

URGENSI PELINDUNGAN DATA PRIBADI KONSUMEN DI ERA EKONOMI DIGITAL

THE URGENCY OF PROTECTION CONSUMER'S DATA IN THE ERA OF DIGITAL ECONOMY

Trias Palupi Kurnianingrum

(Pusat Penelitian, Badan Keahlian Sekretariat Jenderal DPR RI
Jalan Gatot Subroto, Ged. Nusantara I, lantai 2,
e-mail: triaspalupikurnianingrum@yahoo.com)

Naskah diterima: 10 Oktober 2020, direvisi: 1 Desember 2020,
disetujui: 15 Desember 2020

Abstract

In the digital era, combined with big data's phenomena and potential, personal's data has become a valuable commodity. This condition is not without reason. They consider that the digital economy's development has been proven to drive economic growth even though it has high economic value, the consumer's data protection still not optimal. Many cases issue consumer's data unsettling society. This article, produced from a normative judicial approach, discusses the cause and impacts of issues consumer data in the digital economic era and the state's role in providing legal protection. Analysis of the problem uses the theory of legal certainty and legal protection. This research indicates the causes of misuse of consumer data caused by the lack of the state in providing protection, the lack of consumer knowledge, and others. Personal data protection material has already been regulated in several laws and regulations, but the protection is not optimal. The number of regulations causes overlapping mechanisms and authorities to protect personal data itself, making consumers disadvantaged. Therefore, there should be special rules governing the protection of consumer data. The state's role to protect consumer personal data can be carried out by approving the draft of personal data protection law, forming particular institutions, and setting strict and binding penalties.

Keywords: *the digital era; consumer's personal data; legal protection; the draft bill of personal data protection.*

Abstrak

Dengan masuknya era digital yang dipadukan dengan fenomena dan potensi *big data* maka data pribadi telah menjelma menjadi suatu komoditas berharga. Hal ini bukannya tanpa sebab mengingat pengembangan ekonomi digital terbukti dapat mendorong pertumbuhan ekonomi. Meskipun memiliki nilai ekonomis tinggi sayangnya pelindungan data pribadi konsumen masih belum maksimal. Banyak kasus penyalahgunaan data pribadi konsumen yang meresahkan masyarakat. Tulisan ini merupakan hasil penelitian yuridis normatif, membahas faktor penyebab dan dampak penyalahgunaan data pribadi konsumen di era digital serta peran negara dalam pelindungan hukum data pribadi konsumen. Analisa permasalahan menggunakan teori kepastian dan pelindungan hukum. Penelitian ini menunjukkan penyebab terjadinya penyalahgunaan data pribadi konsumen di antaranya minimnya negara dalam memberikan pelindungan, minimnya pengetahuan konsumen, dan sebagainya. Pada dasarnya materi pelindungan data pribadi telah diatur di dalam beberapa peraturan perundang-undangan, hanya saja cakupan pelindungannya belum maksimal. Adanya beberapa aturan menyebabkan tumpang tindih mekanisme dan kewenangan dalam melakukan pelindungan data pribadi itu sendiri sehingga yang paling dirugikan adalah pihak konsumen. Oleh karena itu, perlu ada aturan khusus yang mengatur mengenai pelindungan data pribadi konsumen. Selain itu, peran negara untuk melindungi data pribadi konsumen dapat dilakukan dengan cara segera membahas dan mengesahkan RUU tentang Pelindungan Data Pribadi, membentuk lembaga khusus, dan pengaturan sanksi yang tegas dan mengikat.

Kata kunci: era digital; data pribadi konsumen; pelindungan hukum; RUU Pelindungan Data Pribadi.

PENDAHULUAN

Pelindungan privasi dan data pribadi sangat memengaruhi perkembangan ekonomi digital di suatu negara, tak terkecuali Indonesia. Hal ini dikarenakan data telah menjadi sumber daya baru untuk menggerakkan mesin bisnis di era digital. Bahkan, data sudah menjadi identitas bagi seseorang yang dapat dipertukarkan dengan berbagai macam hal.¹ Menurut KBBI, data pribadi adalah data yang berkenaan dengan ciri seseorang, nama, umur, jenis kelamin, pendidikan, pekerjaan, alamat, dan kedudukan dalam keluarga.² Pasal 1 angka 1 Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik (Permenkominfo No. 20 Tahun 2016), mendefinisikan data pribadi sebagai data perseorangan tertentu yang disimpan, dirawat, dan dijaga kebenaran serta dilindungi kerahasiaannya. Adapun Pasal 1 angka 2 Permenkominfo No. 20 Tahun 2016 menyebutkan data perseorangan tertentu adalah setiap keterangan yang benar dan nyata yang melekat dan dapat diidentifikasi, baik langsung maupun tidak langsung, pada masing-masing individu yang pemanfaatannya sesuai ketentuan peraturan perundang-undangan.

Bagi industri 4.0, data pribadi penting untuk dilindungi dikarenakan data telah menjadi roh teknologi kecerdasan buatan (*artificial intelligence*).³ Industri 4.0 yang merupakan penggabungan teknologi otomatisasi dengan teknologi siber yang menekankan pada pola

ekonomi digital, *artificial intelligence*,⁴ big data⁵, dan lainnya telah mengubah banyak kehidupan manusia, termasuk di bidang ekonomi.⁶ Pengembangan ekonomi digital bahkan terbukti dapat mendorong pertumbuhan ekonomi sekaligus mendukung inklusi⁷ keuangan.⁸ Pada level negara, peran industri yang menggunakan teknik analisis data semakin berkembang di beberapa negara. Di Amerika Serikat, sektor ini menjadi katalis pertumbuhan ekonomi paling berpengaruh dengan kontribusi sebesar 1,7 persen dari PDB.⁹ Di Inggris, sektor ekonomi yang berkaitan dengan pengumpulan dan analisis data telah menghasilkan 4,8 milyar nilai tambah kotor dan 73.000 lapangan kerja¹⁰. Sementara di India, industri analisis data diproyeksi tumbuh hampir 8 (delapan) kali lipat menjadi 16 milyar dollar AS pada tahun 2025.¹¹

1 Klik legal.com, 15 Mei 2020, "Pelindungan Data Pada Platform Digital Melalui Pembentukan Komisi Privasi dan Data Protection Officer (DPO)", (*online*), (<https://kliklegal.com/perlindungan-data-pada-platform-digital-melalui-pembentukan-komisi-privasi-dan-data-protection-officer-dpo/>), diakses 18 Juni 2020).

2 Kamus Besar Bahasa Indonesia, "Pengertian Data Pribadi", (*online*), (<https://kbbi.web.id/data>), diakses 23 Juni 2020).

3 Media Indonesia.com, 31 Juli 2019, "Kedaulatan Data Pribadi", (*online*), (https://mediaindonesia.com/editorials/detail_editorials/1757-kedaulatan-data-pribadi), diakses 16 Januari 2021).

4 Menurut Yuval Noah Harari dalam bukunya yang berjudul "Homo Deus Masa Depan Umat Manusia", yang dimaksud dengan *artificial intelligence* atau kecerdasan buatan adalah sistem komputer yang mampu melakukan tugas-tugas yang biasanya membutuhkan kecerdasan manusia. Contoh penerapan teknologi artificial intelligence dapat dilakukan untuk filter email di Gmail, penggunaan dalam media sosial, prediksi pencarian Google, dan sebagainya.

5 *Big data* adalah istilah yang diberikan pada kumpulan data yang berukuran sangat besar dan kompleks sehingga tidak memungkinkan untuk diproses menggunakan perangkat pengelola database konvensional ataupun pemroses data lainnya.

6 Kompasiana.com, 8 November 2019, "Resolusi Industri 4.0, Perlunya Pelindungan Data Pribadi", (*online*), (<https://www.kompasiana.com/machsvorming/5dc575ffd541df266011b652/revolusi-industri-4-0-perlunya-perlindungan-data-pribadi>), diakses 8 Juni 2020).

7 Berdasarkan PP No. 82 Tahun 2016 tentang Strategi Nasional Keuangan Inklusif, yang dimaksud dengan inklusi keuangan adalah sebuah kondisi di mana setiap anggota masyarakat mempunyai akses terhadap berbagai layanan keuangan formal yang berkualitas, tepat waktu, lancar, dan aman dengan biaya terjangkau sesuai dengan kebutuhan dan kemampuan masing-masing.

8 Warta Ekonomi.co.id, 18 Desember 2016, "Manfaat Ganda Pengembangan Ekonomi Digital", (*online*), (<https://www.wartaekonomi.co.id/read124515/manfaat-ganda-pengembangan-ekonomi-digital>), diakses Minggu 31 Mei 2020).

9 Kompasiana.com, 18 Mei 2018, "Menakar Kebijakan Pelindungan Privasi di Era Digital", (*online*), (https://www.kompasiana.com/kanopi_febui/5afec2c95e137354db5a6a82/menakar-kebijakan-perlindungan-privasi-di-era-digital?page=all), diakses 31 Mei 2020).

10 *Ibid.*

11 *Ibid.*

Berada di Asia Tenggara, Indonesia sendiri merupakan pasar yang potensial bagi pertumbuhan ekonomi digital. Besarnya potensi ekonomi digital di Indonesia dibuktikan melalui nilai USD 27 milyar pada tahun 2018.¹² Selain itu, pertumbuhan ekonomi digital di Indonesia ditandai dengan meningkatnya penetrasi pengguna internet. Berdasarkan data Badan Pusat Statistik (BPS) tahun 2019, pengguna internet telah mencapai 47,69 persen dari penduduk Indonesia berusia di atas 5 tahun atau sekitar 115 juta jiwa.¹³ Adapun menurut data Asosiasi Pengguna Jasa Internet Indonesia (APJII), penetrasi pengguna internet tahun 2019 diperkirakan mencapai 64,8 persendari penduduk Indonesia atau sekitar 171,17 juta jiwa.¹⁴ Angka ini secara tidak langsung menempatkan Indonesia pada urutan kelima sebagai negara dengan jumlah pengguna internet terbesar di dunia setelah Cina, India, Amerika Serikat, dan Brazil.¹⁵

Penguatan ekonomi digital di Indonesia juga tidak terlepas dari peran pemerintah, dimana Presiden Jokowi telah menegaskan untuk menargetkan Indonesia menjadi kekuatan ekonomi digital terbesar di ASEAN pada tahun 2025. Prediksi ini bukannya tanpa sebab mengingat pada tahun 2015, nilai ekonomi digital Indonesia tercatat di angka 8 milyar dollar AS. Angka tersebut kemudian terus meningkat menjadi 40 milyar dollar AS pada tahun 2019.¹⁶ Konsep ekonomi digital sendiri awalnya diperkenalkan oleh Don Tapscott yang

menyatakan bahwa ekonomi digital merupakan sebuah fenomena sosial yang memengaruhi sistem ekonomi, dimana fenomena tersebut mempunyai karakteristik sebagai sebuah ruang intelijen, meliputi informasi, berbagai akses terhadap instrumen informasi, kapasitas informasi dan pemrosesan informasi.¹⁷ Sementara menurut Zimmerman, konsep ekonomi digital merupakan konsep yang sering dipergunakan untuk menjelaskan dampak global terhadap pesatnya perkembangan teknologi informasi dan komunikasi yang berdampak pada kondisi sosial ekonomi.¹⁸ Meskipun terkesan menguntungkan, tren pertumbuhan ekonomi digital di Indonesia belum menyentuh sisi pelindungan konsumen khususnya terkait pelindungan terhadap data pribadi.

Disadari atau tidak, dengan adanya era digital, peredaran data menjadi semakin tidak terkontrol. Disrupsi pemanfaatan teknologi internet yang mencangkup segala lini mengakibatkan pemilik data menjadi kehilangan kendali atas data pribadinya.¹⁹ Hal ini menjadi ancaman yang nyata terlebih lagi perkembangan teknologi informasi yang pesat telah menimbulkan adanya suatu gaya baru di dalam sistem perdagangan. Pesatnya angka pengguna internet di Indonesia secara tidak langsung menunjukkan besarnya potensi pasar yang akan memengaruhi munculnya berbagai peluang bisnis baru. Era industri 4.0 telah menyebabkan transaksi jual beli konsumen dan produsen menjadi tidak terbatas hingga ke luar negeri. Dalam era ini, hampir segala hal menggunakan perangkat digital sehingga

12 Jaringan Prima.co.id, 29 Agustus 2019, "Potensi Ekonomi Digital di Indonesia", (*online*), (<https://www.jaringanprima.co.id/id/potensi-ekonomi-digital-di-indonesia>), diakses 31 Mei 2020).

13 Kominfo.go.id, 26 Februari 2020, "Masuki era Digital, Indonesia Butuh UU Pelindungan Data Pribadi", (*online*), (<https://aptika.kominfo.go.id/2020/02/masuki-era-digital-indonesia-butuh-uu-pelindungan-data-pribadi/>), diakses 31 Mei 2020).

14 *Ibid.*

15 Antara News.com, 7 September 2020, "Kemkominfo: Indonesia Urutan Kelima Pengguna Internet", (*online*), (<https://www.antaraneews.com/berita/219498/kemkominfo-indonesia-urutan-lima-pengguna-internet>), diakses Senin 11 Januari 2021).

16 Bill Clinton, 27 Februari 2020, "Jokowi: Ekonomi Digital Indonesia Terbesar di Asia Tenggara", (*online*), (<https://tekno.kompas.com/read/2020/02/27/18010097/jokowi-ekonomi-digital-indonesia-terbesar-di-asia-tenggara>), diakses Senin 8 Juni 2020.

17 Balitbang Kemenkominfo, "Perkembangan Ekonomi Digital di Indonesia: Strategi dan Sektor Potensial", (*online*), (https://www.google.co.id/url?sa=t&srct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwi7pafFhqXvAhXTW3wKHR3yBrOQFjABegQIARAD&url=https%3A%2F%2Fbalitbangsdm.kominfo.go.id%2Fpublikasi_665_3_230&usg=AOvVaw1fXsBhZKCCWxcCRU-G8EUi), diakses Jumat 7 November 2020).

18 Hans Dieter Zimmerman, Understanding the Digital Economy: Challengers for New Business Models, AMCIS 2000 Proceedings, dikutip tidak langsung oleh Aan Ansori, "Digitalisasi Ekonomi Syariah", *Jurnal Ekonomi Keuangan dan Bisnis Islam*, Vol. 7 No. 1, Januari 2016, hal. 1-18.

19 Tempo Online, "Urgensi Regulasi Pelindungan Data Pribadi di Indonesia", (*online*), (<https://indonesiana.tempo.co/read/68772/2016/04/04/lintangsetianti/urgensi-regulasi-pelindungan-data-pribadi-di-indonesia>), diakses 23 Februari 2019).

secara tidak langsung memengaruhi juga pola perilaku konsumen di Indonesia. Hal ini dapat menjadi ancaman yang nyata dengan semakin meningkatnya pemanfaatan teknologi yang tidak lagi dapat dibendung khususnya secara *online*.

Hasil penelitian yang dilakukan penulis di lapangan²⁰ menunjukkan beberapa kasus kebocoran data pribadi konsumen yang berbuntut pada aksi penipuan, sebut saja misalnya penyalahgunaan data pribadi dalam transaksi elektronik (*e-commerce*), perbankan, industri perusahaan teknologi (*fintech*), perusahaan jasa angkutan *online* (Gojek, Grab), dan sebagainya. Bahkan kasus terbaru menyebutkan 91 juta konsumen aplikasi Tokopedia merasa dirugikan dengan bocornya data pribadi mereka yang rawan untuk disalahgunakan.²¹ Kasus tersebut telah dibawa ke ranah hukum dengan nomor registrasi perkara di Pengadilan Negeri Jakarta Pusat, yaitu nomor pendaftaran PN JKT.PST-050201 tertanggal 6 Mei 2020.²² Kejadian bocornya data pribadi konsumen menunjukkan betapa pentingnya urgensi penguatan perlindungan data pribadi di Indonesia. Hal ini semakin diperparah dengan belum adanya kepastian hukum terhadap perlindungan data pribadi konsumen di Indonesia.

Berbeda dengan negara lain yang telah memiliki aturan khusus terkait perlindungan data pribadi, Indonesia nyatanya hingga saat ini belum memiliki aturan yang mengatur mengenai data pribadi. Pengaturan data pribadi di Indonesia masih bersifat umum dan tersebar ke dalam beberapa aturan undang-undang. Beragam aturan yang mengatur mengenai perlindungan data pribadi tanpa disadari justru berakibat pada tumpang tindihnya mekanisme dan kewenangan dalam melakukan perlindungan data pribadi itu

sendiri sehingga yang paling dirugikan adalah pihak konsumen. Padahal di dalam transaksi perdagangan, konsumen mutlak untuk diberikan perlindungan.

Secara umum, aturan untuk melindungi konsumen diatur di dalam UU No. 8 Tahun 1999 tentang Perlindungan Konsumen (UU Perlindungan Konsumen). Undang-undang tersebut diberlakukan dengan tujuan untuk melindungi konsumen dengan mencantumkan hak dan kewajiban konsumen, pelaku bisnis serta tanggung jawab pemerintah. Namun sayangnya, ketentuan di dalam UU Perlindungan Konsumen yang dapat diterapkan adalah hak atas kenyamanan dan keamanan dalam mengkonsumsi barang dan/atau jasa, tidak ada pasal khusus di dalam undang-undang ini yang bertujuan untuk melindungi data pribadi konsumen sehingga materi di dalam UU Perlindungan Konsumen dinilai belum mengatur mengenai mekanisme pemulihan jika terjadi pelanggaran data pribadi. Padahal hingga kini, aplikasi seringkali masih menerapkan “klausul baku” ketika meminta data pribadi konsumen yang hendak memanfaatkan aplikasi mereka. Dengan tidak diaturnya detail dalam klausul mengenai sejauhmana rincian batasan data yang dapat dimanfaatkan atau tidak oleh pelaku usaha maka konsumen dapat terjebak dengan *terms of use* dan tanpa sadar memberikan hak untuk menggunakan dan menyebarkan data pribadi mereka kepada pihak ketiga. Parahnya lagi pelaku usaha seringkali tidak memberikan pilihan (*option*) bagi konsumen untuk memilih setuju atau tidak dengan detail data tertentu dan justru cenderung menerbitkan *disclaimer*²³ bahwa pihaknya tidak dapat dituntut atau tidak bertanggungjawab dengan alasan apapun. Lebih lanjut, UU Perlindungan Konsumen juga belum mengakomodir kerugian konsumen dalam hal kebocoran data.

Penelitian terkait perlindungan data pribadi konsumen pernah dilakukan oleh peneliti lain dengan judul: “Konsep Perlindungan Hukum

20 Laporan Hasil penelitian kelompok “Politik Hukum Terhadap Pelindungan Data Pribadi” di Provinsi Jawa Tengah dan Provinsi Sulawesi Selatan.

21 Cesar Akbar, 5 Mei 2020, Kasus Data Bocor, DPR: Tokopedia Harus Bertanggungjawab, (*online*), (<https://bisnis.tempo.co/read/1338931/kasus-data-bocor-dpr-tokopedia-harus-bertanggung-jawab>, diakses 11 Januari 2020).

22 CNN Indonesia.com, “Data Pengguna Dicuri, Menkominfo-Tokopedia Digugat ke PN”, (*online*), (<https://www.cnnindonesia.com/teknologi/20200507175240-192-501083/data-pengguna-dicuri-menkominfo-tokopedia-digugat-ke-pn>, diakses 5 Juli 2020).

23 *Disclaimer* merupakan kalimat peringatan yang ditujukan untuk konsumen atau publik mengenai kualitas barang, artikel, anjuran, dan sebagainya. Tujuan *disclaimer* adalah untuk melepaskan tanggungjawab atau memindahkan tanggungjawab dari sumber ke pengguna.

Atas Privasi dan Data Pribadi Dikaitkan Dengan Penggunaan *Cloud Computing* di Indonesia”, “Pelindungan Privasi dan Data Pribadi Konsumen Daring Pada *Online Marketplace System*”, “Pemanfaatan *Big Data* dan Pelindungan Privasi Konsumen di Era Ekonomi Digital”. Penelitian pertama dilakukan oleh Sinta Dewi yang memfokuskan mengenai pelindungan hukum terhadap data pribadi dikaitkan dengan teknologi *cloud computing*. *Cloud computing* merupakan teknologi yang menggunakan internet dan server pusat untuk menjaga atau mengelola data pengguna.²⁴ Penelitian kedua dilakukan oleh Masitoh Indriyani dkk yang membahas mengenai pelindungan data pribadi dan privasi *e-consumer* pada *online marketplace system*.²⁵ Penelitian ketiga dilakukan oleh Agung Pujianto dkk, yang membahas mengenai sejauhmana teknologi *big data* sudah dimanfaatkan di Indonesia baik oleh lembaga pemerintah maupun swasta.²⁶

Perbedaan dengan beberapa penelitian sebelumnya, penelitian ini menganalisis lebih mendalam mengenai pelindungan data pribadi konsumen di era ekonomi digital. Data pribadi konsumen yang dimaksud tidak terbatas hanya pada data pribadi di bidang perbankan dan kependudukan saja namun lebih kepada setiap data tentang seseorang baik teridentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung. Penelitian ini akan melihat apa yang menjadi faktor penyebab dan dampak terjadinya penyalahgunaan data pribadi serta melihat peran negara dalam pelindungan data pribadi konsumen. Belum adanya peran dan tanggungjawab negara menjadi salah satu bukti bahwa penyalahgunaan data pribadi masih marak terjadi dikarenakan hingga kini Indonesia belum memiliki aturan

husus yang mengatur mengenai pelindungan data pribadi. Oleh karena itu, negara dinilai perlu bertanggungjawab karena pada dasarnya negara memiliki kewenangan untuk memegang kedaulatan mengatur data pribadi guna melindungi kepentingan rakyat serta melindungi kepentingan bangsa dan negara sebagaimana amanat Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 (UUD NRI 1945). Berdasarkan uraian tersebut maka permasalahan yang akan dibahas, yaitu: **pertama**, apa yang menjadi faktor penyebab penyalahgunaan data pribadi?; **Kedua**, bagaimana dampak penyalahgunaan data pribadi konsumen di era ekonomi digital?; dan **Ketiga**, bagaimana peran negara dalam pelindungan data pribadi konsumen? Penelitian ini bertujuan untuk mengetahui faktor penyebab dan dampak penyalahgunaan data pribadi konsumen di era digital serta peran negara dalam pelindungan data pribadi. Penelitian ini diharapkan dapat menjadi masukan bagi Anggota Komisi I DPR RI dalam melaksanakan fungsi legislasi terutama dalam penyusunan RUU tentang Pelindungan Data Pribadi.

METODE PENELITIAN

Penelitian ini disusun dengan menggunakan metode penelitian yuridis normatif yakni dilakukan dengan cara meneliti peraturan perundang-undangan dan konvensi internasional terkait pelindungan data pribadi. Beberapa peraturan yang dimaksud, diantaranya UU No. 8 Tahun 1999 tentang Pelindungan Konsumen, UU No. 39 Tahun 1999 tentang Hak Asasi Manusia, UU No. 36 Tahun 2009 tentang Kesehatan, UU No. 24 Tahun 2013 tentang Perubahan Atas Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan (UU Adminduk), UU No. 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), PP No. 40 Tahun 2019 tentang Pelaksanaan Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan Sebagaimana Telah Diubah Dengan Undang-Undang Nomor 24 Tahun 2013 tentang Perubahan Atas Undang-Undang Nomor 23 Tahun 2006 tentang

24 Sinta Dewi, “Konsep Pelindungan Hukum Atas Privasi dan Data Pribadi Dikaitkan Dengan Penggunaan *Cloud Computing* di Indonesia”, *Jurnal Yustisia*, Vol. 5 No. 1, Januari 2016, Hal. 22-30.

25 Masitoh Indriyani dkk. “Pelindungan Privasi dan Data Pribadi Konsumen Daring Pada *Online Marketplace System*”, *Justitia Jurnal Hukum*, Vol.1, No. 2 Tahun 2017, Hal. 191-208.

26 Agung Pujianto dkk. “Pemanfaatan *Big Data* dan Pelindungan Privasi Konsumen di Era Ekonomi Digital”, *Majalah Ilmiah Bijak*, Vol.15, No. 2, September 2018, Hal. 127-137.

Administrasi Kependudukan, dan Peraturan Menteri Komunikasi dan Informatika No. 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik. Sementara untuk konvensi internasional yang dimaksud Konvensi Eropa tentang Hak Asasi Manusia (*European Charter of Human Rights*), Deklarasi Hak Asasi Manusia Perhimpunan Bangsa-Bangsa Asia Tenggara (*Asean Human Rights Declaration*), Deklarasi Umum Hak Asasi Manusia (*Universal Declaration of Human Rights*) dan Konvensi Internasional tentang Hak Sipil dan Politik (*International Covenant on Civil and Political Rights*).

Penelitian ini memerlukan data sekunder dan data primer. Data sekunder terdiri dari bahan hukum primer dan bahan hukum sekunder. Bahan hukum primer adalah bahan yang isinya mengikat, seperti peraturan perundang-undangan yang berkaitan dengan data pribadi. Bahan hukum sekunder adalah bahan hukum yang memberi petunjuk dan penjelasan terhadap bahan hukum primer, seperti buku, laporan penelitian, dan literatur lain mengenai perlindungan data pribadi. Penelitian ini juga dilengkapi dengan data primer melakukan observasi, wawancara dan *Focus Group Discussion* (FGD) dengan instansi-instansi terkait.

HASIL DAN PEMBAHASAN

Faktor Penyebab Penyalahgunaan Data Pribadi Konsumen

Perkembangan teknologi informasi dan komunikasi yang melaju dengan pesat pada dasarnya telah menimbulkan berbagai peluang dan tantangan. Teknologi informasi dan komunikasi telah mengubah perilaku masyarakat dan peradaban manusia secara global.²⁷ Salah satu bidang yang dipengaruhi oleh perkembangan teknologi informasi adalah terjadinya interaksi yang aktif antara individu dengan pihak penyedia jasa informasi. Berbagai sektor kehidupan telah memanfaatkan sistem informasi, sebut saja misalnya, bidang perdagangan (*e-commerce*), pariwisata, transportasi, bidang pemerintahan,

industri keuangan (*e-payment*), dan sebagainya.²⁸

Dengan globalisasi, hampir tidak ada hal bersifat “pribadi” yang disembunyikan. Dengan masuknya dunia digital yang dipadukan dengan fenomena dan potensi *big data*, privasi telah menjelma menjadi suatu komoditas berharga.²⁹ Informasi termasuk di dalamnya data pribadi, di era ekonomi digital merupakan aset yang sangat berharga dikarenakan memiliki nilai ekonomis tinggi sehingga banyak dimanfaatkan oleh pebisnis.³⁰ Bagi kalangan industri, *big data* telah membuka peluang untuk menetapkan strategi bisnis serta inovasi dalam hal memproses, menganalisis dan menyimpan data dengan volume serta tingkat vitalitas yang tinggi, cepat dan efektif.³¹ Besarnya peranan dan nilai ekonomi dari data inilah yang mendorong banyak pihak kemudian melakukan penyalahgunaan dengan berupaya meretas data via *online* maupun *offline*, baik secara pribadi maupun atas nama institusi tanpa sepengetahuan pemilik data tersebut.

Potensi pelanggaran privasi atas data pribadi secara *online* misalnya banyak terjadi dalam kegiatan pengumpulan data pribadi secara massal (*digital dossier*),³² pemasaran langsung (*direct selling*),³³ media sosial, pelaksanaan program e-KTP, pelaksanaan program *e-health*, dan

28 Muh Hasrul dalam Lidya Suryani, dkk. “Politik Hukum Terhadap Pelindungan Data Pribadi”, *Laporan Penelitian*, Jakarta: Pusat Penelitian Setjen DPR RI, 2019, Hal. 43.

29 Rifha Aditya Nugraha, “Pelindungan Data Pribadi dan Privasi Penumpang Maskapai Penerbangan Pada Era Big Data”, *Jurnal Mimbar Hukum*, Vol. 30 No. 2, Tahun 2018, hal. 262-276.

30 Sinta Dewi, “Konsep Pelindungan Hukum Atas Privasi dan Data Pribadi Dikaitkan Dengan Penggunaan *Cloud Computing* di Indonesia”, *Jurnal Yustisia*, Vol.5 No. 1, Januari 2016, hal. 22-30.

31 Agung Pujiyanto dkk, “Pemanfaatan Big Data dan Pelindungan Privasi Konsumen di Era Ekonomi Digital”, *Majalah Ilmiah Bijak*, Vol. 15 No. 2, September 2018, hal. 127-137.

32 *Digital dossier* merupakan suatu pengumpulan data privasi seseorang dalam jumlah banyak dengan menggunakan teknologi digital. Kegiatan ini dilakukan sejak tahun 1970 di negara Eropa dan Amerika Serikat.

33 *Direct selling* yakni praktik yang dilakukan para penjual untuk memasarkan barang dengan cara pemasaran secara langsung. Dengan berkembangnya cara pemasaran tersebut maka telah berkembang industri bank data yang khusus mengkoleksi informasi mengenai konsumen.

27 Ahmad M. Ramli, *Cyber law dan HAKI dalam Sistem Hukum Indonesia*, Bandung: PT. Refika Aditama, 2004, hlm. 1.

kegiatan komputasi awan³⁴(*cloud computing*).³⁵ Lebih parah lagi penyalahgunaan data pribadi juga dilakukan untuk tindak pidana kriminal, seperti pembuatan akun palsu, penipuan dalam jaringan, komersialisasi data operator telekomunikasi yang berbuntut *spamming* bagi pengguna jasa telekomunikasi, penjualan data nasabah perbankan, ataupun penjualan data kependudukan.³⁶

Banyaknya penyalahgunaan data pribadi dinilai sangat meresahkan masyarakat. Misalnya E-KTP dan kartu identitas anak (KIA) dinilai sangat rentan memiliki kebocoran data apabila diunggah melalui media sosial (medsos), sebab data tersebut akan muncul dalam pencarian data mesin pencari google sehingga beresiko mudah disalahgunakan bahkan diperjualbelikan.³⁷Selain penyalahgunaan data pribadi kependudukan, maraknya berita mengenai penipuan dengan menggunakan situs *e-commerce* (situs perdagangan) juga merupakan hal yang sering dijumpai dan merugikan konsumen.³⁸ Tidak dipungkiri bahwa besarnya pengguna internet di Indonesia secara tidak langsung telah mendorong lahirnya banyak sektor usaha baru (*start up*), khususnya yang bergerak di sektor *e-commerce*. Banyaknya *start up* khususnya yang bergerak di bidang *e-commerce* telah melahirkan data baru yang sangat besar jumlahnya. Sebab saat seseorang melakukan aktivitas belanja *online*, yang bersangkutan harus memasukkan data pribadinya,

termasuk nama, alamat, nomor telepon, dan email. Ketika melakukan pembayaran, pembeli juga akan memasukkan data kartu kreditnya. Sekali berbelanja *online* di satu situs, data pribadi pembeli sudah dimiliki oleh pemilik toko atau *market place*. Jika konsumen rutin berbelanja di satu situs, data perilaku (*behavior*) konsumen terkait dengan produk yang dibeli dan intensitas belanja juga masuk ke toko *online* tersebut.

Hal ini berlaku juga untuk seseorang yang membeli tiket kereta ataupun pesawat dari agen perjalanan *online*. Bahkan data yang dimasukkan lebih terperinci lagi, tidak hanya nama, alamat, nomor telepon namun juga nomor KTP dan paspor. Kasus lain seiring perkembangan moda transportasi *online* seperti Gojek dan Grab juga dinilai dapat menimbulkan permasalahan berkenaan dengan data pribadi karena rentan terjadinya kebocoran data pengguna, di mana rute sehari-hari pengguna dapat dilacak. Data pribadi seperti nama, alamat, nomor telepon, koordinat dan tujuan dapat diakses dari API *endpoint* yang dimiliki Gojek³⁹.

Beberapa kejadian di atas menunjukkan bahwa kasus penyalahgunaan data pribadi konsumen di Indonesia kian memprihatinkan. Hal ini dipertegas oleh Prof Dr. Marwati Riza, yang menyatakan bahwa jumlah kejahatan *cyber* bahkan berada pada puncaknya sejak tahun 2013 sampai dengan tahun 2019. Dengan demikian, potensi dan tingkat kejahatan *cyber* di Indonesia sudah memasuki status darurat.⁴⁰

Lebih lanjut, data Direktorat Tindak Pidana Siber Bareskrim Polri juga menyatakan bahwa sejak Januari s.d. 17 April 2020 terdapat 4.008 laporan (1.322 melalui Polda dan 2.686 melalui portal Patrolisiber) terkait kejahatan *cyber* yang telah mencapai kerugian dengan total estimasi Rp10.74 milyar. Laporan tersebut di antaranya 2.157 laporan penipuan *online* dan sisanya

34 Komputasi awan (*cloud computing*) merupakan gabungan pemanfaatan teknologi komputer dalam suatu jaringan dengan pengembangan berbasis internet. Beberapa perusahaan teknologi informasi terkemuka telah mengeluarkan aplikasi dalam menyediakan ruang penyimpanan data pengguna seperti *Dropbox*, *Google Drive*, *Sky Drive*, *Scribd*, dan sebagainya.

35 Sinta Dewi Rosadi, *Cyber Law Aspek Data Privasi Menurut Hukum Internasional, Regional, dan Nasional*, PT. Refika Aditama: Bandung, 2015, hal. 10.

36 Lia Sautunnida, "Urgensi Undang-Undang Pelindungan Data Pribadi di Indonesia Studi Perbandingan Hukum Inggris dan Malaysia", *Kanun Jurnal Ilmu Hukum*, Vol. 20 No. 2, Agustus 2018, hal. 369-384.

37 Rita dalam Lidya Suryani, dkk. "Politik Hukum Terhadap Pelindungan Data Pribadi", *Laporan Penelitian*, Jakarta: Pusat Penelitian Setjen DPR RI, 2019, Hal. 44.

38 Polrestabes Surakarta dalam Lidya Suryani, dkk. "Politik Hukum Terhadap Pelindungan Data Pribadi", *Laporan Penelitian*, Jakarta: Pusat Penelitian Setjen DPR RI, 2019, Hal. 63.

39 Reska K. Nistanto, 20 Januari 2016, "Kebocoran Go-Jek Memuncak, Rute Sehari-Hari Pengguna Bisa Dilacak", (*online*), (<https://Tekno.Kompas.Com/Read/2016/01/20/16031307/Kebocoran.Go-Jek.Memuncak.Rute.Sehari-Hari.Pengguna.Bisa.Dilacak>), diakses 11 September 2019).

40 Hasil Wawancara Penelitian Kelompok Politik Hukum Terhadap Pelindungan Data Pribadi dengan Prof. Dr. Marwati Riza, SH., M.Si (Dosen Fakultas Hukum Universitas Hasanuddin), Tanggal 11 April 2019.

penyalahgunaan data pribadi konsumen seperti manipulasi data, pencurian data/identitas dan sebagainya.⁴¹

Privasi dan data pribadi pada dasarnya telah menjadi hal penting karena pengguna dalam jaringan tidak akan melakukan sebuah transaksi digital apabila merasa keamanan akan privasi dan data pribadinya terancam.⁴² Di dalam sejarah perkembangannya, privasi merupakan konsep yang bersifat universal dan dikenal di berbagai negara, baik tertulis dalam bentuk undang-undang maupun tidak tertulis dalam bentuk aturan moral. Konsep hak privasi pertama kali dikembangkan pada tahun 1890 ketika Samuel Warren dan Louis Brandeis menulis esai dengan judul *"The Right to Privacy"* yang diterbitkan oleh *Harvard Law Review*⁴³. Di dalam esai tersebut, diusulkan pengakuan hak individu *"right to be let alone"* atau hak untuk tidak diganggu yang harus dilindungi oleh hukum yang ada mengingat hak individu merupakan bagian dari hak asasi manusia.⁴⁴

Untuk perlindungan data pribadi, secara umum dianggap sebagai bagian dari perlindungan atas privasi, yang merupakan konsep spesifik dari privasi itu sendiri, yaitu privasi merupakan hak asasi manusia yang fundamental, sedangkan perlindungan data adalah salah satu cara untuk melindungi privasi itu sendiri.⁴⁵ Sederhananya

privasi merupakan bagian dari hak asasi manusia yang mengidentifikasi perlindungan data pribadi sebagai hak yang penting. Hak privasi melalui perlindungan data bukan hanya penting melainkan juga merupakan elemen kunci bagi kebebasan dan harga diri individu.

Konvensi Eropa tentang Hak Asasi Manusia (*European Charter of Human Rights*) dan Deklarasi Hak Asasi Manusia Perhimpunan Bangsa-Bangsa Asia Tenggara (*Asean Human Rights Declaration*) telah mengakui hak atas perlindungan data pribadi sebagai salah satu jenis hak asasi manusia. Hak atas perlindungan data pribadi merupakan suatu hak hasil bentukan dan irisan penggabungan hak atas informasi dan hak atas privasi yang telah melalui evolusi panjang sejak diakuinya hak asasi manusia dalam *Universal Declaration of Human Rights* (Deklarasi Umum Hak Asasi Manusia). Pasal 12 Deklarasi Umum Hak Asasi Manusia telah menegaskan bahwa: *"no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attack"*.⁴⁶ Deklarasi Umum Hak Asasi Manusia merupakan elemen utama dari peraturan perundang-undangan hak asasi manusia internasional (*International Bill of Rights*) yang mengatur mengenai hak dan kebebasan fundamental.⁴⁷

Lebih lanjut, perlindungan data pribadi di Indonesia merupakan salah satu hak asasi manusia yang menjadi bagian dari perlindungan diri pribadi sebagaimana telah ditegaskan di dalam konstitusi negara kita.⁴⁸ Dalam konteks hukum Indonesia, Indonesia resmi menjamin hak asasi manusia termasuk di dalamnya perlindungan data pribadi sebagai salah satu hak konstitusional

41 Ira Aprilianti, 20 April 2020, "Opini Hari Konsumen Nasional Pelindungan Data Pribadi di Tengah Pandemi Covid-19", (online), (<https://www.cips-indonesia.org/post/opini-hari-konsumen-nasional-perlindungan-data-pribadi-di-tengah-pandemi-covid-19>, diakses 22 Juni 2020).

42 Sinta Dewi dkk. "Pelindungan Privasi dan Data Pribadi Dalam Era Ekonomi Digital di Indonesia", *Jurnal Vej*, Volume 4 No. 1 Tahun 2018, hlm. 88-101.

43 Menurut Warren dan Lois Brandeis sebagaimana dikutip oleh Sinta Dewi, dengan adanya perkembangan dan kemajuan teknologi maka timbul suatu kesadaran masyarakat bahwa telah lahir suatu kesadaran bahwa ada hak seseorang untuk menikmati hidup. Hak untuk menikmati hidup tersebut diartikan sebagai hak seseorang untuk tidak diganggu kehidupan pribadinya baik oleh orang lain atau oleh negara. Oleh karena itu hukum harus mengakui dan melindungi hak privasi tersebut.

44 Sinta Dewi, "Konsep Pelindungan Hukum Atas Privasi dan Data Pribadi Dikaitkan dengan Penggunaan *Cloud Computing* di Indonesia", *Jurnal Yustisia*, Vol. 5 No. 1, Januari 2016, hlm. 22-30.

45 Muh Hasrul dalam Lidya Suryani, dkk. "Politik Hukum Terhadap Pelindungan Data Pribadi", *Laporan Penelitian*, Jakarta: Pusat Penelitian Setjen DPR RI, 2019, Hal. 43.

46 Artinya *"tidak seorangpun boleh diganggu secara sewenang-wenang dalam urusan pribadi, keluarga, rumah tangga atau hubungan surat menyuratnya, juga tidak boleh dilakukan serangan terhadap kehormatan dan reputasinya. Setiap orang berhak mendapatkan pelindungan hukum terhadap gangguan atau penyerangan seperti itu"*.

47 Rhona K.M Smith, *Hukum Hak Asasi Manusia*, Yogyakarta: PUSHAM UI, 2010, hlm. 88.

48 Masitoh Indriani dalam Trias Palupi K, dkk. "Optimalisasi Pelindungan Terhadap Pengelolaan Data Pribadi", *Laporan Penelitian*, Jakarta: Pusat Penelitian Setjen DPR RI, 2020, Hal.7.

warga negara dalam UUD NRI Tahun 1945. Pasal 28G ayat (1) UUD NRI Tahun 1945 menyatakan bahwa “setiap orang berhak atas pelindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya, serta berhak atas rasa aman dan pelindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi”. Lebih lanjut, Pasal 28H ayat (4) UUD NRI Tahun 1945, menyatakan bahwa “setiap orang mempunyai hak milik pribadi dan hak milik tersebut tidak boleh diambil alih secara sewenang-wenang oleh siapapun”. Meskipun telah ditegaskan di dalam Deklarasi Umum Hak Asasi Manusia dan juga konstitusi negara kita, namun realitanya aturan tersebut belum berjalan sebagaimana mestinya di dalam melindungi data pribadi konsumen di Indonesia.

Berdasarkan hasil penelitian di lapangan, penyebab penyalahgunaan data pribadi konsumen di era digital disebabkan oleh beberapa faktor: **Pertama**, minimnya pelindungan negara terhadap data pribadi konsumen. Dengan populasi yang besar, Indonesia sebenarnya merupakan pasar yang sangat potensial untuk perkembangan industri ekonomi digital. Namun hingga saat ini, Indonesia belum memiliki undang-undang yang mengatur pelindungan data pribadi secara khusus. Menurut ELSAM,⁴⁹ isu pelindungan data pribadi justru tersebar di dalam 30 aturan perundangan dan turunannya. Akibatnya pelaksanaan dan pengawasan terkait data pribadi juga ikut tersebar di berbagai kementerian atau lembaga sehingga rentan saling tumpang tindih karena tidak terintegrasi dalam konsep besar pelindungan data pribadi. Selain itu, pengaturan data pribadi yang tersebar di 30 undang-undang juga belum sepenuhnya mengacu pada prinsip-prinsip pelindungan data pribadi.

Asia Pasific Economic Cooperation (APEC) Privacy Framework sebagaimana disampaikan oleh Kemenkominfo dalam rapat Panja RUU Pelindungan Data Pribadi Komisi I DPR RI, menyebutkan prinsip-prinsip pelindungan data pribadi meliputi: a) pengumpulan data pribadi dilakukan secara terbatas dan spesifik,

sah secara hukum, patut, dan transparan; b) pemrosesan data pribadi dilakukan sesuai dengan tujuannya; c) pemrosesan data pribadi dilakukan dengan menjamin hak pemilik data pribadi; d) pemrosesan data dilakukan secara akurat, lengkap, tidak menyesatkan, mutakhir, dan dapat dipertanggungjawabkan; e) pemrosesan data pribadi dilakukan dengan melindungi keamanan data pribadi dari pengaksesan yang tidak sah, pengungkapan yang tidak sah, perubahan yang tidak sah, penyalahgunaan, perusakan, dan/atau kehilangan data pribadi; f) pemrosesan data pribadi dilakukan dengan memberitahukan tujuan dan aktivitas pemrosesan, serta kegagalan pelindungan data pribadi; g) data pribadi dimusnahkan dan/atau dihapus setelah masa retensi berakhir atau berdasarkan permintaan pemilik data pribadi kecuali ditentukan lain oleh peraturan perundang-undangan; dan h) pemrosesan data pribadi dilakukan secara bertanggungjawab dengan memenuhi pelaksanaan prinsip pelindungan data pribadi dan dapat dibuktikan secara jelas.⁵⁰

Tersebarannya berbagai aturan terkait data pribadi di dalam 30 undang-undang di Indonesia jika dicermati hanya mengatur mengenai pelindungan data pribadi secara sebagian dan menyesuaikan dengan muatan utama dari peraturan perundang-undangan tersebut. Ketiadaan aturan khusus jelas dapat menimbulkan permasalahan, yakni tidak adanya harmonisasi dalam tataran normatifnya sehingga dikhawatirkan tidak tercapainya kepastian pelindungan hukum yang kuat khususnya bagi pemilik data (konsumen). Pengaturan pelindungan data pribadi sangat penting dan perlu dilakukan di era ekonomi digital untuk melindungi kepentingan konsumen dan memberikan manfaat ekonomi bagi Indonesia. Pengaturan ini nantinya akan melindungi data pribadi konsumen terhadap penyalahgunaan data pada saat data tersebut memiliki nilai ekonomis tinggi untuk kepentingan bisnis. Perkembangan pengaturan terhadap pelindungan data pribadi secara umum juga akan menempatkan Indonesia

49 ELSAM dalam Lidya Suryani, dkk. “Politik Hukum Terhadap Pelindungan Data Pribadi”, *Laporan Penelitian*, Jakarta: Pusat Penelitian Setjen DPR RI, 2019, hlm. 8.

50 Paparan Kementerian Komunikasi dan Informatika dalam Rapat Panja RUU Pelindungan Data Pribadi Komisi I DPR RI, Jakarta: 19 Januari 2021, Hal. 3.

sejajar dengan negara-negara dengan tingkat perekonomian yang maju. Jika hal ini terjadi, akan memperkuat dan memperkuat posisi Indonesia sebagai pusat bisnis dan investasi.

Bagi kepentingan konsumen, perlindungan data pribadi dinilai sangat penting karena menjadi bagian tidak terpisahkan dari perlindungan konsumen. Hal ini dikarenakan peran data sendiri pada dasarnya merupakan bagian dari transaksi antara konsumen dengan pelaku usaha atau pihak penyedia jasa. Terlebih lagi di era ekonomi digital, *big data* memungkinkan untuk para penyedia konten atau penyedia jaringan menyimpan setiap aktivitas pengguna untuk dapat dilakukan *profiling*⁵¹ terhadap pengguna tersebut. Artinya di era ekonomi digital, *big data* memegang peran penting tidak hanya untuk menganalisis potensi pasar, produk, namun juga konsumen. Informasi data pribadi konsumen akan dikumpulkan dari interaksi antara konsumen dengan penyedia jasa yang kemudian akan dianalisis untuk memaksimalkan strategi pengembangan bisnis.

Kegiatan *profiling* tentu akan sangat menguntungkan bagi pelaku usaha namun tidak bagi konsumen. Tindakan tersebut justru dianggap berbahaya apabila tidak diatur dan dibatasi karena dapat merugikan konsumen, mengingat data pribadi konsumen merupakan aset yang berharga, sehingga secara tidak langsung dapat menimbulkan kekhawatiran apabila data pribadi tersebut disalahgunakan tanpa sepengetahuan dan seizin pihak konsumen (pemilik hak). Oleh karena itu, menurut penulis, negara perlu hadir dengan cara benar-benar menjamin perlindungan data pribadi konsumen dengan membentuk aturan khusus perlindungan data pribadi, dimana salah satu materinya perlu menekankan hak dari konsumen selaku pemilik data pribadi untuk mengajukan keberatan atas tindakan *profiling* yang dilakukan pihak pengendali.⁵² Hal

ini bukannya tanpa sebab mengingat selama ini pihak pengendali mempunyai akses untuk mengumpulkan dan menganalisis data pribadi konsumen bahkan tanpa sepengetahuan dan seizin pemilik hak.

Kedua, minimnya akses konsumen terhadap informasi untuk meningkatkan literasi mereka atas hak dan kewajiban konsumen. Masih banyak pemilik data (konsumen) yang merasa bahwa data pribadi bukanlah merupakan hal yang sangat penting untuk dilindungi. Banyak konsumen dengan mudah membagikan informasi terkait data pribadi mereka di sosial media dan cenderung mengabaikan resiko keamanan yang melekat. Akibatnya marak terjadi penyalahgunaan data pribadi di sosial media.⁵³ Dengan jumlah 150 juta pengguna aktif media sosial di Indonesia, konsumen sebaiknya perlu memahami kebijakan privasi suatu *platform* media sosial. Konsumen perlu memahami tujuan pemrosesan, jenis produk, layanan yang disediakan, dan memahami jenis data pribadi serta relevansinya.⁵⁴ Kewajiban konsumen untuk memahami, membaca atau mengikuti petunjuk (kebijakan) telah ditegaskan di dalam Pasal 5 huruf a UU Perlindungan Konsumen, di mana "*konsumen wajib membaca atau mengikuti petunjuk informasi dan prosedur pemakaian atau pemanfaatan barang dan/atau jasa demi keamanan dan keselamatan*".

Untuk mencapai hal tersebut, konsumen perlu dibantu edukasi dengan pihak-pihak terkait. Literasi pemahaman sangat dibutuhkan, hal ini bukannya tanpa sebab mengingat konsumen cenderung langsung menyetujui syarat dan ketentuan yang diberikan pihak pelaku usaha atau penyedia jasa tanpa membaca terlebih dahulu. Tidak mengetahui dengan jelas hak dan kewajiban yang melekat di dalam diri konsumen. Tindakan berlebihan untuk mengunggah kegiatan termasuk data pribadi

salah satu contoh pihak pengendali.

51 Menurut Pasal 10 RUU tentang Pelindungan Data Pribadi, yang dimaksud dengan *profiling* adalah suatu tindakan pengambilan keputusan yang hanya didasarkan pada pemrosesan secara otomatis terkait *profil* seseorang.

52 Pasal 1 angka 3 RUU Pelindungan Data Pribadi menyebutkan yang dimaksud dengan pengendali adalah pihak yang menentukan kendali pemrosesan data pribadi. Pihak bank atau penyedia jasa telekomunikasi merupakan

53 Rita dalam Lidya Suryani, dkk. "Politik Hukum Terhadap Pelindungan Data Pribadi", *Laporan Penelitian*, Jakarta: Pusat Penelitian Setjen DPR RI, 2019, Hal. 44.

54 Direktorat Jenderal Aplikasi Informatika Kementerian Komunikasi dan Informatika Republik Indonesia, 13 Mei 2019, "Pahami Kebijakan Privasi di Media Sosial Untuk Lindungi Data Pribadi", (*online*), (<https://aptika.kominfo.go.id/2019/05/pahami-kebijakan-privasi-di-media-sosial-untuk-lindungi-data-pribadi/>), diakses 23 Juni 2020).

di media sosial justru akan memicu terjadinya kejahatan berupa penyalahgunaan data pribadi. Padahal hak atas data pribadi pada dasarnya merupakan hak yang bersifat *intangibile* sehingga banyak konsumen yang tidak menyadari bahwa publikasi tersebut justru dapat menimbulkan persoalan di kemudian hari. Selain itu, banyak konsumen juga kurang memahami bahwa data pribadi merupakan bagian dari hak asasi manusia yang harus dilindungi, karena secara global kita memiliki kontrol terhadap data pribadi kita sendiri sebagaimana telah dijamin dalam Pasal 12 Deklarasi Universal tentang Hak Asasi Manusia dan Pasal 17 Konvensi Internasional tentang Hak Sipil dan Politik (ICCPR).⁵⁵

Ketiga, minimnya pengetahuan instansi daerah terkait pelindungan data pribadi. Hasil penelitian menunjukkan, minimnya pengetahuan dalam memahami data pribadi tidak hanya dilakukan oleh konsumen, namun hal ini juga berlaku bagi aparat instansi di daerah. Masih banyak instansi di daerah yang belum memahami pentingnya menjaga kerahasiaan data pribadi. Bahkan banyak aparat instansi daerah yang kurang mengetahui adanya aturan pelindungan data pribadi (Peraturan Menteri Komunikasi dan Informatika No. 20 Tahun 2016 tentang Pelindungan Data Pribadi dalam Sistem Elektronik).⁵⁶ Tidak hanya itu saja, banyak file-file data pribadi konsumen dibiarkan begitu saja tanpa adanya penanganan yang baik dan rapi oleh instansi daerah. Instansi daerah kurang memahami bahayanya apabila data pribadi tersebut disalahgunakan oleh oknum yang tidak bertanggungjawab.

Keempat, koordinasi yang buruk antara pusat dan daerah. **Kelima**, masifnya pengumpulan data

pribadi yang tidak hanya dilakukan oleh pemerintah namun juga pihak swasta. Misalnya dalam sektor perbankan, rumah sakit, perusahaan asuransi, telekomunikasi, dan sebagainya. Banyaknya entitas yang terlibat dalam pengumpulan dan penyimpanan data pribadi konsumen secara tidak langsung justru cenderung akan membuka banyak celah terjadinya penyalahgunaan data pribadi konsumen. Ketika kebocoran data terjadi, akan sulit melacak dari mana sumber kebocoran data tersebut.⁵⁷ Untuk itu, penulis berpendapat perlu adanya pembatasan sejauhmana data pribadi itu dapat diberikan oleh pihak swasta. Perlu penegasan klausul di dalam aturan dimana pemilik data berhak untuk menunda atau membatasi data pribadi sesuai dengan tujuan pemrosesan data pribadi. Hal ini sangat penting mengingat selama ini akses yang diberikan kepada pihak penyedia jasa belum diatur secara rinci di dalam peraturan. Selain itu, prinsip-prinsip yang tertuang di dalam pelindungan data pribadi juga perlu ditegaskan khususnya prinsip data minimalisasi. Prinsip data minimalisasi pada dasarnya menekankan bahwa pemrosesan data hanya dapat dilakukan bagi data yang diperlukan dan relevan untuk tujuan yang telah disetujui sebelumnya. Pembatasan akses data pribadi yang dilakukan swasta menjadi sangat penting guna melindungi data pribadi warga negara.

Dampak Penyalahgunaan Data Pribadi Konsumen di Era Ekonomi Digital

Berdasarkan hasil penelitian yang dilakukan oleh penulis di lapangan, dampak dari penyalahgunaan data pribadi konsumen di era ekonomi digital adalah sebagai berikut: **Pertama**, konsumen menjadi pihak pertama yang rentan dan dirugikan terhadap kejahatan dunia maya akibat masifnya pengambilan dan pengumpulan data pribadi. Hal ini bukannya tanpa sebab mengingat pemerintah dan juga pihak swasta dapat melakukan kegiatan pengambilan dan pengumpulan data pribadi konsumen secara sepihak. Pengumpulan data pribadi mulai dari

55 Pelindungan hak atas privasi juga ditegaskan melalui pengaturan dalam Konvensi Internasional Hak-Hak Sipil dan Politik khususnya Pasal 17 yang menyatakan: (1) "Tidak boleh seorangpun yang dapat secara sewenang-wenang atau secara tidak sah dicampuri masalah-masalah pribadinya, keluarganya, rumah, atau hubungan surat-menyuratnya, atau secara tidak sah diserang kehormatan dan nama baiknya". (2) "Setiap orang berhak atas pelindungan hukum terhadap campur tangan atau serangan seperti tersebut di atas".

56 Dinas Komunikasi dan Informatika Statistik Surakarta dalam Lidya Suryani, dkk. "Politik Hukum Terhadap Pelindungan Data Pribadi", *Laporan Penelitian*, Jakarta: Pusat Penelitian Setjen DPR RI, 2019, hlm. 51.

57 APINDO Surakarta dalam Lidya Suryani, dkk. "Politik Hukum Terhadap Pelindungan Data Pribadi", *Laporan Penelitian*, Jakarta: Pusat Penelitian Setjen DPR RI, 2019, hlm. 65.

nama, NIK, alamat tempat tinggal, email, nomor telepon, dan sebagainya dinilai belum mengacu pada standarisasi prinsip perlindungan data pribadi. Jika terjadi permasalahan (sengketa), konsumen akan menjadi pihak yang lemah dan dirugikan, terlebih lagi hasil penelitian menunjukkan bahwa minimnya pengetahuan konsumen terhadap perlindungan data pribadi secara tidak langsung justru melemahkan posisi konsumen sendiri.

Kebanyakan konsumen cenderung tidak aktif bertanya kepada pelaku usaha atau penyedia jasa ketika melakukan sebuah transaksi. Minimnya informasi yang disediakan perusahaan dalam ketentuan perjanjian (klausul baku) yang diajukan kepada konsumen juga ikut memperparah posisi kedudukan konsumen. Konsumen dapat terjebak dengan *term of uses* dalam situs sehingga tanpa sadar memberikan hak untuk menggunakan dan menyebarkan data pribadi miliknya kepada pihak ketiga tanpa sepengetahuan konsumen sebagai pemilik data.⁵⁸ Hal ini bukannya tanpa sebab dikarenakan belum ada aturan yang menyinggung mengenai masalah pembukaan data pribadi dan akuntabilitas perusahaan dalam mengelola data pribadinya di Indonesia. Bahkan aturan yang ada juga sama sekali belum menyinggung mengenai *term of uses* dan *privacy policy* suatu perusahaan yang seharusnya hal ini menjadi hak informasi bagi konsumen.

Banyak perusahaan tidak mencantumkan kewajiban perusahaannya untuk memberikan notifikasi kebocoran atau kerusakan data kepada konsumen. Perusahaan juga sering kali tidak menjelaskan mengenai mekanisme pemulihan data konsumen dimana hak privasi mereka sebenarnya telah dilanggar. Padahal hal ini seharusnya merupakan bentuk komitmen perusahaan dalam melindungi data pribadi konsumen. Lebih lanjut, perusahaan juga sering kali tidak mencantumkan jangka waktu retensi data konsumen yang telah dipergunakan. Memang ada juga perusahaan yang mencantumkan mengenai perihal retensi namun sayangnya tidak menyampaikan secara jelas kepada pihak konsumen berapa lama data

tersebut akan disimpan atau dihancurkan.⁵⁹ Akibatnya konsumen sendiri yang dirugikan. Parahnya di dalam UU Perlindungan Konsumen juga belum mengakomodir kerugian konsumen jika terjadi kebocoran data pribadi.

Penulis berpendapat bahwa selain konsumen diharapkan lebih bijak dan selektif ketika akan memberikan data pribadi mereka, juga perlu adanya ketegasan di dalam undang-undang mengenai batasan data agar konsumen tidak terjebak dalam *term of use*. Batasan tersebut: *pertama*, wajib mendapatkan persetujuan konsumen. Persetujuan pemrosesan data pribadi antara konsumen sebagai pemilik data dengan pihak pengendali ini nantinya dilaksanakan berdasarkan kesepakatan. Kesepakatan tersebut harus jelas, menggunakan bahasa Indonesia, tidak menggunakan singkatan yang membingungkan konsumen. *Kedua*, maksud dan tujuan untuk mengambil data pengguna harus jelas sejak awal serta tipe/jenis informasi seperti apa saja yang akan diambil. Hal ini sesuai dengan Pasal 28 huruf b Permenkominfo No. 20 Tahun 2016 yang menyatakan bahwa “*setiap penyelenggara sistem elektronik wajib menjaga kebenaran, keabsahan, kerahasiaan, keakuratan dan relevansi serta kesesuaian penggunaan data dengan tujuan perolehan, pengumpulan, pengolahan, penganalisisan, penyimpanan, penampilan, pengumuman, pengiriman, penyebaran dan pemusnahan data pribadi*”.

Kedua, terhambatnya investasi. Tidak disangkal bahwa penyalahgunaan data pribadi konsumen di era ekonomi digital dinilai juga akan membawa dampak buruk bagi negara, yakni dapat mengancam kepercayaan investor untuk berinvestasi di Indonesia. Terlebih lagi Indonesia saat ini belum mengatur secara spesifik regulasi perlindungan data pribadi dalam satu undang-undang. Dengan meningkatnya kasus penyalahgunaan data pribadi konsumen tentu para investor akan menolak untuk melakukan kerjasama dengan Indonesia dikarenakan tidak ada jaminan kepastian hukum. Hal ini bukannya

58 Deni Hidayat dalam Lidya Suryani, dkk. “Politik Hukum Terhadap Pelindungan Data Pribadi”, *Laporan Penelitian*, Jakarta: Pusat Penelitian Setjen DPR RI, 2019, hlm. 65.

59 APINDO Surakarta dalam Lidya Suryani, dkk. “Politik Hukum Terhadap Pelindungan Data Pribadi”, *Laporan Penelitian*, Jakarta: Pusat Penelitian Setjen DPR RI, 2019, Hal. 65.

tanpa sebab mengingat kepercayaan bertransaksi antara konsumen dengan pelaku usaha harus tetap dijaga. Jika salah satu pihak merasa tidak aman (*unsecure*) maka ekonomi akan menjadi terhambat. Kebijakan pelindungan data pribadi juga dinilai akan meningkatkan posisi tawar Indonesia dalam melakukan kerjasama dengan negara lain. Hal ini dikarenakan data merupakan aset penting dari ekonomi digital sehingga tidak dapat ditransfer begitu saja dari satu negara ke negara lain. Negara yang sudah memiliki aturan pelindungan data pribadi cenderung tidak akan mau mentransfer data ke negara yang belum memiliki aturan pelindungan data yang paling tidak setara dengan mereka.

Ketiga, dapat merugikan kredibilitas penyedia *platform*. Meningkatnya penyalahgunaan data pribadi konsumen di era ekonomi digital yang dilakukan tanpa seizin pemilik data bukan saja merugikan pihak konsumen namun juga merugikan kredibilitas *platform* yang secara tidak langsung juga ikut merugikan pelaku usaha. Sebagai sebuah identitas, data sudah menjadi hal berharga untuk dapat ditukarkan dengan berbagai macam hal. Salah satu kegunaan data adalah untuk mendaftarkan diri dan mendapatkan layanan dari beragam *platform* digital. *Platform* sendiri merupakan salah satu perangkat elektronik yang termasuk ke dalam sistem elektronik.

Surat Edaran Menteri Komunikasi dan Informatika No. 5 Tahun 2016 tentang Batasan dan Tanggungjawab Penyedia *Platform* dan Pedagang (*Merchant*) Perdagangan Melalui Sistem Elektronik (*Electronic Commerce*) Yang Berbentuk *User Generated Content* telah menyebutkan bahwa *platform* merupakan wadah berupa aplikasi situs internet, dan/atau layanan konten lainnya berbasis internet yang digunakan untuk transaksi dan/atau fasilitas perdagangan melalui sistem elektronik. Penyalahgunaan data pribadi konsumen yang dilakukan oleh oknum yang tidak bertanggungjawab dapat merugikan pelaku usaha (penyedia *platform*) baik kerugian reputasi maupun finansial dimana penyedia *platform* dapat dipersepsikan terlibat atas perbuatan yang melanggar hukum. Persepsi ini

nantinya akan menjadi bumerang bagi penyedia *platform* sendiri jika tidak dilakukan penempatan pada posisi yang tepat karena akan berpengaruh pada kelangsungan bisnis layanannya.

Peran Negara Dalam Memberikan Pelindungan Data Pribadi Konsumen di Era Ekonomi Digital

Dalam beberapa dekade terakhir, dunia telah masuk ke era teknologi internet. Bahkan saat ini internet sudah menjadi *platform* global utamanya dalam bidang perdagangan dan komunikasi, tak terkecuali di Indonesia. Pengakuan pemerintah Indonesia atas keberadaan internet terlihat sejak bergabungnya Indonesia dalam *World Summit on The Information Society* (WSIS) yang dibentuk oleh UNESCO.⁶⁰ Dengan bergabungnya Indonesia melalui WSIS, Indonesia secara tidak langsung berupaya mengejar ketertinggalannya dengan negara-negara yang lebih maju dalam bidang internet seperti negara Eropa dan Amerika.⁶¹

Tidak main-main sejumlah 171,17 juta jiwa atau sekitar 64,8 persen dari total 264 juta jiwa penduduk Indonesia bahkan telah terhubung di internet berdasarkan data APJII tahun 2019.⁶² Lonjakan jumlah pengguna internet dan kemudahan akses informasi kemudian memunculkan variabel baru yang harus dilindungi, salah satunya yakni data pengguna. Data pengguna lazim digunakan dalam *platform* digital. Meskipun memberikan kemudahan, namun penggunaan *platform* digital rentan terhadap penyalahgunaan.⁶³

Dengan makin maraknya penyalahgunaan data pribadi konsumen di era ekonomi digital,

60 Klik Legal.com, 15 Mei 2020, "Pelindungan Data Pada Platform Digital Melalui Pembentukan Komisi Privasi dan Data Protection Officer (DPO)", (*online*), (<https://kliklegal.com/perlindungan-data-pada-platform-digital-melalui-pembentukan-komisi-privasi-dan-data-protection-officer-dpo/>), diakses 5 Juli 2020).

61 Muhammad Rustam, "Internet dan Penggunaannya (Survei di Kalangan Masyarakat Kabupaten Talakar Provinsi Sulawesi Selatan)", *Jurnal Studi Komunikasi dan Media*, Vol. 21 No. 1, Januari 2017, hal. 13-24.

62 Klik Legal.com, 15 Mei 2020, "Pelindungan Data Pada Platform Digital Melalui Pembentukan Komisi Privasi dan Data Protection Officer (DPO)", (*online*), (<https://kliklegal.com/perlindungan-data-pada-platform-digital-melalui-pembentukan-komisi-privasi-dan-data-protection-officer-dpo/>), diakses 5 Juli 2020).

63 *Ibid.*

secara tidak langsung menempatkan Indonesia pada posisi urgensi untuk segera menerbitkan aturan hukum yang mengikat guna mengatur dan menjamin perlindungan data pribadi baik yang dikelola oleh pemerintah maupun swasta. Pengamanan berupa landasan hukum diperlukan guna mencegah kejahatan dan menyelesaikan permasalahan yang terjadi khususnya di era ekonomi digital. Hal ini bukannya tanpa sebab mengingat Forum Ekonomi Dunia (*World Economic Forum*) menyebutkan bahwa pertumbuhan digitalisasi dan konektivitas internet yang demikian cepat telah menjelma menjadi tulang punggung revolusi industri keempat, dan berpotensi untuk mendorong model bisnis yang inovatif serta menciptakan transformasi bangunan politik dan sosial.⁶⁴

Pentingnya urgensi pengukuhan pengamanan data pribadi juga telah disinggung Presiden Jokowi dalam pidato kenegaraan pada tahun 2019 dimana aturan untuk melindungi kedaulatan data harus segera dilakukan. Kedaulatan data harus diwujudkan guna melindungi hak warga negara atas data pribadi mengingat data memiliki nilai komoditas yang berharga karena dapat diperjualbelikan atau dimanfaatkan untuk memperoleh keuntungan sehingga menjadi sumber daya baru bagi bangsa.⁶⁵ Bahkan laporan *The Economist* tahun 2017 juga menyebutkan bahwa saat ini sumber daya yang paling berharga bukanlah minyak, melainkan data karena dianggap sebagai entitas berharga guna mendorong kegiatan yang menguntungkan.⁶⁶

Meskipun hingga saat ini Indonesia belum memiliki aturan hukum yang secara spesifik mengatur mengenai perlindungan privasi dan data pribadi. Namun jaminan akan perlindungan data pribadi konsumen di Indonesia telah

ditegaskan di dalam konstitusi negara kita dan juga setidaknya bersinggungan dengan beberapa aturan perundang-undangan yang juga mengatur mengenai data pribadi. Tercatat ada sekitar 30 aturan perundang-undangan di Indonesia yang juga mengatur mengenai data pribadi, sebut saja misalnya: UU No. 44 Tahun 2009 tentang Rumah Sakit⁶⁷, UU No. 14 Tahun 2008 tentang Keterbukaan Informasi Publik⁶⁸, dan UU No. 36 Tahun 2009 tentang Kesehatan yang mengatur mengenai rahasia kondisi pribadi pasien⁶⁹, UU No. 7 Tahun 1992 tentang Perbankan sebagaimana diubah dengan UU No. 10 Tahun 1998 tentang Perubahan atas UU No. 7 Tahun 1992 tentang Perbankan yang mengatur mengenai data pribadi nasabah penyimpan dan simpanannya⁷⁰, UU No. 36 Tahun 1996 tentang Telekomunikasi yang mengatur mengenai privasi dan data pribadi⁷¹, UU No. 39 Tahun 1999 tentang Hak Asasi Manusia yang mengatur mengenai perlindungan diri pribadi⁷², UU No. 24 Tahun 2013 tentang Administrasi Kependudukan yang mengatur mengenai perlindungan data pribadi⁷³, UU No.

67 Pasal 32 huruf I UU No. 44 Tahun 2009 tentang Rumah Sakit menyatakan bahwa setiap pasien berhak mendapatkan privasi dan kerahasiaan penyakit yang diderita termasuk data-data medisnya.

68 Pasal 17 huruf h angka 2 UU No. 14 Tahun 2008 tentang Keterbukaan Informasi Publik menyatakan bahwa setiap badan publik wajib membuka akses bagi setiap pemohon informasi publik untuk mendapatkan informasi publik kecuali salah satunya mengenai riwayat, kondisi dan perawatan, pengobatan kesehatan fisik, dan psikis seseorang, karena apabila dibuka dan diberikan kepada pemohon informasi publik dapat mengungkapkan rahasia pribadi.

69 Pasal 57 ayat (1) UU No. 36 Tahun 2009 tentang Kesehatan menyatakan bahwa setiap orang berhak atas rahasia kondisi kesehatan pribadinya yang telah dikemukakan kepada penyelenggara pelayanan kesehatan.

70 Pasal 40 ayat (1) UU No. 10 Tahun 1998 tentang Perbankan menyatakan bahwa bank wajib merahasiakan keterangan mengenai nasabah penyimpan dan simpanannya.

71 Pasal 42 ayat (1) UU No. 36 Tahun 1996 tentang Telekomunikasi yang menyatakan bahwa penyelenggara jasa telekomunikasi wajib merahasiakan informasi yang dikirim dan/atau yang diterima oleh pelanggan jasa telekomunikasi melalui jaringan telekomunikasi dan/atau jasa telekomunikasi yang diselenggarakan.

72 Pasal 29 ayat (1) UU No. 39 Tahun 1999 tentang Hak Asasi Manusia menyatakan bahwa setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan hak miliknya.

73 Pasal 1 angka 22 UU no. 23 Tahun 2014 tentang

64 Tempo.com, 26 April 2017, "Dorong Ekonomi Digital, Pakar: Perlu UU Pelindungan Data Pribadi", (*online*), (<https://bisnis.tempo.co/read/869696/dorong-ekonomi-digital-pakar-perlu-uu-perlindungan-data-pribadi/full&view=ok>, diakses 5 Juli 2020).

65 Klik Legal.com, 15 Mei 2020, "Pelindungan Data Pada Platform Digital Melalui Pembentukan Komisi Privasi dan Data Protection Officer (DPO)", (*online*), (<https://kliklegal.com/perlindungan-data-pada-platform-digital-melalui-pembentukan-komisi-privasi-dan-data-protection-officer-dpo/>, diakses 5 Juli 2020).

66 *Ibid.*

19 Tahun 2016 tentang Informasi dan Transaksi Elektronik yang mengatur mengenai larangan pemindahan data pribadi secara sewenang-wenang⁷⁴. Selain itu, ada beberapa aturan turunannya untuk pelindungan data pribadi seperti PP No. 82 Tahun 2016 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, dan SE OJK No. 14/SEOJK.07/2014 tentang Kerahasiaan dan Keamanan Data dan/atau Informasi Pribadi Konsumen.

Beragam aturan yang mengatur mengenai data pribadi tanpa disadari justru berakibat pada tumpang tindihnya mekanisme dan kewenangan dalam melakukan pelindungan data pribadi itu sendiri. Hal ini dikarenakan adanya perbedaan sudut pandang dalam hal tujuan pengolahan data pribadi, notifikasi atau persetujuan pemilik data, rentang waktu retensi data pribadi, penghapusan data pribadi, tujuan pembukaan data pribadi kepada pihak ketiga, serta sanksi bagi pelanggar pelindungan data pribadi. Misalnya dalam hal pembukaan data pribadi, dimana KUHAP dan UU No. 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik menyebutkan kewenangan polisi untuk membuka data pribadi seseorang harus berdasarkan Ketua Pengadilan Negeri. Sementara pada undang-undang lainnya, yaitu UU No. 8 Tahun 2010 tentang Tindak Pidana Pencucian Uang dan UU No. 19 Tahun 2019 tentang Komisi Pemberantasan Tindak Pidana Korupsi tidak membutuhkan izin Ketua Pengadilan Negeri dalam mengakses data pribadi melainkan cukup hanya berdasarkan bukti dan izin dari ketua lembaga internal.

Contoh lainnya, dalam hal ruang lingkup data pribadi, dimana UU No. 7 Tahun 2017 tentang Pemilihan Umum memperbolehkan partai politik untuk mengakses salinan daftar pemilih tetap (DPT) yang berisi data pribadi.

Administrasi Kependudukan menyatakan bahwa data pribadi adalah data perorangan tertentu yang disimpan, dirawat, dan dijaga kebenaran serta dilindungi kerahasiaannya. Lebih lanjut Pasal 2 huruf c UU no. 23 Tahun 2014 tentang Administrasi Kependudukan menyatakan setiap penduduk mempunyai hak untuk memperoleh pelindungan atas data pribadi.

74 Pasal 26 ayat (1) UU No. 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik menyatakan bahwa setiap pemindahan data pribadi seseorang harus terlebih dahulu mendapatkan izin dari pemilik data.

Sementara UU Adminduk justru mengharuskan bahwa data pribadi harus disimpan, dirawat, dan dijaga kebenarannya serta dilindungi kebenarannya. Terlepas dari adanya perbedaan tersebut, pada dasarnya peran negara dalam melindungi data pribadi konsumen di era ekonomi digital dapat dilakukan dengan cara: **pertama**, segera membentuk aturan tersendiri/khusus mengenai pelindungan data pribadi. Saat ini, Pemerintah bersama dengan Komisi I DPR RI sedang membahas mengenai RUU tentang Pelindungan Data Pribadi. Masuknya RUU Pelindungan Data Pribadi ke dalam Prolegnas Prioritas tahun 2020 menjadi tanda bukti bahwa negara telah berkomitmen untuk memberikan penguatan terhadap pelindungan data pribadi di Indonesia. Hal ini sesuai dengan teori kepastian dan pelindungan hukum.

Teori kepastian hukum yang dikemukakan oleh Hans Kelsen mengartikan hukum sebagai suatu norma. Norma merupakan suatu pernyataan yang menekankan aspek “seharusnya” atau *das sollen*, dengan menyertakan beberapa peraturan tentang apa yang harus dilakukan.⁷⁵ Tiap-tiap manusia memiliki kebebasan, tetapi dalam hidup bersama ia memikul tanggung jawab untuk menciptakan hidup bersama yang tertib.⁷⁶ Untuk mewujudkan hidup bersama yang tertib tersebut, diperlukan pedoman-pedoman yang efektif yang harus dipatuhi bersama pula. Pedoman inilah yang disebut dengan hukum. Jika hukum telah menentukan pola perilaku tertentu, maka tiap orang seharusnya berperilaku sesuai pola yang telah ditentukan tersebut.

Sementara pelindungan hukum menurut Satjipto Raharjo, yakni memberikan pengayoman terhadap Hak Asasi Manusia (HAM) yang dirugikan orang lain dan pelindungan itu diberikan kepada masyarakat agar dapat menikmati semua hak-hak yang diberikan oleh hukum.⁷⁷ Roscoe Pound mengemukakan hukum merupakan alat rekayasa sosial (*law as tool of*

75 Bernard L. Tanya, dkk. *Teori Hukum Strategi Tertib Manusia Lintas Ruang dan Generasi*, Yogyakarta: Genta Publishing, 2010, hlm. 127.

76 *Ibid.*

77 Satjipto Raharjo, *Ilmu Hukum*, Bandung: PT. Citra Aditya Bakti, 2000, hlm. 54.

social engineering). Kepentingan manusia adalah suatu tuntutan yang dilindungi dan dipenuhi manusia dalam bidang hukum. Roscoe Pound membagi kepentingan manusia yang dilindungi hukum menjadi 3 (tiga) macam, yakni: *pertama*, kepentingan terhadap negara sebagai salah satu badan yuridis; *kedua*, kepentingan sebagai negara sebagai penjaga kepentingan sosial; dan *ketiga*, kepentingan terhadap perseorangan terdiri dari pribadi (*privacy*).⁷⁸

Kedua teori tersebut saling berkaitan yaitu kepastian hukum diperlukan untuk mewujudkan adanya perlindungan hukum. Pembahasan RUU Pelindungan Data Pribadi yang sedang berlangsung antara DPR RI dan pemerintah sangat dinanti banyak orang tak terkecuali konsumen. RUU Pelindungan Data Pribadi pantas dijadikan momentum karena konsumen berhak mendapatkan kepastian dan perlindungan hukum atas data pribadi mereka agar tidak disalahgunakan oleh oknum yang tidak bertanggungjawab. Hak-hak tersebut diatur di dalam Bab III tentang hak pemilik data pribadi Pasal 4 s.d. Pasal 16 RUU Pelindungan Data Pribadi, seperti hak atas informasi. Pasal 4 RUU Pelindungan Data Pribadi menyatakan bahwa "*pemilik data pribadi berhak meminta informasi tentang kejelasan identitas, dasar kepentingan hukum, tujuan permintaan dan penggunaan data pribadi, dan akuntabilitas pihak yang meminta data pribadi*". Ini artinya konsumen sebagai pemilik data nantinya berhak mengetahui bagaimana data pribadinya akan diolah, termasuk ketika akan dimanfaatkan oleh pihak ketiga. Pihak penyelenggara dataupun juga harus menginformasikan seluruh kerjasama pengelolaan data kepada pemilik data.

Selanjutnya hak untuk mengakses, dimana pemilik data berhak untuk meminta salinan data pribadi yang dikuasai atau dikendalikan oleh pengendali data. Pasal 6 RUU Pelindungan Data Pribadi menyebutkan bahwa "*pemilik data berhak mengakses data pribadi miliknya sesuai dengan ketentuan perundang-undangan*". Dari ketentuan tersebut misal seorang pasien rumah sakit di daerah ketika ingin melakukan perawatan ke rumah sakit lain maka dapat meminta data rekam

medis (*medical record*) untuk dibawa ke rumah sakit lain yang akan merawatnya lebih lanjut. Hak untuk menuntut dan menerima ganti rugi juga diatur di dalam Pasal 13 RUU Pelindungan Data Pribadi, yang menyatakan bahwa "*pemilik data pribadi berhak menuntut dan menerima ganti rugi atas pelanggaran data pribadi miliknya sesuai dengan ketentuan peraturan perundang-undangan*".

Sementara UU Perlindungan Konsumen sendiri belum mengakomodir kepastian hukum jika terjadi penyalahgunaan data pribadi konsumen mengingat data dan informasi yang diatur di dalam UU Pelindungan Konsumen adalah informasi mengenai kondisi barang dan jasa, bukan informasi mengenai data pribadi konsumen. Padahal Pasal 2 UU Pelindungan Konsumen secara jelas menyatakan bahwa perlindungan konsumen berasaskan manfaat, keadilan, keseimbangan, keamanan dan keselamatan konsumen, serta kepastian hukum sehingga perlindungan konsumen juga seyogyanya mencakup pula perlindungan data dan informasi.

Data pribadi konsumen sangat rentan untuk disalahgunakan mengingat data pribadi konsumen pada dasarnya sering dikaitkan ketika konsumen menggunakan jasa atau membeli suatu barang. Misalnya penyalahgunaan data pribadi akibat promosi yang dilakukan oleh penyedia layanan/pelaku usaha untuk kepentingan tertentu. Tindakan promosi memang diatur di dalam Pasal 1 angka 6 UU Perlindungan Konsumen⁷⁹ namun sayangnya di dalam UU Pelindungan Konsumen sendiri justru tidak mengatur ketentuan larangan kegiatan promosi yang menggunakan data pribadi konsumen tanpa seizin/sepersetujuan yang bersangkutan. Pasal 9 UU Pelindungan Konsumen hanya melarang pelaku usaha untuk menawarkan, memproduksi, mengiklankan suatu barang dan/atau jasa yang tidak benar. Ketentuan tersebut tidak menyinggung mengenai perlindungan data pribadi konsumen. Oleh karena itu konsumen tidak memiliki dasar

79 Pasal 1 angka 6 UU No. 8 Tahun 1999 tentang Pelindungan Konsumen menyatakan bahwa promosi adalah kegiatan pengenalan atau penyebarluasan informasi suatu barang dan/atau jasa untuk menarik minat beli konsumen terhadap barang dan/atau jasa yang akan dan sedang diperdagangkan.

hukum kuat guna menjamin hak privasi sebagai konsumen sehingga UU Perlindungan Konsumen masih memiliki ruang kosong atau celah dan menyebabkan pelaku usaha tidak menghormati hak privasi atas data pribadi konsumen. Beberapa hal di atas menunjukkan meskipun penerapan pelindungan data pribadi secara sektoral sudah diatur di dalam beberapa aturan perundangan, namun masih diperlukan aturan khusus yakni undang-undang pelindungan data pribadi yang dapat menyelesaikan masalah lintas sektoral, mengingat model bisnis ekonomi digital bersifat kompleks dan lingkupnya lintas sektoral.

Kedua, membentuk lembaga khusus pelindungan data pribadi. Pembentukan lembaga khusus diperlukan tidak hanya untuk mengawasi dan melindungi data pribadi agar tidak disalahgunakan baik dari korporasi maupun pemerintah, tetapi juga bertugas menangani sengketa pelindungan konsumen. Untuk upaya pencegahan penyalahgunaan data pribadi, lembaga ini nantinya juga diharapkan dapat mendorong kesadaran publik. Sebagai bahan perbandingan, Uni Eropa sudah memiliki lembaga khusus pelindungan data pribadi (*Data Protection Authority* atau DPA) yang bertugas mengawasi pertukaran data pribadi. Mengacu pada regulasi umum pelindungan data (*General Data Protection Regulation* atau GDPR), DPA bersifat independen dan tidak terafiliasi dengan pemerintah maupun pihak swasta manapun. Terkait dengan hal tersebut, maka pembentukan lembaga khusus pelindungan data pribadi sangat diperlukan mengingat banyak entitas yang terlibat di dalam kegiatan pengumpulan dan penyimpanan data di Indonesia. Terlebih lagi, aturan mengenai data pribadi nantinya akan mengikat semua pihak, baik dari sektor publik, swasta, dan pemerintah. Oleh karena itu sebaiknya lembaga khusus tersebut nantinya bersifat independen dan memiliki anggaran sendiri tidak menempel pada lembaga lain.

Ketiga, memberikan sanksi tegas dan mengikat. Aturan perundang-undangan yang ada selama ini dinilai belum maksimal dalam memberikan sanksi bagi penyalahgunaan data pribadi, misalnya UU ITE. Pasal 26 UU ITE telah

menegaskan bahwa penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan orang yang bersangkutan dan bahwa setiap orang yang dilanggar haknya dapat mengajukan gugatan namun sayangnya norma tersebut tidak mengatur secara rinci bagaimana mekanisme ketentuan yang mewajibkan kepada lembaga-lembaga siapa saja yang diberikan tanggungjawab sebagai penugasan untuk melaksanakan kewajiban tersebut. Hal inilah yang menyebabkan potensi penyalahgunaan data pribadi marak terjadi. Tidak ada konsekuensi hukum (sanksi) bagi lembaga yang bertanggungjawab dan bagi pelanggar sendiri ketentuan ini masih berupa pasal karet sehingga mudah ditafsirkan meluas dan batasan-batasannya tidak jelas.

Sementara di dalam RUU Pelindungan Data Pribadi, sanksi tegas diberikan tidak hanya bagi pengendali data namun juga pihak prosesor data dan/atau pihak ketiga yang terbukti dengan sengaja dan melawan hukum melakukan penyalahgunaan data pribadi. Sanksi yang diberikan pun tidak hanya pidana namun juga perdata, bahkan ganti kerugian imateriil lebih ditekankan di dalam RUU ini. Sanksi tegas dan mengikat diperlukan tidak hanya untuk konflik antar pribadi, swasta/korporasi namun juga lembaga negara. Tidak dipungkiri bahwa potensi penyalahgunaan data pribadi dapat juga dilakukan oleh negara misalnya dalam hal ketika negara berhubungan atau melakukan kerjasama perjanjian kerja dengan pihak swasta. Pengumpulan data secara masif yang dilakukan oleh negara dinilai riskan membuka celah terjadinya penyalahgunaan data pribadi yang dilakukan oleh negara. Sayangnya di dalam RUU Pelindungan Data Pribadi justru belum mengakomodir aturan sanksi terhadap lembaga negara. Oleh karena itu, menurut penulis, dalam hal negara berkomitmen memberikan pelindungan data pribadi maka negara perlu membuat aturan di mana di dalamnya terdapat sanksi bagi negara manakala negara melakukan pelanggaran terhadap pelindungan data pribadi. Dengan demikian, maka rakyat akan merasa terlindungi dari penyalahgunaan kewenangan atau kekuasaan yang memperlakukan data

pribadi masyarakat (konsumen) untuk kepentingan sepihak.

PENUTUP

Kesimpulan

Urgensi perlindungan data pribadi konsumen di era digital sangat penting untuk segera diberlakukan. Masuknya era digital yang dipadukan dengan fenomena dan potensi *big data*, mengakibatkan data pribadi telah menjelma menjadi suatu komoditas berharga. Hal ini bukannya tanpa sebab mengingat pengembangan ekonomi digital terbukti dapat mendorong pertumbuhan ekonomi. Meskipun memiliki nilai ekonomis tinggi, perlindungan data pribadi konsumen masih belum maksimal. Masih banyak penyalahgunaan data pribadi yang meresahkan konsumen sebagai pemilik data. Hal ini dipengaruhi oleh beberapa faktor: a) minimnya perlindungan negara terhadap data pribadi konsumen; b) minimnya akses konsumen terhadap informasi untuk meningkatkan literasi mereka atas hak dan kewajiban konsumen; c) minimnya pengetahuan instansi daerah terkait perlindungan data pribadi; d) koordinasi yang buruk antara pusat dan daerah; dan e) masifnya pengumpulan data pribadi yang tidak hanya dilakukan oleh pemerintah namun juga pihak swasta. Adapun dampak penyalahgunaan data pribadi konsumen dapat mengakibatkan: a) konsumen menjadi pihak pertama yang rentan dan dirugikan terhadap kejahatan dunia maya akibat masifnya pengambilan dan pengumpulan data pribadi; b) timbulnya kerugian negara; dan c) dapat merugikan kredibilitas penyedia *platform*. Adanya faktor penyebab dan timbulnya dampak penyalahgunaan data pribadi tersebut menuntut tanggung jawab negara dalam melaksanakan fungsi perlindungan (*protection function*) atas data pribadi setiap manusia sebagai bentuk pengakuan, penghormatan, dan perlindungan hak asasi manusia sebagaimana diamanatkan oleh UUD NRI Tahun 1945. Untuk itu, peran negara dalam melindungi data pribadi konsumen di era ekonomi digital dapat dilakukan dengan cara: membentuk aturan tersendiri/khusus mengenai perlindungan data pribadi, membentuk

lembaga khusus perlindungan data pribadi, dan memberikan sanksi tegas dan mengikat.

Saran

Berdasarkan kesimpulan tersebut, maka terdapat beberapa saran atau rekomendasi untuk perlindungan data pribadi: *pertama*, RUU tentang Pelindungan Data Pribadi perlu segera diselesaikan dan disahkan di tahun 2021 demi menciptakan kepastian dan perlindungan hukum khususnya bagi konsumen. *Kedua*, perlu dibentuk lembaga independen regulator data pribadi yang setara dengan komisi perlindungan data pribadi agar pemanfaatan data pribadi terpantau dengan maksimal, termasuk pemanfaatannya oleh negara. Dengan demikian, adanya lembaga independen tersebut diharapkan tidak ada lagi *abuse of power* dari negara terkait data pribadi masyarakat (konsumen). *Ketiga*, perlu ada sanksi yang tegas dan mengikat, bagi perseorangan, korporasi, maupun negara, mengingat penerapan sanksi di dalam RUU Pelindungan Data Pribadi masih dinilai rancu.

DAFTAR PUSTAKA

Buku

- Ramli, Ahmad (2004). *Cyber law dan HAKI dalam Sistem Hukum Indonesia*, Bandung: PT. Refika Aditama.
- Raharjo, Satjipto. (2000). *Ilmu Hukum*, Bandung: PT. Citra Aditya Bakti.
- Smith, Rhona K.M. (2010). *Hukum Hak Asasi Manusia*, Yogyakarta: PUSHAM UI.
- Rosadi, Sinta Dewi (2015). *Cyber Law Aspek Data Privasi Menurut Hukum Internasional, Regional, dan Nasional*, Bandung: PT. Refika Aditama.
- Tanya, Bernard L.dkk. (2010). *Teori Hukum Strategi Tertib Manusia Lintas Ruang dan Generasi*, Yogyakarta: Genta Publishing.

Jurnal

- Aditya Nugraha, Rifha. (2018). Pelindungan Data Pribadi dan Privasi Penumpang Maskapai Penerbangan Pada Era Big Data, *Jurnal Mimbar Hukum*, Vol. 30 No. 2.
- Ansori, Aan. (2016). Digitalisasi Ekonomi Syariah, *Jurnal Ekonomi Keuangan dan Bisnis Islam*, Vol. 7 No. 1.
- Dewi, Sinta. (2016). Konsep Pelindungan Hukum Atas Privasi dan Data Pribadi Dikaitkan Dengan Penggunaan *Cloud Computing* di Indonesia, *Jurnal Yustisia*, Vol.5 No. 1.
- Dewi, Sinta. (2018). Pelindungan Privasi dan Data Pribadi Dalam Era Ekonomi Digital di Indonesia, *Jurnal Vej*, Volume 4 No. 1.
- Indriyani, Masitoh. dkk. (2017). Pelindungan Privasi dan Data Pribadi Konsumen Daring Pada Online Marketplace System, *Justitia Jurnal Hukum*, Vol.1, No. 2.
- Pujianto, Agung.dkk. (2018). Pemanfaatan Big Data dan Pelindungan Privasi Konsumen di Era Ekonomi Digital, *Majalah Ilmiah Bijak*, Vol. 15 No. 2.
- Rustam, Muhammad. (2017). Internet dan Penggunaannya (Survei di Kalangan Masyarakat Kabupaten Talakar Provinsi Sulawesi Selatan), *Jurnal Studi Komunikasi dan Media*, Vol. 21 No. 1.
- Sautunnida, Lia. (2018). Urgensi Undang-Undang Pelindungan Data Pribadi di Indonesia Studi Perbandingan Hukum Inggris dan Malaysia, *Kanun Jurnal Ilmu Hukum*, Vol. 20 No. 2.

Internet

- Akbar, Cesar. (2020), Kasus Data Bocor, DPR: Tokopedia Harus Bertanggungjawab, (*online*), (<https://bisnis.tempo.co/read/1338931/kasus-data-bocor-dpr-tokopedia-harus-bertanggung-jawab>, diakses 11 Januari 2021)
- Antara News.com. (2020) Kemkominfo: Indonesia Urutan Kelima Pengguna Internet, (*online*), (<https://www.antaranews.com/berita/219498/kemkominfo-indonesia-urutan-lima-pengguna-internet>, diakses 11 Januari 2021).
- Aprilianti, Ira. (2020). Opini Hari Konsumen Nasional Pelindungan Data Pribadi di Tengah Pandemi Covid-19. (*online*), (<https://www.cips-indonesia.org/post/opini-hari-konsumen-nasional-perlindungan-data-pribadi-di-tengah-pandemi-covid-19>, diakses 22 Juni 2020).
- Clinton, Bill. (2020), Jokowi: Ekonomi Digital Indonesia Terbesar di Asia Tenggara. (*online*), (<https://tekno.kompas.com/read/2020/02/27/18010097/jokowi-ekonomi-digital-indonesia-terbesar-di-asia-tenggara>, diakses 8 Juni 2020).
- CNN Indonesia.com. (2020) Data Pengguna Dicuri, Menkominfo-Tokopedia Digugat ke PN. (*online*), (<https://www.cnnindonesia.com/teknologi/20200507175240-192-501083/data-pengguna-dicuri-menkominfo-tokopedia-digugat-ke-pn>, diakses 5 Juli 2020).
- Jaringan Prima.co.id. (2019), Potensi Ekonomi Digital di Indonesia. (*online*), (<https://www.jaringanprima.co.id/id/potensi-ekonomi-digital-di-indonesia>, diakses 31 Mei 2020).
- Kamus Besar Bahasa Indonesia. (2020). Pengertian Data Pribadi. (*online*) (<https://kbbi.web.id/data>, diakses 23 Juni 2020).
- Klik Legal.com. (2020), Pelindungan Data Pada Platform Digital Melalui Pembentukan Komisi Privasi dan Data Protection Officer (DPO). (*online*), (<https://kliklegal.com/perlindungan-data-pada-platform-digital-melalui-pembentukan-komisi-privasi-dan-data-protection-officer-dpo/>, diakses 5 Juli 2020).
- Kominfo.go.id. (2020), Masuki Era Digital Indonesia Butuh UU Pelindungan Data Pribadi. (*online*), (<https://aptika.kominfo.go.id/2020/02/masuki-era-digital-indonesia-butuh-uu-pelindungan-data-pribadi/>, diakses 31 Mei 2020).
- Kominfo.go.id. (2020). Perkembangan Ekonomi Digital di Indonesia: Strategi dan Sektor Potensial, (*online*), (https://www.google.co.id/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwi7pafFhqXvAhXTW3wKHR3yBr0QFjABegQIARAD&url=https%3A%2F%2Fbalitbangs.dm.kominfo.go.id%2Fpublikasi_665_3_230&u sg=AOvVaw1fXsBhZKCCWxcCRU-G8EUi, diakses Jumat 7 November 2020).

Kompasiana.com. (2018), Menakar Kebijakan Pelindungan Privasi di Era Digital. (*online*) (https://www.kompasiana.com/kanopi_febui/5afec2c95e137354db5a6a82/menakar-kebijakan-perlindungan-privasi-di-era-digital?page=all, diakses 31 Mei 2020).

Kompasiana.com. (2019), Resolusi Industri 4.0, Perlunya Pelindungan Data Pribadi. (*online*) (<https://www.kompasiana.com/machsvorming/5dc575ffd541df266011b652/revolusi-industri-4-0-perlunya-perlindungan-data-pribadi>, diakses 8 Juni 2020)

Media Indonesia.com. (2021). Kedaulatan Data Pribadi. (*online*), (https://mediaindonesia.com/editorials/detail_editorials/1757-kedaulatan-data-pribadi, diakses 16 Januari 2021).

Nistanto, Reska K. (2016). Kebocoran Go-Jek Memuncak, Rute Sehari-Hari Pengguna Bisa Dilacak. (*online*), (https://Tekno.Kompas.Com/Read/2016/01/20/16031307/___Kebocoran.Go-Jek.Memuncak.Rute.Sehari-Hari.Pengguna.Bisa.Dilacak, diakses 11 September 2019)

Setianti, Lintang. (2019) Urgensi Regulasi Pelindungan Data Pribadi di Indonesia. (*online*) (<https://indonesiana.tempo.co/read/68772/2016/04/04/lintangsetianti/urgensi-regulasi-pelindungan-data-pribadi-di-indonesia>, diakses 23 Februari 2019).

Tempo Online. (2019) Urgensi Regulasi Pelindungan Data Pribadi di Indonesia. (*online*), (<https://indonesiana.tempo.co/read/68772/2016/04/04/lintangsetianti/urgensi-regulasi-pelindungan-data-pribadi-di-indonesia>, diakses 23 Februari 2019).

Tribun Online. (2019). Data E-KTP Dan KK Warga Diperjualbelikan Secara Illegal. (*online*) (<https://video.tribunnews.com/view/88310/data-e-ktp-dan-kk-warga-diperjualbelikan-secara-ilegal>, diakses Kamis 12 September 2019).

Warta Ekonomi.co.id. (2016) Manfaat Ganda Pengembangan Ekonomi Digital. (*online*) (<https://www.wartaekonomi.co.id/read124515/manfaat-ganda-pengembangan-ekonomi-digital>, diakses 31 Mei 2020).

Peraturan Perundang-undangan

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.

Indonesia, Undang-Undang No. 8 Tahun 1999 tentang Pelindungan Konsumen. Undang-Undang Nomor 8, LN No. 42 Tahun 1999. TLN. No. 3821.

Indonesia, Undang-Undang No. 24 Tahun 2013 tentang Perubahan Atas Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan. Undang-Undang Nomor 24, LN No. 232 Tahun 2013. TLN. No.5475.

Indonesia, Undang-Undang No. 19 Tahun 2016 tentang Perubahan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Undang-Undang Nomor 19, LN No. 251 Tahun 2016. TLN. No. 5952.

Indonesia, Undang-Undang No. 44 Tahun 2009 tentang Rumah Sakit. Undang-Undang Nomor 44, LN No. 153 Tahun 2009. TLN. No. 5072.

Indonesia, Undang-Undang No. 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Undang-Undang Nomor 14, LN No. 61 Tahun 2008. TLN. No. 4846.

Indonesia, Undang-Undang No. 10 Tahun 1998 tentang Perbankan. Undang-Undang Nomor 10, LN No. 182 Tahun 1998. TLN. No. 3790.

Indonesia, Undang-Undang No. 36 Tahun 2009 tentang Kesehatan. Undang-Undang Nomor 36, LN No. 144 Tahun 2009. TLN. No. 5063.

Dokumen Lainnya

Hasil wawancara penelitian kelompok dengan judul Politik Hukum Terhadap Pelindungan Data Pribadi di Provinsi Jawa Tengah dan Provinsi Sulawesi Selatan.

Hasil wawancara penelitian AKD dengan judul Optimalisasi Pelindungan terhadap Pengelolaan Data Pribadi di Indonesia di Provinsi Jawa Timur dan Kabupaten Garut.