi pun turut menjadi penyebab perlindungan terhadap konsumen di Indonesia belum maksimal. Hal ini disebabkan undang-undang mengenai perlindungan data pribadi konsumen yang sudah ada masih dirasa belum mampu mengatasi problematika yang ada. Oleh karena itu, para penulis memberikan solusi efektif dengan konsep *Consumer Protection System* (CPS): Optimalisasi Sistem Perlindungan Data Pribadi Konsumen Daring melalui *Collaboration Concept* dalam Menghadapi Revolusi Industri 4.0. Adapun metode penelitian yang digunakan adalah jenis penelitian Yuridis Normatif, dengan pendekatan Perundang-Undangan (*Statute Approach*) dan pendekatan konsep (*Conceptual Approach*). Penulis kaji berdasarkan pada problematika perlindungan konsumen daring di Indonesia dan kemudian divisualisasikan dalam kerangka berpikir. Dengan konsep tersebut diharapkan dapat mengoptimalkan perlindungan konsumen di Indonesia.

**Kata Kunci:** *Data Pribadi; E-commerce; Fintech; Perlindungan Konsumen Daring;*

## 1. Pendahuluan

Di Era revolusi industri 4.0 kegiatan perdagangan dan peminjaman uang yang bersifat konvensional tidak pernah diprediksi bahwa model perdagangan dan peminjaman uang konvensional ini yang dahulu ketika masyarakat ingin berbelanja maupun ingin meminjam uang harus menuju ke tempat tersebut, namun pada era revolusi industri 4.0 model perdagangan dan peminjaman uang konvensional ini sudah sedikit digunakan oleh masyarakat, dimana sekarang menjamurnya berbagai macam *e-commerce* dan *fintech*. Dampak dari perkembangan teknologi yang semakin berkembang secara pesat ialah masyarakat menjadi lebih mudah mendapatkan barang yang diinginkan maupun mendapatkan uang secara mudah.

Tidak hanya menyuguhkan kemanfaatan, era revolusi industri 4.0 juga menyuguhkan berbagai permasalahan yang menjadi tantangan bagi negara untuk menyelesaikannya. Keterbukaan perdagangan dan perkembangan era digital dan teknologi dapat mempengaruhi kebijakan perekonomian suatu negara. Hal ini merupakan tugas dari Negara sebagai penyelenggara pemerintahan untuk menciptakan kebijakan yang melindungi pelaku kegiatan ekonomi. Dalam kegiatan ekonomi, konsumen merupakan pihak yang paling beresiko terhadap

kerugian dan harus dijamin hak-haknya, dalam hal ini adalah perwujudan kepastian hukum yang dijamin oleh Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 pasal 28G ayat (1) yang menyatakan “Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi”.<sup>1</sup> Mahkamah Konstitusi Republik Indonesia memberikan tafsir terhadap pasal 28G ayat (1) perihal hak privasi yang dapat dikaitkan dengan hak atas perlindungan data pribadi dalam Putusan 20/PUU-XIV/2016. Walaupun dalam konsep *privacy and data protection*, dua hak tersebut memiliki perbedaan. Dalam Putusan No.5/PUU-VIII/2011, MK menyatakan bahwa *right to privacy* merupakan bagian dari hak asasi manusia (*derogable rights*) dan cakupan dari *right to privacy* meliputi *right to information privacy*, disebut juga *data privacy (data protection)*.<sup>2</sup>

Berdasarkan hasil studi Polling Indonesia yang bekerja sama dengan Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), jumlah pengguna internet dari total populasi sebanyak 264 juta jiwa penduduk Indonesia, ada sebanyak 171,17 juta jiwa atau sekitar 64,8% yang sudah terhubung ke internet pada tahun 2020.<sup>3</sup> Banyaknya angka pengguna internet di Indonesia menunjukkan potensi pasar yang besar yang akan mempengaruhi munculnya berbagai peluang bisnis baru melalui daring.<sup>4</sup> Disisi lain, ada beberapa hal yang perlu diperhatikan dalam kegiatan belanja daring adalah isu tentang perlindungan data pribadi dan para konsumen daring. Bahwa dalam aktifitas daring, data pribadi merupakan salah satu hal esensial dan menjadi semakin penting dalam segala aspek kehidupan manusia.

<sup>1</sup>Pasal 28G ayat (1) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.

<sup>2</sup>Daniar Supriyadi. 2017. *Data Pribadi dan Dua Dasar Legalitas Pemanfaatannya*. Diakses 29 April 2020. <https://m.hukumonline.com/berita/baca/lt59cb4b3feba88/data-pribadi-dan-dua-dasar-legalitas-pemanfaatannya-oleh-daniar-supriyadi/>.

<sup>3</sup>Yudha Pratomo. 2019. *APJII: Jumlah Pengguna Internet di Indonesia Tembus 171 Juta Jiwa*. Diakses 29 April 2020. <https://Tekno.Kompas.Com/Read/2020/05/16/03260037/Apjii-Jumlah-Pengguna-Internet-Di-Indonesia-Tembus-171-Juta-Jiwa>.

<sup>4</sup>Hari Widowati. 2019. *Indonesia Jadi Negara Dengan Pertumbuhan E-Commerce Tercepat di Dunia*. Diakses 29 April 2020. <https://Databoks.Katadata.Co.Id/Datapublish/2020/04/25/Indonesia-Jadi-Negara-Dengan-Pertumbuhan-E-Commerce-Tercepat-Di-Dunia>.

Data pribadi adalah data yang berkenaan dengan ciri seseorang, nama, umur, jenis kelamin, pendidikan, pekerjaan, alamat, dan kedudukan dalam keluarga.<sup>5</sup> Secara yuridis data pribadi menurut Peraturan Pemerintah Republik Indonesia Nomor 82 Tahun 2012 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik adalah data perseorangan tertentu yang disimpan, dirawat, dan dijaga kebenaran serta dilindungi kerahasiaannya. Data Pribadi Penduduk yang harus dilindungi memuat: nomor KK, NIK, tanggal/bulan/tahun lahir, keterangan tentang kecacatan fisik dan/atau mental, NIK ibu kandung, NIK ayah, dan beberapa isi catatan peristiwa penting.<sup>6</sup> Data pribadi berkenaan dengan kependudukan seperti NIK, *e-KTP* dan KK sangat penting dilindungi agar tidak mudah dieksploitasi.

Ada beberapa bentuk penyalahgunaan data seperti penjualan data, data profiling, tujuan pemasaran, penelitian, pemantauan/spionase, termasuk penyalahgunaan data pribadi untuk tindak kriminal seperti pembuatan akun palsu, penipuan dalam jaringan, pencucian uang, pasar palsu dan juga transaksi ilegal.<sup>7</sup> Banyaknya penipuan menggunakan situs *e-commerce* merupakan hal yang sering dijumpai. Seiring banyaknya situs *e-commerce* di Indonesia memerlukan jaminan perlindungan privasi dan data pribadinya yang komprehensif.

Selain itu, teknologi finansial (tekfin) atau *financial technology (fintech)* berkembang pesat seiring kemajuan teknologi internet dan *gadget* seperti *handphone*, *smartphone*, PC, tablet PC, *netbook* dan *notebook*. Berbekal *gadget* dan internet, setiap orang bisa mengakses berbagai macam aplikasi yang dapat digunakan untuk mempermudah kehidupan manusia. Sistem pembayaran kini bisa dilakukan melalui internet menggunakan aplikasi dompet elektronik (*e-wallet*). Masyarakat juga bisa mengakses utang/pinjaman secara *online* melalui laman perusahaan jasa “Pinjam Meminjam berbasis Teknologi Finansial” (PM-Tekfin) tanpa melalui perbankan atau lembaga pembiayaan.

Resiko datang ketika konsumen tidak harus mengeluarkan biaya untuk menggunakan jasa sebuah *fintech* melalui aplikasi, namun, dibalik skema yang

<sup>5</sup>Anonim, *Kamus Bahasa Indonesia Data Pribadi*. Diakses 29 April 2020. <http://Kamusbahasaindonesia.Org/Data%20pribadi/Miripkamusbahasaindonesia.Org>.

<sup>6</sup>Pasal 84 Undang-Undang Nomor 23 Tahun 2006 Tentang Administrasi Kependudukan.

<sup>7</sup>Lia Sautunnida. 2018. Urgensi Undang-Undang Perlindungan Data Pribadi Di Indonesia. *Kanun Jurnal Ilmu Hukum, Volume 20, Nomor 2*. hlm. 370.

ada, terdapat penjualan data pribadi oleh penyelenggara jasa kepada pihak ketiga tanpa menghargai privasi seseorang.<sup>8</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*.<sup>9</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>10</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.<sup>11</sup> Hal tersebut akan mencederai hak seorang konsumen apabila data tersebut jatuh ke pihak lain dan dimanfaatkan secara melawan hukum.

Ketidaktertiban yang terjadi dalam perlindungan masyarakat di tengah era ekonomi digital memerlukan hukum sebagai penjaga agar perkembangan ke arah ekonomi digital berjalan dengan tertib. Namun, perlindungan privasi dan data pribadi di Indonesia dalam instrumen hukum yang khusus belum ada dan masih bersifat sektoral sehingga belum cukup untuk mendorong pembangunan ekonomi digital di Indonesia. Oleh karena itu, perlu ditelaah peraturan-peraturan yang ada di Indonesia mengenai privasi dan data pribadi yang dapat mendorong perkembangan ekonomi digital. Selain itu perlu diketahui bagaimana seharusnya perlindungan privasi dan data pribadi di Indonesia dapat responsif terhadap era digital.

<sup>8</sup>EDPS. 2018. *Privacy and Competitiveness in the Age of Big Data*. Diakses 29 April 2020. [https://edps.europa.eu/presspublications/press-news/press-releases/2014/privacy-and-competitiveness-age-big-data\\_en](https://edps.europa.eu/presspublications/press-news/press-releases/2014/privacy-and-competitiveness-age-big-data_en).

<sup>9</sup>Louis de Koker, *Op Cit.*, note 5, hlm. 6.

<sup>10</sup>Terjadi skema *location-based messaging* untuk mempromosikan produk dari lokasi tertentu bagi konsumen yang sedang berada pada lokasi; Naskah Akademik RUU PDP hlm. 6.

<sup>11</sup>John S. Pruitt *et al.* 2017. *Big Data and Cybersecurity: The Federal Insurance Office Explores New Frontiers for Consumer Protection*. Diakses 29 April 2020. <https://www.lexology.com/library/detail.aspx?g=b2663a0a-6603-4ca4-831e-5c94ca42a296>.

Regulasi dan kebijakan mengenai perlindungan data pribadi harus dapat menjamin ketertiban perubahan masyarakat dari era ekonomi tradisional ke era ekonomi digital. Ketentuan-ketentuan yang ada harus dapat menjadi pelindung masyarakat di tengah era ekonomi digital. Karya tulis ini akan memberikan solusi alternatif atas permasalahan mengenai perlindungan data pribadi konsumen daring di Indonesia agar lebih responsif dalam menghadapi era Revolusi Industri 4.0 melalui *Consumer Protection System (CPS)* dengan *collaboration concept* yang melibatkan peran Otoritas Jasa Keuangan (OJK), Badan Penyelesaian Sengketa Konsumen (BPSK), Badan Regulasi Telekomunikasi Indonesia (BRTI), dan Kementerian Komunikasi dan Informatika (Kominfo).

## 2. Analisis

### 2.1 Problematika Perlindungan Data Pribadi Konsumen Daring di Indonesia di Era Revolusi Industri 4.0

Pemanfaatan internet dalam berbagai bidang kehidupan tidak saja membuat segala sesuatunya menjadi lebih mudah, namun juga melahirkan sejumlah permasalahan termasuk masalah hukum. Salah satu masalah hukum yang muncul adalah masalah yang berkaitan dengan perlindungan data pribadi (*the protection of privacy rights*).

Terjadi beberapa kasus pembobolan data pribadi yang beritanya sampai ke masyarakat. Salah satunya adalah kasus pembobolan Sony Corp, dimana pada bulan April 2011, sekelompok hacker membobol jaringan *playstation sony* dan mencuri data lebih dari 77 juta *account*. Serangan ini dipercaya sebagai yang terbesar dalam sejarah Internet yang menyebabkan Sony menutup *Playstation Network*. Akibat pembobolan itu, perusahaan memperkirakan akan kehilangan keuntungan hingga Rp 1,45 triliun. Sebagai kompensasi Sony telah menawarkan insentif bagi pengguna *PlayStation Network* untuk kembali ke sistem mereka setelah terjadinya serangan hacker

tersebut.<sup>12</sup> Pada tahun 2011 yang lalu juga terjadi kasus pembobolan data pribadi 25 juta pelanggan Telkomsel.

Mayoritas serangan tersebut hadir dalam bentuk *malware* ataupun *phishing* dan lebih menasar pada institusi perbankan dan pemerintahan. *Phishing* adalah usaha untuk mendapatkan suatu informasi penting dan rahasia secara tidak sah, seperti User ID, Password, PIN, informasi rekening bank, informasi kartu kredit, atau informasi rahasia lainnya. Istilah *phishing* sendiri berasal dari bahasa Inggris yaitu *fishing* (memancing), yang dalam hal ini berarti memancing informasi rahasia dari orang lain. *Phishing* merupakan salah satu kejahatan di dunia maya (*cyber crime*) yang sering terjadi.

Ancaman penyalahgunaan data pribadi di Indonesia menjadi kian mengemuka terutama sejak pemerintah menggulirkan program KTP elektronik (*e-KTP*) yang merupakan program perekaman data pribadi oleh pemerintah. Program *e-KTP* pertama kali diluncurkan pada awal tahun 2011, yang merupakan implementasi dari program Nomor Induk Kependudukan (NIK). Program ini menghendaki identitas tunggal setiap penduduk, yang berlaku seumur hidup, satu kartu untuk setiap penduduk, yang di dalamnya terdapat NIK. Selanjutnya perekaman data penduduk dilakukan pemerintah dalam rangka pelaksanaan program ini. Seluruh informasi pribadi warga negara direkam, termasuk identitas dan ciri-ciri fisiknya. Khusus perekaman ciri-ciri fisik, dilakukan dengan pemindaian terhadap sidik jari dan retina mata, yang akan digunakan untuk validasi biometrik pemegang KTP. Menurut informasi Kemendagri, hasil dari perekaman data tersebut kemudian akan ditanam di dalam KTP, dengan terlebih dahulu dienkripsi menggunakan algoritma kriptografi tertentu. Data pribadi yang terekam dalam *e-KTP* rawan disalahgunakan oleh pihak-pihak yang tidak bertanggungjawab, terutama apabila pengamanannya kurang.

Selain itu problematika juga terdapat pada industri *fintech* yang pada dasarnya memanfaatkan teknologi informasi dalam sistem keuangan yang

<sup>12</sup>Tempo.co. 2011. *Jaringan Sony Dibobol Lagi Jutaan Data Dicuri*. Diakses 29 April 2020. <http://www.tempo.co/read/news/2011/06/03/072338366/>.

menghasilkan produk, layanan, teknologi, dan/atau model bisnis baru. 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>13</sup>

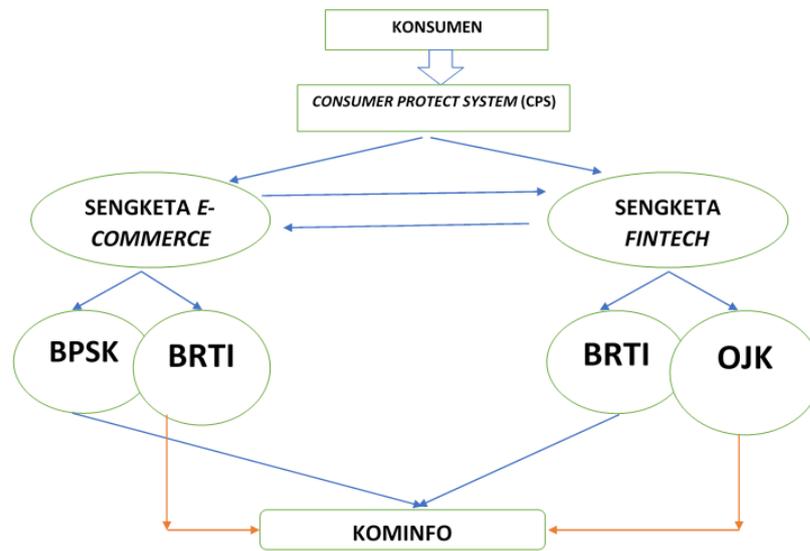
Selain itu juga banyaknya masyarakat yang bingung terhadap banyaknya lembaga perlindungan konsumen yang menyebabkan kebanyakan masyarakat tidak melaporkan problematika yang dihadapinya. Hal inilah yang menjadi salah satu penyebab perlindungan terhadap konsumen di Indonesia belum maksimal.

Permasalahan terkait regulasi pun turut menjadi penyebab perlindungan terhadap konsumen di Indonesia belum maksimal. Hal ini disebabkan undang-undang mengenai perlindungan data pribadi konsumen yang sudah ada masih dirasa belum mampu mengatasi problematika yang ada. Salah satu usaha pemerintah ialah merancang Undang-Undang Perlindungan Data Pribadi yang kini masih belum di sahkan.

Dari berbagai permasalahan di atas, diperlukan suatu sistem keamanan dan pengaturan hukum lebih lanjut mengenai perlindungan data pribadi konsumen dalam pemanfaatan teknologi agar penggunaannya dapat berkembang secara optimal.

## **2.2. *Consumer Protection System (CPS): Optimalisasi Sistem Perlindungan Data Pribadi Konsumen Daring melalui Collaboration Concept dalam Menghadapi Revolusi Industri 4.0***

<sup>13</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.



**Bagan 1. Konsep Consumer Protection System (CPS)**

*Sumber: Ide Penulis*

**Keterangan:**

Berdasarkan bagan diatas menjelaskan optimalisasi peran *Consumer Protection System (CPS)* dalam melakukan perlindungan data konsumen daring melalui *collaboration concept* dengan *stakeholder* terkait. Adapun tujuan dibentuknya CPS ini ialah untuk mengoptimalkan *stakeholder* terkait dalam upaya perlindungan konsumen yang dimana masing masing *stakeholder* ini sebetulnya memiliki kemiripan tugas namun dalam praktiknya belum sepenuhnya berjalan. Hal ini bisa dilihat masyarakat merasa bingung apabila memiliki sengketa yang kompleks akan dibawa kemana, terlalu banyaknya lembaga yang memiliki kemiripan tugas dan sebagainya. Sehingga, dengan adanya CPS diharapkan dapat mengatasi problematika yang dihadapi masyarakat serta dapat mengoptimalkan perlindungan konsumen daring dalam menghadapi revolusi industri 4.0 ini.

**1. Konsumen Mengajukan Keluhan Kepada *Consumer Protection System (CPS)***

Dalam menghadapi problematika yang dialami oleh konsumen yang

dimana problematika tersebut menyangkut sengketa dalam *e-commerce*, *fintech* maupun keduanya, konsumen dapat mengajukan keluhannya kepada CPS, nantinya dari CPS akan meneliti apakah sengketa tersebut masuk dalam ranah *e-commerce*, *fintech*, maupun keduanya. CPS ini terdiri atas tim peneliti dari *stakeholder* terkait yang akan menangani berbagai macam sengketa.

## 2. Standarisasi Penilaian Penelitian yang Dilakukan CPS dalam problematika Perlindungan Data Pribadi

Kriteria dan standar yang ditetapkan oleh CPS ialah 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 tentang di mana data tersebut disimpan, siapa sajakah yang dapat mengakses data tersebut, penggunaan *encryption* bagi mekanisme pengaksesan data, dan lain-lain.<sup>14</sup>

## 3. Consumer Protection System (CPS) Menyerahkan Hasil Penelitian E-commerce

Setelah melakukan penelitian, CPS akan melaporkan sengketa *e-commerce* kepada BPSK dan BRTI. Dalam konteks penyelesaian sengketa *e-commerce*, peran BPSK sangat penting untuk segera memberikan perlindungan bagi para konsumen. Hal ini tentunya dilakukan sesuai dengan tugas BPSK yaitu melalui penanganan dan penyelesaian sengketa konsumen dengan cara konsiliasi, mediasi, atau arbitrase. Oleh karena itu, agar dapat melakukan tugas tersebut secara efektif pada penyelesaian sengketa *e-commerce*, BPSK juga harus dapat menyesuaikan dengan karakteristik dari penyelenggaraan sistem dan transaksi elektronik yang ada saat ini. Penyelenggaraan sistem dan transaksi elektronik saat ini diatur dalam Undang-Undang ITE dan PP PSTE. Artinya, BPSK sudah seharusnya menyesuaikan diri dengan ketentuan tersebut yang dalam hal ini BPSK dapat

<sup>14</sup> Seperti diamanatkan oleh Pasal 25 dan 32 – 34 GDPR yang mana akan berlaku juga bagi penyelenggara jasa *fintech* dengan konsumen dari Uni Eropa.

menangani pengaduan dari masyarakat terkait data pribadi mengingat banyaknya *e-commerce* yang meminta data pribadi konsumen.

Selain itu juga BPSK akan bekerjasama dengan BRTI (Badan Regulasi Telekomunikasi Indonesia) untuk melakukan pemblokiran terhadap nomer telepon pelaku *e-commerce* yang telah terindikasi melakukan penjualan data pribadi terhadap konsumen yang dirugikan. Hal ini sesuai dengan Ketetapan (TAP) BRTI Nomor: 04 Tahun 2018 tentang Penanganan Pengaduan Penyalahgunaan Jasa Telekomunikasi yang sudah berlaku sejak 10 Desember 2018.

#### **4. *Consumer Protection System (CPS) Menyerahkan Hasil Penelitian Fintech***

Selain menyerahkan hasil penelitian menyangkut *e-commerce*, CPS juga menyerahkan hasil penelitian terhadap sengketa *fintech* kepada OJK dan BRTI. Dalam hal ini OJK dapat melakukan pencabutan izin usaha pelaku *fintech* yang terbukti melakukan perbuatan penjualan data pribadi konsumen berdasarkan Peraturan Otoritas Jasa Keuangan Nomor 1 /POJK.07/2013 tentang Perlindungan Konsumen Sektor Jasa Keuangan. Nantinya CPS juga menyediakan alternatif penyelesaian sengketa secara non litigasi yang dipimpin anggota komisi khusus dari CPS, namun apabila konsumen ingin menggunakan jalur litigasi 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.

Selain itu juga OJK akan bekerjasama dengan BRTI (Badan Regulasi Telekomunikasi Indonesia) untuk melakukan pemblokiran terhadap nomer telepon pelaku *fintech* yang telah terindikasi melakukan penjualan data pribadi terhadap konsumen yang dirugikan. Hal ini sesuai dengan Ketetapan (TAP) BRTI Nomor: 04 Tahun 2018 tentang Penanganan Pengaduan Penyalahgunaan Jasa Telekomunikasi yang sudah berlaku sejak 10

### 5. Apabila Konsumen Memiliki Problematika Terhadap *E-commerce* dan *Fintech*

Apabila konsumen memiliki problematika mengenai perlindungan data pribadi yang berkaitan dengan *e-commerce* maupun *fintech*, nantinya BPSK, OJK, dan BRTI dapat melakukan kerjasama dalam penyelesaiannya. Yang dimana BPSK dapat menyelesaikan sengketa dengan menyesuaikan Undang-Undang ITE dan PP PSTE. OJK dapat melakukan pencabutan izin usaha pelaku *fintech* yang terbukti melakukan perbuatan penjualan data pribadi konsumen berdasarkan Peraturan Otoritas Jasa Keuangan Nomor 1 /POJK.07/2013 tentang Perlindungan Konsumen Sektor Jasa Keuangan. Untuk menangani penyelesaian sengketa maka dapat digunakan jalur non litigasi, namun apabila konsumen ingin menggunakan jalur litigasi 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.

Dan BRTI dapat melakukan pemblokiran terhadap nomor telepon yang telah terindikasi melakukan penjualan data pribadi terhadap konsumen yang dirugikan. Hal ini sesuai dengan Ketetapan (TAP) BRTI Nomor: 04 Tahun 2018 tentang Penanganan Pengaduan Penyalahgunaan Jasa Telekomunikasi yang sudah berlaku sejak 10 Desember 2018.

### 6. Pemblokiran yang Dilakukan oleh Kominfo

Kominfo dapat melakukan pemblokiran terhadap *e-commerce* maupun *fintech* yang telah terbukti melakukan penyalahgunaan terhadap data pribadi konsumen melalui hasil penelitian CPS. Adapun dasar kominfo melakukan pemblokiran melalui Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi

### 3. Penutup

Pemanfaatan internet dalam berbagai bidang kehidupan tidak saja membuat segala sesuatunya menjadi lebih mudah, namun juga melahirkan sejumlah permasalahan termasuk masalah hukum. Salah satu masalah hukum yang muncul adalah masalah yang berkaitan dengan perlindungan data pribadi (*the protection of privacy rights*). Disisi lain, masih banyak masyarakat yang bingung terhadap banyaknya lembaga perlindungan konsumen yang akhirnya menyebabkan kebanyakan masyarakat tidak melaporkan problematika yang dihadapinya. Hal inilah yang menjadi salah satu penyebab perlindungan terhadap konsumen di Indonesia belum maksimal.

Permasalahan terkait regulasi pun turut menjadi penyebab perlindungan terhadap konsumen di Indonesia belum maksimal. Hal ini disebabkan undang-undang mengenai perlindungan data pribadi konsumen yang sudah ada masih dirasa belum mampu mengatasi problematika yang ada. Salah satu usaha pemerintah ialah merancang Undang-Undang Perlindungan Data Pribadi yang kini masih belum di sahkan.

Berdasarkan problematika tersebut dibutuhkan *Consumer Protection System* (CPS) sebagai optimalisasi sistem perlindungan data pribadi konsumen daring melalui *collaboration concept* dalam menghadapi Revolusi Industri 4.0 yang nantinya dapat mengoptimalkan *stakeholder* terkait dalam upaya perlindungan konsumen yang dimana masing masing *stakeholder* ini sebetulnya memiliki kemiripan tugas namun dalam praktiknya belum sepenuhnya berjalan. Hal ini bisa dilihat masyarakat merasa bingung apabila memiliki sengketa yang kompleks akan dibawa kemana, terlalu banyaknya lembaga yang memiliki kemiripan tugas dan sebagainya. Sehingga, dengan adanya CPS diharapkan dapat mengatasi problematika yang dihadapi masyarakat serta dapat mengoptimalkan perlindungan konsumen daring.



## DAFTAR PUSTAKA

**Buku**

Roni Hanitijo Soemitro. 1988. *Metodologi Penelitian Hukum Dan Jurimetri*. Jakarta: Penerbit Ghalia.

**Jurnal**

Lia Sautunnida, 2018. Urgensi Undang-Undang Perlindungan Data Pribadi Di Indonesia. *Kanun Jurnal Ilmu Hukum, Volume 20, Nomor 2*.

**Situs Internet/Halaman Web**

Anonim, *Kamus Bahasa Indonesia Data Pribadi*. Diakses 29 April 2020. <http://Kamusbahasaindonesia.Org/Data%20pribadi/Miripkamusbahasaindonesia.Org>.

Daniar Supriyadi. 2017. *Data Pribadi dan Dua Dasar Legalitas Pemanfaatannya*. Diakses 29 April 2020. <https://m.hukumonline.com/berita/baca/lt59cb4b3feba88/data-pribadi-dan-dua-dasar-legalitas-pemanfaatannya-oleh-daniar-supriyadi/>.

EDPS. 2018. *Privacy and Competitiveness in the Age of Big Data*. Diakses 29 April 2020. [https://edps.europa.eu/presspublications/press-news/press-releases/2014/privacy-and-competitiveness-age-big-data\\_en](https://edps.europa.eu/presspublications/press-news/press-releases/2014/privacy-and-competitiveness-age-big-data_en).

Hari Widowati. 2019. *Indonesia Jadi Negara Dengan Pertumbuhan E-Commerce Tercepat di Dunia*. Diakses 29 April 2020. <https://Databoks.Katadata.Co.Id/Datapublish/2020/04/25/Indonesia-Jadi-Negara-Dengan-Pertumbuhan-E-Commerce-Tercepat-Di-Dunia>.

John S. Pruitt *et al.* 2017. *Big Data and Cybersecurity: The Federal Insurance Office Explores New Frontiers for Consumer Protection*. Diakses 29 April 2020. <https://www.lexology.com/library/detail.aspx?g=b2663a0a-6603-4ca4-831e-5c94ca42a296>.

Tempo.co. 2011. *Jaringan Sony Dibobol Lagi Jutaan Data Dicuri*. Diakses 29



April 2020. <http://www.tempo.co/read/news/2011/06/03/072338366/>.

Yudha Pratomo. 2019. *APJII: Jumlah Pengguna Internet di Indonesia Tembus 171 Juta Jiwa*. Diakses 29 April 2020. <https://Tekno.Kompas.Com/Read/2020/05/16/03260037/Apjii-Jumlah-Pengguna-Internet-Di-Indonesia-Tembus-171-Juta-Jiwa>

## Peraturan

Data Protection Act 1998, Pasal 1 ayat (1).

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.

Undang-Undang Nomor 23 Tahun 2006 Tentang Administrasi Kependudukan, Lembaran Negara Republik Indonesia Tahun 2006 Nomor 124, Tambahan Lembaran Negara Republik Indonesia Nomor 4674.

Undang-Undang Republik Indonesia Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen, Lembaran Negara Republik Indonesia Tahun 1999 Nomor 42, Tambahan Lembaran Negara Republik Indonesia Nomor 3821.

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 4843.

Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251, Tambahan Lembaran Negara Republik Indonesia Nomor 5952.

Undang-Undang Nomor 4 Tahun 2018 tentang Pengesahan *Protocol to Implement the Sixth Package of Commitments on Financial Service Under the Asean Framework Agreement on Service* (Protokol Untuk Melaksanakan Paket Komitmen Keenam Bidang Jasa Keuangan dalam Persetujuan Kerangka Kerja Asean Dibidang Jasa), Lembaran Negara Republik Indonesia Tahun 2018 Nomor 82, Tambahan Lembaran Negara Republik Indonesia Nomor 6211.

Peraturan Pemerintah Republik Indonesia Nomor 82 Tahun 2012 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik, Lembaran Negara

Republik Indonesia Tahun 2012 Nomor 189, Tambahan Lembaran Negara Republik Indonesia Nomor 5348.

Peraturan Otoritas Jasa Keuangan Nomor 1/POJK.07/2013 Tentang Perlindungan Konsumen Sektor Jasa Keuangan, Lembaran Negara Republik Indonesia Tahun 2013 Nomor 118, Tambahan Lembaran Negara Republik Indonesia Nomor 5431.

Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik, Berita Negara Republik Indonesia Tahun 2016 Nomor 1829.

Ketetapan Badan Regulasi Telekomunikasi Indonesia Nomor 04 Tahun 2018 tentang Penanganan Pengaduan Penyalahgunaan Jasa Telekomunikasi.

