PENGATURAN PERLINDUNGAN DATA PRIBADI DI INDONESIA

PERSPEKTIF TEORI KEADILAN BERMARTABAT

Rizky P.P. Karo Karo, S.H., M.H.
Prof. Dr. Teguh Prasetyo, S.H., M.Si

PENGATURAN PERLINDUNGAN DATA PRIBADI DI INDONESIA

PERSPEKTIF TEORI KEADILAN BERMARTABAT

NUSAMEDIA

PENGATURAN PERLINDUNGAN DATA PRIBADI DI INDONESIA

PERSPEKTIF TEORI KEADILAN BERMARTABAT

Oleh
Rizky P.P. Karo Karo, S.H., M.H
Prof. Dr. Teguh Prasetyo, S.H., M.Si.

NUSAMEDIA

Katalog Dalam Terbitan (KDT)

Pengaturan Perlindungan Data Pribadi di Indonesia; Perspektif Teori Keadilan Bermartabat

—Bandung: 2020
xii+341 hal.; 140x210 mm
ISBN: 978-602-6913-88-3

Cetakan I: Juli 2020

Diterbitkan oleh
Penerbit Nusa Media
PO Box 137 Ujungberung, Bandung

Disain cover: MF Mahardika
Tata Letak: Nusamed Studio

KATA SAMBUTAN

Rektor Universitas Pelita Harapan
Dr. (Hon.) Jonathan L. Parapak, M. Eng. Sc.

Law as a tool of social engineering (hukum adalah alat merekayasa masyarakat). Ungkapan *Roscoe Pound* ini tentu tidak asing di telinga dan hati orang hukum. Namun, dalam perkembangannya, bukan hanya hukum melainkan teknologi (internet) juga menjadi alat rekayasa sosial sehingga berlakulah *Law and Technology (Internet) as tools of social engineering*.

Manusia dari pelbagai umur, dari *Baby Boomer-Generation* (1946-1964) sampai dengan *Alpha Generation* (2011-2024) tidak asing lagi dengan *smartphone,* internet, media sosial *(facebook, instagram, twitter, youtube), whatsapp, Tokopedia, OVO* dan beberapa mulai menerapkan teknologi *Blockchain* dan aplikasi *online* dan lain sebagainya - terlebih pada tahun 2020 ini di kala seluruh umat manusia dan korporasi menghadapi pandemi *Covid-19*.

Apakah penggunaan aplikasi *online,* teknologi berbahaya? Jawabannya adalah tergantung. Apabila teknologi internet tersebut dipergunakan untuk kebaikan maka hasilnya akan membawa kedamaian, persatuan; namun apabila disalahgunakan maka akan menimbulkan kerugian, baik

kerugian materiil bagi pengguna, kerugian imateriil bagi pengguna, persatuan dan Bangsa Indonesia.

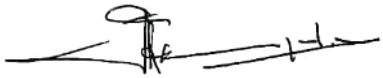
Pelbagai *platform* yang disebutkan diatas membutuhkan data pribadi yang harus dimasukkan ke dalam sistem elektronik untuk dapat digunakan. Calon pengguna mau tidak mau harus memasukkan data pribadi termasuk namun tidak terbatas pada nama, alamat domisili, alamat *e-mail,* nomor ponsel, bahkan beberapa mengharuskan untuk mengunggah foto diri beserta KTP (Kartu Tanda Penduduk) untuk mendapatkan layanan ekstra. Calon pengguna pelbagai aplikasi *online* tersebut hanya memiliki 2 (dua) pilihan, *yes or no, agree or disagree* atau *take it or leave it* dan pada umumnya pengguna hanya memilih *yes, agree* karena jika memilih tidak, maka aplikasi *online* tersebut tidak dapat dimanfaatkan.

Saya menyambut baik buku yang disusun oleh Prof. Dr. Teguh Prasetyo, S.H, M.Si dan Dosen muda Fakultas Hukum Universitas Pelita Harapan, Saudara Rizky P.P. Karo Karo, S.H, M.H. yang berjudul "Pengaturan Perlindungan Data Pribadi di Indonesia: Perspektif Teori Keadilan Bermartabat". Saya paham betul dengan konsep 'keadilan bermartabat' yang digagas oleh Prof. Teguh yang memiliki tujuan yang mulia, yakni memanusiakan manusia atau dalam Bahasa Jawa *'Nguwongke Uwong'.* Data pribadi wajib dijaga kerahasiaannya karena merupakan hak asasi, hak privasi yang berlaku secara universal dan dilindungi dalam amanat konstitusi Bangsa Indonesia. Penyelenggara baik lingkup privat ataupun publik wajib menjaga keamanan data pribadi dari potensi kebocoran data pribadi, potensi jual beli data, karena hal tersebut melawan hukum *(onrechmatige daad).*

Selamat atas kerja keras penyusunan buku ini yang dimulai dari akhir tahun 2019 dan menurut saya buku ini dapat

dipergunakan oleh pelbagai kalangan, masyarakat umum terlebih yang awam hukum, pengguna aplikasi *online,* pegiat hukum siber, pemerhati teknologi, advokat yang menggeluti hukum teknologi dan penegak hukum lainnya.

Jakarta, 2 Juni 2020



Dr. (Hon.) Jonathan L. Parapak, M.Eng.Sc
Rektor Universitas Pelita Harapan

KATA SAMBUTAN

Dekan Fakultas Hukum Universitas Pelita Harapan
Prof. Dr. Bintan R. Saragih, S.H.

Saya. sebagai Pimpinan Fakultas Hukum Universitas Pelita Harapan menyambut baik penerbitan buku "Pengaturan Perlindungan Data Pribadi di Indonesia: Perspektif Keadilan Bermartabat". Buku ini dapat dijadikan acuan, bahan/referensi dan mengisi kekosongan buku-buku tentang hukum siber, tentang perlindungan data pribadi.

Perkembangan teknologi internet memberikan manfaat bagi umat manusia sebagai individu dan korporasi sebagai pelaku usaha. Teknologi, aplikasi *online* digunakan untuk transaksi *online,* melakukan *virtual meeting* dengan *video conference,* mengajar*/online class,* melakukan perizinan berusaha terintegrasi secara elektronik *(Online Single Submission),* melakukan persidangan secara elektomik *(e-court)*

Penggunaan aplikasi *online* tersebut membutuhkan data pribadi berupa nama, alamat, nomor *HP, Email,* tempat tanggal lahir. Data pribadi adalah privasi setiap individu warga negara yang wajib dijaga dan dilindungi oleh Pemerintah, oleh Penyelenggara Sistem Elektronik baik di sektor privat atau publik.

Amanat Pasal 28G ayat (1) Undang-undang Dasar Negara Republik Indonesia Tahun 1945 dengan tegas bahwa '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". Jual beli data, kebocoran data baik yang disebabkan oleh kesengajaan atau kelalaian penyelenggara adalah perbuatan melawan hukum (*onrechmatige daad)* sehingga pelaku ataupun penyelenggara wajib bertanggung jawab apabila perbuatan melawan hukum tadi terbukti sebagai bentuk perlindungan terhadap konsumen/pengguna aplikasi tersebut.

Saya menilai, buku ini dapat digunakan oleh seluruh kalangan, termasuk juga penegak hukum, legislator yang saat ini sedang menyusun Rancangan Undang-Undang Pelindungan Data Pribadi (RUU PDP). Demikian, saya sambut baik penerbitan buku ini dan teruslah berkarya!

Jakarta Selatan, 28 Mei 2020

Dekan Fakultas Hukum UPH
Prof. Dr. Bintan R. Saragih. S.H.

KATA PENGANTAR

Penulis memanjatkan syukur dan rahmat kepada Tuhan Yang Maha Esa yang memberikan hikmat, dan nikmat serta kesehatan sehingga buku ini dapat selesai. Penulis berharap agar buku ini dapat dimanfaatkan oleh pelbagai pihak, oleh masyarakat sebagai konsumen/pengguna layanan aplikasi online, oleh pelaku usaha/penyelenggara, oleh penegak hukum (polisi, advokat, jaksa, hakim) dan juga masyarakat umum.

Perkembangan teknologi, internet berkembang dengan pesat. Perkembangan tersebut membawa dampak negatif dan positif. Teknologi memudahkan manusia untuk bekerja, bertransaksi elektronik, berkomunikasi, menjaga hubungan/relasi dengan keluarga tetap berjaga, bahkan juga dipergunakan untuk keperluan penegakan hukum (e-litigation, memeriksa saksi menggunakan video conference, melakukan perizinan online). Namun, apabila oknum tidak memiliki martabat yang baik maka oknum tersebut menggunakan otak/ilmu yang dimiliki untuk melakukan perbuatan melawan hukum, misalnya melakukan peretasan, penipuan menggunakan layanan teknologi.

Manusia, korporasi sebagai subyek hukum pada abad ke-21 tidak dapat tidak dilepaskan dari aplikasi online, sistem elektronik yang dikembangkan oleh penyelenggara sistem elektronik (penyelenggara/aplikator). Syarat untuk menggunakan aplikasi online adalah pengguna/konsumen wajib memasukan data

pribadi ke dalam sistem tersebut dan apabila ingin menggunakan layanan ekstra/tambahan dari aplikasi tersebut, pengguna diwajibkan menggunggah foto diri sambil memegang Kartu Tanda Penduduk (KTP) ke dalam sistem tersebut. Konsumen/ pengguna tidak memiliki pilihan dalam aplikasi online pada saat harus mengisi disclaimer, karena pilihannya hanya yes or no, agree or disagree. Jika tidak memilih yes/agree maka konsumen/ pengguna tidak dapat menggunakan aplikasi online tersebut.

Data pribadi merupakan wujud/personifikasi perpanjangan diri manusia/badan hukum dalam sistem elektronik. Manusia/ badan hukum cukup dengan memasukan data pribadi termasuk namun tidak terbatas pada nama, nomor ponsel, e-mail (surat elektronik), nomor rekening setelah memasukan data pribadi tersebut maka konsumen/pengguna dapat melakukan perbuatan hukum melalui aplikasi online. Penyelenggara wajib menjaga, melindungi data pribadi pengguna/konsumen dari oknum yang tidak bertanggung jawab. Namun, dugaan kebocoran data pribadi, praktik jual beli data pribadi marak terjadi di Negara di dunia, khususnya di Indonesia. Data pribadi dijual dengan harga tertentu, dan diberi harga tinggi jika data yang dijual memiliki riwayat tabungan/riwayat keuangan. Kebocoran data pribadi akan menimbulkan dugaan tindak pidana lainnya, misalnya penipuan, diganggu oleh telemarketer yang menawarkan pelbagai produk di sektor jasa keuangan.

Keadilan bermartabat berangkat dari postulat sistem; bekerja mencapai tujuan, yaitu keadilan bermartabat. Keadilan yang memanusiakan manusia atau keadilan yang 'nge wong ke wong'. Konsepsi keadilan bermartabat digali dari falsafah Bangsa Indonesia. Jati diri Bangsa Indonesia, yang termanifestasikan dalam Pancasila. Pancasila merupakan sumber dari segala sumber

hukum dan sebagai ideologi, sebagai falsafah bangsa dan Negara.

Keadilan bermartabat berhubungan erat dengan penggunan teknologi, dan kewajiban perlindungan data pribadi. Penyelenggara memiliki kewajiban menjaga data pribadi pengguna/konsumen, pemilik data pribadi memiliki hak hukum karena merupakan hak privasi/hak asasi manusia (HAM). Penyelenggara memiliki tanggung jawab memberikan ganti rugi kepada pengguna/konsumen dan memperbaiki sistem keamanan apabila terbukti terjadi kebocoran data. keadilan bermartabat bertujuan untuk menyeimbangkan, membuat serasi kepentingan pelaku usaha, konsumen. Keadilan bermartabat bertujuan untuk menjaga hak privasi, melindungi konsumen dari penyalahgunaan data pribadi karena konsumen berada di posisi lemah, tidak berdaya melawan perusahaan teknologi yang besar, kuat.

Saat ini, pengaturan perlindungan data pribadi masih tersebar di pelbagai peraturan perundang-undangan dan peraturan yang fokus mengatur tentang perlindungan data pribadi adalah berbentuk Peraturan Menteri Komunikasi dan Informatika. Saat penyusunan buku ini (Desember – Juli 2020), Pemerintah sedang menyusun dengan saksama, cermat Rancangan Undang-undang Pelindungan Data Pribadi (RUU PDP). RUU PDP masuk ke dalam Program Legislasi Nasional Prioritas. Salah satu pengaturan dalam RUU PDP yakni ada ketentuan/delik 'jual-beli' data pribadi diancam dengan pidana penjara sekian waktu tertentu atau pidana denda dengan nominal tertentu. General Data Protection Regulation (GDPR) di Uni Eropa menjadi salah satu acuan (wisdom/nilai internasional) dalam penyusunan RUU PDP namun yang harus diperhatikan dan dijunjung tinggi dalam penyusunan

RUU PDP yakni wajib tetap mengutamakan nilai luhur, filosofi Bangsa&Negara Indonesia yakni Pancasila.

Keadilan bermartabat tidak anti dengan wisdom/ nilai internasional. Apabila ada pertentangan dengan nilai internasional dalam prinsip GDPR maka Pancasila sebagai local wisdom adalah yang digunakan dan untuk mengadaptasikannya/menyaringnya sesuai nilai Bangsa sehingga terjadi penggabungan dan harmonisasi.

Oleh karena itu, keadilan bermartabat bertujuan untuk membuat pengaturan perlindungan data pribadi sesuai dengan nilai-nilai Pancasila dan bertujuan agar penegakan hukum jika terjadi kebocoran data pribadi tidak hanya bertujuan untuk menghukum pelaku (penggabungan sanksi&tindakan/double track system), namun juga harus memberikan pemulihan kepada konsumen melalui pendekatan kuratif (curative approach) sehingga menghasilkan konsep kebaharuan triple track system.

Akhir kata, Penulis mengucapkan terimakasih kepada Sri Purnama, Agrippina Ngadiman dan Olivia Celia Sebayang dan para pihak yang telah memberikan dukungan dalam penyusunan buku ini, kepada keluarga, rekan-rekan di Fakultas Hukum UPH, rekan dosen lainnya, teman-teman Penulis yang memiliki minat dan bekerja di dunia IT.

Penulis mengharapkan kritik dan saran yang dapat disampaikan melalui e-mail atau sarana lain dari para pembaca agar kedepannya Penulis dapat lebih baik lagi karena Penulis sadar bahwasanya kesempurnaan hanyalah milik Tuhan Yang Maha Esa.

Penulis,
Jakarta, 20 Mei 2020

DAFTAR ISI

DAFTAR GRAFIK

DAFTAR TABEL

DAFTAR GAMBAR

GLOSARIUM/DAFTAR SINGKATAN

No	Singkatan	Keterangan
1	**AFPI**	Asosiasi Fintech Pendanaan Bersama Indonesia
2	***AI***	*Artificial Intelligence*
3	***APEC***	*Asia – Pacific Economic Cooperation*
4	**APS**	Alternatif Penyelesaian Sengketa, misalnya mediasi, negosiasi, arbitrase
5	***B2B***	*Business to Business*
6	***B2C***	*Business to Consumer*
7	***B2G***	Business to Government
8	**BUMN**	Badan Usaha Milik Negara
9	***C2C***	Consumer to Consumer
10	***C2G***	*Consumer to Government*
11	**CPNS**	Calon Pegawai Negeri Sipil
12	**Directive 95/46/EC**	The Data Protection Directive 95/46
13	***E2EE***	End to End Encryption
14	***E-Commerce***	*Electronic Commerce* (Perdagangan secara elektronik)
15	***E-court***	Layanan bagi Penggunan Terdaftar untuk Pendaftaran Perkara secara *online,* mendapatkan taksiran panjar biaya perkara secara *online* , pembayaran secara *online,* pemanggilan yang dilakukan dengan saluran elektronik, dan persidangan yang dilakukan secara elektronik.
16	***EDI***	Electronic Data Interchange
17	***Email***	*Electronic Mail* (Surat Elektronik)
18	***FB***	*Facebook*

19	***G2G***	Government to Government
20	***GAR 45/95***	Guidelines for the Regulation of Computerized Personal Data Files
21	***GDPR***	General Data Protection Regulation
22	**HAM**	Hak Asasi Manusia
23	***HIR***	*Het Herziene Indonesisch Reglement* (*HIR* atau Reglement Indonesia yang diperbaharui: S. 1848 No. 16, S. 1941 No. 44)
24	***HP***	*Handphone*
25	***ICCPR***	*International Covenant on Civil and Political Rights*
26	**IKD**	Inovasi Keuangan Digital
27	***IoE***	*Internet of Everything*
28	***ISO***	*International Organization for Standardization*
29	***jo.***	*Juncto*
30	***JWP***	*Joint Work Programme*
31	**KK**	Kartu Keluarga
32	**KKMMD**	Kedaruratan Kesehatan Masyarakat yang Meresahkan Dunia
33	**Kominfo**	Kementerian Komunikasi dan Informatika
34	**Konvensi Eropa 108/1981**	*The Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data No. 108 Year 1981*
35	**KTP**	Kartu Tanda Penduduk
36	**Kuh.Perdata**	Kitab Undang-Undang Hukum Perdata
37	**KUHAP**	Kitab Undang-undang Hukum Acara Pidana
38	**KUHP**	Kitab Undang-undang Hukum Pidana
39	**LPPM UPH**	Lembaga Penelitian dan Pengabdian Masyarakat Universitas Pelita Harapan
40	**Menkominfo**	Menteri Komunikasi dan Informatika (Menkominfo) pada Kabinet Indonesia Maju (2019-sekarang) Johny G. Plate
41	**NIK**	Nomor Induk Kependudukan
42	**NPWP**	Nomor Pokok Wajib Pajak
43	***OECD***	*The Organization for Economic Cooperation and Development*
44	**OJK**	Otoritas Jasa Keuangan
45	***OSS***	*Online Single Submission*

46	***OTP***	*One Time Password*
47	***P2P***	*Peer to Peer Lending (*Pinjaman *Online)*
48	**Perma 13/2016**	Peraturan Mahkamah Agung Republik Indonesia No. 13 Tahun 2016 tentang Tata Cara Penangananan Perkara Tindak Pidana oleh Korporasi
49	**Permendagri 102/19**	Peraturan Menteri Dalam Negeri Republik Indonesia Nomor 102 Tahun 2019 tentang Pemberian Hak Akses Pemanfaatan Data
50	**Permenkominfo 4/2016**	Peraturan Menteri Komunikasi dan Informatika No. 4 Tahun 2016 tentang Sistem Manejemen Pengamanan Infromasi
51	**Permenkominfo PDPSE**	Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik
52	**Perpres 54/2015**	Peraturan Presiden Nomor 54 Tahun 2015 tentang Kementerian Komunikasi dan Informatika
53	***PHEIC***	*Public Health Emergency of International Concern*
54	***PIN***	*Personal Identification Number*
55	**POJK 13/2018**	Peraturan Otoritas Jasa Keuangan Nomor 13/POJK.02/2018 tentang Inovasi Keuangan Digital di Sektor Jasa Keuangan
56	**POJK 77/2016**	Peraturan Otoritas Jasa Keuangan Nomor 77/POJK.01/2016 tentang Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi
57	**PP Adminduk**	Peraturan Pemerintah No. 40 Tahun 2019 tentang Pelaksanaan Undang-undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan sebagimana telah diubah dengan Undang-undang No. 24 Tahun 2013 tentang Perubahan Atas Undang-undang No. 23 Tahun 2006 tentang Administrasi Kependudukan
58	**PP PMSE**	Peraturan Pemerintah No. 80 Tahun 2019 tentang Perdagangan Melalui Sistem Elektronik

59	**PP PSTE**	Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik
60	**PPATK**	Pusat Pelaporan dan Analisis Transaksi Keuangan
61	***Rbg***	*Rechtsglement Buitengewesten (Rbg. atau Reglement* daerah seberang: S. 1927 No. 227) untuk luar Jawa dan Madura
62	**RKUHP**	Rancangan Undang-undang tentang Kitab Undang-undang Hukum Pidana (Pembahasan September 2019)
63	**RUU PDP**	Rancangan Undang-undang tentang Pelindungan Data Pribadi (Pembahasan per Desember 2019)
64	**SEOJK Perjanjian Baku**	Surat Edaran Otoritas Jasa Keuangan Nomor 13/SEOJK.07/2014 tentang Perjanjian Baku
65	***SMS***	*Short Message Service*
66	**UPH**	Universitas Pelita Harapan
67	**UU 12/2005**	Undang-undang No. 12 Tahun 2005 tentang Pengesahan *International Covenant on Civil and Political Rigts* (Konvenan Internasional tentang Hak-Hak Sipil dan Politik)
68	**UU Admin Pemerintahan**	Undang-undang No. 30 Tahun 2014 tentang Administrasi Pemerintahan
69	**UU ADMINDUK**	Undang-undang No. 24 Tahun 2013 tentang Perubahan Atas Undang-Undang No. 23 Tahun 2006 tentang Administrasi Kependudukan
70	**UU HAM**	Undang-undang No. 39 Tahun 1999 tentang Hak Asasi Manusia
71	**UU ITE**	Undang-undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-undang No. 19 Tahun 2016
72	**UU Perbankan**	Undang-Undang No.10 tahun 1998 tentang Perubahan Atas Undang-Undang Nomor 7 tahun 1992 tentang Perbankan
73	**UU Perdagangan**	Undang-Undang No. 7 Tahun 2014 tentang Perdagangan
74	**UU Perlinkos**	Undang-undang No. 8 tahun 1999 tentang Perlindungan Konsumen

75	**UU Praktik Kedokteran**	Undang-undang No. 29 Tahun 2004 tentang Praktik Kedokteran
76	**UUD 1945**	Undang-Undang Dasar Negara Kesatuan Republik Indonesia Tahun 1945;
77	***WHO***	*World Health Organization*
78	***WWW***	*World Wide Web*

BAB I

PERKEMBANGAN TEKNOLOGI, KOMUNIKASI, DAN INFORMATIKA

I. Perkembangan Teknologi, Komunikasi, Dan Informatika

Tuhan Yang Maha Esa menciptakan manusia menurut gambaran-Nya, memberikan manusia akal budi-pemikiran sehingga terpikirkan dasar-dasar/filosofi kehidupan, filsafat ilmu, tercipta ilmu pengetahuan, teknologi dari yang mudah sampai dengan sulit, Tuhan Yang Maha Esa memberikan hikmat untuk memutus suatu sengketa agar berisikan keadilan bermartabat bagi hakim/pimpinan, untuk melakukan pekerjaan yang baik bagi manusia lainnya (*nguwongke uwong*/ memanusiakan manusia) atau hidup dalam keharmonisan antar kehidupan bemasyarakat (*men and women for and with others)*, tidak serakah, sehingga dari akal budi/pikiran tersebut manusia dapat bertahan hidup (*survive)*.

'Perkembangan' (*development-eng; de ontwikkeling-dutch)* ataupun 'Perubahan' (*transformation-eng; een vernadering-dutch)* adalah kepastian. Kita pasti ingat dengan kehidupan manusia pada zaman dahulu baik melalui pelajaran sejarah, mengunjungi museum, yakni, pada zaman batu (*palaeolithikum*, *mesozoikum, neolitikum)* hingga pada zaman logam (zaman, tembaga, dan

besi) yang mana teknologi-teknologi pada zaman tersebut masih sangat sederhana (misalnya pada zaman *neolithikum*, manusia bertahan hidup dengan cara bercocok tanam) namun dapat dimanfaatkan oleh manusia karena akal budi, pemberiaan Sang Pencipta. Dan kehidupan manusia berkembang dengan pesat pada masa revolusi industri (sekitar tahun 1750-1850) di Inggris. **Penulis** mengutip dari *website: britannica.com* bahwa banyak sekali penemuan penting akibat revolusi industri.

> *"Important inventions of the Industrial Revolution included the steam engine. used to power steam locomotives, steamboats, steamships, and machines in factories; electric generators and electric motors; the incandescent lamp (light bulb); the telegraph and telephone; and the internal-combustion engine and automobile, whose mass production was perfected by henry ford, in the early 20th century*[1]*."*

Revolusi Industri di Inggris tersebut dapat dikatakan sebagai revolusi industri 1.0. Namun, sekarang revolusi industri tersebut sudah pada revolusi industri 4.0[2]., era *Society 5.0*[3]. dan pada era *internet of everything*[4] *(IoE)*.

---

[1] https://www.britannica.com/event/Industrial-Revolution diakses tanggal 1 Maret 2020

[2] Pemerintah Indonesia telah menetapkan langkah terhadap industri 4.0. ini dengan menetapkan 10 prioritas nasional untuk "Making Indonesia 4.0." yakni: 1. Perbaikan alur aliran material; 2. Mendesain ulang zona industri; 3. Akomodasi standar *sustainability;* 4. Pemberdayaan UMKM; 5. Membangun infrastruktur digital nasional; 6. Menarik investasi asing; 7. Peningkatan kualitas SDM; 8. Pembentukan ekosistem inovasi; 9. Menerapkan insentif investasi teknologi; 10. Harmonisasi aturan dan kebijakan. (Sumber: Kementerian Perindustrian, "Making Indonesia 4.0." yang telah disampaikan pada Seminar Nasional Standardisasi Badan Standardisasi Nasional (BSN), Surabaya 25 Oktober 2018.

[3] "Implementasi dari Society 5.0 ini meliputi pengolahan data yang masif di ruang maya (cyberspace) yang dikumpulkan dari aktivitas manusia dan benda-benda fisik lainnya. Hasil olahan tersebut akan menjadi dasar dalam keputusan yang menciptakan efisiensi, keamanan, kenyamanan, kesehatan, serta distribusi kesejahteraan yang lebih berimbang". Dikutip dari https://www.its.ac.id/news/2019/06/13/bagaimana-industri-4-0-dan-society-5-0-bantu-ciptakan-kesejahteraan/, diakses tanggal 20 Maret 2020.

[4] Hingga penyusunan buku ini, belum ada definsi baku tentang *internet of*

Cara manusia berkomunikasi dari masa ke masa juga mengalami perubahan dan perkembangan. Apabila pada zaman dahulu, manusia menggunakan tanda untuk berkomunikasi, mengirimkan pesan bahkan menggunakan burung merpati sebagai penyampai pesan dan berkembang menggunakan telegraf kemudian telepon kabel serta akhirnya berkembang menjadi *smartphone*, dan didukung dengan media internet.

Pada abad ke-21, manusia tidak dapat dilepaskan dari penggunaan *gadget,* gawai, komputer, *laptop, smartphone* dan internet. Seluruh kehidupan manusia bergantung pada teknologi, jika dahulu ibu-ibu hanya membeli sayur di pasar, namun sekarang dapat dilakukan dengan *smartphone* secara *online (*dalam jaringan/daring – dalam Bahasa Indonesia). Kita dapat melakukan apapun dengan *smartphone, laptop* kita, kita dapat memesan tiket transportasi, kita dapat membeli barang kebutuhan pokok, kita dapat mengirimkan uang, kita dapat melihat kondisi rumah kita dengan *CCTV (closed circuit television)* yang terkoneksi dengan *HP*, kita dapat memesan makanan, bahkan Pemerintahan juga telah menerapkan pelayanan mereka dengan teknologi internet atau biasa dikenal dengan *E-Governance* ataupun *E-Government* misalnya dengan penggunaan *online single submission (OSS)* menurut **Olivia Sebayang, dkk**

> *"the OSS system is also integrated with the Online General Law Administration (AHU Online) system of the Ministry of Law and Human Rights because it relates to the status of a business entity as a legal entity as well as with the Population and Civil Registry Office. Checking NPWP (Nomor Pokok Wajib Pajak) and business entity status is one of a series of intial*

everything (IoE) namun menurut hemat **Penulis,** *IoE* adalah sistem elektronik yang sangat bergantung dengan internet dan *artificial intelligence* untuk membawa manusia dengan manusia, badan hukum dengan perwakilannya melakukan suatu proses/perbuatan dan membutuhkan data untuk saling terhubung dengan tujuan peningkatan ekonomi, peningkatan layanan birokrasi, dan peningkatan sosial.

stages of issuing business licenses in OSS. The next stages, business actors are required to upload several documents or fulfill requirements and/or commitments so that the status of the business license granted become effective".[5]

Hakim pemeriksa perkara menggunakan layanan *video conference* untuk memeriksa saksi dalam suatu perkara. Para peneliti (mahasiswa, *jurist)* juga melakukan penelitian, *legal research* melalui *artificial intelligence. Machine learning algorithms have already demonstrated some capacity to assist legal decision-makers. Further development of these methods has the potential to reduce inefficiencies and bolster the productivity of legal practitioners*[6].

Aktivitas dalam dunia maya, dunia internet tersebut membutuhkan data pribadi yang wajib dimasukan secara sadar oleh pengguna (*user)* ke dalam sistem elektornik penyelenggara sistem elektornik (*platform)*. Menurut hemat **Penulis,** banyak ahli mendefinisikan data pribadi. Namun, menurut **Penulis,** data pribadi adalah informasi tunggal ataupun sekumpulan informasi yang dapat dilihat, didengar, dibaca tentang seseorang/badan hukum yang dihimpun ke dalam sistem elektronik dan dipergunakan untuk tujuan yang disepakati, serta wajib dijaga kerahasiaanya.

Namun, tidak semua orang menggunakan akal budi, pengetahuanya dengan baik dan bermartabat sebagaimana dipaparkan diatas. Orang tertentu, oknum dengan pelbagai

[5] Inggarwati, M. P., Celia, O., & Arthanti, B. D. (2020). Online Single Submission For Cyber Defense and Security in Indonesia. *Lex Scientia Law Review*, *4*(1), 89-102. https://journal.unnes.ac.id/sju/index.php/lslr/article/view/37709/16023 diakses tanggal 11 Mei 2020

[6] Jonathan Jenkins, *"What Can Information Technology Do for Law?", Harvard Journal of Law&Technology, Vol. 21, No. 2, (Harvard University, Massachusetts,* 2008 diakses dari http://jolt.law.harvard.edu/articles/pdf/v21/21HarvJLTech589.pdf tanggal 10 Mei 2020), Hlm. 602.

cara dan untuk memperoleh keuntungan pribadi dapat menyalahgunakan data pribadi tersebut, mereka dapat meretas media elektronik, sistem elektronik, mereka dapat menjual data pribadi tersebut dengan posisi/jabatan yang mereka duduki sekarang, mereka dapat menyalahgunakan data pribadi tersebut seolah-olah pemilik data pribadi yang sah sehingga menimbulkan transaksi keuangan yang melawan hukum – sangat berbahaya. Pertanyaan kritis lebih lanjut, peretas / *hacker* tersebut lebih baik diapakan? Mereka memiliki kemampuan untuk meretas sistem keamanan bahkan sistem keamanan elektronik milik Pemerintah, apakah cukup hanya dengan diberi sanksi penjara selama beberapa tahun? Apakah ada cara lain yang dapat memartabatkan para penyalahguna kemampuan *IT* tersebut? Inilah tugas bersama kita untuk dapat memartabatkan kemampuan *hacker* yang salah arah tersebut.

Pengembangan teknologi adalah hak asasi manusia, hak untuk terus maju dengan pemanfaatan teknologi. Berdasarkan Pasal 13 Undang-undang No. 39 Tahun 1999 tentang Hak Asasi Manusia (UU HAM) bahwa "Setiap orang berhak untuk mengembangkan dan memperoleh manfaat dari ilmu pengetahuan dan teknologi, seni dan budaya sesuai dengan martabat manusia demi kesejahteraan pribadinya, bangsa, dan umat manusia".

Pemerintah telah berupaya untuk mengejar ketertinggalan hukum dari teknologi (*het recht hink achter de feiten aan)*. Pada tahun 2008, Pemerintah telah menerbitkan Undang-undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-undang No. 19 Tahun 2016 (selanjutnya disebut UU ITE). Pertimbangan

dibentuknya UU ITE sangatlah mulia yakni: pertama, bahwa pembangunan nasional adalah suatu proses yang berkelanjutan yang harus senantiasa tanggap terhadap berbagai dinamika yang terjadi di masyarakat; kedua, bahwa globalisasi informasi telah menempatkan Indonesia sebagai bagian dari masyarakat informasi dunia sehingga mengharuskan dibentuknya pengaturan mengenai pengelolaan Informasi dan Transaksi Elektronik di tingkat nasional sehingga pembangunan Teknologi Informasi dapat dilakukan secara optimal, merata, dan menyebar ke seluruh lapisan masyarakat guna mencerdaskan kehidupan bangsa; ketiga, bahwa perkembangan dan kemajuan Teknologi Informasi yang demikian pesat telah menyebabkan perubahan kegiatan kehidupan manusia dalam berbagai bidang yang secara langsung telah memengaruhi lahirnya bentuk-bentuk perbuatan hukum baru; keempat, bahwa penggunaan dan pemanfaatan Teknologi Informasi harus terus dikembangkan untuk menjaga, memelihara, dan memperkukuh persatuan dan kesatuan nasional berdasarkan Peraturan Perundang-undangan demi kepentingan nasional; kelima, bahwa pemanfaatan Teknologi Informasi berperan penting dalam perdagangan dan pertumbuhan perekonomian nasional untuk mewujudkan kesejahteraan masyarakat; keenam, bahwa pemerintah perlu mendukung pengembangan Teknologi Informasi melalui infrastruktur hukum dan pengaturannya sehingga pemanfaatan Teknologi Informasi dilakukan secara aman untuk mencegah penyalahgunaannya dengan memperhatikan nilai-nilai agama dan sosial budaya masyarakat Indonesia.

Selain UU ITE, Pemerintah melalui Instansi yang berwenang telah membuat peraturan sektoral untuk mengejar ketertinggalan hukum dari teknologi, 2 (dua) diantaranya: Peraturan Menteri

Komunikasi dan Informatika No. 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik; Peraturan Otoritas Jasa Keuangan No. 77 / POJK. 01/2016 tentang Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi, dan pelbagai peraturan perundang-undangan lainnya.

Teknologi, internet memudahkan kehidupan manusia, baik dalam komunikasi, melakukan transaksi elektronik, berbelanja, melakukan *video conference,* melakukan peradilan secara elektronik (*e-court, e-litigation)*. Teknologi membuat hubungan masyarakat menjadi tidak terbatas (*borderless, cyberspace)*, pengembang teknologi memiliki peluang untuk melakukan usaha di bidang bisnis teknologi namun harus menjunjung tinggi prinsip persaingan usaha sehat dan prinsip kehati-hatian (*prudential principle)*. Namun, dibalik pengembangan teknologi, internet yang baik, terdapat oknum yang menyalahgunakan kepintarannya untuk melakukan perbuatan melawan hukum, mencuri data pribadi dan memperjualbelikannya di *darkweb* (*web* gelap, halaman *website* yang berbahaya). Pelaku usaha di bidang teknologi, penyelenggara sistem elektronik (aplikasi *online)* wajib menjalankan usahanya dengan berlandaskan keadilan bermartabat. Keadilan bermartabat berangkat dari postulat sistem; bekerja mencapai tujuan, yaitu keadilan bermartabat. Keadilan yang memanusiakan manusia atau keadilan yang '*nge wong ke wong'*. Konsepsi keadilan bermartabat digali dari falsafah Bangsa Indonesia. Jati diri Bangsa Indonesia, yang termanifestasikan dalam Pancasila. Pancasila merupakan sumber dari segala sumber hukum dan sebagai *ideology*, sebagai falsafah bangsa dan Negara[7].

[7] Konsep keadilan bermartabat dilahirkan dan digagas oleh Prof. Dr. Teguh Prasetyo, S.H., M.Si. (Guru Besar Fakultas Hukum Universitas Pelita Harapan)

Teknologi, para pihak yang menyelenggarkan apabila tidak menjalankan keadilan bermartabat maka teknologi tersebut akan rentan dengan pelbagai persamalahan hukum. Hukum, masyarakat, teknologi sangat berkaitan satu sama lain.

II. Hubungan Hukum, Masyarakat dan Teknologi: Interaksi dan Interdependensi

Hukum mengawal pelbagai aktifitas, seluruh kehidupan manusia di setiap saat. Sebelum manusia itu lahir hukum sudah mulai mencampuri urusanya, begitu pula setelah dia lahir hingga dia meninggal dunia dan ketika jasadnya sudah dimakamkan bahkan setelah meninggal hukum masih bersinggungan dengan harta peninggalan (warisan) orang tersebut. Hukum melahirkan hak kepada seorang anak yang lahir yakni hak atas ibu dan bapak. Hukum juga membebani kewajiban kepada orang tua terhadap bayi yang baru dilahirkan itu. Hukum menjadikan manusia dan/atau badan hukum (korporasi) sebagai subyek hukum[8].

Manusia dengan segala sifat, psikologisnya (misalya: introvert, ekstrovert, ambivert) pasti hidup bermasyarakat, saling berinteraksi baik secara langsung ataupun tidak langsung melalui media komunikasi dan internet. Oleh karenanya, hukum, masyarakat dan teknologi saling memiliki keterkaitan satu sama lain, saling mempengaruhi satu sama lain demi mendapatkan rasa keadilan yang bermartabat (*nguwongke uwong*-Bahasa Jawa, memanusiakan manusia-Bahasa Indonesia) **Penulis** mengimajinasikannya dalam grafik berikut

[8] Teguh Prasetyo, *Pengantar Ilmu Hukum*, Edisi Pertama, Cetakan ke-I, (Depok: PT RajaGrafindo Persada, 2018), hlm. 8.

Grafik 1. Interdependensi antara hukum, masyarakat dan teknologi.
Sumber: Dokumen Pribadi

Interdependensi dan interaksi antara teknologi dan manusia adalah hal yang lumrah, biasa sehingga untuk mencegah terjadinya kerugian baik materiil atau imateriil dalam penggunaan teknologi maka diperlukan hukum sebagai sarana pengendalian, sarana menciptakan ketertiban umum, sarana mewujudkan keadilan bermartabat.

Teknologi memudahkan manusia untuk menyelesaikan pekerjaannya, melakukan transaksi elektronik, menyelesaikan perkara di pengadilan melalui *e-court*[9], dan lain sebagainya.

[9] Berdasarkan Pasal 1 Angka 7 Peraturan Mahkamah Agung No. 1 Tahun 2019 tentang Administrasi Perkara dan Persidangan di Pengadilan Secara Elektronik, bahwa persidangan secara elektronik adalah serangkaian proses memeriksa dan mengadili perkara oleh pengadilan yang dilaksanakan dengan dukungan teknologi informasi dan komunikasi. Pengertian *e-court* sendiri dapat ditemukan dalam *website* resmi https://ecourt.mahkamahagung.go.id/ bahwa *e-court* adalah layanan bagi Penggunan Terdaftar untuk Pendaftaran Perkara secara *online*, mendapatkan taksiran panjar

Namun, pelbagai aktivitas tersebut memerlukan data pribadi, data pribadi yang kita masukkan, isi ke dalam sistem elektronik penyelenggara sistem elektronik. Pengalaman **Penulis,** bahwa apabila kita telah memasukan data pribadi tersebut maka akan terdapat *e-mail* (surat elektronik) balasan yang berisikan data-data yang telah kita himpun tadi, berdasarkan hal tersebut, secara tidak langsung, orang yang bekerja di bidang informasi dan teknologi mengetahui data yang telah kita masukan ke dalam sistem elektronik tersebut.

Hukum memungkinkan semua kepentingan dari orang (manusia, dan badan hukum/korporasi) yang telah menjadi subyek hukum itu mewujudkan diri dalam kerja sama-melakukan perbuatan melawan hukum karena manusia, badan hukum tidak dapat hidup sendiri tanpa peranan manusia/ badan hukum lainnya. Hukum menjelma dalam pergaulan hidup yang disebut masyarakat yang teratur, namun hukum bukan masyarakat.

Hukum merupakan peraturan (baik tertulis ataupun tidak tertulis) yang mengatur hubungan hidup antar manusia berubah wujudnya tanpa kehilangan esensinya menjadi pergaulan hidup. Hukum tidak dapat hanya sekedar dimaknai sebagai urusan Pasal-pasal dalam Undang-undang melainkan menjadi hidup sebagai pergaulan hidup, yang oleh tiap-tiap orang diwujudkan dalam hidup sehari-hari, sekalipun kadang kala orang tidak menyadari akan hal tersebut. Peraturan tersebut sebagian usianya sudah berabad-abad telah menjadi bagian dari kesadaran banyak bangsa beradab dan dilakukan setiap orang sebagai sesuatu yang demikian adanya. Sebagian

biaya perkara secara *online*¸ pembayaran secara *online,* pemanggilan yang dilakukan dengan saluran elektronik, dan persidangan yang dilakukan secara elektronik.

lagi muncul kemudian dan menjadi peraturan-peraturan yang baru karena munculnya berbagai hubungan-hubungan yang baru yang juga berisikan peraturan-peraturan baru[10].

Semenjak manusia dilahirkan, manusia telah bergaul dengan manusia lainnya dalam wadah yang kita kenal sebagai masyarakat. Mula-mula ia berhubungan dengan orang tuanya dan setelah usianya meningkat dewasa ia hidup bermasyarakat, dalam masyarakat tersebut manusia saling berhubungan dengan manusia lainnya, sehingga menimbulkan kesadaran pada diri manusia bahwa kehidupan dalam masyarakat berpedoman pada suatu aturan yang oleh sebagian besar warga masyarakat tersebut ditaati[11].

Ubi Societas Ibi Ius, di mana ada masyarakat – disitu ada hukum. Sebuah ungkapan mendasar yang dikemukakan oleh filsuf **Cicero**. Apabila ditilik secara abstrak maka sifat hukum yang ada di mana-mana itu dapat disebut sebagai suatu gejala universal. Meskipun kemungkinan ada persamaan, namun apabila ditilik dari sudut isinya, hukum tidak sama di mana-mana. Ketidaksamaan isi hukum disebabkan oleh ketidaksamaan dalam pergaulan hidup manusia di masing-masing persekutuan bangsa. Setiap persekutuan bangsa memiliki hukum dan sistem hukum sendiri–sendiri. Ibarat peribahasa yang mengatakan bahwa 'di mana bumi dipijak disitu langit dijunjung'. Salah satu contoh, dalam layanan toko *online (e-commerce)* pengguna yang sebagai penjual dalam *e-commerce* membutuhkan pengguna yang sebagai pembeli untuk membeli barang penjual tersebut sehingga penjual pun mendapatkan untung dan barang dagangannya laku.

[10] *Ibid*, hlm.9.

[11] Teguh Prasetyo, *Hukum Pidana*, Edisi Revisi, Cetakan ke-9, (Depok: PT RajaGrafindo Persada, 2018), hlm.1.

Pada tahun 2008, Pemerintah telah menerbitkan UU ITE untuk memberikan jaminan perlindungan bagi pemanfaatan teknologi, dan yang terpenting agar teknologi tersebut tidak disalahgunakan yang membawa kerugian bagi orang perorangan, korporasi ataupun kepada Negara. Sebagaimana dijelaskan dalam Penjelasan[12] UU ITE (2008) dalam paragraf pertama Penjelasan bagian Umum yakni "Pemanfaatan Teknologi Informasi, media, dan komunikasi telah mengubah baik perilaku masyarakat maupun peradaban manusia secara global. Perkembangan teknologi informasi dan komunikasi telah pula menyebabkan hubungan dunia menjadi tanpa batas (*borderless*) dan menyebabkan perubahan sosial, ekonomi, dan budaya secara signifikan berlangsung demikian cepat. Teknologi Informasi saat ini menjadi pedang bermata dua karena selain memberikan kontribusi bagi peningkatan kesejahteraan, kemajuan, dan peradaban manusia, sekaligus menjadi sarana efektif perbuatan melawan hukum"[13] dan kedua, dalam paragraf kedua Penjelasan bagian Umum UU ITE (2008) bahwa "Saat ini telah lahir suatu rezim hukum baru yang dikenal dengan hukum siber atau hukum telematika. Hukum siber atau *cyber law*, secara internasional digunakan untuk istilah hukum yang terkait dengan pemanfaatan teknologi informasi dan komunikasi. Demikian pula, hukum telematika yang merupakan perwujudan dari konvergensi hukum telekomunikasi, hukum media, dan hukum informatika. Istilah lain yang juga digunakan adalah hukum teknologi informasi (*law of information technology*),

[12] Penjelasan berfungsi sebagai tafsir resmi pembentuk peraturan perundang-undangan atas norma tertentu dalam batang tubuh. Oleh karena itu, Penjelasan hanya memuat uraian terhadap kata, frasa, kalimat atau padanan kata/istilah asing dalam norma yang dapat disertai dengan contoh. (Lihat buku: Teguh Prasetyo, *Sistem Hukum Pancasila*....., hlm. 187-191.

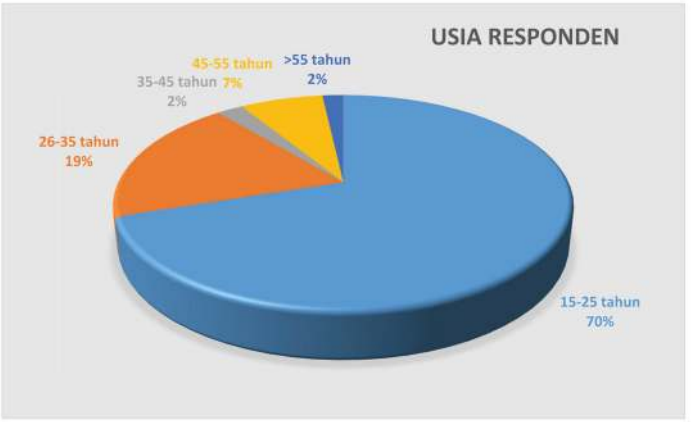
[13] Paragraf I Penjelasan bagian Umum Penjelasan UU ITE tahun 2008

hukum dunia maya (*virtual world law*), dan hukum mayantara. Istilah-istilah tersebut lahir mengingat kegiatan yang dilakukan melalui jaringan sistem komputer dan sistem komunikasi baik dalam lingkup lokal maupun global (Internet) dengan memanfaatkan teknologi informasi berbasis sistem komputer yang merupakan sistem elektronik yang dapat dilihat secara virtual. Permasalahan hukum yang seringkali dihadapi adalah ketika terkait dengan penyampaian informasi, komunikasi, dan/atau transaksi secara elektronik, khususnya dalam hal pembuktian dan hal yang terkait dengan perbuatan hukum yang dilaksanakan melalui sistem elektronik".[14]

III. Penggunaan Aplikasi Online & Kasus Kebocoran Data Pribadi

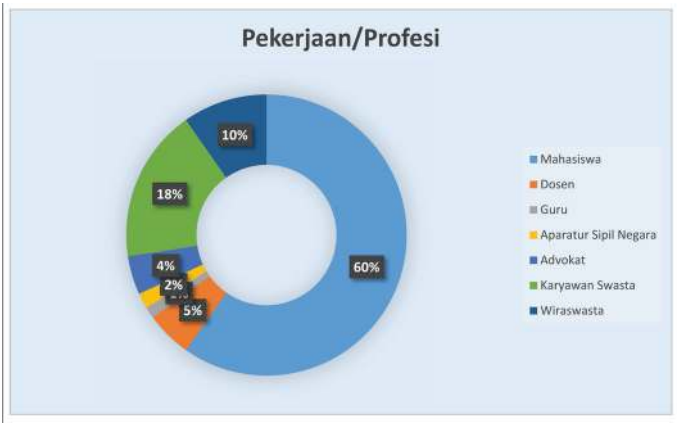
Penulis melakukan penelitian menggunakan kuisioner yang dibagikan melalui layanan *google form* pada bulan April-Mei tahun 2020 dengan target responden yakni 200 (dua ratus) responden, namun melebihi target, sehingga total repsonden yang berpartisipasi ialah 226 (dua ratus dua puluh enam) responden. Responden yang terlibat dalam kuisioner ini terdiri dari usia yang berusia: a. 15-25 tahun berjumlah 70,5% (158 orang); b. 26-35 tahun berjumlah 19% (43 orang); c. 35-45 tahun berjumlah 2.2% (5 orang); d. 45-55 tahun berjumlah 7,1% (16 orang); e. lebih dari 55 tahun berjumlah 1.8% (4 orang).

[14] Paragraf II Penjelasan bagian Umum UU ITE tahun 2008



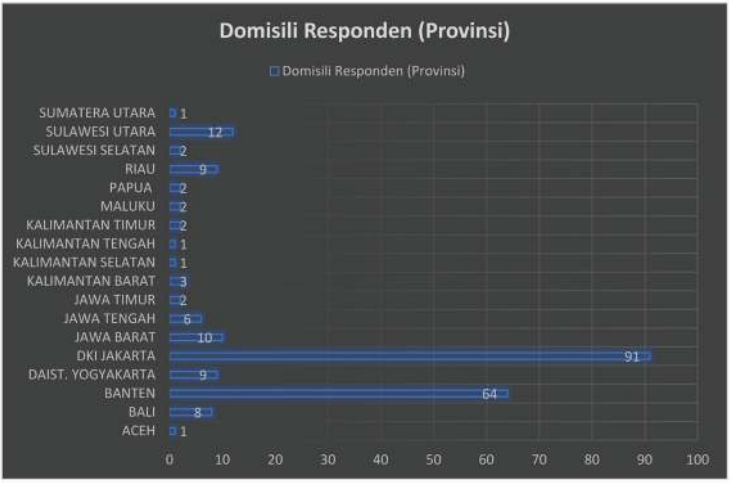
Grafik 2. Usia Responden.
Sumber: Dokumen pribadi.

Pekerjaan/profesi yang terlibat dalam kuisioner penelitian ini terdiri dari: a. Mahasiswa berjumlah 59,7% (135 orang); b. Dosen berjumlah 5,3% (12 orang); c. Guru berjumlah 1,3% (3 orang); d. Aparatur Sipil Negara 1.8% (4 orang); e. Advokat berjumlah 4,4% (10 orang); f. Karyawan Swasta berjumlah 17,7% (40 orang); g. Wiraswasta berjumlah 9.7% (22 orang).



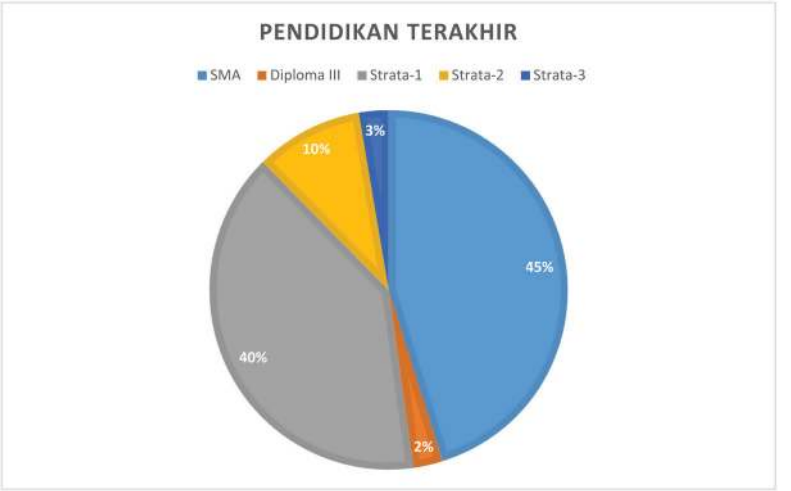
Grafik 3. Pekerjan/Profesi Responden.
Sumber: Dokumen pribadi.

Domisili responden yang terlibat dalam kuisioner ini berasal dari Provinsi : 1. Aceh (1 orang); 2. Bali (8 orang); 3. Banten (64 orang);4. Daist. Yogyakarta (9 orang); 5. DKI Jakarta (91 orang); 6. Jawa Barat (10 orang); 7. Jawa Tengah (6 orang); 8. Jawa Timur (2 orang); 9. Kalimantan Barat (3 orang); 10. Kalimantan Selatan (1 orang); 11. Kalimantan Tengah: 1 orang 12. Kalimantan Timur (2 orang); 13. Maluku (2 orang); 14. Papua (2 orang); 15. Riau (9 orang); 16. Sulawesi Selatan (2 orang);17. Sulawesi Utara (4 orang); 18. Sulawesi Utara (8 orang); 19. Sumatera Selatan (1 orang);



Grafik 4. Domisili Responden.
Sumber: Dokumen pribadi.

Pendidikan terakhir responden penelitian ini ialah: a. SMA (Sekolah Menengah Atas) yakni: 45,1% (102 orang); b. Diploma-3 yakni 2,7% (6 orang); c. Strata-1 yakni 39,8% (90 orang); d. Strata-2 yakni 9,7% (22 orang); e. Strata-3 yakni 2,7% (6 orang).



Grafik 5. Pendidikan Terakhir
Sumber: Dokumen pribadi.

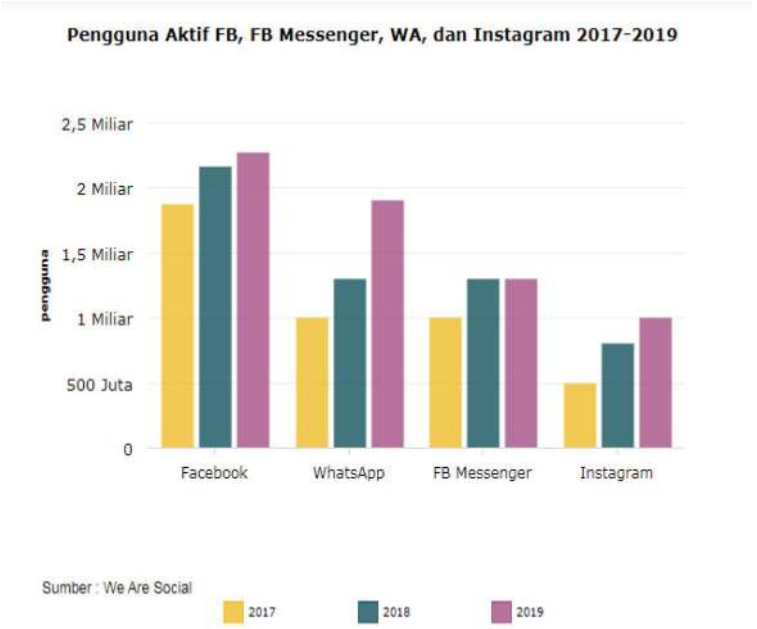
Berdasarkan penelitian, didapatkan bahwa 96% (sembilan puluh enam per seratus) atau sebanyak 218 responden adalah pengguna aplikasi *online* sedangkan 4% (empat per seratus) atau sebanyak 8 respoden tidak menggunakan aplikasi *online*. Hal ini menunjukkan bahwa aplikasi *online* adalah dapat dikategorikan sebagai kebutuhan yang tidak dapat tidak ada dalam kehidupan manusia.

Penggunaan internet di dunia sudah sangat banyak. Menurut Perserikatan Bangsa-Bangsa sebagaimana dikutip oleh cnnindonesia.com bahwa hingga tahun 2018 tercatat saat ini ada 3,9 miliar orang atau lebih dari setengah populasi dunia yang menggunakan internet[15]. Menurut data lembaga riset *Statisca,* menunjukan bahwa Indonesia masuk dalam 10

[15] CNN Indonesia, artikel tanggal 10-12-2018, "3,9 Miliar Orang di Dunia Telah Terhubung Internet" diakses dari https://www.cnnindonesia.com/teknologi/20181210094556-192-352374/39-miliar-orang-di-dunia-telah-terhubung-internet diakses tanggal 8 Mei 2020

(sepuluh) Negara dengan pengguna internet terbesar di dunia. Indonesia berada di peringkat kelima dengan pengguna internet sebanyak 143,26 juta per Maret 2019[16].

Pengguna aktif *platform* media sosial juga menunjukan angka yang sangat fantastis pada tahun 2017-2019. Menurut *We Are Social* sebagaimana dimuat dalam katadata.co.id dalam grafik berikut:



Grafik 6. Pengguna Aktif Media Sosial.

Sumber: *We Are Social*, sumber dari: https://katadata.co.id/berita/2019/12/20/terulang-lagi-267-juta-data-pengguna-facebook-bocor

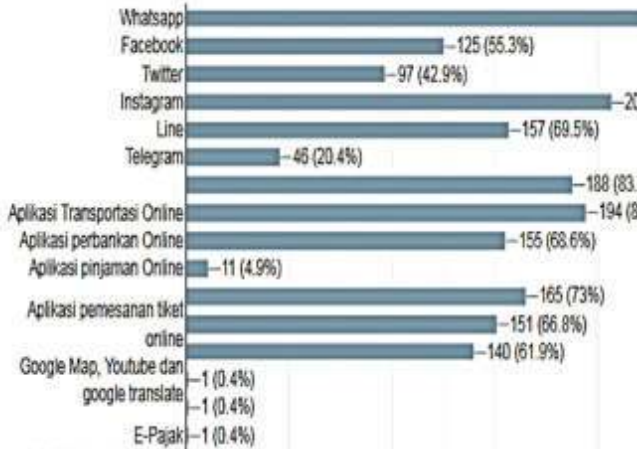
Menurut hemat **Penulis,** tingginya angka ini dikarenakan pelbagai faktor, misalnya faktor ingin tetap menjalin tali

[16] Dwi H, "Indonesia Peringkat Kelima Dunia dalam Jumlah Pengguna Internet", artikel tanggal 11-09-2019 diakses dari https://databoks.katadata.co.id/datapublish/2019/09/11/indonesia-peringkat-kelima-dunia-dalam-jumlah-pengguna-internet diakses tanggal 8 Mei 2020

silahturami, *keep contact* dengan teman-teman, rekan kerja, dengan keluarga yang jauh, selain itu, penggunana media sosial juga digunakan untuk berjualan *online,* untuk menunjukan prestasi, untuk menunjukkan kabar ataupun berbagi kesenangan dengan keluarga lain saat menikmati liburan atau makanan.

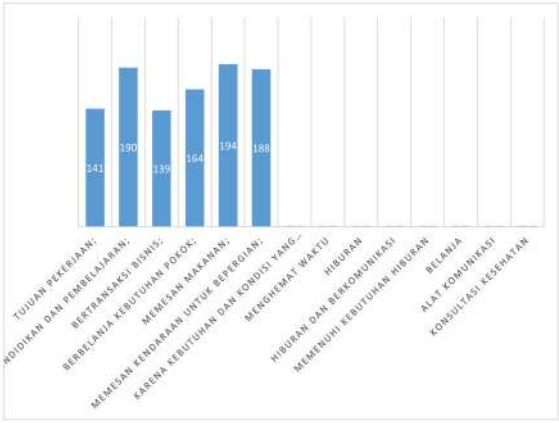
Grafik 7. Angka Pengguna Aplikasi *Online*
Sumber: Dokumen pribadi.

Berdasarkan data yang telah terkumpulkan didapatkan bahwa Aplikasi (*platform*) Online/Penyelenggara Sistem Elektronik (penyedia jasa layanan aplikasi Online) apa yang sering saudara/i sering gunakan sangat beragam dan tujuan penggunaan aplikasi *online* tersebut juga sangat beragam sebagaimana digambarkan pada grafik dibawah ini:



Grafik 8. Jenis Aplikasi *Online* yang Digunakan
Sumber: Dokumen pribadi.

Berdasarkan grafik tersebut, dapat disimpulkan bahwa aplikasi *online* yang paling sering digunakan adalah aplikasi komunikasi *online* & media sosial seperti, *whatsapp, Instagram*, disusul oleh aplikasi transportasi *online*, dan aplikasi perbankan *online*.



Grafik 9. Jenis Aplikasi *Online* yang Digunakan
Sumber: Dokumen pribadi.

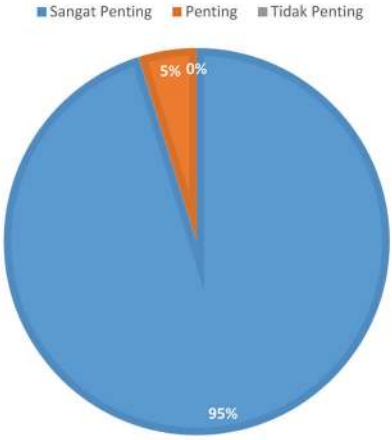
Berdasarkan grafik tersebut, dapat terlihat bahwa penggunaan aplikasi *online* banyak digunakan untuk tujuan memesan makanan, diurutan kedua yakni untuk tujuan pendidikan dan pembelajaran, diurutan ketiga untuk memesan kendaraan untuk bepergian, diurutan keempat untuk berbelanja kebutuhan pokok, diurutan kelima untuk tujuan pekerjaan, diurutan keenam untuk tujuan bertransaksi bisnis.

Pelbagai aplikasi *online* itu membutuhkan data pribadi untuk dapat digunakan, pengguna harus memasukan data pribadi antara lain: nama, tempat/tanggal lahir, alamat *e-mail* dan beberapa apabila ingin menggunakan layanan *premium* atau layanan yang lebih mewajibkan untuk meng-*upload* (menggunggah) *softfile* Kartu Tanda Penduduk (KTP) si pengguna. Berdasarkan data yang **Penulis** dapatkan diketahui bahwa 95% (sembilan puluh lima per seratus) menjawab bahwa perlindungan data pribadi dalam aplikasi *online* adalah hal yang sangat penting, 5% (lima per seratus) menjawab penting, dan 0% menjawab tidak. Berdasarkan data ini dapat terlihat bahwa konsumen/pengguna sudah *aware,* sadar terhadap perlindungan data pribadi milik mereka. Data pribadi wajib dilindungi baik oleh penyelenggara lingkup publik dan lingkup privat. *Data security in the OSS system is important to protect electronic information and to keep the licensing process smooth. Data and information security in OSS is a form of cyber security. OSS data security is also a manifestation of cyber defense to cope with cyber attacks that cause disturbances to the implementation of national defense*[17].

Namun menurut hemat **Penulis,** tingkat kesadaran ini harus ditingkatkan lagi, disosialiasikan lagi untuk pengguna

[17] Inggarwati, M.P. *Op.Cit.*

yang ada di tempat yang jauh dari perkotaan, disosialisasikan lagi kepada warga dari pelbagai golongan, pekerjaan, dari pelbagai usia yang rentan mudah percaya terhadap berita-berita di media sosial, bahkan saat mereka menerima telepon atau pesan singkat (*SMS)* mendapatkan hadiah namun wajib melengkapi syarat-syarat tertentu untuk menebus hadiah itu.



Grafik 10. Sifat Perlindungan Data Pribadi
Sumber: Dokumen pribadi.

Dugaan kebocoran data pribadi dapat saja terjadi karena peretas yang canggih dan meretas sistem elektronik ataupu karena kecerobohan si pengguna yang mudah percaya terhadap modus-modus penipuan yang menggunakan data pribadi. Data adalah barang mahal yang dicari-cari saat ini. *Data not only defines us, it is the lifeblood of AI. Data science is the new discipline of the digital age. Companies like Facebook, Snapchat, or Google are not primarily in the social media or consumer tools business; rather they are in the data business. The products they offer (in most cases free to the end user) are vehicles to collect massive*

quantities of rich data, making the user essentially the product.[18] *Data mining enables firms to discover or infer previously unknown facts and patterns in a database. It relies not on causation but on correlations that arise from the application of non-public algorithms to large collections of data. Consequently, the newly discovered information is not only unintuitive and unpredictable, but also results from a fairly opaque process*[19].

Data-data yang dikumpulkan, digunakan, dikelola, dianalisis akhirnya membentuk 'BIG DATA' maka jangan heran jika kita pernah meng-klik, mencari merek tertentu di *google,* atau *e-commerce* lainnya, maka merek atau produk tersebut akan muncul lagi. *Big Data is most commonly defined with reference to its key common characteristics, which are frequently described as 'volume, velocity, and variety'*[20]. *Big Data analytics rely on having a mountain of data about many people in order to find the correlations that allow researchers to make relatively accurate predictions about individuals including those whose data did not contribute to building the model. In other words, even people who do not consent to have their data in a database may find that they are just as subject to the models' extrapolations as the people who contributed data to it*[21]. *Big Data thus poses the risk of going "viral" as the algorithms' inputs and outputs*

[18] Karl Manheim *and Lyric Kaplan, "Artificial Intelligence: Risks to Privacy and Democracy",* (The Yale Journal of Law&Technology, Vol. 21) diakses dari https://yjolt.org/sites/default/files/21_yale_j.l._tech._106_0.pdf Hlm. 119.

[19] Tal Z Zarsky, *'Desperately Seeking Solutions: Using ImplementationBased Solutions for the Troubles of Information Privacy in the Age of Data Mining and the Internet Society' (2004)* 56 Maine Law Review 13

[20] Doug Laney, '3D Data Management: Controlling Data Volume, Velocity, and Variety' on Gartner Blog Network (6 February 2001) . See also the longer list provided in Kitchin, above n 2, 1–2.

[21] A. Michael Froomkin, "Big Data: Destroyer of Informed Consent", (YALE JOURNAL OF LAW AND TECHNOLOGY 21:3 (2019)), Hlm. 33 https://yjolt.org/big-data-destroyer-informed-consent diakses tanggal 1 Maret 2020

influence each other recursively[22]. *Ultimately, Big Data leaves us in a paradox. On the one hand, we gather more data and evidence in order to gain an ostensibly more accurate and complete understanding of the phenomenon we seek to influence. On the other, the more data we have, the more we have to simplify it in order to gain any useful insights*[23].

Data-data yang telah dikumpulkan tersebut jika tidak dijaga maka berpotensi untuk dibocorkan. **Penulis** akan paparkan kasus-kasus, dugaan kebocoran pribadi yang terjadi di Indonesia ataupun kasus-kasus internasional:

1. Berdasarkan hasil investigasi, salah satu pers terkemuka di Indonesia (**Harian Kompas**), ditemukan bahwa ditemukan praktik jual beli data pribadi nasabah di kalangan tenaga pemasaran kartu kredit dengan harga bervariasi. Informasi data pribadi yang diperjualbelikan secara bebas tersebut bukan hanya berupa nama, alamat, nomor telepon dan nama ibu kandung, namun juga 'kemampuan finansial'. Data pribadi yang memuat informasi nama, nomor telepon hingga nama orang tua, tanpa dilengkapi 'kemampuan finansial', dijual seharta Rp300 (tiga ratus rupiah) per data. Namun, apabila data yang 'dilengkapi informasi kemampuan finansial pemiliknya dihargai Rp20.000 (dua puluh ribu rupiah) hingga Rp50.000 (lima puluh ribu rupiah)[24].
2. Hasil investigasi kedua yakni, penjualan data pribadi juga terjadi dalam dua *platform e-commerce online*. Data dari

[22] Caryn Devins, Teppi Fellin, Stuart Kauffman & Rogel Koppl, "*The Law and Big Data" (*CORNELL JOURNAL OF LAW AND PUBLIC POLICY [Vol. 27:357]) Hlm. 361

[23] *Ibid*, hlm. 385.

[24] Harian Kompas, edisi cetak, tanggal 11 Mei 2019 "Data Pribadi Dijual Bebas".

kedua toko *online* itu memuat infrormasi yang sudah usah meski datanya lengkap, banyak nomor ponsel di dalam itu yang sudah tidak aktif[25].

3. Menurut pengakuan JS, coordinator pemasran kartu kredit kepada *Harian Kompas*, bahwa kriteria data pribadi yang berkualitas bagus adalah dilengkapi dengan informasi gaji dan keuangan. Data tersebut diperoleh dari lembaran kertas formulir pendaftaran kartu kredit yang diajukan calon nasabah. Menurut JS, harga Rp1.000.000 (satu juta rupiah) untuk 50 (lima puluh) data pribadi itu tergolong wajar. Alasanya, komisi yang akan diperoleh dari setiap kartu kredit yang disetujui cukup besar, Rp200.000 (dua ratus ribu rupiah) untuk kartu kredit jenis *gold* dan Rp400.000 (empat ratus ribu rupiah) untuk jenis platinum[26];
4. Pada Agustus 2019, Polisi, Penyidik di Direktorat Tindak Pidana Siber Bareskrim Polri berhasil menangkap terduga berinisial (pada tahun 2019) di daerah Depok dengan dugaan membantu memperdagangkan data kependudukan, dari perbuatanya C mampu mendapatkan Rp250.000 (dua ratus lima puluh ribu rupiah) per hari. C diduga menjual data kependudukan melalui sebuah situs bernama temanmarketing.com. C dikenakan Pasal 48 ayat (2) *jo.* Pasal 32 ayat (2) UU ITE dan Pasal 95A UU Kependudukan[27]. C diketahui menyimpan jutaan data pribadi Warga Negara Indonesia yang terdiri dari 761.435 nomor ponsel, 129.421 kartu kredit, 1.162.864 Nomor

[25] Harian Kompas, edisi cetak, tanggal 11 Mei 2019 "Dari Alamat hingga Nama Ibu Kandung".

[26] Harian Kompas, edisi cetak, tanggal 11 Mei 2019 "Data Pribadi Dijual Bebas".

[27] Devina Halim, "Tersangka Jual Beli Data Kependudukan Raup Untung Rp250.000 per hari", artikel tanggal 15-08-2019, diakses dari https://nasional.kompas.com/read/2019/08/15/21362431/tersangka-jual-beli-data-kependudukan-raup-untung-rp-250000-per-hari tanggal 7 Mei 2020

Induk Kependudukan (NIK), 50.854 Nomor Kartu Keluarga (KK) dan 64.164 nomor rekening[28];

5. Dugaan skandal kebocoran data *Cambridge Analytice* sehingga Pemerintah Australia menuntut *facebook* Rp 7 Triliun. Menurut Pemerintah Australia *facebook* telah membagikan sekitar 311.127 data pribadi pengguna kepada pengebang aplikasi bernama *'This is Your Digital Life'* sejak Maret 2014 hingga Mei 2015. Data yang telah diperoleh itu kemudian secara sengaja dijual kepada *Cambridge Analytica* untuk kepentingan politik. Pihak Komisari Informasi Australia menilai bahwa *facebook* telah lalai dalam menjaga kerahasiaan data pribadi penggunanya sehingga apabila terbukti menyebarkan data pribadi pengguna secara sengaja maka pihak *facebook* dituntut uang sebesar 529 dollar AS atau setara dengan Rp. 7.7 Triliun[29];
6. Dugaan penjualan data dijual di pasar gelap oleh pihak *platform Zoom*. *Platform video conference zoom* diduga mengalami kebocoran data lebih dari 500.000 akun *zoom* dan dijual ke pasar gelap dunia maya (*dark web)*. Menurut *Cyble,* firma keamanaan siber sebagaimana dikutip oleh kompas.com bahwa, ratusan ribu akun *zoom* hasil curian ini dijual di forum peretas di *darkweb* dengan harga sekitar 0,0020 dolar AS (setara Rp31. Tiga puluh satu rupiah) untuk masing-masing akun. Ratusan akun tersebut

[28] Devina Halim,, "Polri: Kasus Jual-Beli Data Pribadi di *WEB* berbeda dengan di *Grup Facebook* diakses dari https://nasional.kompas.com/read/2019/08/16/08272631/polri-kasus-jual-beli-data-pribadi-di-web-berbeda-dengan-di-grup-facebook tanggal 7 Mei 2020

[29] Kevin Rizky, "Tuntut Skandal *Cambridge Analytica, Autralia Tuntut Facebook Rp 7 Triliun",* artikel tanggal 14-03-2020 diakses dari https://tekno.kompas.com/read/2020/03/14/12090007/buntut-skandal-cambridge-analytica-australia-tuntut-facebook-rp-7-triliun diakses tanggal 8 Mei 2020

diduga dibobol dengan teknik *credential stuffing* dengan memanfaatkan alat peretas pihak ketiga yang masih belum diketahui. Pihak *zoom* telah melakukan langkah untuk mengatasinya, pihak *zoom* telah bekerja sama dengan beberapa firma intelijen untuk melacak kumpulan kata sandi yang dibobol dan alat untuk mengumpulkannya, serta meminta firma tersebut untuk memblokir ribuan situs yang berpotensi bisa mencuri informasi *credential* pengguna. Selain itu, masalah yang beberapa kali terjadi yakni '*Zoombombing'* bahwa ada oknum tidak bertanggung jawab bisa masuk ke sebuah ruangan *meeting* virtual *zoom* tanpa diundang dan mengacaukan suasana rapat[30]

Kasus-kasus diatas adalah beberapa kasus tentang dugaan kebocoran data. Pada awal Mei 2020, konsumen Indonesia juga dibuat khawatir karena ada dugaan salah satu *platform e-commerce* di Indonesia diretas, dan data 91juta pengguna diduga bocor dan beberapa data konsumen diduga dijual oleh oknum di *darkweb*[31]. Kasus-kasus kebocoran data tersebut seharusnya tidak terjadi, karena data pribadi dalam sistem elektronik bersifat rahasia. Penyelenggara/*platform* aplikasi *online* wajib memiliki keamanan sistem yang baik, melindungi sistem mereka, melakukan pengecekan sistem secara berkala sehingga tindakan melawan hukum berupa *data mining* yang tidak sah.

[30] Bill Clinten "Lebih dari 500.000 Akun *Zoom* Curian Dijual di Pasar Gelap Internet, diakses dari https://tekno.kompas.com/read/2020/04/15/10240047/lebih-dari-500.000-akun-zoom-curian-dijual-di-pasar-gelap-internet?page=all#page3 diakses tanggal 8 Mei 2020

[31] Adiya Jaya, " Data 91 juta Pengguna Tokopedia Diduga Bocor, Media Asing Ikut Soroti" artikel tanggal 3-5-2020 https://www.kompas.com/global/read/2020/05/03/133257970/data-91-juta-pengguna-tokopedia-diduga-bocor-media-asing-ikut-soroti?page=all diakses tanggal 8 Mei 2020

Kebocoran data pribadi menimbulkan pelbagai risiko, risiko kejahatan antara lain: 1. Informasi yang dicuri lalu dijual ke *dark web*. *Dark web* adalah bagian tersembunyi dari internet yang hanya bisa diakses menggunakan *software*/aplikasi khusus[32]. Risiko lain yang dapat terjadi yakni modus penipuan dengan iming-iming mendapatkan hadiah, atau diganggu oleh *telemarketer* yang mencoba memasarkan usaha mereka.

Kebocoran data selain merugikan konsumen namun dapat merugikan perusahaan, penyelenggara sistem elektronik. *Every data breach reduces the trust of internet users in Big Data companies as well as the security on other websites. In turn, the risk of consequent identty thef as well as consequent fnancial or reputaton damage rises. This later efect in partcular not only eventuates because of a data breach, it occurs as a result of the subsequent leak of stolen data. Afer a data breach has happened, the loss of control results in the disclosure of the stolen data by hackers*[33].

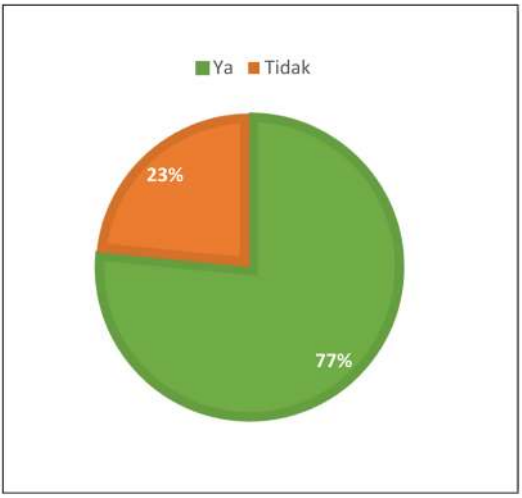
Berdasarkan observasi **Penulis,** pengaturan perlindungan data pribadi masih tersebar di pelbagai peraturan perundang-undangan di Indonesia, antara lain, a. peraturan di sektor perbankan; b. peraturan di sektor administrasi kependudukan; c. peraturan di sektor kesehatan dan sampai dengan penyusunan buku ini (**PEN**-Juni tahun 2020) bahwasanya pengaturan tentang data pribadi masih dalam bentuk Peraturan Menteri yakni Peraturan Menteri Komunikasi dan Informatika

[32] CNN Indonesia "Risiko Ketika Data Prbadi Dicuri" artikel tanggal 27 Desember 2018, diakses dari https://www.cnnindonesia.com/teknologi/20181226210103-185-356593/risiko-ketika-data-pribadi-dicuri diakses tanggal 1 Maret 2020

[33] Oliver Vetterman, "*Self-made data protection – is it enough? Prevention and after care of identity theft" (United Kindgom:* European Journal of Law and Technology, Vol.10, Issue 1, 2019) hlm.1. diakses dari http://ejlt.org/article/view/673/911 tanggal 5 Mei 2020

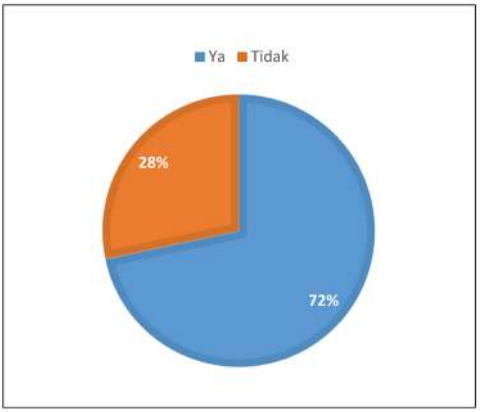
No. 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik (selanjutnya disebut Permenkominfo PDPSE). Pemerintah saat ini telah merancang Rancangan Undang-undang tentang Pelindungan Data Pribadi **(RUU PDP – saat ini naskah RUU PDP yang terakhir adalah terakhir pada Desember 2019)** dan masuk ke dalam Program Legislasi Nasional Prioritas. Dua norma dalam RUU PDP tersebut yang sangat dibutuhkan dalam pelindungan data pribadi sekarang ini ialah pertama, norma tentang larangan memalsukan data pribadi dengan maksud menguntungkan diri sendiri atau orang lain atau yang mengakibatkan kerugian bagi orang lain; kedua, norma larangan untuk menjual atau membeli data pribadi.

Berdasarkan pertanyaan yang Penulis ajukan kepada responden ('apakah Saudara/I mengetahui bahwa pengaturan perlindungan data pribadi di Indonesia masih tersebar di pelbagai peraturan perundang-undangan?') yang Penulis sebarkan melalui media online. Hasilnya adalah 77% (173 responden) menjawab Ya dan 23% (53 responden) menjawab tidak. Kedua, pertanyaan tentang 'Apakah Saudara/i mengetahui adanya regulasi tentang Perlindungan Data Pribadi di Indonesia, misalnya Peraturan Menteri Komunikasi dan Informatika No. 20 Tahun 2016 tentang Perlindungan data Pribadi dalam Sistem Elektronik?" dan hasilnya bahwa 162 responden (72%) menjawab tahu, dan 64 responden menjawab tidak tahu.



Grafik 11. Pertanyaan tentang Apakah Saudara/i mengetahui bahwa pengaturan perlindungan data pribadi di Indonesia masih tersebar di pelbagai peraturan perundang-undangan di Indonesia?

Sumber: dokumen pribadi.



Grafik 12. Pertanyaan tentang Apakah Saudara/i mengetahui adanya regulasi tentang Perlindungan Data Pribadi di Indonesia, misalnya Peraturan Menteri Komunikasi dan Informatika No. 20 Tahun 2016 tentang Perlindungan data Pribadi dalam Sistem Elektronik?

Sumber: dokumen pribadi.

Berdasarkan hal tersebut, Penulis berharap lembaga legislatif segera mengesahkan Rancangan Undang-Undang tentang Perlindungan Data Pribadi supaya hukum positif di Indonesia tidak tertatih-tatih mengejar cepatnya teknologi dan agar Indonesia memiliki *lex specialis* pengaturan data pribadi. Hukum tentang perlindungan data pribadi yang berisikan keadilan bermartabat masih akan terus berlangsung (*suistanable)* secara terus-menerus mengikuti dan berada di dalam serta menuntun kehidupan hukum dan sistem hukum *de lege lata*[34]. Konsep *de lege lata* ini menurut hemat Penulis telah tertuang dalam salah 2 (dua) peraturan berikut; pertama, Peraturan Menteri Komunikasi dan Informatika Republik Indonesia No. 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik; kedua, Peraturan Otoritas Jasa Keuangan RI No, 13/POJK.02/2018 tentang Inovasi Keuangan Digital di Sektor Jasa keuangan. Penulis akan mengupas dan menganalisis kedua peraturan tersebut lebih lanjut dan peraturan perundang-undangan lainnya yang berkaitan dengan perlindungan data pribadi pada bab berbeda di dalam buku ini.

Harapan Penulis tersebut juga didukung oleh 226 responden yang turut serta dalam kuisioner dengan pertanyaan 'Apakah

[34] Konsep *de lege lata* adalah *maxim – latin* yang meng-Indonesia. *De lege lata* dimengerti sebagai; sesuai dengan hukum atau menurut kehendak hukum. Maksudnya, menurut kesepakatan yang ada di dalam masyarakat, lokal, nasional, maupun internasional. Menurut konvensi atau praktik penyelenggaran Negara yang timbul dan terpelihara di kalangan ahli hukum yang memiliki wibawa keilmuan yang sangat tinggi, bermartabat karena tidak mau menghina budaya hukumnya sendiri serta menurut peraturan perundang-undangan yang sedang berlaku karena dibuat oleh Penguasa yang berwenang untuk itu; dengan kata lain, menurut Diskresi. Diskresi itu adalah hikmat kebijaksanaan dalam permusyawaratan perwakilan atau menurut Rakyat. Secara sederhana, semua itu dirumuskan dengan keadilan bermartabat. Konsep ini dapat ditemukan dalam Teguh Prasetyo, *Keadilan Bermartabat: Perspektif Teori Hukum,* Edisi Pertama, Cetakan ke-I, (Bandung: Nusa Media, 2015), hlm. 21.

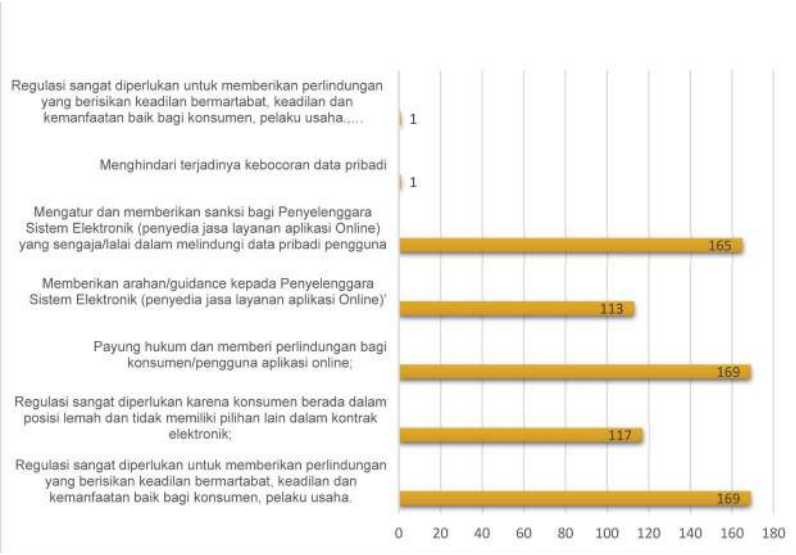
dalam penggunaan aplikasi online memerlukan regulasi atau cukup perjanjian/kontrak elektronik antara konsumen dengan Penyelenggara Sistem Elektronik (penyedia jasa layanan aplikasi Online)?' bahwa 206 responden menjawab ya, sedangkan 20 responden menjawab tidak.

Grafik 13. Pertanyaan 'Apakah dalam penggunaan aplikasi online memerlukan regulasi atau cukup perjanjian/kontrak elektronik antara konsumen dengan Penyelenggara Sistem Elektronik (penyedia jasa layanan aplikasi Online)?

Sumber: Dokumen Pribadi.

Penulis melakukan pertanyaan lebih lanjut bagi responden yang menjawab ya dengan pertanyaan 'Apakah arti penting dari regulasi/pengaturan tersebut? (*Dapat memilih lebih dari 1 jawaban) adapun hasil yang didapatkan yakni: bahwa 169 responden menjawab bahwa regulasi dapat: 1. Regulasi sangat diperlukan untuk memberikan perlindungan yang berisikan keadilan bermartabat, keadilan dan kemanfaatan baik bagi konsumen, pelaku usaha.; 2. Payung hukum dan memberi perlindungan bagi konsumen/pengguna aplikasi online. Dan 165 responden memilih bahwa Mengatur dan memberikan

sanksi bagi Penyelenggara Sistem Elektronik (penyedia jasa layanan aplikasi Online) yang sengaja/lalai dalam melindungi data pribadi pengguna.



Grafik 14. Pertanyaan 'Apakah arti penting dari regulasi/pengaturan tersebut?'

Sumber: Dokumen Pribadi.

Selain itu, **Penulis** melakukan bertanya apabila Saudara/i menjawab tidak. Mengapa perjanjian antara konsumen dengan Penyelenggara Sistem Elektronik (penyedia jasa layanan aplikasi *Online*) lebih penting dari regulasi? Dan hasil yang didapatkan sebagaimana grafik dibawah ini:

Grafik 15. Pertanyaan: Mengapa perjanjian antara konsumen dengan Penyelenggara Sistem Elektronik (penyedia jasa layanan aplikasi Online) lebih penting dari regulasi?

Sumber: Dokumen Pribadi.

Berdasarkan grafik tersebut dapat terlihat, bahwa perjanjian antara konsumen dengan penyelenggara sistem elektronik menjadi lebih penting dari regulasi dengan alasan paling banyak yakni karena penyusunan regulasi sangat lama dan sulit untuk mengikuti perubahan dalam aplikasi *online*. Namun, menurut hemat **Penulis,** peraturan berbentuk Undang-undang jauh lebih penting ketimbang perjanjian karena melalui Undang-undang semua pihak dapat memenuhi keadilan bermartabat, dan telah memiliki kepastian hukum serta sebagai bentuk kehadiran Negara untuk melindungi warga negaranya.

BAB II
TEORI KEADILAN BERMBARTABAT

I. Hakikat Teori Hukum

Teori hukum sangat bermanfaat bagi penegak hukum, pencari keadilan, masyarakat pada umumnya yang hendak memahami *bottom line* atau hakikat paling mendasar, misalnya tujuan dari hukum. Hakikat teori hukum itu adalah suatu filsafat hukum atau suatu *jurisprudence* yang sering dikenal dengan ilmu hukum[35]. Namun hendak diperhatikan dengan saksama bahwa terminologi *jurisprudence* itu berbeda dengan terminologi 'yurisprudensi' yang dipergunakan dalam sistem hukum di Indonesia, dan dengan terminologi *judge-made-law,* yang dipergunakan dalam sistem hukum di Inggris.

Jurisprudence atau ilmu hukum itu adalah filsafat hukum atau disebut dengan teori hukum, sedangkan yang dimaksud dengan 'yurisprudensi' adalah putusan-putusan badan peradilan atau hakim yang telah berkekuatan hukum tetap *(inkracht van gewijsde),* yang mengandung kaidah dan asas hukum yang diikuti oleh hakim-hakim dalam memutus perkara yang sejenis *(The binding force of precedent)*.

[35] Teguh Prasetyo, *Pengantar Ilmu Hukum,* Edisi Pertama, Cetakan ke-I, (Depok: PT RajaGrafindo Persada, 2018), hlm. 212

II. Keadilan Bermartabat

Keadilan bermartabat berangkat dari postulat sistem; bekerja mencapai tujuan, yaitu keadilan bermartabat. Keadilan yang memanusiakan manusia atau keadilan yang '*nge wong ke wong'*. Konsepsi keadilan bermartabat digali dari falsafah Bangsa Indonesia. Jati diri Bangsa Indonesia, yang termanifestasikan dalam Pancasila. Pancasila merupakan sumber dari segala sumber hukum dan sebagai *ideology*, sebagai falsafah bangsa dan Negara[36].

Sejak merdeka, para pemikir (*jurists)* berusaha untuk membangun sub-sistem atau elemen yang sangat penting dalam setiap sistem yang mau memenuhi syarat sebagai 'sistem hukum modern' tersebut. Mula-mula para *jurists* bersemangat dan memang tidak dapat disalahkan apabila hal itu masih berlangsung hingga detik ini, bahwa sub-sistem itu dibangun dengan cara meminjam atau mencari justifikasi serta pembenaran teori-teori barat seperti yang dikembangkan di Jerman oleh **Kelsen** dengan '*Stufentheorie*' dan **Nawiasky** dengan *Theorie von Stufenaufbau der Rechtsordnung*. Cara seperti ini adalah cara penundudukan diri. Sulit orang menerima, apabila baik **Kelsel** atau **Nawiasky** dirujuk untuk membenarkan Pancasila sebagai sumber dari segala sumber hukum bagi sistem hukum di Indonesia[37].

Namun, lambat laun, para *jurists* Indonesia sudah mulai menyadari pentingnya membangun suatu justifikasi atas sistem hukum atau keadilan yang bermartabat. Justifikasi dari suatu

[36] Konsep keadilan bermartabat dilahirkan dan digagas oleh Prof. Dr. Teguh Prasetyo, S.H., M.Si. (Guru Besar Fakultas Hukum Universitas Pelita Harapan)

[37] Teguh Prasetyo, *Sistem Hukum Pancasila (Sistem, Sistem Hukum, dan Pembentukan Peraturan Perundang-undangan di Indonesia) Perspektif Teori Keadilan Bermartabat*, (Bandung: Penerbit Nusa Media, 2016), hlm. v.

sistem hukum bermartabat yakni justifikasi yang dibangun karena bahan-bahannya adalah bahan-bahan asli yang digali dari bumi Indonesia itu sendiri. Bumi adalah suatu metafora atau perumpamaan tentang isi kepala dan pikiran orang Indonesia itu sendiri termasuk semua bahan hukum untuk membangun struktur dan susunan atau tata – urutan hukum yang berlaku dalam 'sistem hukum Indonesia'. Ketergantungan pada justifikasi yang menyandarkan diri kepada 'teori barat' berangsur-angsur mulai ditinggalkan. Sekalipun, seperti telah dikemukakan diatas, saat ini harus diakui, belum sepenuhnya semua menyadari atau berkenan akan menyadari 'agenda' untuk meninggalkan ketergantungan kepada justifikasi teori dari luar, terutama 'teori (**Pen**-Hukum) barat'. Masih banyak diantara kita, *jurists* Indonesia yang merasa bahwa teori dari luar, termasuk 'barat' adalah 'teori superior', kebenaran mutlak tentang hukum[38].

Hukum berisikan peraturan-peraturan yang mengatur tingkah laku manusia dan atau masyarakat (orang) di dalam masyarakat. Peraturan-peraturan tingkah laku yang mengatur orang yang disebut kaidah hukum itu mungkin saja jatuh sama artinya dengan peraturan tingkah laku manusia yang juga dikenal namun berada di luar sistem hukum. Peraturan tingkah laku atau kaidah yang mengatur manusia yang berada dalam sistem luar hukum tersebut adalah 'etika'.[39]

Sudikno Mertokusumo mengkategorisasikan kaidah etika sebagai etika sosial yang berfungsi untuk melindungi kepentingan manusia di dalam masyarakat[40]. Penekanan

[38] *Ibid*, hlm. vi.

[39] Teguh Prasetyo, *Pengantar Ilmu Hukum, Op.Cit,* hlm.19

[40] Sudikno Mertokusumo, *Mengenal Hukum Suatu Pengantar*, edisi keempat, Cetakan Peratama (Yogyakarta: Liberty, 1996), hlm.5

makna etika yang diutarkan **Profesor Sudikno Mertoksumo** adalah peraturan sosial atau kemasyarakatan yang diciptakan masyarakat untuk melindungi manusia di dalam masyarakat namun bukan hasil ciptaan hukum. Sama dengan **Van Apeldoorn**, **Mertokusumo** nampaknya sempat memasukkan hukum ke dalam bidang penyelidikan etika sebab menurut **Mertoksumo** bahwa semula kaidah sosial itu tidak dibedakan[41]. Baru setelah melalui proses yang lama, tidak disebutkan proses apa, seperti apa, berapa lama dan mulai kapan proses itu, menurut **Mertokusumo**, manusia membedakan kaidah-kaidah tersebut. Juga dikatakan oleh **Profesor Sudikno Mertokusumo**, kaidah hukum dikeluarkan dari sistem etika menjadi sistem yang berdiri sendiri. Hanya, sangat disayangkan, baik **Profesor Apeldoorn** ataupun **Profesor Sudikno Mertokusumo** keduanya 'tidak secara eksplisit' menjelaskan saat yang tepat ketika orang mempelajari kaidah-kaidah etika yang sudah dikeluarkan dari sistem hukum.

Ternyata, saat yang tepat itu dijelaskan dalam '**Teori Keadilan Bermartabat'** (*The Dignified Justice Theory)* dan sering juga disebut dengan Keadilan Bermartabat. Teori ini membagi hukum ke dalam 2 (dua) periode. Periode itu adalah periode sebelum adanya Negara dan periode setelah adanya Negara. Berikutnya Teori Keadilan Bermartabat menunjuk saat pembagian hukum dan peraturan lain-lainnya tersebut, yakni ketika manusia pertama, dalam hal ini Adam dan Hawa masih belum diusir Tuhan Yang Maha Esa untuk keluar dari Taman Eden. Dalam periode belum adanya Negara, yakni pada waktu Tuhan Yang Maha Esa bersepakat dengan Adam dan Hawa

[41] Hal yang sama juga diutarakan oleh Purnadi Purbacaraka & Soerjono Soekanto, *Perihal Kaidah Hukum*, Cetaka Pertama (Bandung: Alumni, 1978), hlm.16.

agar mereka tidak memakan buah dari pohon yang terdapat di tengah-tengah Taman Eden tersebut. Apabila mereka makan buah dari pohon pengetahuan baik dan jahat, atau mungkin dapat dipahami sebagai mereka melanggar 'kodifikasi' atau perjanjian yang disebut itu, kata Tuhan Yang Maha Esa maka mereka sepakat pula dapat dikenakan sanksi hukuman mati.

Berdasarkan rumusan itu diketahui, bahwa pada saat belum adanya Negara, yakni ketika Negara itu adalah suatu perjanjian antara Tuhan Yang Maha Esa dan Adam dan Hawa (masyarakat) itu sendiri, ada campur aduk antara peraturan keagamaan, kesusilaan juga hukum dan adat-kebiasaan, tidak ada pembedaan yang jelas antara berbagai kaidah tersebut. Namun yang pasti, pada mulanya pada waktu itu, di Taman Eden, yakni di-yurisdiksi asal mula keberadaan dan penciptaan manusia yang diyakini oleh agama-agama Samawi yang ada di Indonesia, kaidah yang diperintahkan Tuhan Yang Maha Esa tersebut adalah kaidah hukum (perjanjian yang lahir karena konvensi). Dikatakan juga sebagai kaidah hukum sebab hal itu memenuhi struktur rumusan kaidah yang mengatur delik yakni ada provisi (syarat) dan juga ada provisi tentang (sanksi) yang disertai dengan pengetahuan bagi pihak-pihak yang diatur kaidah itu bahwa ada otoritas pelaksana (eksekutor) dari ancaman sanksi yang diancamkan[42].

Keadilan bermartabat, bukanlah jenis pengertian keadilan, namun suatu teori hukum yang memberi petunjuk mengenai tujuan dalam setiap institusi hukum[43]. Tujuan dalam Keadilan Bermartabat menunjuk kepada Pancasila sebagai sumber dari segala sumber inspirasi hukum. Maka dari itu, dalam Keadilan

[42] Teguh Prasetyo, *Keadilan Bermartabat: Perspektif Teori Hukum*, Edisi Pertama, Cetakan ke-I, (Bandung: Nusa Media, 2015), hlm. v-vi,

[43] *Ibid*, hlm.1.

Bermartabat terkandung nilai-nilai sentra sosio-politik, ekonomi, kebudayaan dan lain sebagainya yang ada dalam Pancasila. Dalam Keadilan Bermartabat, Pancasila adalah jiwa bangsa (*volksgeist)*. Rujukan kepada Pancasila dikarenakan hal itu menjadi keharusan ketika pada tanggal 17 Agustus 1945 Indonesia diproklamasikan. Proklamasi mengharuskan pembentukan suatu sistem hukum yang murni, hasil saringan dan penggantian pemahaman dan pemaknaan atas konsep, kaidah, asas hukum-hukum yang pernah dipakai penjajah. Dalam Keadilan Bermartabat, tujuan hukum harus mengisi kemerdekaan dengan etos kebangsaan. Tujuan demikian itu disebut juga dengan pembaruan hukum[44].

"Keadilan Bermartabat itu bukan suatu jenis konsep keadilan seperti yang sudah sangat umum dipahami selama ini, maka ada baiknya deskripsi singkat mengenai Keadilan Bermartabat itu saya gambarkan secara singkat sebagai berikut". "Keadilan Bermartabat adalah suatu Grand Teori Hukum. Sebagai Teori Hukum yang baru, Keadilan Bermartabat berfungsi untuk menjelaskan dan memberi justifikasi suatu sistem hukum yang berlaku, yang berbeda dengan teori-teori barat yang selama ini dirujuk". "Teori Keadilan Bermartabat menjelaskan dan memberi justifikasi suatu sistem hukum dengan antara lain suatu postulat bahwa hukum itu ada dan tumbuh dalam jiwa bangsa atau *Volksgeist*"[45].

Sebagai suatu filsafat, Keadilan Bermartabat menggambarkan tujuan hukum yang ada di dalam setiap sistem hukum terutama tujuan hukum dalam sistem hukum

[44] Teguh Prasetyo, *Pengantar Ilmu Hukum, Op.Cit.* hlm.214.

[45] Teguh Prasetyo, "Kejahatan Pertambangan Dalam Perspektif Keadilan Bermartabat", Jurnal PERSPEKTIF Vol XXI No. 1 Tahun 2016 Edisi Januari, Nomor ISSN Cetak 1410- 3648 dan ISSN Online 2406-7385.

berdasarkan Pancasila. Penekanannya dilakukan terhadap asas kemanusiaan yang adil dan beradab, yang mendasari konsepsi memanusiakan manusia (*nguwongke uwong)*; di samping keadilan sosial dan sila-sila lainnya. Keadilan Bermartabat juga menjelaskan tujuan hukum dalam pengertian keadilan, kepastian dan kemanfaatan yang ada di dalam setiap asas dan kaidah hukum yang saling berkaitan satu sama lain di dalam sistem tersebut. Keadilan Bermartabat berpendirian bahwa baik keadilan, kemanfaatan dan kepastian hukum adalah merupakan satu kesatuan yang berhimpun dalam 'keadilan'. Suatu penyelarasan yang berbeda dengan dikotomi keadilan, kepastian hukum dan kemanfaatan yang sudah dipahami merupakan temuan ahli hukum **'Gustav Radbruch'.** [46]

Berdasarkan Keadilan Bermartabat ukuran moralitas termaktub dalam Sila Pertama Pancasila 'Ketuhanan Yang Maha Esa'. Ukuran tersebut harus menjadi jiwa atau roh yang terkandung dalam setiap kaidah dan asas hukum yang berlaku. Dengan demikian maka Pancasila itu adalah sumber dari segala sumber hukum. Dalam perspektif Sila Pertama Pancasila maka semua institusi hukum harus dimengerti sebagai hukum yang keberadaanya untuk menjunjung tinggi nilai etika dan moral atau sejalan dengan ajaran agama[47].

Sila kedua: dalam pembaruan hukum harus menghargai dan melindungi hak asasi manusia. Dalam Keadilan Bermartabat, maka hal itu dirumuskan sebagai berikut:

> *Hukum menciptakan masyarakat bermartabat adalah hukum yang mampu memanusiakan manusia (nguwongke uwong) artinya bahwa hukum yang memperlakukan dan menjunjung tinggi nilai-nilai kemanusiaan menurut*

[46] Teguh Prasetyo, *Keadilan Bermartabat... Op.Cit*, hlm.52.
[47] Teguh Prasetyo, *Pengantar Ilmu Hukum, Op.Cit.* hlm.215.

hakikat dan tujuan hidupnya. Hal ini dikarenakan manusia adalah makhluk yang mulia sebagai ciptaan Tuhan Yang Maha Esa sebagaimana yang tercantum dalam Sila Kedua Pancasila, yakni kemanusiaan yang adil dan beradab. Sila itu mempunyai nilai pengakuan terhadap harkat dan martabat manusia dengan segala hak dan kewajibannya serta mendapatkan perlakuan yang adil sebagai manusia, terhadap diri sendiri, alam sekitar dan terhadap Tuhan[48].

Setiap institusi hukum harus memenuhi tuntutan Sila Kedua Pancasila yakni perlindungan terhadap hak asasi manusia (HAM). Suatu institusi hukum berfungsi untuk mempertahankan nilai-nilai dalam Sila Kedua Pancasila, yakni perlindungan terhadap HAM, pelaku, korban dan masyarakat. Namun lebih daripada itu, apabila merujuk pada 'Teori Keadilan Bermartabat' yang berusaha untuk memahami pikiran Tuhan Yang Maha Esa. Hal ini dapat pula disebut sebagai produk kebudayaan Indonesia dalam hukum (*the product of civilization)*[49].

Hukum itu, dalam Keadilan Bermartabat berfungsi untuk mempertahankan nilai kemanusiaan yang ada di balik setiap kaidah dan asas hukum yang berlaku. Hal itu dapat dilihat contohnya, dalam Pasal 23 ayat (2) Undang-undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia diatur bahwa "setiap orang bebas untuk mempunyai, mengeluarkan dan menyebarluaskan pendapat sesuai hati nuraninya, secara lisan dan/atau tulisan melalui media cetak maupun elektronik dengan memerhatikan nilai-nilai agama, kesusilaan, ketertiban, kepentingan umum, dan keutuhan bangsa". Sila Ketiga Pancasila: dalam pembaruan hukum harus menghargai dan mampu mengakomodasi nilai-nilai yang hidup dalam

[48] Teguh Prasetyo, *Keadilan Bermartabat... Op.Cit*, hlm.93.
[49] Teguh Prasetyo, *Pengantar Ilmu Hukum, Op.Cit.* hlm.215-216

setiap masyarakat. Sila Keempat Pancasila: dalam pembaruan hukum kepentingan masyarakat diperhatikan tanpa mengabaikan kepentingan individu. Sila Kelima Pancasila: dalam pembaruan hukum harus memberikan jaminan perlindungan hukum yang sama dan membatasi kesewang-wenangan kekuasaan[50].

Pancasila dapat pula dikatakan sebagai *the supra–principle* dari *the structure of scientific legal theory* di Indonesia. Oleh karena itu, maka pembicaraan mengenai tiap institusi hukum tidak dapat dilepaskan dari pembicaraan *supra-principle* dari suatu sistem hukum. Sekedar mengemukakan suatu bahan perbandingan, maka dalam sistem hukum dan juga filsafat serta teori hukum barat, pada umumnya orang memahami bahwa asas yang utama dalam *supra-principle* dari struktur ilmiah suatu teori hukum di Barat yakni asas kebebasan memilih. Asas tersebut selalu dihubungkan dengan tanda keunggulan dari manusia jika dibandingkan dengan makhluk lainnya. Tanda keunggulan manusia tersebut ialah bahwa manusia adalah makhluk yang berpikir. Di dalam tanda keunggulan manusia itu terdapat suatu asas hukum yang terpenting dalam perspektif teori-teori yang berkembang di Barat, yakni asas *the principle of free choice*. Prinsip kemerdekaan untuk memilih tersebut juga sangat dikenal dalam sistem hukum Pancasila. Hal tersebut dapat dijelaskan sebagai berikut:

> *Dalam Keadilan Bermartabat, asas the principle of free choice digambarkan sebagai asas yang bukan monopoli masyarakat Barat. Undang-undang Dasar Negara Republik Indonesia Tahun 1945 (UUD 1945) bahkan menempatkan prinsip kemerdekaan manusia yang menjadi the supra principle tersebut dibaris pertamanya. Dirumuskan dalam*

[50] *Ibid*, hlm. 216.

> *UUD 1945: "Bahwa sesungguhnya kemerdekaan itu ialah hak segala bangsa dan oleh sebab itu, maka penjajahan di atas dunia harus dihapuskan, karena tidak sesuai dengan peri-kemanusiaan dan peri-keadilan". Frasa "kemerdekaan itu ialah hak segala bangsa" dalam rumusan Pembukaan UUD 1945 tersebut membuktikan bahwa the principle of free choice juga merupakan nilai hukum asli yang ada dalam bumi Indonesia tetapi juga sebagai suatu nilai hukum yang universal*[51].

Dikatakan universal karena dapat dijumpai pula di bumi Negara-negara dan bangsa beradab atau *civilized nations* lainnya dan sudah barang tentu tidak jauh berbeda esensinya. Perbedaan yang perlu diperhatikan yakni adanya aspek nilai hukum substantif dalam Pancasila yang perlu disesuaikan dalam memahami asas seperti itu, terutama nilai-nilai menurut dalam Sila Ketuhanan Yang Maha Esa. Sehubungan dengan *the principle of free choice*, dalam Teori Keadilan Bermartabat terdapat rumusan:

> *Periode pertama keberadaan hukum berlangsung di Taman Eden. Pada waktu itu, hukum mengambil bentuk lisan, yakni komunikasi langsung antara Tuhan dan manusia, di dalam suatu yurisdiksi yang bernama Taman Eden. Di dalam yurisdiksi itu manusia yang telah memperoleh peneyerahan dari Tuhan suatu kaidah fundamental yakni kebebasan untuk memilih. Manusia memilih untuk menjadi hakim bagi dirinya sendiri sebagai suatu society, karena hidup berdua sebagai suatu keluarga. Pilihan tersebut, yakni: apakah mengikuti perintah dan menikmati segala sesuatu, manfaat yang tersedia secara penuh bagi mereka... Ketuhanan Yang Maha Esa di dalam Taman Eden itu. Ataukah sebaliknya mereka dapat memilih memberontak atau tidak menuruti kaidah tersebut dan sebagai konsekuensi menerima sanksi yang tegas dari Tuhan, otoritas pembuat hukum*[52].

---

[51] *Ibid*, hlm.217.

[52] Teguh Prasetyo, *Keadilan Bermartabat... Op.Cit*, hlm. v-vi

III. Keadilan Bermartabat dan Data Pribadi

Penggunaan teknologi baik bagi pelaku usaha/penyelenggara sistem elektronik wajib menjalankan usahanya dengan berlandaskan keadilan bermartabat. Keadilan bagi semua orang, adil bagi konsumen/pengguna sistem elektronik/aplikasi *online,* adil bagi mitra kerja, adil bagi para pekerja. Penyelenggara membutuhkan konsumen/pengguna dan pengguna membutuhkan penyelenggara untuk memenuhi kebutuhan mereka melalui aplikasi *online* – semua saling membutuhkan. Konsumen/pengguna wajib memasukan data pribadi bagi mereka termasuk namun tidak terbatas pada, nama, alamat domisili, *email,* tempat/tanggal lahir, bahkan untuk menggunakan aplikasi dengan layanan plus/premium maka mensyaratkan untuk menggunggah KTP (Kartu Tanda Penduduk) beserta foto wajah/pribadi.

Penyelenggara wajib menjamin keamanan, privasi data yang telah dimasukan oleh pengguna/konsumen. Penyelenggara wajib menyediakan sistem keamanan yang mutakhir, canggih untuk mecengah oknum melakukan peretasan dan mendidik/ melatih pekerja khususnya yang bertugas mengontrol data pribadi agar bekerja secara bermartabat, berintegritas, tidak memiliki niat untuk membocorkan data pribadi secara melawan hukum.

Penyelenggara yang bermartabat tentu akan memuliakan konsumen, menghargai penggunanya. Apabila konsumen sudah kecewa, tidak percaya lagi maka reputasi aplikasi *online* bisa hancur, pengguna baik sebagai penjual ataupun pembeli dalam aplikasi itu pasti akan menarik dan menghapus akun mereka dari aplikasi bahkan dapat saja memberi *rating/* peringkat buruk (bintang 1) di *playstore* atau *istore* (tempat

pengguna mengunduh aplikasi *online)* dan akan berujung pada penutupan aplikasi, *marketplace* tersebut dan beralih ke *marketplace* yang lebih aman.

Apabila konsumen/pengguna mengeluh, secara keadilan bermartabat maka layani keluhan tersebut, tanggapi dengan baik, cari solusi bersama karena pengguna misalnya sebagai penjual yang baik di *marketplace* tersebut tentu telah beritikad baik misalnya dalam pengiriman barang, namun bisa saja pengguna sebagai pembeli beritikad buruk sehingga menyebabkan kerugian dari sisi penjual atau bahkan sebaliknya. Keadilan bermartabat adalah wadah agar sengketa diselesaikan secara *win-win solution*.

BAB III

PERLINDUNGAN DATA PRIBADI OLEH PENYELENGGARA (PEMERINTAH ATAU PRIVAT)

Masyarakat pada abad ke-21 tidak dapat tidak dilepaskan dari teknologi, internet, komputer, *smartphone*. Sebagaimana yang Penulis paparkan di bab 1 penggunaan teknologi internet sangat memerlukan data pribadi – bahkan setelah abad ke-21 dapat saja manusia lebih ber-interdependensi dengan teknologi, semua dengan *smart technology, smart car* (mobil yang dikendarai dengan sistem elektronik), *smart tv, smart contract*. Penulis ulangi dengan memberi contoh, apabila kita ingin menggunakan *platform* aplikasi *online,* Ojek *Online,* kita diminta untuk memasukkan data pribadi kita (nama, alamat, no *handphone*).

Menurut analisis Penulis, data pribadi sangat penting dilindungi karena data pribadi memuat jati diri seseorang, dimiliki orang tersebut dan dengan data tersebut maka orang tersebut baru dapat melakukan 'perbuatan hukum' (perbuatan yang menimbulkan hak dan kewajiban bagi yang membuat) dalam bentuk apapun, melakukan pembelian *online (e-commerce), teleconference* untuk mengobrol, untuk memeriksa saksi dalam perkara tertentu.

Apabila sebelum ada digitalisasi dalam sistem misalnya perbankan, kita harus data ke *customer service* untuk membuka rekening, namun sekarang dengan teknologi, kita hanya menghimpun data dengan benar dan jelas, mengunggah data pribadi. Oleh karena itu, perkembangan teknologi memberikan pergeseran paradigma *One on One* (bertemu langsung) menjadi *One on One by Internet*.

Internet merubah paradgima, pola interaksi antara *consumer to consumer (C2C), business to business (B2B), business to cosumer (B2C), consumer to government (C2G), business to government (B2G), government to government (G2G)* dari yang harus tatap muka, datang membawa dokumen sangat tebal ke kantor pemerintahan ataupun melakukan penawaran sekaang hanya dengan *scan* dokumen yang dibutuhkan, *upload* atau unggah dokumen maka perbuatan hukum kita selesai, Instansi Pemerintahan juga menjalankan prinsip *e-government* (pelayanan pemerintahan secara elektronik).

Data pribadi yang kita/pengguna himpun ke dalam sistem elektronik bersifat rahasa dan wajib dilindungi. Penyelenggara Sistem Transaksi Elektronik/*platform* wajib menjaga keutuhan, kerahasiaan data tersebut dari *hacker*/ peretas dan menjamin untuk tidak disalahgunakan, dijual. Penulis juga menghimbau seyogyanya aplikator melakukan *double check* terhadap data pribadi misalnya dengan menelpon pemilik data pribadi tersebut karena dewasa ini, modus penipuan semakin *online*, oknum dapat dengan mudah mendapatkan data pribadi kita di internet, menggunakanya seolah-olah itu adalah data pribadinya.

Kepintaran intelektual baik berupa otak manusia, ataupun kepintaran buatan (*artificial intelligence*[53]) harus dipergunakan dengan baik, tidak melawan hukum dan bermuatan keadilan bermartabat. Sebagaimana Penulis jelaskan di Bab II dan akan Penulis tekankan lagi bahwasanya, keadilan bermartabat berangkat dari postulat sistem; bekerja mencapai tujuan yakni keadilan bermartabat. Keadilan yang memanusiakan manusia atau keadilan yang *'nguwongke uwong'*. Konsepsi keadilan bermartabat digali dari falsafah Bangsa Indonesia. Jati diri Bangsa Indonesia yang termanifestasikan dalam Pancasila. Pancasila merupakan sumber dari segala hukum dan sebagai ideologi, sebagai falsafah bangsa dan Negara. Apabila ada oknum yang melakukan pembocoran data pribadi maka oknum tersebut tidak bermartabat dan patut untuk diberikan sanksi.

Pengaturan data pribadi yang ideal adalah peraturan yang mengikuti perkembangan zaman berlandaskan nilai-nilai filosofis, landasan sosiologis dan landasan yuridis. Walaupun media data pribadi adalah teknologi komputer, internet dan sistem elektornik namun wajib tetap berlandaskan nilai-nilai kejujuran, nilai tanggung jawab, dan nilai saling menghargai. Pengaturan data pribadi yang ideal berangkat dari fakta empiris bahwa data pribadi masih banyak disalahgunakan, oknum yang bekerja atau menguasi IT melakukan *'knock down'* yang bermuatan melawan hukum. Data pribadi wajib dilindungi, Penulis teringat perkataan guru Penulis, Prof.

[53] Definisi *Artificial Intelligence* masih menjadi perdebatan. Namun jika mengacu pada Rusell *and* Norvig (2009, *Artificil Intelligence: A Modern Approach (3rd edition)*. Harlow: Pearson bahwa untuk memberikan definisi *AI* maka harus berpatokan pada 4 empat pendekatan: *the ratonal agent approach, the "law of thought" approach, the cognitve modelling approach, and the Turing test approach*. Dapat diakses di http://ejlt.org/article/view/675/915 diakses tanggal 18 Mei 2020

Sudarto bahwa kejahatan tidak akan sepi dari dunia, maka dari itu menurut Penulis, hukum harus bermartabat, hukum mau tidak mau harus menyesuaikan perkembangan zaman. Dan data pribadi wajib dijaga karena hal tersebut akan berpengaruh terhadap reputasi perusahaan *e-commerce* atau penyelenggara sistem elektronik.

I. Tinjauan Umum Perlindungan Data Pribadi

I.1. Definisi Data Pribadi

Apabila merujuk pada *Black's Law Dictionary*, data pribadi termasuk sebagai *classified information. Data or material that, having been designated as secret or confidential, only a limited number of authorized persons may know about*[54]. Definsi *data protection ialah any method of securing information, esp. information stored on a computer, from being either physically lost or seen by an unauthorized person.* Menurut hemat **Penulis,** data pribadi adalah informasi tunggal ataupun sekumpulan informasi baik yang bersifat rahasia ataupun tidak yang diberikan oleh pemilik data pribadi/konsumen dan dihimpun ke dalam sistem elektronik yang diproses oleh penyelenggara sistem elektronik untuk dipergunakan sesuai dengan tujuan&kegunaanya serta apabila disalahgunakan maka pemilik/konsumen dapat menyelesaikannya melalui media hukum administrasi Negara dan/atau media hukum perdata dan/atau media hukum pidana.

Penulis akan memaparkan pelbagai peraturan perundang-undangan yang memberikan definisi tentang 'data pribadi' secara eksplisit, yakni:

---

[54] *Black's Law Dictonary,* hlm. 753

a. UU ITE tidak memberikan definisi data pribadi dalam Pasal 1. Namun dalam Penjelasan Pasal 26 ayat (1) UU ITE bahwa perlindungan data pribadi merupakan salah satu bagian dari hak pribadi (*privacy rights)*.
b. Data pribadi adalah setiap data tentang seseorang baik yang teridentifikasi dan/atau dapat diidentifikasi secara tersendiri dan/atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik dan/atau non-elektronik. (Dasar Hukum: Pasal 1 Angka 29 Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik);
c. Peraturan Pemerintah No. 80 Tahun 2019 tentang Perdagangan Melalui Sistem Elektronik tidak memberikan definisi 'data pribadi' dalam Pasal 1 namun pengaturan 'data pribadi' diatur dalam Bab XI, Pasal 58, Pasal 59. Salah satu pengaturannya yakni Setiap data pribadi diberlakukan sebagai hak milik pribadi dari orang atau pelaku usaha yang bersangkutan.
d. Undang-undang No. 24 Tahun 2013 tentang Perubahan Atas Undang-undang No. 23 Tahun 2006 tentang Administrasi Kependudukan (UU Adminduk). UU Adminduk memberikan 2 (dua) terminilogi antara data kependudukan dengan data pribadi. Definsi data kependudukan adalah data perseorangan[55] dan/atau data

[55] Berdasarkan Pasal 58 ayat (2) UU Adminduk bahwa Data perseorangan meliputi: a. nomor KK; b. NIK; c. nama lengkap; d. jenis kelamin; e. tempat lahir; f. tanggal/bulan/tahun lahir; g. golongan darah; h. agama/kepercayaan; i. status perkawinan; j. status hubungan dalam keluarga; k. cacat fisik dan/atau mental; l. pendidikan terakhir; m. jenis pekerjaan; n. NIK ibu kandung; o. nama ibu kandung; p. NIK ayah; q. nama ayah; r. alamat sebelumnya; s. alamat sekarang; t. kepemilikan akta kelahiran/surat kenal lahir; u. nomor akta kelahiran/nomor surat kenal lahir; v. kepemilikan akta perkawinan/buku nikah; w. nomor akta perkawinan/buku nikah; x.

agregat[56] yang terstrtukur sebagai hasil dari kegiatan pendaftaran penduduk[57] dan pencatan sipil[58] (Pasal 1 Angka 9 UU Adminduk), sedangkan definisi 'data pribadi' adalah data perseorangan tertentu yang disimpan, dirawat dan dijaga kebenaran serta dilindungi kerahasiannya (Dasar Hukum, Pasal 1 Angka 22 UU Adminduk).

e. Data pribadi adalah data perseorang tertentu yang disimpan, dirawat, dan dijaga kebenaran serta dilindungi kerahasiananya (Pasal 1 Angka 20 Peraturan Menteri Dalam Negeri RI No. 102 Tahun 2019 tentang Pemberian hak akses dan pemanfaataan data kependudukan (Berita Negara RI Tahun 2019 No. 1611).
f. Data pribadi adalah data perseorangan tertentu yang disimpan, dirawat dan dijaga kebenaran serta dilindungi kerahasiaannya. (Dasar Hukum: Pasal 1 Angka 1 Peraturan Menteri Komunikasi dan Informatika No. 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik);
g. Data pribadi nasabah adalah identitas yang lazim disediakan oleh nasabah kepada Bank dalam rangka melakukan transaksi keuangan dengan Bank (Dasar Hukum: Pasal 1 Angka 6 Peraturan Bank Indonesia No: 7/6/PBI/2005 tentang

---

tanggal perkawinan; y. kepemilikan akta perceraian; z. nomor akta perceraian/surat cerai; aa. tanggal perceraian; bb. sidik jari; cc. iris mata; dd. tanda tangan; dan ee. elemen data lainnya yang merupakan aib seseorang.

[56] Yang dimaksud dengan "data agregat" adalah kumpulan data tentang Peristiwa Kependudukan, Peristiwa Penting, jenis kelamin, kelompok usia, agama, pendidikan, dan pekerjaan. Penjelasan Pasal 58 ayat (3) UU Adminduk

[57] Berdasarkan Pasal 1 Angka 10 UU Adminduk, Pendaftaran Penduduk adalah pencatatan biodata Penduduk, pencatatan atas pelaporan Peristiwa Kependudukan dan pendataan Penduduk rentan Administrasi Kependudukan serta penerbitan Dokumen Kependudukan berupa kartu identitas atau surat keterangan kependudukan.

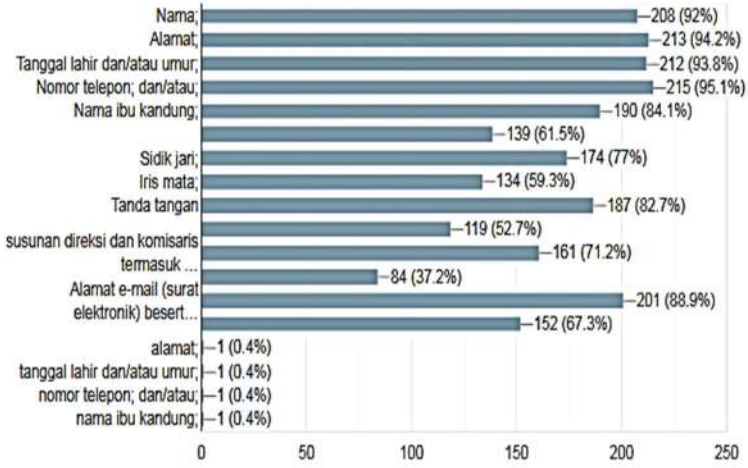
[58] Berdasarkan Pasal 1 Angka 15 UU Adminduk, Pencatatan Sipil adalah pencatatan Peristiwa Penting yang dialami oleh seseorang dalam register Pencatatan Sipil pada Instansi Pelaksana.

Transparansi Informasi Produk Bank dan Penggunaan Data Pribadi Nasabah).

h. Data dan/atau informasi pribadi konsumen adalah data dan/atau informasi, yang mencakup sebagai berikut:
   1. Perseorangan; a. nama; b. alamat; c. tanggal lahir dan/atau umur; d. nomor telepon; dan/atau; e. nama ibu kandung;
   2. Korporasi: a. nama; b. alamat; c. nomor telepon; d. susunan direksi dan komisaris termasuk dokumen identitas berupa Kartu Tanda Penduduk/Paspor/Izin tinggal; dan/atau; e. susunan pemegang saham. (Dasar Hukum: Surat Edaran Otoritas Jasa Keuangan No: 14/SEOJK.07/2014 tentang Kerahasiaan dan Keamanan Data dan/atau Informasi Pribadi Konsumen);

i. Data pribadi adalah setiap data tentang seseorang baik yang teridentifikasi dan/atau dapat secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung ataupun tidak langsung melalui sistem elektronik dan/atau non-elektronik (Naskah Rancangan Undang-undang Pelindungan Data Pribadi per Desember 2019).

Berdasarkan data yang **Penulis** dapatkan bahwa responden telah memiliki pengetahuan yang baik tentang bentuk data pribadi sebagaimana digambarkan pada grafik dibawah ini:



Grafik 16. Bentuk Data Pribadi
Sumber: Dokumen pribadi.

I.2. Definisi Perlindungan Data Pribadi

Menurut hemat **Penulis,** perlindungan data pribadi adalah upaya yang dilakukan oleh pengguna data pribadi, penyelenggara sistem elektronik baik secara preventif (pencegahan), persuasif (pengarahan), represif ataupun kuratif terhadap data pribadi yang dihimpun oleh pemilik data pribadi/konsumen ke dalam sistem elektronik penyelenggara supaya data tersebut dijaga, dilindungi dan terhindar dari penyalahgunaan yang merugikan pemilik data/konsumen tersebut. *Protecting the privacy of personal information is important because of the key role of privacy in protecting core values which underlie many other human rights*[59].

Apabila merujuk pada Penjelasan Pasal 26 ayat (1) UU ITE dipaparkan bahwa "dalam pemanfaatan teknologi informasi,

[59] Moira Paterson *and* Maeve McDonagh *"Data Protection in an Era of Big Data: The Challenges Posed by Big Personal Data"*. Monash University Law Review (Vol 44, No 1), hlm. 6

perlindungan data pribadi merupakan salah satu bagian dari hak pribadi (*privacy rights)*. Hak pribadi mengandung pengertian sebagai berikut: a. hak pribadi merupakan hak untuk menikmati kehidupan pribadi dan bebas dari segala macam gangguan; b. hak pribadi merupakan hak untuk dapat berkomunikasi dengan orang lain tanpa tindakan memata-matai; c. hak pribadi merupakan hak untuk mengawasi akses informasi tentang kehidupan pribadi dan data seseorang.

I.3. Landasan Filosofis Perlindungan Data Pribadi di Indonesia

Menurut hemat **Penulis,** landasan filosofis perlindungan data pribadi di Indonesia ialah Pancasila dan Undang-undang Dasar Negara Kesatuan Republik Indonesia Tahun 1945 Hasil Amandemen ke-IV (selanjutnya disebut UUD 1945) mengamanatkan dalam Pasal 28G ayat (1) bahwa "setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat dan harta benda yang di bawah kekuasannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi". Data pribadi wajib dijaga dan dilindungi untuk mengejawantahkan Sila ke-2 Pancasila yakni "Kemanusiaan yang Adil dan Beradab". Tindakan membocorkan data bukanlah perbuatan yang beradab melainkan perbuatan melawan hukum, tidak bermartabat dan pelakunya wajib bertanggung jawab. Pelaku usaha yang memanfaatkan teknologi wajib membuat sistem keamanan yang canggih dan menjamin bahwa pekerjanya tidak akan membocorkan data pribadi dalam sistem elektronik yang dikendalikannya.

Apabila merujuk pada Naskah Akademik Rancangan Undang-undang Pelindungan Data Pribadi (RUU PDP). Dasar

pertimbangan filosofis perlindungan data pribadi sebagaimana dimuat dalam Rancangan Undang Undang Perlindungan Data Pribadi (RUU PDP) ialah bahwa: a. bahwa privasi atas data pribadi adalah pengakuan dan perlindungan atas hak-hak dasar manusia yang telah dilindungi berdasarkan Hukum Internasional, Regional dan Nasional; b. bahwa perlindungan privasi atas data pribadi merupakan hak asasi yang diamanatkan langsung oleh konstitusi Negara Republik Indonesia; c. bahwa privasi atas data pribadi merupakan kebutuhan untuk melindungi hak-hak individual di dalam masyarakat sehubungan dengan pengumpulan, pemrosesan, penyelenggaraan, dan penyebarluasan data pribadi.

Apabila merujuk pada hukum internasional, *Article 12 Universal Declaration of Human Rights "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 attacks"* (**PEN-**terjemahan bebas: Setiap orang dilindungi hukum dan seyogyanya tidak mengalami gangguan terhadap privasi, keluarga, rumah atau korespondensi. Setiap orang berhak atas perlindungan hukum terhadap gangguan hak privasi tersebut).

I.4. Landasan Sosiologis Perlindungan Data Pribadi di Indonesia

Menurut hemat **Penulis,** Masyarakat di Indonesia di era abad ke-21 tidak dapat dilepaskan dari ketergantungan teknologi, internet, komputer, telepon genggam canggih (*smartphone)*. Fenomena ini dapat kita lihat di lingkungan kita, di dalam keluarga kita. Sedikit-sedikit perhatian, mata tertuju pada *handphone (HP)* walaupun tidak ada notifikasi/

pemberitahuan pada *HP* kita tersebut. Apabila diperhatikan di trotoar dibilangan daerah Sudirman, Jakarta Pusat, pekerja, orang berjalan kaki namun memperhatikan *HP* mereka bahkan penggunaan *HP* tetap dilakukan saat berkendara yang notabene diketahui dapat membahayaan keselamatan dan walapun sudah dilarang oleh Undang-undang.

Keberadaan *HP,* gawai lainnya yang berfungsi untuk mengirimkan informasi/dokumen elektronik memang ada sisi positifnya yakni memudahkan pekerjaan, kehidupan masyarakat, namun juga memiliki sisi negatif, yakni terhadap keamanan data pribadi (*privacy data)*. Penggunaan internet gratis di ruang publik (*free wifi)* berpotensi terhadap tindak pidana peretasan (*hacking)* gawai, dan mengambil serta menyalahgunakan data privasi dalam gawai tersebut. Potensi kejahatan tersebut harus diantisipasi.

Salah 1 pertimbangan sosiologis dalam RUU PDP ialah bahwa perlindungan yang memadai atas privasi menyangkut data pribadi akan mampu memberikan kepercayaan masyarakat untuk menyediakan data dan/atau informasi pribadi, guna berbagai kepentingan masyarakat yang lebih besar tanpa disalahgunakan atau melanggar hak-hak pribadinya.

Perumusan aturan tentang Privasi atas Data Pribadi dapat dipahami karena adanya kebutuhan untuk melindungi hak-hak individual di dalam masyarakat sehubungan dengan pengumpulan, pemrosesan, penyelenggaraan, penyebarluasan data pribadi. Perlindungan yang memadai atas privasi menyangkut data dan pribadi akan mampu memberikan kepercayaan masyarakat untuk menyediakan data dan informasi pribadi guna berbagai kepentingan masyarakat yang lebih besar tanpa disalahgunakan atau melanggar hak-hak

pribadinya. Dengan demikian, pengaturan ini akan menciptakan keseimbangan antara hak-hak individu dan masyarakat yang diwakili kepentingannya oleh negara. Pengaturan tentang privasi atas data dan informasi pribadi ini akan memberikan kontribusi yang besar terhadap terciptanya ketertiban dan kemajuan dalam masyarakat informasi[60].

I.5. Landasan Yuridis Perlindungan Data Pribadi di Indonesia

Landasan yuridis perlindungan data pribadi di Indonesia berdasarkan Naskah Akademik RUU PDP yakni: Pasal 28G Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 "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 merupakan hak asasi". Selain itu, dalam Undang-Undang Nomor 17 Tahun 2007 tentang Rencana Pembangunan Jangka Panjang Nasional 2005-2025 juga telah ditentukan bahwa untuk mewujudkan bangsa yang berdaya saing harus meningkatkan pemanfaatan ilmu pengetahuan dan teknologi. Amanah perlindungan hak asasi manusia terkait data pribadi tersebut kemudian diimplementasikan dalam UU HAM. Selain itu pengaturan perlindungan data pribadi terdapat dalam ketentuan mengenai data pribadi di antaranya, dalam Undang-Undang Nomor 24 Tahun 2013 tentang Perubahan atas Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan, Undang-Undang Nomor 36 Tahun 2009 tentang Kesehatan, Undang-Undang Nomor 11 Tahun 2008

[60] Paragraf ke-4 Penjelasan Bagian Umum Rancangan Undang-Undang Perlindungan Data Pribadi

tentang Informasi dan Transaksi Elektronik, Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan, dan Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen. Di samping itu terdapat pula ketentuan-ketentuan yang terkait dengan keberadaan data pribadi, namun belum secara tegas dan efektif melindungi data pribadi di antaranya, Undang-Undang Nomor 40 Tahun 2014 tentang Perasuransian, Undang-Undang Nomor 21 Tahun 2011 tentang Otoritas Jasa Keuangan, dan Undang-Undang Nomor 28 Tahun 2007 tentang Perubahan Ketiga atas Undang-Undang Nomor 6 Tahun 1983 tentang Ketentuan Umum dan Tata Cara Perpajakan[61].

Namun menurut hemat **Penulis,** landasan yuridis tersebut masih harus dilengkapi. *Lex Specialis* tentang perlindungan data pirbadi di Indonesia saat ini belum ada dan hingga penyusunan buku ini (**Pen-Juni 2020)** pengaturan tentang perlindungan data pribadi di Indonesia masih tersebar dalam pelbagai peraturan sektoral. RUU PDP pun masih dalam pembahasan. Pemerintah telah berupaya untuk memberikan perlindungan data pribadi di Indonesia dengan menerbitkan peraturan perundang-undangan, antara lain:

1) Undang-undang No. 8 Tahun 1997 tentang Dokumen Perusahaan (Lembaran Negara Republik Indonesia Tahun 1997 No. 18, Tambahan Lembaran Negara RI No. 3674);
2) Undang-undang No. 10 Tahun 1998 (Lembaran Negara Republik Indonesia Tahun 1998 No. 182, Tambahan Lembaran Negara Republik Indonesia No. 3790) tentang Perubahan Atas Undang-undang No. 7 Tahun 1992

[61] Naskah Akademik RUU PDP hlm. 127-129

tentang Perbankan (Lembaran Negara Republik Indonesia Tahun 1992 No. 31, Tambahan Lembaran Negara Republik Indonesia No. 3472)

3) Undang-undang No. 39 Tahun 1999 tentang Hak Asasi Manusia (Lembaran Negara Republik Indonesia Tahun 1999 Nomor 165, Tambahan Lembaran Negara Republik Indonesia Nomor 3886), selanjutnya disebut UU HAM;
4) Undang-undang No. 29 Tahun 2004 tentang Praktik Kedokteran (Lembaran Negara Republik Indonesia Tahun 2004 No. 116, Tambahan Lembaran Negara RI No. 4431);
5) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik lndonesia Tahun 2008 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 4843) sebagaimana telah diubah dengan 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), selanjutnya disebut UU ITE;
6) Undang-undang No. 21 Tahun 2008 tentang Perbankan Syariah (Lembaran Negara Republik Indonesia Tahun 2008 No. 94, Tambahan Lembaran Negara RI No. 4867);
7) Undang-undang No. 36 Tahun 2009 tentang Kesehatan (Lembaran Negara Republik Indonesia Tahun 2009 No. 144, Tambahan Lembaran Negara RI No. 5063);
8) Undang-undang No. 21 Tahun 2011 tentang Otoritas Jasa Keuangan (Lembaran Negara Republik Indonesia Tahun 2011 No. 111, Tambahan Lembaran Negara RI No. 5253);
9) Undang-undang No. 11 Tahun 2012 tentang Sistem Peradilan

Pidana Anak (Lembaran Negara Republik Indonesia Tahun 2012 No. 153, Tambahan Lembaran Negara RI No. 5332);

10) Undang-undang No. 24 Tahun 2013 (Lembaran Negara RI Tahun 2003, Nomor 232, Tambahan Lembaran Negara Republik Indonesia No. 5475) tentang Perubahan Atas Undang-undang No. 23 Tahun 2006 tentang Administrasi Kependudukan Lembaran Negara Republik Indonesia Tahun 2006, Nomor 124, Tambahan Lembaran Negara Republik Indonesia No. 4674)
11) Undang-Undang Nomor 7 Tahun 2014 tentang Perdagangan (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 45, Tambahan Lembaran Negara Republik Indonesia Nomor 5512), selanjutnya disebut UU Perdagangan;
12) Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2019 Nomor 185, Tambahan Lembaran Negara Republik Indonesia Nomor 6400), selanjutnya disebut PP PSTE;
13) Peraturan Pemerintah No. 80 Tahun 2019 tentang Perdagangan Melalui Sistem Elektronik (Lembaran Negara Republik Indonesia Tahun 2019 Nomor 222, Tambahan Lembaran Negara Republik Indonesia Nomor 6420), selanjutnya disebut PP PMSE;
14) 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), selanjutnya disebut Permenkominfo PDPSE;

I.6. Prinsip Perlindungan Data Pribadi dalam Instrumen Hukum Internasional

Menurut hemat **Penulis,** Data pribadi dalam sistem elektronik berupa informasi elektronik di sistem elektronik, di dunia maya, pengiriman data, transmisi data dilakukan dengan sangat cepat melintasi batas Negara, batas teritorial dengan menggunakan internet (*borderless)* dan bersifat *cyberspace.*

Berdasarkan instrumen hukum internasional, perlindungan data pribadi dalam sistem elektronik sangat diperlukan karena merupakan hak privasi (*the right to privacy)*. **Penulis** akan menguraikan beberapa instrumen hukum internasional yang mengatur tentang perlindungan data pribadi dan standar internasional dalam pengamanan data di sistem elektronik, yakni:

1) ***The Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data No. 108 Year 1981*** **(Selanjutnya disebut Konvensi Eropa 108/1981)*;***

   Konvensi Eropa 108/1981 terdiri dari 27 Pasal. *Article* I membahas tentang objek dan tujuan; *Article 2* membahas tentang defines; *Article 3* tentang jangkauan; *Article 4* membahas tentang kewajiban para pihak; *Article 5* membahas tentang kualitas data; *Article 6* membahas tentang data dengan kategori khusus; *Article 7* membahas tentang keamanan data; *Article 8* membahas tentang perlindungan tambahan untuk subyek data (*additional safeguards for the data subject)*; *Article 9* membahas tentang pengecualian dan pembatasan; *Article 10* membahas tentang sanksi dan pemulihan; *Article 11* membahas

tentang perpanjangan perlindungan (*Extended protection); Article 12* membahas tentang lintas batas data pribadi dan hukum domestik (*Transborder flows of personal data and domestic law); Article 13* membahas tentang kerjasama antara para pihak; *Article 14* membahas tentang bantuan untuk subyek data yang menetap di luar negeri *(Assistance to data subjects resident abroad); Article 15* mengatur tentang perlindungan tentang bantuan yang diberikan oleh otoritas yang ditunjuk (*Safeguards concerning assistance rendered by designated authorities); Article 16* mengatur tentang penolakan untuk permintaan bantuan; *Article 17* mengatur tentang biaya dan prosedur pembantuan; *Article 18* mengatur tentang komposisi komite/pengurus; *Article 19* mengatur tentang fungsi komite; *Article 20* membahas tentang prosedur; *Article 21* mengatur tentang amandemen/ perubahan konvensi; *Article 22* mengatur tentang waktu berlaku konvensi *(Entry into force); Article 23* mengatur tentang aksesi oleh Negara bukan anggota *(Accession by non-member States*); *Article 24* mengatur tentang klausa territorial; *Article 25* mengatur tentang reservasi; *Article 26* mengatur tentang pengaduan (*Denunciation*); *Article 27* mengatur tentang pengumuman (*Notifications*);
Pokok-pokok pengaturan dalam konvensi ini ialah:

1.1 Dengan pertimbangan untuk memperluas perlindungan atat hak dasar, dan kebebasan semua orang, khususnya hak untuk menghormati privasi dengan mempertimbangkan meningkatnya pertukaran batas data pribadi yang diproses secara otomatis[62].

[62] *Bagian Preamble,* Konvensi 108/1981

1.2 Definisi data pribadi ialah: pelbagai informasi yang berkaitan dengan individu yang telah teridentifikasi ataupun dapat diidentifikasi *("personal data" means any information relating to an identified or identifiable individual ("data subject")*[63]*;*

1.3 Konvensi ini berlaku bagi para pihak yang menjalankan pemrosesan otomatis data pribadi baik di sektor publik dan swasta. *(The Parties undertake to apply this Convention to automated personal data files and automatic processing of personal data in the public and private sectors.)*[64]*;*

1.4 Syarat Data. *Personal data undergoing automatic processing shall be: a obtained and processed fairly and lawfully; b stored for specified and legitimate purposes and not used in a way incompatible with those purposes; c adequate, relevant and not excessive in relation to the purposes for which they are stored; d accurate and, where necessary, kept up to date; e preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored*[65]*;*

1.5 Tindakan Keamanan. *Appropriate security measures shall be taken for the protection of personal data stored in automated data files against accidental or unauthorised destruction or accidental loss as well as against unauthorised access, alteration or dissemination*[66]*;*

---

[63] *Article 2 (a)* Konvensi Eropa 108/1981
[64] *Article 3 (1)* Konvensi Eropa 108/1981
[65] Article 5 Konvensi Eropa 108/1981– Qualitu of data
[66] *Article 7* Konvensi Eropa 108/1981 – *Data Security*

1.6 Sanksi dan Pemulihan. *Each Party undertakes to establish appropriate sanctions and remedies for violations of provisions of domestic law giving effect to the basic principles for data protection set out in this chapter*[67].

2) The Organization for Economic Cooperation and Development Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data Year 2013;

*The Organization for Economic Cooperation and Development (*Selanjutnya disebut OECD) adalah organisasi internasioal yang bekerja untuk membuat kebijakan yang lebih baik untuk mewujdukan kehidupan yang lebih baik dan telah aktif sejak 60 tahun lalu[68].

Keterlibatan OECD dengan Indonesia berdasarkan Kerangka Perjanjian Kerja Sama yang pertama kali ditandatangani pada tahun 2012 dan diperbarui pada tahun 2017 oleh Sekretaris Jenderal OECD Angel Gurría dan Menteri Keuangan Indonesia, Sri Mulyani Indrawati. Kerangka perjanjian ini disusun berdasarkan Program Kerja Bersama (*Joint Work Programme/JWP*), yang biasanya berlangsung selama dua tahun, tetapi akan berjalan selama tiga tahun, mulai tahun 2019. JWP dikembangkan melalui konsultasi mendalam dengan para pemangku kepentingan kebijakan utama di Indonesia serta direktorat OECD substantif, dan didasarkan pada prioritas kebijakan strategis negara[69]. Hingga penyusunan buku ini dibuat (Februari 2020), Indonesia masih belum menjadi *member countries OECD.*

[67] *Article 10* Konvensi Eropa 108/1981 – *Sanctions and remedies*.

[68] https://www.oecd.org/about/ diakses tanggal 24 Maret 2020

[69] OECD, "OECD dan Indonesia", Oktober 2018, Perancis: Global Relations Secretariat, Hlm. 7.

Hingga saat ini, anggota *OECD* berjumlah 36 (tiga puluh enam) Negara dari Amerika bagian Utara, Amerika Bagian Selatan, Eropa dan Asia Pasifik[70].

OECD mengeluarkan panduan terhadap perlindungan data pribadi. *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (2013) yang terdiri dari 5 (lima) bagian yakni: bagian 1 definisi umum; bagian 2 prinsip dasar penerapan nasional; bagian 3 prinsip aplikasi internasional: Aliran bebas dan pembatasan yang sah; bagian 4 implementasi nasional; bagian 5 kerjasama internasional[71].

Adapun pokok-pokok pengaturan perlindungan data pribadi menurut panduan OECD (2013) yakni:

3.1 Bahwa pertimbangan panduan ini yakni: (1). *That, although national laws and policies may differ, Member countries have a common interest in protecting privacy and individual liberties, and in recording fundamental but competing values such as privacy and te free flow of information; (2). That automatic processing and transborder flows of personal data create new forms of relationship among countries an require the development of compatible rules and practices; (3). That transborder flows of personal data contribute to economic and social development; (4). Thet domestic legislation concerning privacy protection and transborer flows of personal data may hinder such transborder flows.*

[70] https://www.oecd.org/about/members-and-partners/ diakses tanggal 25 Maret 2020

[71] https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm diakses tanggal 25 Maret 2020

3.2 Prinsip-prinsip dasar untuk diterapkan nasional

1. ***Collection limitation principle***. *There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and where appropriate, with the knowledge or consent of the data subject;*
2. ***Data Quality Principle.*** *Personal data should be relevant to the purposes for which they are to be used, and to the extent necessary for those purposes, shoul be accurate, complete and kept up-to-date;*
3. ***Purpose Specifiaction Principle.*** *The purpose for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others are not incompatible with those purposes and as are specified on each occasion of change of purpose;*
4. ***Use Limitation Principle.*** *Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in: a. with the consent of the data subject; or b. by the authority of law;*
5. ***Security Safeguards Principle.*** *Personal data should be protected by reasonable security safeguards against such risk as loss or unauthorized access, destruction, use, modificiation or disclosure of data;*
6. ***Openness Principle.*** *There should be a general policy of openness about developments, practices, and policies with respect to personal data. Means should*

be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller;

7. ***Individual Participation Principle.*** *An individual should have the right: a. to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; b. to have communication to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him; c. to be given reasons if a request made nder subparagrpahs (a) and (b) is denied, and to be able to challenge such denial; and d. to challenge data relating to hm; and if the challenge is successful to have the data erased, rectified, completed or amended.*
8. ***Accountability Principle.*** *A data controller should be accountable for complying with measures which give effect to the principles stated above*[72].

3) The Guidelines for the Regulation of Computerized Personal Data Files (General Assembly Resolution 45/95)*, selanjutnya disebut *GAR 45/95

Guidelines for the Regulation of Computerized Personal Data Files Adopted by General Assembly resolution 45/95 of 14 December 1990. Dalam *guidelines* ini terdapat 10 (sepuluh) prinsip yang seyogyanya diterapkan dalam legislasi nasional, yakni:

[72] https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm diakses tanggal 25 Maret 2020

1. ***Principle of lawfulness and fairness.*** *Information about person should not be collected or processed in unfair or unlawful ways;*
2. ***Principle of Accuracy.*** *Persons responsible for the compilation of files or those responsible for keeping them have an obligation to conduct regular checks on the accuracy and revelance of the data recorded and to ensure that they are kept as complete as possible in order to avoid errors of omission and that they are kept up to date regulary or when the information contained in a file is used, as long as they are being processed;*
3. ***Principle of the purpose-specification****. The purpose which a file is to serve and its utilization in terms of that purpose should be specified, legitimate.*
4. ***Principle of interested-person access.*** *Everyone who offers proof or identity has the right to know whether information concerning him is being processed and to obtain it an intelligible form, without undue delay or expense, and to have appropriate rectificiations or erasures made in the case of unlawful, unnecessary or inaccurate entries, and wen it is being communicated to be informed of the addresses.*
5. ***Principle of non-discrimination.*** *Subject to cases of exceptions restrictively envisaged under principle 6 (***PEN-***power to make exceptions), data likely to give rise to unlawful or arbitrary discrimination, including information on racial or ethnic origin, colour, sex life, political opinions, religious, philosophical and other beliefs as well as membership of an association or trade union, should not be compiled;*

6. ***Power to make exceptions.*** *Departures from principles 1 to 4 (1. Principle of lawfulness and fairness, 2. Principle of accuracy, 3. Principle of the purpose – specification, 4. Principle of interested - person access) may be authorized only if they are necessary to 'protect national security', public order, public health or morality, as well as inter alia, the rights and freedoms of others, especially persons being presucated (humanitarian clause) provided that such departures are expressly specified in a law or equivalent regulation promulgated in accordance with the internal legal system whicy expressly states their limits and sets forth appropriate safeguards.*

   *Exceptions to principle 5 (***PEN-***Principle of non-discrimination) relating to the prohibition of discrimination, in addition to being subject to the same safeguards as those prescribed for exceptions tio principles 1 (Principle of lawfulness and fairness) and 4 (Principle of interested - person access), may be authorized only within the limits prescribed by the International Bill of Human Rights and the other relevant instruments in the filed of protection of human rights and the prevention of discrimination.*

7. ***Principle of Security.*** *Appropriate measures should be taken to protect the files against both natural dangers, such as accidental loss or destruction and human dangers, such as unauthorized access, fraudulent misuse of data or contaminationby computer viruses.*

8. ***Supervision and sanctions****. The law of every country shall be designate the authority which, in accordance with its domestic legal system, is to*

be responsible for supervising observance of the principles set forth above. This authority shall offer guarantess of impartiality, independence vis-à-vis persons or agencies responsible for processing and establishing data, and technical competence. In the event of violation of the provisions of the national law implementing the aforementioned principles, criminal or other penalties should be envisaged together with the appropriate individual remedies.

9. ***Transborder Data Flows.*** *When the legislation of two or more countries concerned by a transborder data flow offers comparable safeguards for the protection of privacy, information should be able to circulate as freely as inside each of the territories concerned. If there are no reciprocal safeguards, limitations on such circulation may not be imposed unduly and only in so far as the protection of privacy demands.*
10. ***Filed of Application.*** *The present principles should be made applicable, in the first instance, to all public and private computerized files as well as, by means of optional extension and subject to appropriate adjustmenst, to manual files. Special provision, also optional, might be made to extend all or part of the principles to files on legal persons particularly when they contain some information on individuals.*

4) The Data Protection Directive 95/46

Directive 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

Definisi *personal data: shall mean any information relating to an identified or identifiable natural person ('data subject'); an indetifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.* Definisi *'processing of personal data' ('processing') shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making availbale, alignment or combination, blocking, erasure or destruction.*

Prinsip perlindungan data dalam *the data protection directive 95/46 article 6 (1) member states shall provide that personal data must be: (a). processed fairly and lawfully; (b). collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purpose. Further processing of data for historical, statistical or scientific purposes shall not be considered as incaompatible provided that member states provide appropriate safeguards; (c). adequate, relevant and not excessive in relation to the purposes for which they are collected and/or futher processed; (d). accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified; (e). kept in a form which permits identification of data subjects for no longer than is*

necessary for the purposes for which the data were collected or for which they are further processed. Member states shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.

Syarat data yang dapat diproses. Berdasarkan *article 7 member states shall provide that personal data may be processed only if: (a). the data subject has unambiguously given his consent; or (b). processing is necessary for the performance of a contract tpo which the data subject is party or in order to take steps at the request of the data subject prior to entering info a contract; or (c). processing is necessary for compliance with a legal obligation to which the controller is subject; or (d). processing is necessary in order to protect the vital interests of the data subject: (e). processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the date are disclosed; or (f). processing is necessary for the purposes of the legitimate interest pursued by the controller or by the third party or partiesn whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms the data subject which require protection under Article 1 (1)*[73].

***5) General Data Protection Regulation (GDPR)* di Uni Eropa;**

Pada tahun 2016, peraturan perlindungan data umum Uni Eropa, *General Data Protection Regulation (GDPR)* disahkan dan mulai berlaku di Negara Anggota Uni Eropa

[73] *Artickle 1 (1) Directive 95/46 : in accordance with this directive, Member States shall protect the fundamental rights and freedoms of natural persons, and particular their right to privacy with respect to the processing of personal data.*

pada tahun 2018 Bulan Mei tanggal 25[74]. Negara-negara yang tergabung dalam Uni Eropa ialah Negara Italia, Negara Latvia, Negara Lithuania, Negara Luxembourg, Negara Malta, Negara Netherlands, Negara Poland, Negara Portugal, Negara Romania, Negara Slovakia, Negara Slovenia, Negara Spanyol dan Negara Swedia[75]. Sebelumnya, Negara *United Kingdom* menjadi bagian dari Uni Eropa, namun *UK* keluar dari Uni Eropa pada 31 Januari 2020. Adapun salah satu alasan mengapa Inggris keluar dari Uni Eropa ialah pada bulan Juni 2016, warga Inggris telah menentukan suara untuk memutuskan keluar yakni sebanyak 17.4 juta suara atau 51,9 persen responden (pemilih ialah warga Inggris, Irlandia, dan warga Negara persemakmuran yang sudah berusia lebih dari 18 tahun dan tinggal di Britania Raya[76].

Prinsip-prinsip perlindungan data dalam *GDPR* ialah sebagaimana diatur dalam *Article 5 GDPR:*

a. Processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
b. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific

[74] *Article 51. (4) Each Member State shall notify to the Commission the provisions of its law which it adopts pursuant to this Chapter, by 25 May 2018 and, without delay, any subsequent amendment affecting them.*

[75] https://europa.eu/european-union/about-eu/countries_en diakses tanggal 10 Februari 2020

[76] Ahmad Naufal, " Jalan Panjang Brexit, Keluarnya Inggris dari Uni Eropa" artikel tanggal 1-Februari 2020, https://www.kompas.com/tren/read/2020/02/01/165308965/jalan-panjang-brexit-keluarnya-inggris-dari-uni-eropa?page=all diakses tanggal 10 Februari 2020

or historical research purposes or statistical purposes shall, in accordance with Article 89 (1),[77] not be considered to be Incompatible with the initial purposes ('purpose limitation');

c. Adequate, relevant and limited to what is necessary in relation to the purpose for which they are processed ('data minimisation');
d. Accurate, and where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
e. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for whitch the personal data processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific, or historical research purposes or statistical purposes in accordance with Article 89 (1) subject to implementation of the appropriate technical and organizational measures required by this regulation in order to safeguard the rights and freedomgs of the data subject ('storage limitation');

[77] *Article 89 (1) GDPR "processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organizational measures are in place in particular in order to ensure respect for the principle of data minimization. Those measures may include pesudonymisation provided that those purposes can be fulfilled in that mannter. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner.*

f. Processed in a manner that ensures appropriate security of the personal data, including protection against unathorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures ('integrity and confidentiality').

Dua pengaturan dalam *GDPR* yang akan **Penulis** uraikan yakni: pada *article 6 (1) (b) GDPR "processing may be permited in the case of a legal obligaton to which the controller is subject. Control, monitoring and order functions in accordance with Art. 23 (1)(h) also justfy such processing."*[78] Berikutnya ialah dalam *article 13 GDPR* bahwa "*where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:*

a. *The identity and the contact details of the controller and where applicable, of the controller's representative;*
b. *The contact details of data protection officer, where applicable;*
c. *The purposes of the processing for which the personal data are intended as well as the legal basis for the processing;*
d. *Where the processing is based on point (f) of Article 6 (1), the legitimate interests pursued by the controller or by a third party;*

[78] Stephanie von Maltzan, *"No Contradiction between Cyber-Security and Data Protection? Designing a Data Protection compliant Incident Response System" (United Kingdom: European Journal of Law and Technology, Vo.10,Issue 1, 2019)* dapat diakses di http://ejlt.org/article/view/665/893, diakses tanggal 17 April 2020

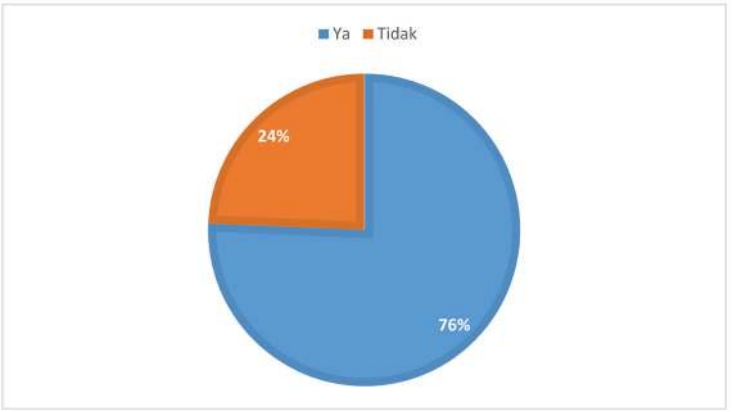
e. The recipients or categories of recipients of the personal data, if any;

f. Where applicable, the fact that the controller intends to transfer personal data to a third country or international organizationand the existence or absence of an adequancy decision by the Commission, or in the case of transfers referred to in Article 46[79] or 47[80], or the scond subparagraph of Article 49 (1), reference to the appropriate or suitable safeguards and te means by which to obtain a copy of them or where they have been made available.

Berdasarkan kuisioner yang **Penulis** sebar tentang pertanyaan "Apakah Saudara/I mengetahui Regulasi Umum Perlindungan Data (*General Data Protection* 2016/679) di Uni Eropa?" Hasil yang didapatkan adalah bahwa 171 responden (76%) menjawab tahu dan 55 responden (24%) tidak tahu. Menurut hemat **Penulis,** apabila melihat pada RUU PDP (pembahasan per Desember 2019) bahwa rancangan pengaturan merujuk atau menjadikan *GDPR* sebagai referensi namun yang harus diingat dan tidak boleh dilupakan bahwasanya penyusunan RUU berlandaskan filosofi pada Pancasila dan wajib bermuatan keadilan bermartabat.

[79] *Article 46 GDPR* mengatur tentang *Transfers Subject to Appropriate Safeguards.*

[80] *Article 47 GDPR* mengatur tentang *Binding Corporate Rules*



Grafik 17. Pertanyaan Apakah Saudara/I mengetahui Regulasi Umum Perlindungan Data (General Data Protection 2016/679) di Uni Eropa?

Sumber: Dokumen Pribadi.

6) ***Asia – Pacific Economic Cooperation (APEC) Privacy Framework***

Prinsip-prinsip perlindungan data pribadi dalam *OECD Guidelines in 1980, the EU General Directive (1995), the APEC Framework* memiliki kesamaan yakni:

1) *Principle of limitation in the collection of information. The information obtained, processed and disseminated should be limited only to lawful and fair purposes and should be upon the knowledge and consent of the information owner;*
2) *Principle concerning the quality of information. Personal information must be obtained in accordance with the intent and purpose of its collection. Quality of information must be maintained in terms of its accuracy, completeness and updates.*
3) *Principle of the objective. Personal information may only be opened in accordance with its intended use.*

4) *Principle of retention. The retention of information for a particular purpose should not be longer than the necessary period of time;*
5) *Principle of maximum security on personal information. Personal information shall be protected by adequate security system in order to avoid the risk of losing or unlawful act such as access, destruction, use, modification or disclosure of such information by other parties;*
6) *Principle of transparency. The management of information must take necessary steps so that the information owners can learn about the kinds of personal information held by the data manager;*
7) *Principle of individual participation of information subject. Information's owners shall have the right to access their personal information maintained by the data manager, including the right to make corrections to their personal information;*
8) *The principle of accountability. Information manager is fully responsible to implement the above mentioned principles.*

Pemerintah Indonesia juga telah meratifikasi *International Covenant on Civil and Political Rigts* (*ICCPR* 1996) dengan Undang-undang Nomor 12 Tahun 2005 tentang Pengesahan *International Covenant on Civil and Political Rigts* (Konvenan Internasional tentang Hak-Hak Sipil dan Politik) (selanjutnya disebut UU 12/2005) dan beradasarkan Pasal 17 ayat (1) UU 12/2005 bahwa "Tidak boleh seorang pun 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."

II. Asas dan Prinsip Perlindungan Data Pribadi

Berdasarkan Pasal 2 ayat (2) Permenkominfo PDPSE, asas perlindungan data pribadi yang baik, meliputi:

a. Penghormatan terhadap data pribadi sebagai privasi[81];
b. Data pribadi bersifat rahasia sesuai Persetujuan[82] dan/atau berdasarkan ketentuan peraturan perundang-undangan;
c. Berdasarkan persetujuan;
d. Relevansi dengan tujuan perolehan, pengumpulan, pengolahan, penganalisisan, penyimpanan, penampilan, pengumuman, pengiriman dan penyebarluasan;
e. Kelaikan sistem elektronik yang digunakan;
f. Iktikad baik untuk segera memberitahukan secara tertulis kepad pemilik data pribadi setiap kegagalan perlindungan data pribadi;
g. Ketersediaan aturan internal pengelolaan perlindungan data pribadi;
h. Tanggung jawab atas data pribadi yang berada dalam penguasaan pengguna;
i. Kemudahan akses dan koreksi terhadap data pribadi oleh pemilik data pribadi; dan

[81] Berdasarkan Pasal 2 ayat (3) Permenkominfo PDPSE, privasi adalah kebebasan pemilik data pribdi untuk menyatakan rahasia atau tidak menyatakan rahasia data pribadinya, kecuali ditentukan lain sesuai dengan ketentuan peraturan perundang-undangan.

[82] Berdasarkan Pasal 2 ayat (4) Permenkominfo PDPSE, persetujuan diberikan setelah 'pemilik data pribadi' menyatakan konfirmasi terhadap kebenaran, status kerahasiaan dan tujuan pengelolaan data pribadi.

j. Keutuhan, akurasi, dan keabsahan[83] serta kemutakhiran[84] data pribadi.

Apabila merujuk pada Rancangan Undang-Undang Perlindungan Data Pribadi (RUU PDP), asas-asas perlindungan data pribadi ialah[85]:

a. Asas perlindungan. Yang dimaksud dengan "Asas Perlindungan" adalah pemerintah wajib memberikan perlindungan data pribadi warga negaranya baik di dalam maupun di luar negeri;
b. Asas kepentingan umum. Yang dimaksud dengan "Asas Kepentingan Umum" adalah bahwa undang-undang ini disusun untuk melindungi kepentingan masyarakat secara luas;
c. Asas keseimbangan. Yang dimaksud dengan "Asas Keseimbangan" adalah keseimbangan antara hak privasi dengan hak negara yang sah berdasarkan kepentingan umum;
d. Asas pertanggungjawaban. Yang dimaksud dengan "Asas Pertanggungjawaban" adalah penyelenggaraan data pribadi harus dapat dipertanggungjawabkan oleh penyelenggara data pribadi[86].

Selain asas-asas perlindungan data pribadi, RUU PDP juga mengamanatkan bahwa penyelenggaraan data pribadi dilakukan berdasarkan prinsip[87]:

---

[83] Berdasarkan Pasal 2 ayat (5) Permenkominfo PDPSE, keabsahan merupakan legalitas dalam perolehan, pengumpulan, pengolahan, penganalisisian, penyimpanan, penampilan, pengumuman, pengiriman, penyebarluasan, dan pemusnahan data pribadi.

[84] Berdasarkan Kamus Besar Bahasa Indonesia, arti kata mutakhir adalah terakhir, terbaru, dan modern.

[85] Pasal 2 RUU PDP beserta Penjelasan Pasal 2 RUU PDP

[86] Pasal 2 RUU PDP beserta Penjelasan Pasal 2 RUU PDP

[87] Pasal 5 RUU PDP beserta Penjelasan Pasal 5 RUU PDP

a. Pembatasan dalam pengumpulan data pribadi. Pengumpulan data pribadi harus dilakukan secara terbatas dan spesifik dan data yang didapatkan harus menggunakan cara-cara yang sah secara hukum dan adil, dan harus sepengatahuan dan persetujuan dari orang yang bersangkutan;
b. Kesepakatan. Penyelenggaraan data pribadi seseorang hanya dapat dilakukan dengan kesepakatan pemilik data pribadi;
c. Proses penyelenggaraan dan pengungkapan data pribadi sesuai dengan tujuan. Penyelenggara data pribadi menjamin data pribadi yang berada di bawah penyelenggaraannya akurat, lengkap, tidak menyesatkan dan mutakhir dengan memperhatikan tujuan penyelenggaraan data pribadi;
d. Kualitas data/integritas data. Penyelenggara data pribadi harus mengelola data pribadi sesuai dengan tujuan penggunaan dan data harus akurat, lengkap dan terus diperbaharui;
e. Keamanan data pribadi. Penyelenggara data pribadi harus dilakukan dengan melindungi keamanan data pribadi dari kehilangan, penyalahgunaan, akses, pengungkapan yang tidak sah, pengubahan atau perusakan data pribadi;
f. Akurasi. Penyelenggara data pribadi harus selalu menjamin akurasi dan ketepatan dan kemutakhiran data pribadi terlebih dahulu kepada pemilik data pribadi, sebelum data pribadi tersebut diberikan kepada pihak ketiga;
g. Akses data. Penyelenggara data pribadi akan mempublikasikan kebijakan privasinya dan persoalan-persoalan pengolahan data pribadi lainnya, dan akan menjamin hak-hak subyek data termasuk hak untuk mengakses informasi pribadinya.

h. Retensi. Penyelenggara data pribadi mempunyai masa retensi yang diatur berdasarkan peraturan perundang-undangan.
i. Notice.
j. Choice.

III. Perlindungan Data Pribadi sebagai Hak Asasi Manusia

UUD 1945 dengan tegas mengamanatkan perlindungan hak asasi manusia. Perlindungan data pribadi termasuk juga sebagai salah satu hak asasi manusia mengingat bahwasanya "Negara Indonesia adalah negara hukum[88]". Berdasarkan Pasal 28D ayat (1) UUD 1945 bahwa "setiap orang berhak atas pengakuan, jaminan, perlindungan dan kepastian hukum yang adil serta perlakuan yang sama di hadapan hukum". Dan berdasarkan Pasal 28G ayat (1) UUD 1945 bahwa "setiap orang berhak atas **perlindungan diri pribadi**, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi".

Adapun dua pertimbangan dibentuknya UU HAM ialah pertama, bahwa hak asasi manusia merupakan hak dasar yang secara kodrati melekat pada diri manusia, bersifat universal dan langgeng, oleh karena itu harus dilindungi, dihormati, dipertahankan, dan tidak boleh diabaikan, dikurangi, atau dirampas oleh siapapun; kedua, bahwa selain hak asasi, manusia juga mempunyai kewajiban dasar antara manusia yang satu terhadap yang lain dan terhadap masyarakat secara keseluruhan dalam kehidupan bermasyarakat, berbangsa, dan bernegara.

[88] Pasal 1 ayat (3) UUD 1945

Definisi hak asasi manusia (HAM) berdasarkan Pasal 1 Angka 1 UU HAM yakni "seperangkat hak yang melekat pada hakikat dan keberadaan manusia sebagai mahkluk Tuhan Yang Maha Esa dan merupakan anugerah-Nya yang wajib dihormati, dijunjung tinggi dan dilindungi oleh negara, hukum, Pemerintah, dan setiap orang demi kehormatan serta perlindungan harkat dan martabat manusia".

Perlindungan data pribadi adalah hak privasi dan harus dilindungi oleh Negara. Perlindungan oleh Negara, sebagai bentuk Negara hadir maka berdasar Pasal 2 UU HAM bahwa "Negara Republik Indonesia mengakui dan menjunjung tinggi hak asasi manusia dan kebebasan dasar manusia sebagai hak yang secara kodrati melekat pada dan tidak terpisahkan dari manusia, yang harus dilindungi, dihormati, dan ditegakkan demi peningkatan martabat kemanusiaan, kesejahteraan, kebahagiaan, dan kecerdasan serta keadilan"[89].

Berdasarkan Pasal 29 ayat (1) UU HAM bahwa "Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan hak miliknya". Berdasarkan Pasal 32 UU HAM bahwa "Kemerdekaan dan rahasia dalam hubungan surat-menyurat termasuk hubungan komunikasi melalui sarana elektronik tidak boleh diganggu, kecuali atas perintah hakim atau kekuasaan lain yang sah sesuai dengan ketentuan peraturan perundang-undangan".

[89] Berdasarkan Penjelasan Pasal 2 UU HAM "Hak asasi manusia dan kebebasan dasar manusia tidak dapat dipaskan dari manusia pribadi karena tanpa hak asasi manusia dan kebebasan dasar manusia yang bersangkutan kehilangan harkat dan martabat kemanusiaannya. oleh karena itu, negara Republik Indonesia termasuk Pemerintah berkewajiban, baik secara hukum maupun secara politik, ekonomi, sosial dan moral untuk melindungi dan memajukan serta mengambil langkah-langkah konkret demi tegaknya hak asasi manusia dan kebebasan dasar manusia."

Di Negara lain, hak privasi adalah bagian dari HAM, misalnya di Negara Uni Eropa. *A fundamental right to data protection sits alongside the right to privacy. The Charter of Fundamental Rights of the EU (the Charter) contains a right to the protection of personal data in Article 8 (the right to data protection), in addition to a right to respect for private life in Article 7 (the right to privacy)*[90].

IV. Para Pihak dalam Perlindungan Data Pribadi

Penyimpanan data pribadi dalam sistem elektronik melibatkan pelbagai pihak, adapun pihak-pihak yang terlibat dalam perlindungan data pribadi ialah:

4.1 Pemerintah. Pemerintah adalah Menteri atau pejabat lainnya yang ditunjuk oleh Presiden[91]. Dan, Menteri yang dimaksud adalah Menteri adalah menteri yang menyelenggarakan urusan pemerintahan di bidang komunikasi dan informatika[92]. Kementerian Komunikasi dan Informatika dibentuk berdasarkan Peraturan Presiden Republik Indonesia No. 54 Tahun 2015 dan memiliki tugas untuk menyelenggarakan urusan pemerintahan di bidang komunikasi dan informatika untuk membantu Presiden dalam menyelenggarakan pemerintahan Negara;

4.2 Kementerian atau lembaga. Kementerian atau Lembaga adalah Instansi Penyelenggara Negara yang bertugas mengawasi dan mengeluarkan pengaturan terhadap sektornya[93];

[90] Menno Mostert, Annelien L. Bredenoord, Bart van der Sloot, Johannes J.M. van Delden, "From Privacy to Data Protection in the EU: Implications for Big Data Health Research", european Journal of health law 25 (2018) 43-55 diakses dari https://brill.com/view/journals/ejhl/25/1/article-p43_43.xml?language=en&body=citedBy-29618 tanggal 12 Februari 2020

[91] Pasal 1 Angka 38 PP PTSE

[92] Pasal 1 Angka 39 PP PTSE

[93] Pasal 1 Angka 7 PP PTSE

4.3 Direktur Jenderal. Direktur Jenderal adalah direktur jenderal yang tugas dan fungsinya di bidang aplikasi informatika[94].

4.4 Instansi Penyelenggara Negara. Instansi Penyelenggara Negara yang selanjutnya disebut Instansi adalah institusi legislatif, eksekutif, dan yudikatif di tingkat pusat dan daerah dan instansi lain yang dibentuk dengan peraturan perundang-undangan[95];

4.5 Penyelenggara sistem elektronik. Penyelenggaraa sistem elektronik adalah setiap Orang, penyelenggara negara, Badan Usaha, dan masyarakat yang menyediakan, mengelola, dan/atau mengoperasikan Sistem Elektronik secara sendiri-sendiri maupun bersama-sama kepada Pengguna Sistem Elektronik untuk keperluan dirinya dan/atau keperluan pihak lain[96]. Penyelenggara sistem elektronik terdiri dari[97]: a.Penyelenggara sistem elektornik lingkup publik[98]; dan b. Penyelenggara Sistem Elektronik Lingkup Privat[99];

---

[94] Pasal 1 Angka 10 Permenkominfo PDPSE. Sebagaimana diatur dalam Pasal 16 Perpres No. 54 Tahun 2015 tentang Kementerian Komunikasi dan Informatika bahwa Direktorat Jenderal Aplikasi Informatika menyelenggarakan fungsi: a. perumusan kebijakan di bidang penatakelolaan *e-Government, e-Business*, dan keamanan informasi, peningkatan teknologi dan infrastruktur aplikasi informatika serta pemberdayaan informatika; b. pelaksanaan kebijakan di bidang penatakelolaan *e-Government, e-Business,* dan keamanan informasi, peningkatan teknologi dan infrastruktur aplikasi informatika serta pemberdayaan informatika; c. penyusunan norma, standar, prosedur, dan kriteria di bidang penatakelolaan *e-Government;* d. pelaksanaan pemberian bimbingan teknis dan supervisi di bidang penatakelolaan e-*Government*; e. pelaksanaan evaluasi dan pelaporan di bidang penatakelolaan e-*Government, e-Business,* dan keamanan informasi, peningkatan teknologi dan infrastruktur aplikasi informatika serta pemberdayaan informatika; f. pelaksanaan administrasi Direktorat Jenderal Aplikasi Informatika; dan g. pelaksanaan fungsi lain yang diberikan oleh Menteri.

[95] Pasal 1 Anga 35 PP PTSE

[96] Pasal 1 Angka 4 PP PSTE – definisi serupa juga terdapat dalam Pasal 1 Angka 6 Permenkominfo PDPSE

[97] Pasal 2 ayat (2) PP PSTE

[98] Berdasarkan Pasal 1 Angka 5 PP PTSE, Penyelenggara Sistem Elektronik Lingkup Publik adalah penyelenggaraan Sistem Elektronik oleh Instansi Penyelenggara Negara atau institusi yang ditunjuk oleh Instansi Penyelenggara Negara.

[99] Berdasarkan Pasal 1 Angka 6 PP PTSE, Penyelenggara Sistem Elektronik

4.6 Pengguna Sistem Elektronik. Pengguna Sistem Elektronik adalah setiap Orang, penyelenggara negara, Badan Usaha, dan masyarakat yang memanfaatkan barang, jasa, fasilitas, atau informasi yang disediakan oleh Penyelenggara Sistem Elektronik[100];

4.7 Pengirim dan Penerima. Pengirim adalah subjek hukum yang mengirimkan Informasi Elektronik dan/atau Dokumen Elektronik[101]. Penerima adalah subjek hukum yang menerima Informasi Elektronik dan/atau Dokumen Elektronik dari Pengirim[102];

4.8 Pelaku usaha. Pelaku Usaha adalah setiap orang perseorangan atau Badan Usaha, baik berbentuk badan hukum maupun bukan badan hukum, yang didirikan dan berkedudukan atau melakukan kegiatan dalam wilayah hukum Negara Republik Indonesia, secara sendiri-sendiri maupun bersama-sama, melalui perjanjian penyelenggaraan kegiatan usaha dalam berbagai bidang ekonomi[103];

4.9 Pemilik Data Pribadi. Pemilik data pribadi adalah individu yang padanya melekat data perseorangan tertentu[104]. Dan, yang dimaksud dengan data perseorangan tertentu adalah setiap keterangan yang benar dan nyata yang melekat dan dapat diidentifikasi, baik langsung ataupun tidak langsung, pada masing-masing individu yang pemanfaatanya sesuai ketentuan peraturan perundang-undangan[105].

Lingkup Privat adalah penyelenggaraan Sistem Elektronik oleh Orang, Badan Usaha, dan masyarakat.

[100] Pasal 1 Angka 16 PP PTSE – definisi serupa juga terdapat dalam Pasal 1 Angka 7 Permenkominfo PDPSE

[101] Pasal 1 Angka 18 PP PTSE

[102] Pasal 1 Angka 19 PP PTSE

[103] Pasal 1 Angka 28 PP PTSE

[104] Pasal 1 Angka 3 Permenkominfo PDPSE

[105] Pasal 1 Angka 2 Permenkominfo PDPSE

V. Data Pribadi dalam Sistem Elektronik, Informasi dan/atau Dokumen Elektronik serta di Internet

Berdasarkan Pasal 3 Permenkominfo PDPSE, perlindungan data pribadi dalam sistem elektronik dilakukan pada proses: a. perolehan dan pengumpulan; b. pengolahan dan penganalisisan; c. penyimpanan; d. penampilan, pengumuman, pengiriman, penyebarluasan, dan/atau pembukaan akses; dan e. pemusanahan.

Sistem elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan Informasi Elektronik[106]. Sistem elektronik untuk kelima proses diatas wajib tersertifikasi[107].

Menurut **Edmon Makarim,** informasi elektronik adalah suatu kode dari kode digit astau disebut *binary* digit 0 dan 1. Dalam kode, huruf a direpresentasikan secara sistem elektronik dalam rangkaian kode *asking*. Kemudian, menjadi besar, dan menjadi *record*, terakhir menjadi *data base*. Dengan demikian, suatu informasi elektronik hakikatnya adalah suatu kode[108]. Informasi elektronik dihasilkan oleh suatu sistem elektronik, sehingga dasar asumsi hukumnya salah suatu informasi yang layak dipercaya karena berasal dari sistem yang layak dipercaya. Oleh karena itu, suatu informasi elektronik bernilai hukum

[106] Pasal 1 Angka 1 PP PSTE

[107] Pasal 4 ayat (1) Permenkominfo PDPSE

[108] Keterangan Ahli, **Edmon Makarim** dalam Putusan Mahkamah Konstitusi RI No. 20 / PUU – XIV / 2016 tentang pengujian materiil Pasal 5 ayat (1), (2) dan Pasal 44 huruf b UU ITE dan PAsal 26A Undang-undang Nomor 20 Tahun 2001 tentang Perubahan Atas Undang-undang No. 31 Tahun 1999 tentang Pemberantasan Tindak Pidana Korupsi terhadap UUD 1945 (selanjutnya disebut Putusan MK No. 20 PUU-XIV/2016), hlm. 63-65

sehingga menjadi alat bukti yang sah untuk semua hukum acara. "Hakim tidak boleh menampik suatu kehadiran informasi elektronik hanya karena bentuknya elektronik".[109]

Suatu sistem elektronik menerangkan suatu peristiwa hukum dan juga pelakunya. Namun dalam konteks elektronik, perlu diperhatikan reliabilitasnya karena hal tersebut tidak diterangkan dalam Penjelasan UU ITE sebab pada saat pembahasan UU ITE dianggap merupakan *based practices*. Di kalangan para IT mengetahui bahwa suatu informasi elektronik tidak dijamin integritasnya, sehingga hal itu berarti dengan sendirinya ada kemungkinan perubahan. Terhadap hal tersebut, merupakan wilayah hakim untuk menilainya[110].

Manusia pada abad ke-21 sangat tidak dapat dilepaskan dari internet, semua aktifitas dan kebutuhanya sangat bergantung dengan internet. Menurut **Susan E. Gindin** sebagaimana dikutip oleh **Edmon Makarim,** pelbagai macam informasi dapat diakses melalui internet, dan terdapat 3 (tiga) macam data dan/atau informasi pribadi seseorang yang terdapat di internet yang dapat dilanggar privasinya, yakni pertama adalah yang tersedia dalam bentuk basis data (*database) online:* kedua, yang diperoleh dalam suatu transaksi *online*, informasi dikumpulkan dengan keikutsertaan seseorang dalam kegiatan-kegiatan *online* dimana informasi-informasi tersebut dapat secara spesifik mengidentifikasikan orang tersebut; dan ketiga, yakni dalam basis data yang dimiliki oleh Negara atau Pemerintah yang terdapat dalam situs-situs milik Pemerintah tersebut[111].

[109] *Ibid*, hlm. 63

[110] Keterangan Ahli, Edmon Makarim dalam Putusan MK No. 20 PUU-XIV/2016, hlm. 65.

[111] Susan E. Gindin, *"Lost and Found in Cyberspace: Informational Privacy in the Age of the Internet," San Diego Law Review* 1153 (1997). Lihat juga dalam Edmon Makarim, *Pengantar Hukum Telematika Suatu Kompilasi Kajian* (Jakarta: PT

a. Informasi Pribadi dalam Basis Data *Online*

Privasi[112] seseorang mungkin saja dilanggar dengan dipublikasikannya informasi tersebut secara *online*. Kini informasi pribadi dalam suatu jumlah yang signifikan tela tersedia di internet, khususnya di *World Wide Web (WWW)*. Sebagai contoh, *database America* yakni suatu direktori telepon untuk rumah tangga dan industri, *Four11: Internet White Pages* yang menyediakan alamat-alamat *e-mail* begitu pula dengan nomor telepon dan alamat rumah, *MapBlast!*, yang menyediakan peta atau denah alamat-alamat yang diminta[113].

b. Informasi Pribadi dalam Transaksi *Online*

Teknologi komputer juga menyediakan cara lain untuk mengumpulkan informasi pribadi yang jika tidak diperhatikan maka dapat menjadi ekses negative dari penggunan pelayanan *online* dan internet. Internet memiliki kapasitas untuk menjadi pengumpul data (*data collector)* yang paling efektif yang pernah ada. Perhatian terhadap pengumpulan dan kemungkinan penyalahgunaan informasi pribadi ini telah berlipat-kali sejak ditemukannya cara-cara baru pengumpulan pribadi secara elektronik. Sehubungan dengan transaksi *online* di internet, situs operator dimungkinkan mengumpulkan data pribadi dari para pengunjungnya melalui media-media berikut[114]:

RajaGrafindo Persada, 2005), hlm.181.

[112] Apabila merujuk pada pendapat Fuster GG, *privacy is a broad concept that relates to various aspects of one's individual and personal sphere of life.* Fuster, G G (2014), *The Emergence of Personal Data Protecton as a Fundamental Right of the EU (Cham: Springer Internatonal Publishing)*.

[113] Edmon Makarim, *Pengantar Hukum Telematika Suatu Kompilasi Kajian* (Jakarta: PT RajaGrafindo Persada, 2005), hlm.181.

[114] *Ibid*, hlm. 182

1) Cookies

Privasi seorang pengguna internet dapat dilanggar dengan penggunaan *feature-feature* tertentu oleh operator situs untuk mengumpulkan informasi pribadi dari setiap orang yang datang ke situs mereka dengan tujuan untuk mempertahankan atau bahkan meningkatkan pelayanan mereka. Beberapa situs menggunakan apa yang dinamakan *'cookies'* untuk mengumpulkan informasi dari konsumen ketika mereka mengunjungi suatu situs. *Cookies* adalah suatu alat yang ditempatkan dalam *hard drive* komputer seseorang oleh situs ketika orang tersebut ada di internet. *Cookies* dapat menyimpan informasi mengenai pengguna internet, seperti nomor kartu kredit, situs-situs yang dikunjungi, alamat *e-mail,* minat ataupun pola belanjanya. Informasi yang diterima oleh *browser* situs tersebut disimpan di dalam *hard disk*. Situs tersebut akan membaca informasi ini setiap kali pengguna internet yang bersangkutan mengunjungi situs mereka[115].

Informasi tersebut digunakan untuk melacak kunjungan-kunjungan ke suatu situs serta untuk mengetahui apa yang disukai atau tidak disukai oleh seorang pengunjung situs tersebut. Namun, sayangnya informasi yang dikumpulkan dan disimpan oleh *cookies* itu sering kali dikumpulkan tanpa sepengetahuan ataupun persetujuan pengguna internet[116].

[115] *Ibid.*
[116] *Ibid*.

2) Pendaftaran *Online (Online Registration)*

Menurut hemat **Penulis,** Pendaftaran secara daring / *online* diperlukan dan wajib untuk dilakukan untuk dapat mengakses suatu informasi elektronik, memberi komentar terhadap suatu berita di internet, untuk mendaftar dan menggunakan suatu layanan *online shop* secara lebih detil. Pendaftaran dalam sistem elektronik, situs *web* umumnya meminta data berupa nama lengkap, tempat tanggal lahir, alamat domisili, nomor *handphone*, alamat *e-mail*, pekerjaan, dan beberapa sistem ada yang mengharuskan untuk menggunggah (*upload)* mandiri *softcopy* KTP. Apabila tidak diberikan maka pengguna tidak dapat mengakses informasi elektronik yang diperlukan secara lengkap.

Apabila merujuk pada Undang-undang No. 19 Tahun 2016 tentang Perubahan Atas Undang-undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) mengenai terminologi yuridis tentang informasi elektronik, dokumen elektronik, sistem elektronik dan penyelenggara sistem elektronik. Definsi yang diberikan yakni:

1. Informasi Elektronik adalah satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, electronic data interchange (EDI), surat elektronik (electronic mail), telegram, teleks, telecopy atau sejenisnya, huruf, tanda, angka, Kode Akses, simbol, atau perforasi yang telah diolah yang

memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya[117];

2. Dokumen Elektronik adalah setiap Informasi Elektronik yang dibuat, diteruskan, dikirimkan, diterima, atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal, atau sejenisnya, yang dapat dilihat, ditampilkan, dan/atau didengar melalui Komputer atau Sistem Elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto atau sejenisnya, huruf, tanda, angka, Kode Akses, simbol atau perforasi yang memiliki makna atau arti atau dapat dipahami oleh orang yang mampu memahaminya[118];
3. Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan Informasi Elektronik[119];

3) Keamanan Melalui Enkripsi

Salah satu mekanisme untuk meningkatkan keamanan sistem elektronik ialah dengan menggunakan mekanisme **'enkripsi'.** Menurut **Budi Raharjo,** enkripsi adalah proses yang dilakukan untuk mengamankan sebuah pesan (yang disebut *plaintext*) menjadi pesan yang tersembunyi (disebut *ciphertext*) adalah enkripsi (*encryption*)[120]. Proses menyandikan

[117] Pasal 1 Angka 1 UU ITE
[118] Pasal 1 Angka 4 UU ITE
[119] Pasal 1 Angka 5 UU ITE
[120] Budi Rahardjo, *Keamanan Sistem Informasi Berbasis Internet,* (Bandung: PT

plainteks menjadi cipherteks disebut enkripsi (encryption) atau enciphering (standar nama menurut ISO 7498-2). Sedangkan proses mengembalikan *cipherteks* menjadi *plainteks* semula dinamakan dekripsi (*decryption*) atau deciphering (standar nama menurut ISO 7498-2). Enkripsi dan dekripsi dapat diterapkan baik pada pesan yang dikirim maupun pada pesan tersimpan. Istilah encryption of data in motion mengacu pada enkripsi pesan yang ditransmisikan melalui saluran komunikasi, sedangkan istilah *encryption of data at-rest* mengacu pada enkripsi dokumen yang disimpan di dalam *storage*. Contoh *encryption of data in motion* adalah pengiriman nomor *PIN* dari mesin *ATM* ke komputer server di kantor bank pusat[121].

Salah satu aplikasi telekomunikasi yang telah menggunakan ini ialah *Whatsapp* dengan metode *end to end encryption*. Enkripsi *end-to-end WhatsApp* memastikan bahwa hanya Anda dan orang yang berkomunikasi dengan Anda sajalah yang dapat membaca pesan yang telah dikirim, dan tidak ada orang lain di antara Anda, bahkan *WhatsApp*. Pesan Anda diamankan dengan kunci dan hanya penerima pesan dan Anda saja yang memiliki kunci spesial yang diperlukan untuk membuka kunci dan membaca pesan Anda. Untuk keamanan tambahan, setiap pesan yang

Insan Komunikasi Indonesia, 2002).

[121] Siswo Wardoyo, Rian Fahrizal, Zaldi Imanullah "Aplikasi Teknik Enkripsi dan Dekripsi *File* dengan Algoritma *Blowfish* pada Perangkat *Mobile* berbasis *Android*", Jurnal Setrum Vol. 3, No. 1 Juni 2014, Hlm. 44,Universitas Sultan Ageng Tirtayasa Cilegon, dapat diakses di http://jnte.ft.unand.ac.id/index.php/jnte/article/view/199 diakses tanggal 2 Mei 2020

Anda kirim memiliki kunci yang unik. Semua hal ini terjadi secara otomatis[122].

WhatsApp menggunakan Signal Protocol yang dikembangkan organisasi perangkat lunak asal Amerika, *Open Whisper Systems*[123]. Berikut cara kerja dari *E2EE* ketika dua orang berkomunikasi melalui WhatsApp: 1. Ketika pengguna pertama kali membuka *WhatsApp*, dua kunci berbeda dibuat. Proses enkripsi berlangsung di telepon itu sendiri. 2. Kunci pribadi harus tetap bersama pengguna, sedangkan kunci publik ditransfer ke penerima melalui server *WhastApp* yang terpusat; 3. Kunci publik mengenkripsi pesan pengirim di telepon, bahan sebelum mencapai *server* yang terpusat; 4. Server hanya digunkan untuk mengirimkan pesan terenkripsi. Pesan hanya dapat dibuka oleh kunci pribadi penerima. Tidak ada pihak ketiga, termasuk *Whatsapp* tidak dapat mencegat dan membaca pesan; 5. Jika seorang *hacker* mencoba meretas dan membaca pesan, mereka akan gagal karena enkripsi.

VI. Keterkaitan antara Data Pribadi, Informasi Elektronik, Klausula Baku, dan Disclaimer serta Kontrak Elektronik

Masyarakat, pengguna, konsumen wajib menggunggah data pribadi apabila ingin menggunakan *platform,* aplikasi *online*. Sebagaimana **Penulis** paparkan diatas, data pribadi elektronik adalah bentuk 'perpanjangan' ataupun 'personifikasi' dari

[122] https://faq.whatsapp.com/id/android/28030015/ diakses tanggal 11 Mei 2020

[123] M. Khiry Alfarizi "Begini Cara Kerja Enkripsi End-to-end Whatsapp" artikel tanggal 11 Januari 2019 https://tekno.tempo.co/read/1163636/begini-cara-kerja-enkripsi-end-to-end-whatsapp/full&view=ok diakses tanggal 11 Mei 2020

manusia sebagai pemilik data, misalnya pengguna baru dapat melaksanakan transaksi *e-commerce* melalui kontrak elektronik setelah pengguna memasukan data pribadi, antara lain nama, alamat, nomor ponsel dan hanya memiliki pilihan *agree/yes* atau *no/disagree* untuk dapat menggunakan aplikasi *online*. Seyogyanya, penyelenggara, perusahaan wajib merancang sistem pengamanan yang canggih sesuai dengan *ISO* sehingga usaha *online* yang dilakukan bermartabat, menghindari dugaan/ancaman peretasan, ataupun mengedukasi juga karyawan-karyawannya terhadap perlindungan data pribadi.

Hukum kontrak telah berkembang, apabila dahulu syarat kontrak di Indonesia termaktub jelas dalam Pasal 1320 Kuh. Perdata, namun di era teknologi, Pasal 1320 Kuh.Perdata tetap berlaku namun dengan perkembangan dan dikaitkan dengan ketentuan yang mengatur tentang kontrak elektronik, salah satunya Pasal 46 PP PSTE. **Penulis** akan paparkan dalam tabel syarat Pasal 1320 Kuh.Perdata dengan Pasal 46 PP PSTE

PERBEDAAN PASAL 1320 KUH.PERDATA DENGAN PASAL 46 PP PSTE	
Pasal 1320 Kuh. Perdata: Supaya terjadi persetujuan yang sah, perlu dipenuhi empat syarat:	**Pasal 46 PP PSTE:** kontrak elektronik dianggap sah apabila:
1. Kesepakatan mereka yang mengikatkan dirinya;	1. Terdapat kesepakatan para pihak;
2. Kecakapan untuk membuat suatu perikatan;	2. Dilakukan oleh subjek hukum yang cakap atau yang berwenang mewakili sesuai dengan ketentuan peraturan perundang-undangan;
3. Suatu pokok persoalan tertentu;	3. Terdapat hal tertentu;

PERBEDAAN PASAL 1320 KUH.PERDATA DENGAN PASAL 46 PP PSTE	
Pasal 1320 Kuh. Perdata: Supaya terjadi persetujuan yang sah, perlu dipenuhi empat syarat:	**Pasal 46 PP PSTE:** kontrak elektronik dianggap sah apabila:
4. Suatu sebab yang tidak terlarang.	4. Objek transaksi tidak boleh bertentangan dengan peraturan perundang-undangan, kesusilaan dan ketertiban umum;

Informasi elektronik merupakan alat bukti yang sah adalah informasi elektronik yang berada dalam komputer pada persidangan ini dipertontonkan dan dilihat. Berarti ada konten elektronik dan tidak ada kesanksian karena sistemnya tidak berubah. Sistem yang ada di dalam persidangan ini menjamin bahwa yang disimpan dan yang dibaca tidak berbeda, sehingga informasi elektronik dari bentuk yang originalnya telah mempunyai nilai pembuktian[124].

Konsepsi berpikir dari informasi adalah baik informasi elektronik ataupun informasi di atas kertas, mempunyai kekuatan fungsional yang sama yang dikenal dengan istilah *functional equivalent approach*, yakni suatu informasi jika ditulis di atas kertas harus dapat dibaca kembali dan memenuhi unsur tertulis, sama halnya dengan informasi elektronik dianggap memenuhi unsur tertulis manakala disimpan dan dapat ditemukan kembali[125].

Informasi elektronik dianggap bertanda tangan manakala ada suatu informasi elektronik yang menjelaskan ada subyek hukum yang bertanggung jawab. Dengan demikian, tanda

[124] Keterangan Ahli, Edmon Makarim dalam Putusan MK No. 20 PUU-XIV/2016, hlm. 64.

[125] Keterangan Ahli, Edmon Makarim dalam Putusan MK No. 20 PUU-XIV/2016, hlm. 64.

tangan mempresentasikan subyek yang membaca dan bertanggung jawab terhadap isinya atau dengan kata lain bertanda tangan dianggap telah memenuhi, manakala ada informasi elektronik yang menjelaskan subyek hukum yang melekat kepada konten tersebut[126].

Informasi elektronik dikatakan autentik atau original manakala informasi yang disimpan dan dibaca kembali, diyakini tidak berubah. Contoh sehari-hari ialah *SMS, Short Message Service*, *SMS* dapat menjadi alat bukti ketika penerima memposisikan sebagai *'end user'*. Keberadaan Pasal 5 UU ITE menjelaskan bahwa informasi elektronik dapat diterima sebagai alat bukti yang sah dengan syarat dapat diakses, dapat ditampilkan, dijamin keutuhannya, dapat dipertanggungjawabkan sehingga dapat menerangkan suatu keadaan[127].

Kontrak elektronik sangat berkaitan erat dengan *disclaimer* ataupun *terms of use* yang diberikan oleh penyelenggara. Data pribadi yang dimasukan ke dalam sistem elektronik sehingga menjadi informasi elektronik dan untuk melaksanakan kontrak elektronik, pengguna/konsumen wajib menekan persetujuan.

Kontrak elektronik dan bentuk kontraktual lainnya sebagaimana dimaksud dalam Pasal 46 ayat (1) yang ditujukan kepada penduduk Indonesia harus dibuat dalam Bahasa Indonesia[128]. Kontrak Elektronik paling sedikit memuat: a. data identitas para pihak; b. objek dan spesifikasi; c. persyaratan Transaksi Elektronik; d. harga dan biaya; e. prosedur dalam hal terdapat pembatalan oleh para pihak; f. ketentuan yang

[126] Keterangan Ahli, Edmon Makarim dalam Putusan MK No. 20 PUU-XIV/2016, hlm. 64.

[127] Keterangan Ahli, Edmon Makarim dalam Putusan MK No. 20 PUU-XIV/2016, hlm. 65.

[128] Pasal 47 ayat (1) PP PSTE

memberikan hak kepada pihak yang dirugikan untuk dapat mengembalikan barang dan/ atau meminta penggantian produk jika terdapat cacat tersembunyi; dan g. pilihan hukum penyelesaian Transaksi Elektronik[129].

Apabila dalam kontrak elektronik, salah satu pihak melakukan ingkar janji maka berlaku akibat hukum sebagaimana yang diatur dalam Kuh.Perdata, dua diantaranya: 1. Debitur diwajibkan membayar ganti kerugian yang telah diderita oleh kerugian (Pasal 1234 Kuh. Perdata); 2. Debitur diwajibkan memenuhi perikatan jika masih dapat dilakukan, atau pembatalan disertai pembayaran ganti kerugian (Pasal 1267 Kuh.Perdata).

Sebelum menggunakan aplikasi *online*, konsumen/ pengguna disuguhi pelbagai ketentuan, *terms of use, disclaimer*. *Disclaimer* menurut *Black's Law Dictionary* ialah 1. *A renunciation of one's legal right or claim; esp, a renunciation of a patent claim, to save the remainder of the application from being rejected; 2. A repudiation of another's legal right or claim; 3. A writing that contains such a renunciation or repudiation*.

Penulis yakin bahwasanya Pengguna/konsumen aplikasi *online* tidak akan membaca *disclaimer* (pernyataan penyangkalan) ataupun membaca *terms of use* (syarat penggunaan) dengan pelbagai alasan. Berdasarkan observasi **Penulis,** pengguna memang hanya memiliki 2 (dua) pilihan yakni: *take it or leave it; yes or no; agree or disagree* dan jika pengguna masih ingin tetap menggunakan aplikasi tersebut maka pilihannya adalah *yes, agree, take it*.

Penulis kutip salah satunya yakni *data policy* pada *website facebook.com*. Tiga Informasi yang *facebook* kumpulkan *yakni:*

[129] Pasal 47 ayat (3) PP PSTE

1. *"To provide the Facebook Products, we must process information about you. The type of information that we collect depends on how you use our Products. You can learn how to access and delete information that we collect by visiting the Facebook settings* and *Instagram settings".*[130]
2. ***"Information and content you provide"**. We collect the content, communications and other information you provide when you use our Products, including when you sign up for an account, create or share content and message or communicate with others.* (terjemahan bebas: Informasi dan konten yang Anda berikan. Kami mengumpulkan konten, komunikasi, dan informasi lain yang Anda berikan saat Anda menggunakan Produk kami, termasuk saat Anda mendaftarkan sebuah akun, membuat atau membagikan konten, dan berkirim pesan atau berkomunikasi dengan orang lain)[131];
3. ***"Your Usage".** We collect information about how you use our Products, such as the types of content that you view or engage with, the features you use, the actions you take, the people or accounts you interact with and the time, frequency and duration of your activities.* (Terjemahan dalam Bahasa Indonesia: Kami mengumpulkan informasi mengenai cara Anda menggunakan Produk kami, seperti jenis konten yang Anda lihat atau libatkan dalam interaksi Anda; fitur yang Anda gunakan, tindakan yang Anda ambil; orang-orang atau akun yang Anda tuju dalam interaksi Anda; beserta waktu, frekuensi, dan durasi aktivitas Anda)[132]

[130] https://en-gb.facebook.com/about/privacy diakses tanggal 11 Mei 2020
[131] https://en-gb.facebook.com/about/privacy diakses tanggal 11 Mei 2020

[132] https://en-gb.facebook.com/about/privacy diakses tanggal 11 Mei 2020

Menurut hemat **Penulis,** data pribadi yang kita unggah ke sistem elektronik menjadi informasi elektronik dalam sistem peyelenggara/*platform* atau penyedia jasa layanan yang wajib dijaga dan apabila pengguna meng-klik, menekan tombol *yes/agree/okay* maka hal tersebut adalah **bentuk pernyataan kesepakatan/otentifikasi** antara Pengguna dengan aplikasi *online* tersebut.

Menurut **Mariam Darus** bahwa dengan semakin majunya teknologi yang dapat memudahkan hubungan antar manusia di dunia, meletakkan Indonesia dalam jaringan yang mudah dicapai atau dijamah oleh kebiasaan (perdagangan) yang dipergunakan di bagian dunia lain. Masuknya perusahaan asing ke Indonesia juga membawa serta berbagai bentuk perjanjian, salah satu diantaranya adalah perjanjian *standard* (perjanjian baku) yang dipergunakan di dalam perjanjian pemberian jasa dan sebagainya[133].

Penggunaan klausula baku dalam suatu perjanjian muncul dari kebutuhan yang ada di dalam masyarakat itu sendiri, bahwa dalam suatu hubungan bisnis yang membutuhkan suatu akta perjanjian yang cukup rumit dan menghabiskan banyak biaya, maka dengan adanya klausula baku diharapkan dapat memangkas biaya operasional yang dibutuhkan serta mempersingkat waktu[134].

Apabila dikritisi lebih lanjut dengan pemikiran yang berkeadilan bermartabat, apakah *disclaimer* atau perjanjian

---

[133] Mariam Darus Badrulzaman, *Perjanjian Kredit Bank*, (Bandung: Alumni Bandung, 1989), hlm.30.

[134] Muaziz, M. H., & Busro, A. (2015). Pengaturan Klausula baku dalam hukum perjanjian untuk mencapai keadilan berkontrak. *Law Reform*, *11*(1), 74-84. Dapat diakses di https://ejournal.undip.ac.id/index.php/lawreform/article/view/15757/11772, diakses tanggal 2 Maret 2020

baku atau klausula baku ini dapat melepaskan kemampuan bertanggung jawab si penyedia jasa layanan *online*?

Berdasarkan penelurusan Penulis, hingga saat ini terdapat 2 (dua) peraturan yang mengatur tentang klausula baku yakni 1. UU Perlindungan Konsumen, 2. PP PSTE dan 1 (satu) Surat Edaran yakni: Surat Edaran Otoritas Jasa Keuangan No. 13/ SEOJK.07/2014 tentang Perjanjian Baku (selanjutnya disebut SEOJK Perjanjian Baku).

PP PSTE juga mengatur tentang klausula baku. Berdasarkan Pasal 47 ayat (2) PP PSTE "kontrak elektronik yang dibuat dengan klausula baku harus sesuai dengan ketentuan mengenai klausula baku sebagaimana diatur dalam peraturan perundang-undangan. Selain PP PSTE, klausula baku diatur dalam UU Perlindungan Konsumen.

Apabila kita mengacu pada UU Perlindungan Konsumen, konsep *disclaimer* ialah sama dengan konsep klausula baku[135]. Pengaturan tentang klausula baku diatur dalam Pasal 18 UU Perlinkos yang pokok-pokok pengaturannya sebagai berikut:

1) Pasal 18 ayat (1) UU Perlinkos: Pelaku usaha dalam menawarkan barang dan/atau jasa yang ditujukan untuk diperdagangkan dilarang membuat atau mencantumkan klausula baku pada setiap dokumen dan/atau perjanjian apabila: a. menyatakan pengalihan tanggung jawab pelaku usaha; b. menyatakan bahwa pelaku usaha berhak menolak penyerahan kembali barang yang dibeli konsumen; c. menyatakan bahwa pelaku usaha berhak menolak

[135] Definisi yuridis 'klausula baku berdasarkan Pasal 1 Angka 10 UU Perlinkos adalah setiap aturan atau ketentuan dan syarat-syarat yang telah dipersiapkan dan ditetapkan terlebih dahulu secara sepihak oleh pelaku usaha yang dituangkan dalam suatu dokumen dan/atau perjanjian yang mengikat dan wajib dipenuhi oleh konsumen."

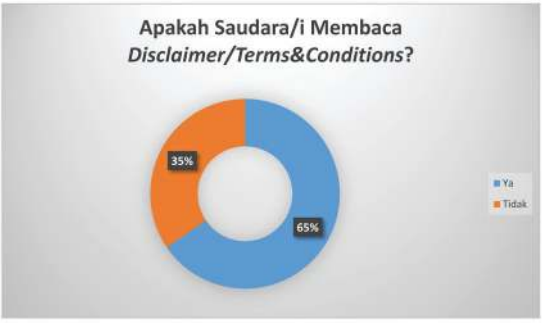
penyerahan kembali uang yang dibayarkan atas barang dan/atau jasa yang dibeli oleh konsumen; d. menyatakan pemberian kuasa dari konsumen kepada pelaku usaha baik secara langsung maupun tidak langsung untuk melakukan segala tindakan sepihak yang berkaitan dengan barang yang dibeli oleh konsumen secara angsuran; e. mengatur perihal pembuktian atas hilangnya kegunaan barang atau pemanfaatan jasa yang dibeli oleh konsumen; f. memberi hak kepada pelaku usaha untuk mengurangi manfaat jasa atau mengurangi harta kekayaan konsumen yang menjadi obyek jual beli jasa; g. menyatakan tunduknya konsumen kepada peraturan yang berupa aturan baru, tambahan, lanjutan dan/atau pengubahan lanjutan yang dibuat sepihak oleh pelaku usaha dalam masa konsumen memanfaatkan jasa yang dibelinya; h. menyatakan bahwa konsumen memberi kuasa kepada pelaku usaha untuk pembebanan hak tanggungan, hak gadai, atau hak jaminan terhadap barang yang dibeli oleh konsumen secara angsuran.

2) Pasal 18 ayat (2) UU Perlinkos: Pelaku usaha dilarang mencantumkan klausula baku yang letak atau bentuknya sulit terlihat atau tidak dapat dibaca secara jelas, atau yang pengungkapannya sulit dimengerti.
3) Pasal 18 ayat (3) UU Perlinkos: Setiap klausula baku yang telah ditetapkan oleh pelaku usaha pada dokumen atau perjanjian yang memenuhi ketentuan sebagaimana dimaksud pada ayat (1) dan ayat (2) dinyatakan batal demi hukum.
4) Pasal 18 ayat (4) UU Perlinkos: Pelaku usaha wajib menyesuaikan klausula baku yang bertentangan dengan Undang-undang ini.

Pengaturan tentang klausula dalam SE OJK tentang Perjanjian Baku yakni

Klausula dalam Perjanjian Baku yang dilarang adalah yang memuat: a. Klausula eksonerasi/eksemsi yaitu yang isinya menambah hak dan/atau mengurangi kewajiban PUJK, atau mengurangi hak dan/atau menambah kewajiban Konsumen. b. Penyalahgunaan keadaan yaitu suatu kondisi dalam Perjanjian Baku yang memiliki indikasi penyalahgunaan keadaan. Contoh terhadap kondisi ini misalkan memanfaatkan kondisi Konsumen yang mendesak karena kondisi tertentu atau dalam keadaan darurat dan secara sengaja atau tidak sengaja PUJK tidak menjelaskan manfaat, biaya dan risiko dari produk dan/atau layanan yang ditawarkan[136].

Berdasarkan data yang Penulis peroleh terkait *disclaimer* dan *terms of use* dapat diketahui bahwa Responden tidak membaca *disclaimers, tems&conditons* sebanyak 65% (enam puluh lima per seratus) namun hanya 35% (tiga puluh lima per seratus) yang membaca *disclaimers, terms&conditions.*



Grafik 18. Angka Responden yang Membaca/Tidak Membaca *Disclaimer/Terms&Conditions*

Sumber: Dokumen pribadi

[136] Bab II angka 3 SE OJK Perjanjian Baku

Penulis melakukan olah data terhadap pertanyaan "Apa alasan Saudara/i tidak membaca *terms and conditions, disclaimer* tersebut? (boleh isi lebih dari satu)" dan hasinya ialah mendapatkan data&fakta bahwa kebanyakan responden tidak membaca *disclaimers, terms&conditions* karena alasan "panjang sehingga menjadi malas" yakni sebanyak 147 responden (78%); alasan kedua karena "Tidak memiliki pilihan lain karena ingin menggunakan aplikasi tersebut" sebanyak 102 responden (55%); alasan ketiga karena "Walaupun mengugunakan Bahasa Indonesia tapi malas membacanya" sebanyak 41 responden (22%); alasan keempat karena "Menggunakan Bahasa Inggris" sebanyak 10 responden (5,3%); alasan kelima karena "Tidak mengerti isinya" sebanyak 9 responden (5%).

Penulis berharap dalam perkembangan pembahasan RUU PDP, Pemerintah juga mengatur memberi pedoman tentang klausula baku, *disclaimer, terms of use*. Pedoman ini berfungsi untuk penyelenggara ataupun calon penyelenggara, sehingga *disclaimer, terms of use* tidak hanya menyalin format yang ada di intenet, format yang tidak jelas siapa yang berwenang untuk mengeluarkanya.

Grafik 19. Pertanyaan "alasan saudara/I tidak membaca *terms&conditions, disclaimer* tersebut?

Sumber: Dokumen pribadi

VII. Perlindungan Data Pribadi oleh Penyelenggara (Lingkup Publik atau Lingkup Privat)

PP PSTE membagi penyelenggara sistem elektronik kedalam 2 (dua) lingkup yakni: 1. Penyelenggara sistem elektronik lingkup publik; 2. Penyeleggara sistem elektronik lingkup privat. Berdasar Pasal 1 Angka 5 PP PSTE Penyelenggara Sistem Elektronik Lingkup Publik adalah penyelenggaraan Sistem Elektronik oleh Instansi Penyelenggara Negara atau institusi yang ditunjuk oleh Instansi Penyelenggara Negara sedangkan berdasarkan Pasal 1 Angka 6 PP PSTE bahwa Penyelenggara Sistem Elektronik Lingkup Privat adalah penyelenggaraan Sistem Elektronik oleh Orang, Badan Usaha, dan masyarakat.

VII.1. Kewajiban Penyelenggara terhadap Perlindungan Data Pribadi

Berdasarkan Pasal 14 ayat (2) UU HAM bahwa "Setiap orang berhak untuk mencari, memperoleh, memiliki, menyimpan, mengolah, dan menyampaikan informasi dengan menggunakan segala jenis sarana yang tersedia".

Kewajiban Penyelenggara Sistem Elektronik, Berdasarkan Pasal 16 ayat (1) UU ITE bahwa:

"Sepanjang tidak ditentukan lain oleh undang-undang tersendiri, setiap Penyelenggara Sistem Elektronik wajib mengoperasikan Sistem Elektronik yang memenuhi persyaratan minimum sebagai berikut:

a. dapat menampilkan kembali Informasi Elektronik dan/atau Dokumen Elektronik secara utuh sesuai dengan masa retensi yang ditetapkan dengan Peraturan Perundang-undangan;

b. dapat melindungi ketersediaan, keutuhan, keotentikan, kerahasiaan, dan keteraksesan Informasi Elektronik dalam Penyelenggaraan Sistem Elektronik tersebut;
c. dapat beroperasi sesuai dengan prosedur atau petunjuk dalam Penyelenggaraan Sistem Elektronik tersebut;
d. dilengkapi dengan prosedur atau petunjuk yang diumumkan dengan bahasa, informasi, atau simbol yang dapat dipahami oleh pihak yang bersangkutan dengan Penyelenggaraan Sistem Elektronik tersebut; dan
e. memiliki mekanisme yang berkelanjutan untuk menjaga kebaruan, kejelasan, dan kebertanggungjawaban prosedur atau petunjuk."

Kewajiban Penyelenggara Sistem Elektronik menurut PP PSTE, beberapa diantaranya yakni:

1) Penyelenggara Sistem Elektronik wajib melaksanakan prinsip Perlindungan Data Pribadi dalam melakukan pemrosesan Data Pribadi meliputi: a. pengumpulan Data Pribadi dilakukan secara terbatas dan spesifik, sah secara hukum, adil, dengan sepengetahuan dan persetujuan dari pemilik Data Pribadi; b. pemrosesan Data Pribadi dilakukan sesuai dengan tujuannya; c. pemrosesan Data Pribadi dilakukan dengan menjamin hak pemilik Data Pribadi; d. pemrosesan Data Pribadi dilakukan secara akurat, lengkap, tidak menyesatkan, mutakhir, dapat dipertanggungjawabkan, dan memperhatikan tujuan pemrosesan Data Pribadi; e. pemrosesan Data Pribadi dilakukan dengan melindungi keamanan Data Pribadi dari kehilangan, penyalahgunaan, Akses dan pengungkapan yang tidak sah, serta pengubahan atau perusakan Data Pribadi; f. pemrosesan Data Pribadi

dilakukan dengan memberitahukan tujuan pengumpulan, aktivitas pemrosesan, dan kegagalan perlindungan Data Pribadi; dan g. pemrosesan Data Pribadi dimusnahkan dan/ atau dihapus kecuali masih dalam masa retensi sesuai dengan kebutuhan berdasarkan ketentuan peraturan perundang-undangan[137].

2) Penyelenggara Sistem Elektronik wajib memastikan Sistem Elektroniknya tidak memuat Informasi Elektronik dan/ atau Dokumen Elektronik yang dilarang sesuai dengan ketentuan perundang-undangan[138];
3) Penyelenggara Sistem Elektronik harus menerapkan manajemen risiko terhadap kerusakan atau kerugian yang ditimbulkan[139];
4) Setiap Penyelenggara Sistem Elektronik wajib menghapus Informasi Elektronik dan/atau Dokumen Elektronik yang tidak relevan yang berada di bawah kendalinya atas permintaan orang yang bersangkutan[140].

Kewajiban Penyelenggara Sistem Elektronik dalam perlindungan data pribadi ialah dalam Permenkominfo PDPSE yakni:

1) Harus mempunyai aturan internal perlindungan data pribadi dan untuk upaya mencegah menghindari kegagalan dalam perlindungan data pribadi yang dikelolanya. [Pasal 5 ayat (1), (2) Permenkominfo PDPSE];
2) Harus melakukan pencegahan terjadinya kegagalan dalam perlindungan data pribadi, paling sedikit berupa kegiatan:

[137] Pasal 14 ayat (1) PP PSTE
[138] Pasal 5 ayat (1) PP PSTE
[139] Pasal 12 PP PSTE
[140] Pasal 15 ayat (1) PP PSTE

a. meningkatkan kesadaran sumber daya manusia di lingkunganya untuk memberikan perlindungan data pribadi dalam sistem elektronik yang dikelolanya; b. mengadakan pelatihan pencegahan kegagalan perlindungan data pribadi. [Pasal 5 ayat (4) Permenkominfo PDPSE];

3) wajib menyediakan formulir persetujuan dalam Bahasa Indonesia untuk meminta Persetujuan dari Pemilik Data Pribadi yang dimaksud. (Pasal 6 Permenkominfo PDPSE);
4) perolehan dan pengumpulan data pribadi harus dibatasi pada informasi yang relevan dan sesuai dengan tujuanya. [Pasal 7 ayat (1) Permenkominfo PDPSE];
5) Dalam memperoleh dan mengumpulkan Data Pribadi, Penyelenggara Sistem Elektronik harus menghormati Pemilik Data Pribadi atas Data Pribadinya yang bersifat privasi. Penghormatan tersebut dilakukan melalui penyediaan pilihan dalam Sistem Elektronik untuk Pemilik Data Pribadi terhadap: a. kerahasiaan atau ketidakrahasiaan Data Pribadi; dan b. perubahan, penambahan, atau pembaruan Data Pribadi. [Pasal 8 ayat (1), (2) Permenkominfo PDPSE];
6) Perolehan dan pengumpulan Data Pribadi oleh Penyelenggara Sistem Elektronik wajib berdasarkan Persetujuan atau berdasarkan ketentuan peraturan perundang-undangan dan Pemilik data pribadi dapat menyatakan data perseorangan tertentu miliknya bersifat rahasia. [Pasal 9 ayat (1), (2) Permenkominfo PDPSE];
7) Data yang pribadi wajib disimpan dalam sistem elektronik:
   7.1 Sesuai dengan ketentuan peraturan perundang-undangan yang mengatur kewajiban jangka waktu penyimpanan data pribadi pada masing-masing Instansi Pengawas dan Pengatur Sektor; atau

7.2 Paling singkat 5 (lima) tahun, jika belum terdapat ketentuan peraturan perundang-undangan yang secara khusus mengatur untuk itu.

8) Penyelenggara wajib memberikan data pribadi yang terdapat dalam sistem elektronik atau data pribadi yang dihasilkan oleh sistem elektronik atas permintaan yang sah dari aparat penegak hukum berdasarkan ketentuan peraturan perundang-undangan [Pasal 23 ayat (1) Permenkominfo PDPSE];
9) Melakukan sertifikasi Sistem Elektronik yang dikelolanya sesuai dengan ketentuan peraturan perundang-undangan. (Pasal 28 huruf a Permenkominfo PDPSE);
10) Menjaga kebenaran, keabsahan, kerahasiaan, keakuratan dan relevansi serta kesesuaian dengan tujuan perolehan, pengumpulan, pengolahan, penganalisisan, penyimpanan, penampilan, pengumuman, pengiriman, penyebarluasan, dan pemusnahan Data Pribadi. (Pasal 28 huruf b Permenkominfo PDPSE);
11) Memberitahukan secara tertulis kepada Pemilik Data Pribadi jika terjadi kegagalan perlindungan rahasia Data Pribadi dalam Sistem Elektronik yang dikelolanya, dengan ketentuan pemberitahuan sebagai berikut: 1. Harus disertai alasan atau penyebab terjadinya kegagalan perlindungan rahasia Data Pribadi; 2. Dapat dilakukan secara elektronik jika Pemilik Data Pribadi telah memberikan Persetujuan untuk itu yang dinyatakan pada saat dilakukan perolehan dan pengumpulan Data Pribadinya; 3. Harus dipastikan telah diterima oleh Pemilik Data Pribadi jika kegagalan tersebut mengandung potensi kerugian bagi yang bersangkutan; dan 4. Pemberitahuan tertulis dikirimkan

kepada Pemilik Data Pribadi paling lambat 14 (empat belas) hari sejak diketahui adanya kegagalan tersebut. (Pasal 28 huruf c Permenkominfo PDPSE);

12) Memiliki aturan internal terkait perlindungan Data Pribadi yang sesuai dengan ketentuan peraturan perundang-undangan. (Pasal 28 huruf d Permenkominfo PDPSE);
13) Menyediakan rekam jejak audit terhadap seluruh kegiatan penyelenggaraan Sistem Elektronik yang dikelolanya. (Pasal 28 huruf e Permenkominfo PDPSE);
14) Memberikan opsi kepada Pemilik Data Pribadi mengenai Data Pribadi yang dikelolanya dapat/atau tidak dapat digunakan dan/atau ditampilkan oleh/pada pihak ketiga atas Persetujuan sepanjang masih terkait dengan tujuan perolehan dan pengumpulan Data Pribadi. (Pasal 28 huruf f Permenkominfo PDPSE);
15) Memberikan akses atau kesempatan kepada Pemilik Data Pribadi untuk mengubah atau memperbarui Data Pribadinya tanpa menganggu sistem pengelolaan Data Pribadi, kecuali ditentukan lain oleh ketentuan peraturan perundang-undangan. (Pasal 28 huruf g Permenkominfo PDPSE);
16) Memusnahkan Data Pribadi sesuai dengan ketentuan dalam Peraturan Menteri ini atau ketentuan peraturan perundang-undangan lainnya yang secara khusus mengatur di masing-masing Instansi Pengawas dan Pengatur Sektor untuk itu. (Pasal 28 huruf h Permenkominfo PDPSE); dan
17) Menyediakan narahubung (contact person) yang mudah dihubungi oleh Pemilik Data Pribadi terkait pengelolaan Data Pribadinya. (Pasal 28 huruf i Permenkominfo PDPSE);

VIII. Relevansi Perlindungan Data Pribadi dengan Perlindungan Konsumen

Lex general, peraturan yang umum tentang perlindungan konsumen di Indonesia adalah Undang-undang No. 8 Tahun 1999 tentang Perlindungan Konsumen (selanjutnya disebut UU Perlinkos). Salah satu pertimbangan dibentuknya UU Perlinkos ialah bahwa untuk meningkatkan harkat dan martabat konsumen perlu meningkatkan kesadaran, pengetahuan, kepedulian, kemampuan dan kemandirian konsumen untuk melindungi dirinya serta menumbuhkembangkan sikap pelaku usaha yang bertanggung jawab.

Tujuan perlindungan konsumen ialah sebagai berikut: a. meningkatkan kesadaran, kemampuan dan kemandirian konsumen untuk melindungi diri; b. mengangkat harkat dan martabat konsumen dengan cara menghindarkannya dari ekses negatif pemakaian barang dan/atau jasa; c. meningkatkan pemberdayaan konsumen dalam memilih, menentukan, dan menuntut hak-haknya sebagai konsumen; d. menciptakan sistem perlindungan konsumen yang mengandung unsur kepastian hukum dan keterbukaan informasi serta akses untuk mendapatkan informasi; e. menumbuhkan kesadaran pelaku usaha mengenai pentingnya perlindungan konsumen sehingga tumbuh sikap yang jujur dan bertanggung jawab dalam berusaha; f. meningkatkan kualitas barang dan/atau jasa yang menjamin kelangsungan usaha produksi barang dan/atau jasa, kesehatan, kenyamanan, keamanan, dan keselamatan konsumen.

Penulis akan menjabarkan hak dan kewajiban konsumen sebagaimana diatur dalam UU Perlinkos.

VIII.1. Hak dan Kewajiban Konsumen

VIII.1.1. Hak konsumen. Berdasarkan Pasal 4 UU Perlinkos terdapat 9 (sembilan) hak, 4 (empat) diantaranya:

a. hak atas kenyamanan, keamanan, dan keselamatan dalam mengkonsumsi barang dan/atau jasa;
b. hak untuk memilih barang dan/atau jasa serta mendapatkan barang dan/atau jasa tersebut sesuai dengan nilai tukar dan kondisi serta jaminan yang dijanjikan;
c. hak atas informasi yang benar, jelas, dan jujur mengenai kondisi dan jaminan barang dan/atau jasa;
d. hak untuk didengar pendapat dan keluhannya atas barang dan/atau jasa yang digunakan;

VIII.1.2. Kewajiban Konsumen

Berdasarkan Pasal 5 UU Perlinkos bahwa kewajiban konsumen adalah

a. membaca atau mengikuti petunjuk informasi dan prosedur pemakaian atau pemanfaatan barang dan/atau jasa. Demi keamanan dan keselamatan;
b. beritikad baik dalam melakukan transaksi pembelian barang dan/atau jasa;
c. membayar sesuai dengan nilai tukar yang disepakati;
d. mengikuti upaya penyelesaian hukum sengketa perlindungan konsumen secara patut.

Selanjutnya, **Penulis** akan menjabarkan hak dan kewajiban Pelaku Usaha serta mengaitkannya dengan perlindungan data pribadi.

VIII.2. Hak dan Kewajiban Pelaku Usaha

VIII.2.1. Hak Pelaku Usaha. Berdasarkan Pasal 6 UU Perlinkos terdapat 5 (lima) hak pelaku usaha, 3 (tiga) diantaranya:

a. hak untuk menerima pembayaran yang sesuai dengan kesepakatan mengenai kondisi dan nilai tukar barang dan/atau jasa yang diperdagangkan;
b. hak untuk mendapat perlindungan hukum dari tindakan konsumen yang beritikad tidak baik;
c. hak untuk melakukan pembelaan diri sepatutnya di dalam penyelesaian hukum sengketa konsumen;

VIII.2.2. Kewajiban Pelaku Usaha. Berdasarkan Pasal 7 UU Perlinkos bahwa terdapat 7 (tujuh) kewajiban pelaku usaha, 4 (empat) diantaranya:

a. beritikad baik dalam melakukan kegiatan usahanya;
b. memberikan informasi yang benar jelas dan jujur mengenai kondisi dan jaminan barang dan/atau jasa serta memberi penjelasan penggunaan, perbaikan, dan pemeliharaan;
c. memperlakukan atau melayani konsumen secara benar dan jujur serta tidak diskriminatif;
d. memberi kompensasi, ganti rugi dan/atau penggantian apabila barang dan atau jasa yang diterima atau dimanfaatkan tidak sesuai dengan perjanjian.

Menurut hemat **Penulis,** hak dan kewajiban konsumen&pelaku usaha adalah perbuatan hukum timbal balik yang berlandaskan hukum dan itikad baik. Bayangkan jika ada pembeli yang beritikad buruk, tidak membayar barang yang telah dipesan apabila pembeli tadi memilih untuk membayar ditempat (*COD- Cash on Delivery)* atau apabila pembeli salah mengirimkan

alamat yang adalah salah satu data pribadi untuk 'mengerjai' seseorang terlebih jika barang yang dibeli belum dibayar.

IX. Standar Perlindungan Data Pribadi

Penulis akan menguraikan standar perlindungan data pribadi sebagaimana diatur dalam PP PMSE dan *ISO 27001*

Berdasarkan Pasal 59 ayat (1), (2) bahwa "pelaku usaha wajib menyimpan data pribadi sesuai standar perlindungan data pribadi atau kelaziman praktik bisnis yang berkembang"[141].

PP PMSE memberikan kriteria standar perlindungan data pribadi atau kelaziman paling sedikit memenuhi kaidah perlindungan sebagai berikut:

a. data pribadi harus diperoleh secara jujur dan sah dari pemilik data pribadi yang bersangkutan disertai dengan adanya pilihan dan jaminan adanya upaya pengamanan dan pencegahan kerugian pemilik data tersebut;
b. data pribadi harus dimiliki hanya untuk satu tujuan atau lebih yang dideskripsikan secara spesifik dan sah serta tidak boleh diproses lebih lanjut dengan cara yang tidak sesuai dengan tujuan tersebut;
c. data pribadi yang diperoleh harus layak, relevan, dan tidak terlalu luas dalam hubungannya dengan tujuan pengolahannya sebagaimana disampaikan sebelumnya kepada pemilik data;
d. data pribadi harus akurat dan harus selalu *up-to-date* dengan memberikan kesempatan kepada pemilik data untuk memutakhirkan data pribadinya;

[141] Pasal 59 ayat (1) PP PMSE

e. data pribadi harus diproses sesuai dengan tujuan perolehan dan peruntukkannya serta tidak boleh dikuasai lebih lama dari waktu yang diperlukan;
f. data pribadi harus diproses sesuai dengan hak subyek pemilik data sebagaimana diatur dalam peraturan perundang-undangan;
g. pihak yang menyimpan data pribadi harus mempunyai sistem pengamanan yang patut untuk mencegah kebocoran atau mencegah setiap kegiatan pemrosesan atau pemanfaatan data pribadi secara melawan hukum serta bertanggung jawab atas kerugian yang tidak terduga atau kerusakan yang terjadi terhadap data pribadi tersebut; dan
h. data pribadi tidak boleh dikirim ke negara atau wilayah lain di luar Indonesia kecuali jika negara atau wilayah tersebut oleh Menteri dinyatakan memiliki standar dan tingkat perlindungan yang sama dengan Indonesia[142].

Standar keamanan internet (*internet security*) yakni *ISO 27001* dengan versi terbaru yakni *ISO 27001: 2017. ISO 27001:2013 is the internationally recognised specification for an Information Security Management System (ISMS), and it is one of the most popular standards for information security. The most recent version of the standard is ISO / IEC 27001:2013 and implements improvements made in 2017 as well*[143].

ISO 27001 advantages include: (1). reducing the organisation's information security and data protection risks; (2). helping to attract new customers and retain existing clients, saving time

[142] Pasal 59 ayat (2) PP PMSE. Berdasarkan Penjelasan Pasal 59 ayat (2) PP PMSE bahwa "standar perlindungan data pribadi memperhatikan keberadaan standar perlindungan data Eropa dan/atau *APEC Privacy Frameworks*

[143] https://www.isms.online/iso-27001/ diakses tanggal 2 Januari 2020

and resources; (3). improving reputation and strengthening trust in your organisation[144].

Salah satu standar internasionl tentang *risk management* (manajemen risiko). *Risk management is a comprehensive process within a management system. The specific objectives of risk management in the context of information security are: 1. early identification and elimination of information security risks; 2. establishing consistent assessment methods for identified risks; 3. clear assignment of responsibilities when dealing with risks; 3. clear, standardized documentation of risks, including their assessment; 4. efficient treatment of risks*[145]*;*

Berdasarkan penelusuran **Penulis,** salah satu institusi Negara yang telah menerapkan *ISO* dan standar teknologi lainnya yakni Badan Usaha Milik Negara (BUMN) sebagaimana diatur dalam Peraturan Menteri Badan Usaha Milik Negara No: PER-02/MBU/2013 tentang Panduan Penyusunan Pengelolaan Teknologi Informasi Badan Usaha Milik Negara sebagaimana diubah dengan Peraturan Menteri Badan Usaha Milik Negara No: PER-03/MBU/02/2018. Tujuan pengelolaan ini dapat terwujud dengan melaksankan tata kelola Teknologi Informasi yang baik dengan penerapan pola standarisasi kerangka pengelolan TI pada setiap BUMN untuk dapat mendukung penerapan *GCG* secara komprehensif.

[144] https://www.isms.online/iso-27001/ diakses tanggal 2 Januari 2020

[145] *Implementation Guidline ISO/IEC 27001: 2013. A Practical guideline for Implementing an ISMS in Accordance with The International Standard ISO/ IEC 27001: 2013*, hlm. 19

BAB IV

PENGATURAN PERLINDUNGAN DATA PRIBADI DI INDONESIA

I. Hak Pemilik Data Pribadi

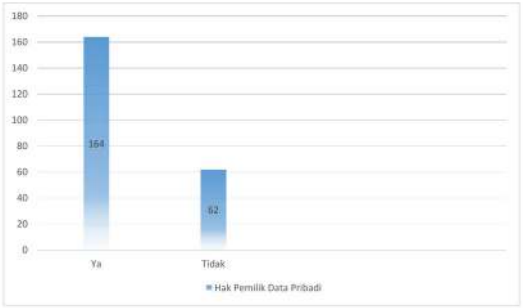
Menurut hemat **Penulis, '**pemilik data pribadi' adalah seseorang yang memiliki hak dan kewajiban terhadap data/ informasi berupa data pribadi baik yang rahasia ataupun sensitif yang ia berikan baik secara langsung ataupun tidak langsung melalui sistem elektronik ataupun konvensional (non-elektronik) untuk dipergunakan sebagaimana mestinya oleh penyelenggara sistem elektronik.

Penulis akan paparkan hak-hak pemilik data pribadi yang tersebar dalam pelbagai peraturan perundang-undangan (*ius constitum)* ataupun dalam Rancangan Undang-undang (*ius constituendum)* di Indonesia:

I.1. Hak Pemilik Data Pribadi dalam Permenkominfo PDPSE

Penulis melakukan penelitian terhadap hak-hak pemilik data pribadi sebagaimana diatur dalam Pasal 26 Pemenkominfo PDPSE melalui kuisioner. Dan berdasarkan data yang didapat bahwa hanya 73% (tujuh puluh tiga per seratus) atau 164 (seratus enam puluh empat) responden yang mengetahui hak-haknya

sebagai pemilik data pribadi sedangkan 27% (dua puluh tujuh per seratus) tidak mengetahui haknya sebagai pemilik data pribadi sebagaimana digambarkan pada grafik dibawah ini:



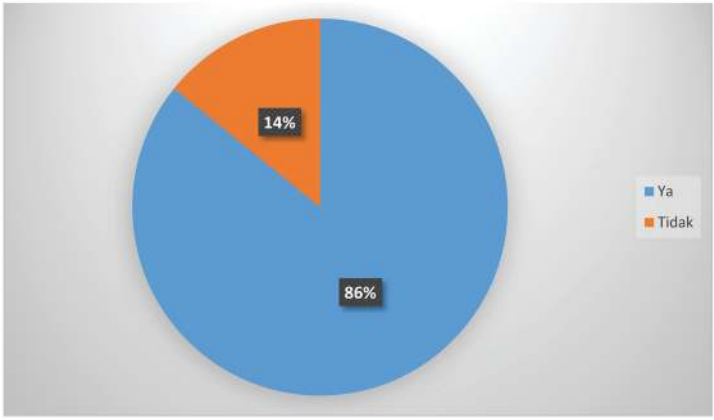
Grafik 20. Hak Pemilik Data Pribadi
Sumber: Dokumen pribadi.

Hak pemilik data pribadi diatur tegas dalam Pasal 26 Permenkominfo PDPSE dan **Penulis** mencoba melakukan penelitian dan 226 (dua ratus dua puluh enam) responden yang berpartisipasi tidak 100% (seratus persen) mengetahui hak-hak ini. Adapun hak-hak dalam Pasal 26 Permenkominfo PDPSE ialah:

a. Atas kerahasiaan data pribadinya;

Grafik 21. Hak Pemilik Data Pribadi dalam Pasal 26 huruf (a) PERMENKOMINFO PDPSE
Sumber: Dokumen pribadi.

b. Mengajukan pengaduan dalam rangka penyelesaian sengketa data pribadi atas kegagalan perlindungan kerahasiaan data pribadinya oleh Penyelenggara Sistem Elektronik kepada Menteri[146];

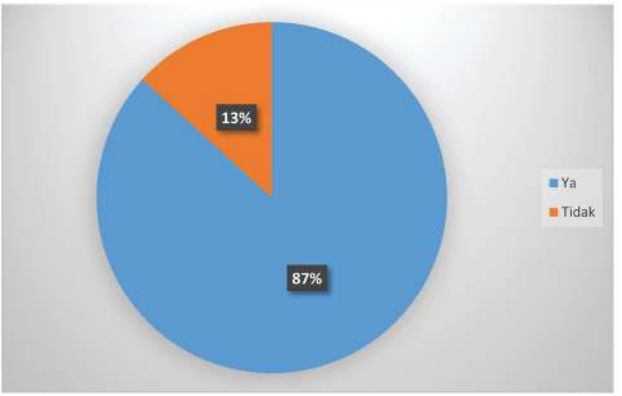


Grafik 22. Hak Pemilik Data Pribadi dalam Pasal 26 huruf (b) PERMENKOMINFO PDPSE

Sumber: Dokumen pribadi.

c. Mendapatkan akses atau kesempatan untuk mengubah atau memperbarui data pribadinya tanpa mengganggu sistem pengelolaan data pribadi, kecuali ditentukan lain oleh ketentuan peraturan perundang-undangan;

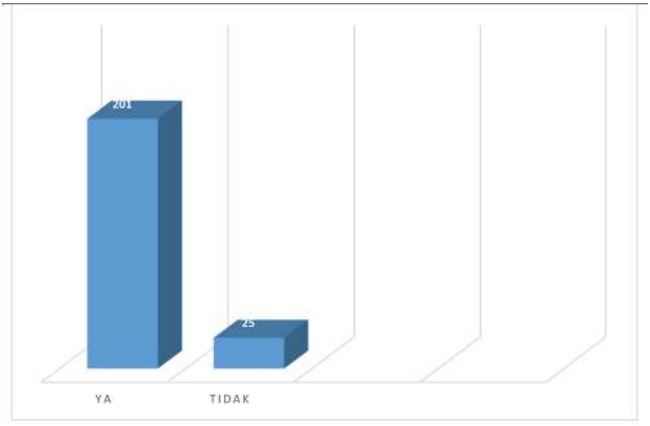
[146] Menteri yang dimaksud adalah menteri yang menyelenggarakan urusan Pemerintahan di bidang komunikasi dan informatika (Pasal 1 Angka 9 Permenkominfo PDPSE).



Grafik 23. Hak Pemilik Data Pribadi dalam Pasal 26 huruf (c) PERMENKOMINFO PDPSE

Sumber: Dokumen pribadi.

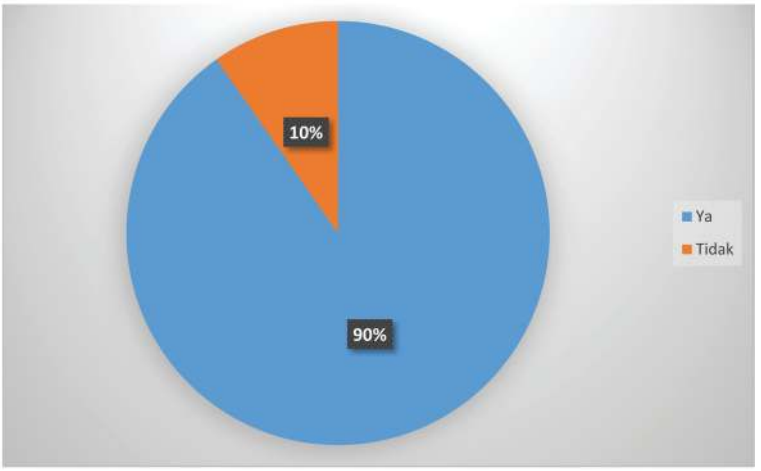
d. Meminta pemusnahan data perseorangan tertentu miliknya dalam sistem elektronik yang dikelola oleh penyelenggara sistem elektronik, kecuali ditentukan lain oleh ketentuan peraturan perundang-undangan.



Grafik 24. Hak Pemilik Data Pribadi dalam Pasal 26 huruf (d) PERMENKOMINFO PDPSE

Sumber: Dokumen pribadi.

e. Meminta pemusnahan Data Perseorangan Tertentu miliknya dalam Sistem Elektronik yang dikelola oleh Penyelenggara Sistem Elektronik, kecuali ditentukan lain oleh ketentuan peraturan perundang-undangan.



Grafik 25. Hak Pemilik Data Pribadi dalam Pasal 26 huruf (d) PERMENKOMINFO PDPSE

Sumber: Dokumen pribadi.

Berdasarkan grafik partisipasi responden tersebut dapat dianalisis bahwa tidak semua orang mengetahui hak-hak pemilik data pribadi dalam sistem elektronik sehingga **'sosialisasi', 'kampanye'** dari Pemerintah melalui Kominfo, Badan Siber dan Sandi Negara juga dari partisipasi masyarakat melalui Lembaga Swadaya Masyarakat, pemerhati data pribadi wajib lebih sering dilakukan hingga ke desa-desa dan kepada semua orang – tidak memandang status, pendidikan.

I.2. Hak Pemilik Data Pribadi dalam RUU PDP

a. Hak untuk mengajukan permintaan akses yang memadai dan salinan atas data pribadi miliknya kepada penyelenggara

data pribadi yang mengelola data pribadi miliknya[147]. Menurut hemat **Penulis,** contohnya adalah apabila pengguna mengisi data-data pribadi untuk melamar pekerjaan maka *website* / sistem elektronik tersebut seyogyanya menyediakan layanan untuk menyimpan atau memperoleh *curriculum vitae* secara daring (*online)* tersebut.

b. Hak untuk dapat mengajukan permintaan kepada penyelenggara data pribadi untuk memperbaiki kesalahan dan ketidakakuratan, dan memperbaharui data pribadi yang berada di dalam penyelenggaraan penyelenggara data pribadi[148]. Menurut hemat **Penulis,** contohnya adalah apabila pemilik data pribadi ingin merubah riwayat pekerjaan, merubah alamat dalam suatu sistem elektronik. Hal ini dapat banyak ditemukan dalam sistem elektronik yang menyelenggarakan lowongan pekerjaan (*website job-seeker)* dan terkadang sistem tersebut yang meminta si pengguna untuk memperbaharui data mereka secara berkala.

c. Hak untuk melengkapi data pribadi sebelum data pribadi tersebut dikelola oleh penyelenggara data pribadi. Menurut hemat **Penulis,** hak ini adalah hak saat pemilik data pribadi memiliki kekurangan dalam pengisian data pribadi, misalnya apabila pengguna atau masyarakat yang ingin mengikuti tes seleksi CPNS (Calon Pegawai Negeri Sipil) melakukan pengisian *online* data pribadi pada sistem suatu *website* Kementerian yang dilamar namun memiliki kekurangan dokumen, maka seyogyanya *website* atau

[147] Pasal 8 RUU PDP
[148] Pasal 9 RUU PDP

sistem elektronik tersebut menyediakan layanan '*save*' / layanan simpan data sebelum data tersebut di-*submit* (dikirimkan kepada sistem)[149];

d. Berhak meminta pemusnahan data pribadi miliknya, khususnya terhadap data pribadi yang: (1). Tidak memiliki nilai guna; (2). Telah habis retensinya dan berketerangan dimusnahkan berdasarkan jadwal retensi arsip; (3). Tidak ada peraturan perundang-undangan yang melarang; (4). Tidak berkaitan dengan penyelesaian proses suatu perkara[150];
e. berhak menuntut dan menerima ganti rugi atas pelanggaran terhadap data pribadinya berdasarkan undang-undang ini ke pengadilan[151];
f. Pemilik data pribadi setiap saat dapat menarik kembali persetujuan penyelenggaraan data yang telah diberikan pada penyelenggara data dengan pemberitahuan tertulis[152].

I.3. Hak Pemilik Data Pribadi dalam Pelbagai Peraturan Perundang-undangan

a. Pasal 2 UU Adminduk, mengatur tentang hak-hak penduduk, yang 4 diantaranya yakni: 1. Dokumen kependudukan; 2. Pelayanan yang sama dalam pendaftaran penduduk dan pencatatan sipil; 3. 'perlindungan atas data pribadi'; dan 6. Ganti rugi dan pemulihan nama baik sebagai akibat kesalahan dalam pendaftaran penduduk dan pencatatan sipil serta penyalahgunaan data pribadi oleh instansi

[149] Pasal 10 RUU PDP
[150] Pasal 11 ayat (1), (2) RUU PDP
[151] Pasal 12 RUU PDP
[152] Pasal 13 RUU PDP

pelaksana153;

b. Hak untuk dilindungi dan dirahasiakan keadaan keuangan dan hal-hal lain sebagai nasabah suatu perbankan (Pasal 40 ayat (1) UU Perbankan);
c. Hak untuk mendapatkan informasi dan edukasi tentang kesehatan yang seimbang dan bertanggung jawab dalam sektor kesehatan (Pasal 7 UU Kesehatan) dan berhak atas rahasia kondisi kesehatan pribadinya yang telah dikemukakan kepada penyelenggara pelayanan kesehatan (Pasal 57 ayat (1) UU Kesehatan);
d. Hak pasien untuk mendapatkan isi rekam medis154 (Pasal 52 huruf e UU Praktik Kedokteran);
e. Informasi

II. Perlindungan Data Pribadi dalam UU ITE

Penulis telah paparkan diatas, bahwa UU ITE mengatur tentang perlindundangan data pribadi. Berdasarkan Pasal 26 ayat (1) UU ITE (tahun 2008) diatur bahwa "Kecuali ditentukan lain oleh Peraturan Perundang-undangan, penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan Orang yang bersangkutan; kedua, berdasarkan Pasal 26 ayat (2) UU ITE (tahun 2008) bahwa "Setiap Orang yang dilanggar haknya sebagaimana dimaksud pada ayat (1) dapat mengajukan gugatan atas kerugian yang ditimbulkan berdasarkan Undang-Undang ini".

[153] Berdasarkan Pasal I Angka 7 UU Adminduk, Instansi Pelaksana adalah perangkat pemerintah Kabupaten/Kota yang bertanggung jawab dan berwenang melaksanakan pelayanan dalam urusan Administrasi Kependudukan.

[154] Rekam medis adalah berkas yang berisikan catatan dan dokumen tentang identitas pasien, pemeriksaan, pengobatan, tindakan dan pelayanan lain yang telah diberikan kepad pasien (Pasal I Angka I Peraturan Menteri Kesehatan No. 269/ MENKES/PER/III/2008

Berdasarkan Penjelasan Pasal 26 ayat (1) UU ITE (tahun 2008) bahwa "Dalam pemanfaatan Teknologi Informasi, perlindungan data pribadi merupakan salah satu bagian dari hak pribadi (*privacy rights*). Hak pribadi mengandung pengertian sebagai berikut: a. Hak pribadi merupakan hak untuk menikmati kehidupan pribadi dan bebas dari segala macam gangguan. b. Hak pribadi merupakan hak untuk dapat berkomunikasi dengan Orang lain tanpa tindakan memata-matai. c. Hak pribadi merupakan hak untuk mengawasi akses informasi tentang kehidupan pribadi dan data seseorang."

Pemerintah juga fokus dalam perlindungan data pribadi sehingga dalam Penjelasan Umum dijelaskan bahwa penggunaan setiap informasi melalui media atau Sistem Elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan Orang yang bersangkutan. Untuk itu, dibutuhkan jaminan pemenuhan perlindungan diri pribadi dengan mewajibkan setiap Penyelenggara Sistem Elektronik untuk menghapus Informasi Elektronik dan/atau Dokumen Elektronik yang tidak relevan yang berada di bawah kendalinya atas permintaan Orang yang bersangkutan berdasarkan penetapan pengadilan[155].

Pemerintah telah berupaya untuk meningkatkan dan mempertegas pengaturan tersebut dengan menambah Ketentuan Pasal 26 dengan penambahan 3 (tiga) ayat, yakni ayat (3), ayat (4), dan ayat (5) dalam UU ITE (tahun 2016). Penambahan tersebut sebagaimana dipaparkan dibawah ini:

Pasal 26 ayat (3) UU ITE (tahun 2016) "Setiap Penyelenggara Sistem Elektronik wajib menghapus Informasi Elektronik dan/atau Dokumen Elektronik yang tidak relevan yang berada di

[155] Paragraf X Penjelasan bagian Umum UU ITE tahun 2016

bawah kendalinya atas permintaan Orang yang bersangkutan berdasarkan penetapan pengadilan";

Pasal 26 ayat (4) UU ITE (tahun 2016) bahwa "Setiap Penyelenggara Sistem Elektronik wajib menyediakan mekanisme penghapusan Informasi Elektronik dan/atau Dokumen Elektronik yang sudah tidak relevan sesuai dengan ketentuan peraturan perundang-undangan";

Pasal 26 ayat (5) UU ITE (tahun 2016) bahwa "Ketentuan mengenai tata cara penghapusan Informasi Elektronik dan/atau Dokumen Elektronik sebagaimana dimaksud pada ayat (3) dan ayat (4) diatur dalam peraturan pemerintah."

III. Perlindungan Data Pribadi Dalam Peraturan Perundang-Undangan Disektor Administrasi Kependudukan

1. Data yang Dilindungi. Payung hukum yang mengatur tentang administrasi kependudukan ialah Undang-undang No. 24 Tahun 2013 tentang Perubahan Atas Undang-Undang No. 23 Tahun 2006 tentang Administrasi Kependudukan (selanjutnya disebut UU ADMINDUK). Definisi dari data pribadi adalah data perseorangan tertentu yang disimpan, dirawat, dan dijaga kebenaran serta dilindungi kerahasiaannya[156]. Adapun data pribadi yang harus dilindungi memuat:

a. Keterangan tentang cacat fisik dan/atau mental;
b. Sidik jari;
c. Iris mata;
d. Tanda tangan; dan
e. Elemen data lainnya yang merupakan aib seseorang[157].

[156] Pasal 1 Angka 22 UU ADMINDUK (perubahan-tahun 2013)

[157] Pasal 84 ayat (1) UU ADMINDUK (perubahan-tahun 2013). Pada UU yang lama (tahun 2006), berdasarkan Pasal 84 ayat (1) bahwa Data Pribadi Penduduk yang harus dilindungi memuat: a. nomor KK; b. NIK; c. tanggal/bulan/tahun lahir;

2. Larangan. Ketentuan perlindungan data perseorangan dan dokumen kependudukan diatur tegas dalam Pasal 79 UU Adminduk yakni: Pasal 79 ayat (1) "Data Perseorangan dan dokumen kependudukan wajib disimpan dan dilindungi kerahasiaannya oleh Negara". Pasal 79 ayat (2) "Menteri sebagai penanggung jawab memberikan hak akses Data Kependudukan kepada petugas provinsi dan petugas Instansi Pelaksana serta pengguna". Pasal 79 ayat (3) "Petugas dan pengguna sebagaimana dimaksud pada ayat (2) dilarang menyebarluaskan Data Kependudukan yang tidak sesuai dengan kewenangannya". Pasal 79 ayat (4) "Ketentuan lebih lanjut mengenai persyaratan, ruang lingkup, dan tata cara mengenai pemberian hak akses sebagaimana dimaksud pada ayat (2) diatur dalam Peraturan Menteri".

Berdasarkan Pasal 77 UU Adminduk dengan tegas mengatur bahwa "setiap orang dilarang memerintahkan dan/atau memfasilitasi dan/atau melakukan manipulasi data kependudukan dan/atau elemen data penduduk". UU Adminduk mengatur dengan tegas delik terhadap penyalahgunaan data kependudukan yakni:

1.4 Pasal 94 UU Adminduk mengatur bahwa "Setiap orang yang memerintahkan dan/atau memfasilitasi dan/atau melakukan manipulasi Data Kependudukan dan/atau elemen data Penduduk sebagaimana dimaksud dalam Pasal 77 dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp75.000.000,00 (tujuh puluh lima juta rupiah)";

1.5 Pasal 95A "Setiap orang yang tanpa hak menyebarluaskan Data Kependudukan sebagaimana dimaksud dalam

d. keterangan tentang kecacatan fisik dan/atau mental; e. NIK ibu kandung; f. NIK ayah;dan g. beberapa isi catatan Peristiwa Penting".

Pasal 79 ayat (3) dan Data Pribadi sebagaimana dimaksud dalam Pasal 86 ayat (1a) dipidana dengan pidana penjara paling lama 2 (dua) tahun dan/atau denda paling banyak Rp25.000.000,00 (dua puluh lima juta rupiah)."

Bagaimana apabila terdapat Kementerian/lembaga dan badan hukum Indonesia yang menggunakan data kependudukan melampaui batas kewenanganya? Indonesia adalah Negara hukum sehingga siapapun adalah sama di mata hukum (*equality before the law)*. Berdasarkan Peraturan Pemerintah No. 40 Tahun 2019 tentang Pelaksanaan Undang-undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan sebagimana telah diubah dengan Undang-undang No. 24 Tahun 2013 tentang Perubahan Atas Undang-undang No. 23 Tahun 2006 tentang Administrasi Kependudukan (Lembaran Negara Republik Indonesia Tahun 2019 No.102, Tambahan Lembaran Negara Republik Indonesia No. 6354), selanjutnya disebut PP Adminduk. PP Adminduk mengatur larangan dan pemberian sanksi administratif bagi Kementerian/lembaga dan badan hukum Indonesia yang memperoleh data pribadi penduduk atau kependudukan yang menggunakan data tersebut namun melampaui kewenanganya.

Adapun hal yang dilarang yakni: a. menggunakan Data Pribadi Penduduk atau Data Kependudukan melampaui batas kewenangannya; atau b. menjadikan Data Pribadi Penduduk atau Data Kependudukan sebagai bahan informasi publik sebelum mendapat persetujuan dari Menteri[158]. Apabila subyek hukum tersebut terbukti melakukan larangan tersebut maka akan dikenai sanksi administratif berupa pencabutan hak akses

[158] Pasal 58 ayat (1) PP Adminduk

pengguna, pemusanahan data yang sudah diakses, dan denda administratif sebesar Rp.10.000.000.000,00 (sepuluh miliar rupiah)[159]. Ketentuan tersebut diatur dalam Peraturan Menteri yang ditetapkan setelah dikoordinasikan dengan Kementerian teknis terkait[160].

3. Pemberian Akses. UU Adminduk dengan tegas mengatur bahwa petugas provinsi dan petugas Instansi Pelaksana dilarang menyebarluaskan data pribadi yang tidak sesuai dengan kewenangannya (Pasal 86 ayat (1a) UU Adminduk tahun 2013). Dalam hal ini Menteri sebagai penanggungjawab memberikan hak akses data pribadi kepada petugas provinsi dan petugas Instansi Pelaksana. Adapun Menteri yang dimaksud adalah menteri yang bertanggung jawab dalam urusan pemerintahan dalam Negeri (Pasal 1 Angka 5 UU Adminduk).

Pemberian hak akses dan pemanfaataan data kependudukan diatur dalam Peraturan Menteri Dalam Negeri RI No. 102 Tahun 2019 (Berita Negara RI Tahun 2019 No. 1611). Adapun beberapa pokok pengaturannya ialah: Berdasarkan Pasal 17 ayat (1). Menteri sebagai penanggung jawab mendelegasikan kepada Direktur Jenderal Kependudukan dan Pencatatan Sipil terkait pemberian Hak Akses Data Pribadi kepada Petugas Disdukcapil Provinsi dan Petugas Disdukcapil Kabupaten/ Kota; Berdasarkan Pasal 17 ayat (2) Untuk kepentingan keamanan negara dan penegakan hukum, Data Pribadi yang harus dilindungi dapat diakses dengan persetujuan Menteri. Berdasarkan Pasal 17 ayat (3) Petugas sebagaimana dimaksud pada ayat (1), dilarang memanfaatkan Data Pribadi yang tidak sesuai dengan kewenangannya.

[159] Pasal 58 ayat (2) PP Adminduk
[160] Pasal 58 ayat (3) PP Adminduk

4. Penyimpinan, Perolehan dan Penggunaan Data Pribadi Penduduk. Data pribadi penduduk disimpan pada basis data Kementerian, Dinas Kependudukan dan Pencatatan Sipil Provinsi, dan Dinas Kependudukan dan Pencatatan Sipil Kabupaten/ Kota[161]. Untuk memperoleh Data Pribadi Penduduk, kementerian/ lembaga dan badan hukum Indonesia harus mendapatkan persetujuan dari Menteri, gubernur, atau bupati/wali kota sesuai dengan lingkup data yang diperlukan. Data Pribadi Penduduk dapat diperoleh dengan ketentuan: a. kementerian/lembaga dan badan hukum Indonesia mengajukan permohonan kepada Menteri, gubernur, atau bupati/wali kota dengan menyertakan maksud dan tujuan penggunaan Data Pribadi Penduduk; b. Menteri, gubernur, atau bupati/wali kota melakukan seleksi untuk menentukan pemberian persetujuan; dan c. pemberian Data Pribadi Penduduk dilaksanakan sesuai dengan persetujuan yang diberikan Menteri, gubernur, atau bupati/wali kota[162].

Data Pribadi Penduduk yang diperoleh sebagaimana dimaksud pada ayat (1) hanya dapat digunakan sesuai keperluan sebagaimana tertuang dalam persetujuan[163]. Untuk kepentingan keamanan negara dan penegakan hukum, Data Pribadi Penduduk yang harus dilindungi hanya dapat diakses dengan persetujuan dari Menteri[164].

IV. Perlindungan Data Pribadi Dalam Peraturan Perundang-Undangan Disektor Kesehatan

UU Kesehatan dengan tegas mengatur bahwa kondisi kesehatan pasien adalah rahasia. Berdasarkan Pasal 57 ayat

[161] Pasal 55 ayat (1) PP Adminduk
[162] Pasal 55 ayat (2) PP Adminduk
[163] Pasal 55 ayat (3) PP Adminduk
[164] Pasal 55 ayat (4) PP Adminduk

(1) UU Kesehatan bahwa "setiap orang berhak atas rahasia kondisi kesehatan pribadinya yang telah dikemukakan kepada penyelenggara pelayanan kesehatan. Namun pengecualiannya, ketentuan tersebut tidak berlaku dalam hal: a. perintah undang-undang; b. perintah pengadilan; c. izin yang bersangkutan; d. kepentingan masyarakat; atau e. kepentingan orang tersebut[165].

Apabila terdapat kesalahan atau kelalaian dalam pelayanan kesehatan yang diterimanya termasuk kebocoran data pasien, pembocoran rahasia kedokteran maka orang tersebut berhak menuntut ganti rugi terhadap seseorang, tenaga kesehatan, dan/atau penyelenggara kesehatan yang menimbulkan kerugian tersebut[166]. Hal ini juga diatur dalam Undang-undang Nomor 29 Tahun 2004 tentang Praktik Kedokteran (Lembaran Negara Republik Indonesia Tahun 2004 No. 116, Tambahan Lembaran Negara Republik Indonesia No. 4431) selanjutnya disebut UU Praktik Kedokteran. Berdasarkan Pasal 48 ayat (1) UU Praktik Kedokteran bahwa "setiap dokter atau dokter gigi dalam melaksanakan praktik kedokteran wajib menyimpan rahasia kedokteran". Dengan **Pengecualian,** bahwa rahasia kedokteran tersebut dapat dibuka hanya untuk kepentingan kesehatan pasien, memenuhi permintaan aparatur penegak hukum dalam rangka penegakan hukum, permintaan pasien sendiri, atau berdasarkan ketentuan perundang-undangan[167].

[165] Pasal 57 ayat (2) UU Kesehatan
[166] Pasal 58 ayat (1) UU Kesehatan
[167] Pasal 48 ayat (2) UU Praktik Kedokteran

V. Perlindungan Data Pribadi Dalam Peraturan Perundang-Undangan Disektor Jasa Keuangan (Bank, dan Non-Bank)

1. Peraturan Otoritas Jasa Keuangan Nomor 13/POJK.02/2018 tentang Inovasi Keuangan Digital di Sektor Jasa Keuangan (POJK 13/2018)

Penulis akan paparkan terlebih dahulu, ketentuan umum/definisi, yakni:

1) Inovasi Keuangan Digital yang selanjutnya disingkat IKD adalah aktivitas pembaruan proses bisnis, model bisnis, dan instrumen keuangan yang memberikan nilai tambah baru di sektor jasa keuangan dengan melibatkan ekosistem digital.
2) Lembaga Jasa Keuangan adalah lembaga yang melaksanakan kegiatan di sektor Perbankan, Pasar Modal, Perasuransian, Dana Pensiun, Lembaga Pembiayaan, dan Lembaga Jasa Keuangan Lainnya sebagaimana dimaksud dalam Undang-Undang Nomor 21 Tahun 2011 tentang Otoritas Jasa Keuangan.
3) Penyelenggara adalah setiap pihak yang menyelenggarakan IKD.
4) *Regulatory Sandbox* adalah mekanisme pengujian yang dilakukan oleh Otoritas Jasa Keuangan untuk menilai keandalan proses bisnis, model bisnis, instrumen keuangan, dan tata kelola Penyelenggara.
5) Ekosistem IKD adalah komunitas yang terdiri dari otoritas, Penyelenggara, konsumen, dan/atau pihak lain yang memanfaatkan platform digital secara bersama untuk mendorong IKD yang bermanfaat bagi masyarakat.

Ruang lingkup IKD meliputi: a. penyelesaian transaksi[168]; b. penghimpunan modal[169]; c. pengelolaan investasi[170]; d. penghimpunan dan penyaluran dana[171]; e. perasuransian[172]; f. pendukung pasar[173]; g. pendukung keuangan digital lainnya[174]; dan/atau h. aktivitas jasa keuangan lainnya[175].

Berdasarkan Pasal 4 POJK 13/2018, kriteria IKD meliputi: a. bersifat inovatif dan berorientasi ke depan; b. menggunakan teknologi informasi dan komunikasi sebagai sarana utama pemberian layanan kepada konsumen di sektor jasa keuangan; c. mendukung inklusi dan literasi keuangan; d. bermanfaat dan dapat dipergunakan secara luas; e. dapat diintegrasikan pada layanan keuangan yang telah ada; f. menggunakan pendekatan kolaboratif; dan

[168] Pasal 3 huruf a POJK 13/2018, Dalam praktiknya penyelesaian transaksi biasa disebut juga dengan settlement. Penyelesaian transaksi antara lain terkait penyelesaian investasi.

[169] Pasal 3 huruf b POJK 13/2018, Yang dimaksud dengan "penghimpunan modal" antara lain equity crowdfunding, virtual exchange and smart contract, serta alternative due diligence.

[170] Pasal 3 huruf c POJK 13/2018, Yang dimaksud dengan "pengelolaan investasi" antara lain advance algorithm, cloud computing, capabilities sharing, open source information technology, automated advice and management, social trading, dan retail algorithmic trading.

[171] Pasal 3 huruf d POJK 13/2018, Yang dimaksud dengan "penghimpunan dan penyaluran dana" antara lain pinjam meminjam berbasis aplikasi teknologi (P2P lending), alternative adjudication, virtual technologies, mobile 3.0, dan third-party application programming interface.

[172] Pasal 3 huruf e POJK 13/2018, Yang dimaksud dengan "perasuransian" antara lain sharing economy, autonomous vehicle, digital distribution, dan securitization and hedge fund.

[173] Pasal 3 huruf f POJK 13/2018, Yang dimaksud dengan "pendukung pasar" antara lain artifial inteligence/machine learning, machine readble news, social sentiment, big data, market information platform, dan automated data collection and analysis.

[174] Pasal 3 huruf g POJK 13/2018, Yang dimaksud dengan "pendukung keuangan digital lainnya" antara lain social/eco crowdfunding, Islamic digital financing, ewaqf, e-zakat, robo advise dan credit scoring.

[175] Pasal 3 huruf h POJK 13/2018, Yang dimaksud dengan "aktivitas jasa keuangan lainnya" antara lain invoice trading, voucher, token, dan produk berbasis aplikasi blockchain

g. memperhatikan aspek perlindungan konsumen dan perlindungan data.

Adapun norma tentang perlindungan data pribadi dalam POJK 13/2018 yakni sebagai berikut:

1. **Prinsip Pemantauan secara Mandiri.** OJK mewajibkan agar penyelenggara menerapkan prinsip pemantauan secara mandiri paling sedikit meliputi: a. prinsip tata kelola teknologi informasi dan komunikasi sesuai dengan peraturan perundang-undangan; b. perlindungan konsumen sesuai dengan ketentuan Peraturan Otoritas Jasa Keuangan ini; c. edukasi dan sosialisasi kepada konsumen; d. kerahasiaan data dan/atau informasi konsumen termasuk data dan/atau informasi transaksi; e. prinsip manajemen risiko dan kehati-hatian; f. prinsip anti pencucian uang dan pencegahan pendanaan terorisme sesuai dengan ketentuan peraturan perundang-undangan; dan g. inklusif dan prinsip keterbukaan informasi[176];
2. **Pusat Data di Indonesia.** OJK mewajibkan penyelenggara untuk menempatkan pusat data dan pusat pemulihan bencana di wilayah Indonesia[177];
3. **Kewajiban Menjaga Kerahasiaan Data.** Penyelenggara wajib menjaga kerahasiaan, keutuhan, dan ketersediaan data pribadi, data transaksi, dan data keuangan yang dikelolanya sejak data diperoleh hingga data tersebut dimusnahkan[178]. Ketentuan pemanfaatan data dan informasi pengguna yang diperoleh Penyelenggara harus memenuhi syarat sebagai berikut: a. memperoleh

[176] Pasal 18 ayat (1) POJK 13/2018
[177] Pasal 29 POJK 13/2018
[178] Pasal 30 ayat (1) POJK 13/2018

persetujuan dari pengguna; b. menyampaikan batasan pemanfaatan data dan informasi kepada pengguna; c. menyampaikan setiap perubahan tujuan pemanfaatan data dan informasi kepada pengguna dalam hal terdapat perubahan tujuan pemanfaatan data dan informasi; dan d. media dan metode yang dipergunakan dalam memperoleh data dan informasi terjamin kerahasiaan, keamanan, serta keutuhannya[179].

4. **Kewajiban Perlindungan Konsumen.** Penyelenggara wajib menerapkan prinsip dasar perlindungan konsumen yaitu: a. transparansi; b. perlakuan yang adil; c. keandalan; d. kerahasiaan dan keamanan data/informasi konsumen; dan e. penanganan pengaduan serta penyelesaian sengketa konsumen secara sederhana, cepat, dan biaya terjangkau[180]. Penyelenggara wajib menyediakan pusat pelayanan konsumen berbasis teknologi[181]. Pusat pelayanan konsumen berbasis teknologi paling sedikit terdiri atas penyediaan pusat layanan konsumen yang dapat dilaksanakan sendiri atau melalui pihak lain[182].;

---

[179] Pasal 30 ayat (2) POJK 13/2018

[180] Pasal 31 ayat (1) POJK 13/2018

[181] Pasal 31 ayat (2) POJK 13/2018

[182] Pasal 31 ayat (3) POJK 13/2018. Berdasarkan Penjelasan Pasal 31 ayat (3) POJK 13/2018 bahwa Cakupan dari pusat pelayanan konsumen berbasis teknologi (customer service tech) antara lain meliputi: a. saluran komunikasi multi kanal adalah penyampaian keluhan dengan berbagai media baik media suara, elektronik, maupun sosial; b. knowledge management adalah proses identifikasi, pembuatan, penelaahan, publikasi, dan penyediaan konten multimedia yang memungkinkan dilaksanakannya penjelasan kepada konsumen melalui web self service; c. aplikasi pencatat keluhan adalah aplikasi dimaksud selain menghasilkan data keluhan konsumen yang dapat dianalisis, juga dimungkinkan untuk melakukan komunikasi antar konsumen; d. customer service analytics adalah pelayanan konsumen dapat optimal sesuai dengan permasalahan yang disampaikan; dan e. data produktivitas agen adalah pencatatan terhadap aktivitas agen dalam menangani keluhan konsumen dan kecepatan dalam menangani keluhan sesuai dengan kebijakan internal Penyelenggara.

5. **Literasi Keuangan.** Penyelenggara wajib melaksanakan kegiatan untuk meningkatkan literasi dan inklusi keuangan[183];
6. **Larangan.** Pertama, Penyelenggara dilarang memberikan data dan/atau informasi mengenai konsumen kepada pihak ketiga[184]. Dengan pengecualian, bahwa Larangan sebagaimana dimaksud pada ayat (1) dikecualikan dalam hal: a. konsumen memberikan persetujuan secara elektronik; dan/atau b. Penyelenggara diwajibkan oleh ketentuan peraturan perundang-undangan untuk memberikan data dan/atau informasi mengenai konsumen kepada pihak ketiga[185]. Pembatalan atau perubahan sebagian persetujuan atas pengungkapan data dan/atau informasi sebagaimana dimaksud pada ayat (2) huruf a dilakukan secara elektronik oleh konsumen dalam bentuk dokumen elektronik[186].
7. **Sanksi Administratif & Tindakan Tertentu.** Ketentuan sanksi diatur dalam Pasal 39 POJK 13/2018 yakni:
   7.1 Dengan tidak mengurangi ketentuan pidana di sektor jasa keuangan, Otoritas Jasa Keuangan berwenang mengenakan sanksi administratif terhadap setiap pihak yang melakukan pelanggaran ketentuan Peraturan Otoritas Jasa Keuangan ini, termasuk pihak yang menyebabkan terjadinya pelanggaran tersebut berupa: a. peringatan tertulis; b. denda, yaitu kewajiban untuk membayar sejumlah uang tertentu; c. pembatalan persetujuan; dan/atau d. pembatalan pendaftaran[187].

[183] Pasal 34 POJK 13/2018
[184] Pasal 38 ayat (1) POJK 13/2018
[185] Pasal 38 ayat (2) POJK 13/2018
[186] Pasal 38 ayat (3) POJK 13/2018
[187] Pasal 39 ayat (1) POJK 13/2018

7.2 Sanksi administratif sebagaimana dimaksud pada ayat (1) huruf b sampai dengan huruf d dapat dikenakan dengan atau tanpa didahului pengenaan sanksi administratif berupa peringatan tertulis sebagaimana dimaksud pada ayat (1) huruf a[188];

7.3 Sanksi administratif berupa denda sebagaimana dimaksud pada ayat (1) huruf b dapat dikenakan secara tersendiri atau secara bersama-sama dengan pengenaan sanksi administratif sebagaimana dimaksud pada ayat (1) huruf c dan huruf d[189];

7.4 Tindakan Tertentu. Selain sanksi administratif sebagaimana dimaksud dalam Pasal 39, Otoritas Jasa Keuangan dapat melakukan tindakan tertentu terhadap setiap pihak yang melakukan pelanggaran ketentuan Peraturan Otoritas Jasa Keuangan ini[190]. Penjelasan Pasal 40 hanya berisikan 'cukup jelas', maka menurut hemat **Penulis,** tindakan tertentu ini adalah kewenangan yang dimiliki OJK untuk menindak pelaku usaha IKD yang terbukti melakukan pembocoran data/kerahasiaan konsumen, seyogyanya tindakan tersebut adalah tindakan yang tidak hanya bersifat hukuman namun juga berisikan keadilan bermartabat, misalnya tindakan agar pelaku usaha tersebut diwajibkan memberikan permintaan maaf secara tertulis di media massa cetak skala nasional selama 1 Minggu berturut-turut, dan sebagainya.

[188] Pasal 39 ayat (2) POJK 13/2018
[189] Pasal 39 ayat (3) POJK 13/2018
[190] Pasal 40 POJK 13/2018

Menurut hemat **Penulis,** OJK sebagai otoritas yang berwenang mengawasi IKD dan juga *peer to peer lending* (*P2P)* dapat memberikan sanski administratif bagi pelaku *platform* IKD ataupun *P2P* yang terdaftar pada OJK yang 'sengaja' ataupun 'lalai' dalam menjaga data pribadi konsumen. Namun yang masih menjadi pekerjaan rumah bersama yakni, bagaimana dengan IKD dan P2P yang illegal yang tidak terdaftar serta melakukan perbuatan melawan hukum dengan cara menyebarkan data pribadi, foto, menyebarlukaskan nama, nomor HP, mengancam, dan lain sebagainya? Jika konsumen ingin melakukan pengaduan atau perlindungan maka konsumen dapat melapor ke kepolisian dengan melampirkan bukti-bukti.

VI. Perlindungan Data Pribadi dalam Layanan Pinjam Meminjam Berbasis Teknologi *(Peer to Peer Lending)*

1. Peraturan Otoritas Jasa Keuangan Nomor 77/POJK.01/2016 tentang Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi (POJK 77/2016)

Penulis akan paparkan beberapa definisi dalam Ketentuan Umum POJK 77/2016, yakni:

1. Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi adalah penyelenggaraan layanan jasa keuangan untuk mempertemukan pemberi pinjaman dengan penerima pinjaman dalam rangka melakukan perjanjian pinjam meminjam dalam mata uang rupiah secara langsung melalui sistem elektronik dengan menggunakan jaringan internet[191];

[191] Pasal 1 Angka 3 POJK 77/2016

2. Penyelenggara Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi yang selanjutnya disebut Penyelenggara adalah badan hukum Indonesia yang menyediakan, mengelola, dan mengoperasikan Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi[192];
3. Penerima Pinjaman adalah orang dan/atau badan hukum yang mempunyai utang karena perjanjian Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi[193];
4. Pemberi Pinjaman adalah orang, badan hukum, dan/atau badan usaha yang mempunyai piutang karena perjanjian Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi[194];
5. Pengguna Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi yang selanjutnya disebut Pengguna adalah Pemberi Pinjaman dan Penerima Pinjaman yang menggunakan Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi[195];

Beberapa Norma yang terdapat dalam POJK 77/2016 tentang pengaturan data pribadi yakni:

1. **Prinsip dasar Perlindungan Pengguna.** Berdasarkan Pasal 29 POJK 77/2016 bahwa penyelenggara wajib menerapkan prinsip dasar dari perlindungan Pengguna yaitu: a. transparansi; b. perlakuan yang adil; c. keandalan; d. kerahasiaan dan keamanan data; dan e. penyelesaian sengketa Pengguna secara sederhana, cepat, dan biaya terjangkau.

[192] Pasal 1 Angka 6 POJK 77/2016
[193] Pasal 1 Angka 7 POJK 77/2016
[194] Pasal 1 Angka 8 POJK 77/2016
[195] Pasal 1 Angka 9 POJK 77/2016

2. **Batas Maksimum Pinjaman.** Penyelenggara wajib memenuhi ketentuan batas maksimum total pemberian pinjaman dana kepada setiap Penerima Pinjaman[196]. Batas maksimum total pemberian pinjaman dana sebagaimana dimaksud pada ayat (1) ditetapkan sebesar Rp2.000.000.000,00 (dua miliar rupiah)[197]. OJK dapat melakukan peninjauan kembali atas batas maksimum total pemberian pinjaman dana sebagaimana dimaksud pada ayat (2)[198];
3. **Kewajiban Pendaftaran&Perizinan.** Penyelenggara wajib mengajukan pendaftaran dan perizinan kepada OJK[199].
4. **Ketidakmampuan Operasional.** Penyelenggara yang memperoleh izin dan menyatakan tidak mampu meneruskan kegiatan operasionalnya, harus mengajukan permohonan kepada OJK disertai dengan alasan ketidakmampuan, dan rencana penyelesaian hak dan kewajiban Pengguna[200];
5. **Berbasis Perjanjian.** Perjanjian pelaksanaan Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi meliputi: a. perjanjian antara Penyelenggara dengan Pemberi Pinjaman; dan b. perjanjian antara Pemberi Pinjaman dengan Penerima Pinjaman[201]. Perjanjian penyelenggaraan Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi antara Penyelenggara dengan Pemberi Pinjaman dituangkan dalam Dokumen Elektronik[202];

[196] Pasal 6 ayat (1) POJK 77/2016
[197] Pasal 6 ayat (2) POJK 77/2016
[198] Pasal 6 ayat (3) POJK 77/2016
[199] Pasal 7 POJK 77/2016
[200] Pasal 13 POJK 77/2016
[201] Pasal 18 POJK 77/2016
[202] Pasal 19 ayat (1) POJK 77/2016

6. **Escrow Account (PEN-Rekening Bersama) dan Virtual Account.** Penyelenggara wajib menggunakan *escrow account*[203] dan *virtual account* dalam rangka Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi[204]. Penyelenggara wajib menyediakan *virtual account* bagi setiap Pemberi Pinjaman[205]. Dalam rangka pelunasan pinjaman, Penerima Pinjaman melakukan pembayaran melalui *escrow account* (**PEN-**nama lainnya ialah 'rekening bersama') Penyelenggara untuk diteruskan ke *virtual account* Pemberi Pinjaman[206]. Adapun tujuan kewajiban penggunaan *virtual account* dan *escrow account* dalam dalam penyelenggaraan kegiatan Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi, yaitu larangan bagi Penyelenggara dalam melakukan penghimpunan dana masyarakat melalui rekening Penyelenggara[207];
7. **Standar Minimum Sistem TI.** Penyelenggara wajib memenuhi standar minimum sistem teknologi informasi, pengelolaan risiko teknologi informasi, pengamanan teknologi informasi, ketahanan terhadap gangguan dan kegagalan sistem, serta alih kelola sistem teknologi informasi[208].

---

[203] Berdasarkan Pasal 4A ayat (1) Peraturan Bank Indonesia Nomor 3/11/PBI/2001 tentang Perubahan Atas Peraturan Bank Indonesia Nomor 2/24/PBI/2000 tentang Hubungan Rekening Giro Antara Bank Indonesia dengan Pihak Estern, bahwa *Escrow Account* yaitu rekening yang dibuka secara khusus untuk tujuan tertentu guna menampung dana yang dipercayakan kepada Bank Indonesia berdasarkan persyaratan tertentu sesuai dengan perjanjian tertulis.

[204] Pasal 24 ayat (1) POJK 77/2016

[205] Pasal 24 ayat (2) POJK 77/2016

[206] Pasal 24 ayat (3) POJK 77/2016

[207] Rancangan Surat Edaran OJK Nomor .. /SEOJK.05/2017 tentang Pendaftaran, Perizinan Usaha dan Kelembagaan Penyelenggara Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi (**PEN-**Hingga penyusunan buku ini, April 2020, SE ini masih dalam bentuk Rancangan). Diakses dari https://www.ojk.go.id/id/regulasi/otoritas-jasa-keuangan/rancangan-regulasi/Documents/LAMPIRAN%20%20RSEOJK%20Pendaftaran%20dan%20Perizinan%20v3%20(Dengar%20%20Pendapat).pdf

[208] Pasal 25 ayat (3) POJK 77/2016

8. **Kewajiban Penyelenggara.** Berdasarkan Pasal 26 POJK 77/2016 bahwa, Penyelenggara wajib untuk:
   17.1 menjaga kerahasiaan, keutuhan, dan ketersediaan data pribadi, data transaksi, dan data keuangan yang dikelolanya sejak data diperoleh hingga data tersebut dimusnahkan;
   17.2 memastikan tersedianya proses autentikasi, verifikasi, dan validasi yang mendukung kenirsangkalan dalam mengakses, memproses, dan mengeksekusi data pribadi, data transaksi, dan data keuangan yang dikelolanya;
   17.3 menjamin bahwa perolehan, penggunaan, pemanfaatan, dan pengungkapan data pribadi, data transaksi, dan data keuangan yang diperoleh oleh Penyelenggara berdasarkan persetujuan pemilik data pribadi, data transaksi, dan data keuangan, kecuali ditentukan lain oleh ketentuan peraturan perundangundangan;
   17.4 menyediakan media komunikasi lain selain Sistem Elektronik Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi untuk memastikan kelangsungan layanan nasabah yang dapat berupa surat elektronik, *call center*, atau media komunikasi lainnya; dan
   17.5 memberitahukan secara tertulis kepada pemilik data pribadi, data transaksi, dan data keuangan tersebut jika terjadi kegagalan dalam perlindungan kerahasiaan data pribadi, data transaksi, dan data keuangan yang dikelolanya.
9. **Sistem Pengamanan.** Dalam Pasal 28 diatur tentang sistem pengamanan bahwa salah satunya, Penyelenggara wajib melakukan pengamanan terhadap komponen sistem teknologi informasi dengan memiliki dan menjalankan

prosedur dan sarana untuk pengamanan Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi dalam menghindari gangguan, kegagalan, dan kerugian[209].

10. **Penyampaian Informasi Terkini.** Penyelenggara wajib menyediakan dan/atau menyampaikan informasi terkini mengenai Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi yang akurat, jujur, jelas, dan tidak menyesatkan[210].
11. **Bahasa yang mudah dimengerti.** Penyelenggara wajib menggunakan istilah, frasa, dan/atau kalimat yang sederhana dalam bahasa Indonesia yang mudah dibaca dan dimengerti oleh Pengguna dalam setiap Dokumen Elektronik[211].

P2P atau di masyarakat awam dikenal dengan nama Pinjol (Pinjaman *Online)*. Pinjol sangat dekat dengan masyarakat umum karena dengan Pinjol, konsumen dapat meminjam dengan nominal kecil dan 'cepat' serta tanpa jaminan. Nilai perputaran uang di Pinjol sangat cepat dan besar. Akumulasi pinjaman lewat *fintech lending* hingga Mei 2019 tercatat sebesar Rp 41,04 triliun. Nilai ini tumbuh 81,11% dibandingkan tahun lalu atau *year to date* (ytd) di 2018 sebesar Rp 22,66 triliun[212]. Namun, Modus pencurian data pribadi pada Pinjol digunakan untuk meminjam di Pinjol. Aksi jual beli data pribadi pengguna aplikasi fintech sempat marak beredar di media sosial. Sebagian penjual data pribadi ini memiliki ribuan hingga jutaan data KTP, KK hingga foto *selfie* menggunakan KTP. Data-data tersebut

[209] Pasal 28 ayat (1) POJK 77/2016

[210] Pasal 30 ayat (1) POJK 77/2016

[211] Pasal 32 ayat (1) POJK 77/2016

[212] Maizal W (Reproter) "Penggunaan Data Pribadi Pengguna P2P lending diatur oleh OJK dan AFPI" artikel tanggal 22 Juli 2019, diakses di https://keuangan.kontan.co.id/news/penggunaan-data-pribadi-pengguna-p2p-lending-diatur-oleh-ojk-dan-afpi diakses tanggal 3 Februari 2020

merupakan data yang sering diminta oleh aplikasi fintech atau pinjaman online (Pinjol) untuk verifikasi akun. Guna verifikasi akun tersebut agar bisa melakukan peminjaman uang dari aplikasi hingga menggunakan fitur *Pay Later*[213].

OJK menunjuk AFPI (Asosiasi Fintech Pendanaan Bersama Indonesia). Asosiasi Fintech Pendanaan Bersama Indonesia (AFPI) merupakan organisasi yang mewadahi pelaku usaha *Fintech Peer to Peer (P2P) Lending* atau Fintech Pendanaan Online di Indonesia. AFPI ditunjuk Otoritas Jasa Keuangan (OJK) sebagai asosiasi resmi penyelenggara layanan pinjam meminjam uang berbasis teknologi informasi di Indonesia, berdasarkan surat No. S-5/D.05/2019[214].

AFPI juga mendukung perlindungan konsumen dalam Pinjol. Apabila Konsumen telah wanprestasi dan memunggak pembayaran angsuran pinjaman, hal tersebut merupakan kewajiban Konsumen yang harus diselesaikan. Pada umumnya Fintech (penyelenggara) akan memberikan data akurat, penjelasan dan prosedur kepada pihak yang melakukan penagihan mengenai hal-hal yang boleh dan tidak boleh dilakukan oleh *debt collector*, apabila *Debt Collector* menghubungi disertai dengan ancaman atau tindak kekerasan lainnya ataupun data pribadi disalahgunakan oleh Fintech maka pengguna dapat menghubungi pihak yang berwajib, dalam hal ini Kepolisian Republik Indonesia. Disamping itu, pengguna juga dapat melaporkan ke AFPI melalui website www.afpi.or.id atau telepon 150505 (bebas pulsa) atau ke OJK melalui Kontak

[213] Tim CNN Indonesia, "Waspada Aksi Jual Beli Data Pribadi Lewat Aplikai Fintech", artikel tanggal 29 Juli 2019 diakses di https://www.cnnindonesia.com/teknologi/20190729082602-185-416323/waspada-aksi-jual-beli-data-pribadi-lewat-aplikasi-fintech diakses tanggal 4 Februari 2020

[214] https://www.afpi.or.id/about diakses tanggal 4 Februari 2020

OJK 157 apabila penyelenggara fintech Lending telah terdaftar/ berizin di OJK[215]

VII. Perlindungan Data Pribadi dalam Perdagangan Melalui Sistem Elektronik

Pemerintah telah mengeluarkan Peraturan Pemerintah No. 80 Tahun 2019 tentang Perdagangan Melalui Sistem Elektronik yang telah diundangkan pada 25 November 2019 (selanjutnya disebut PP PMSE). Definisi Perdagangan Melalui Sistem Elektronik (PMSE) adalah Perdagangan yang transaksinya dilakukan melalui serangkaian perangkat dan prosedur elektronik[216].

Para pihak yang terlibat dalam perdagangan melalui sistem elektronik ialah:

1) Pelaku usaha perdagangan melalui sistem elektronik yang selanjutnya disebut 'Pelaku Usaha' adalah setiap orang perseorangan atau badan usaha yang berbentuk badan hukum atau bukan badan hukum yang dapat berupa Pelaku Usaha Dalam Negeri dan Pelaku Usaha Luar Negeri dan melakukan kegiatan usaha di bidang PMSE[217];
2) Pribadi adalah orang perseorangan yang menjual barang dan/ atau jasa secara temporal dan tidak bertujuan komersial[218];
3) Pedagang (*merchant)* adalah pelaku usaha yang melakukan PMSE baik dengan sarana yang dibuat dan dikelola sendiri secara langsung atau melalui sarana

[215] *FAQ: Kategori Pengguna/Konsumen.* Otoritas Jasa Keuangan, dapat diakses di https://www.ojk.go.id/id/berita-dan-kegiatan/publikasi/Documents/Pages/-FAQ-Terkait-Layanan-Pinjam-Meminjam-Uang-Berbasis-Teknologi-Informasi---Kategori-Konsumen/FAQ%20LPMUBTI%20-%20Kategori%20Konsumen.pdf

[216] Pasal 1 Angka 2 PP PMSE

[217] Pasal 1 Angka 6 PP PMSE

[218] Pasal 1 Angka 9 PP PMSE

milik pihak PPMSE[219], atau sistem elektronik lainnya yang menyediakan sarana PMSE[220];

4) Penyelenggara Perdagangan Melalui Sistem Elektronik yang selanjutnya disingkat PPMSE adalah pelau usaha penyedia sarana komunikasi elektronik[221] yang digunakan untuk transaksi perdagangan[222];
5) Penyelenggara Sarana Perantara (*intermediary services)* adalah pelaku usaha dalam negeri atau pelaku usaha luar negeri yang menyediakan sarana komunikasi elektronik selain penyelenggara telekomunikasi yang hanya berfungsi sebagai perantara dalam komunikasi elektronik antara pengirim dan penerima[223];
6) Konsumen adalah setiap orang pemakai barang dan/atau jasa yang tersedia dalam masyarakat, baik bagi kepentingan diri sendiri, keluarga, orang lain ataupun makhluk hidup lain dan tidak untuk diperdagangkan[224];
7) Menteri adalah menteri yang menyelenggarakan urusan pemerintahan di bidang perdagangan.

Pengaturan perdagangan pada umumnya telah diatur dalam Undang-undang No. 7 Tahun 2014 tentang Perdagangan

[219] PPMSE adalah Penyelenggara Perdagangan Melalui Sistem Elektronik

[220] Pasal 1 Angka 10 PP PMSE

[221] Menurut hemat **penulis**, komunikasi elektronik adalah kegiatan yang termasuk namun tidak terbatas pada aksi reaksi terhadap penawaran suatu prudk barang/jasa, pengajuan pertanyaan, pernyataan ingin membeli suatu produk, pernyataan tidak ingin membeli, konfirmasi yang dilakukan melalui sarana elektronik dan internet. Sedangankan, berdasarkan Pasal 1 Angka 5 PP PMSE bahwa 'komunikasi elektronik adalah setiap komunikasi yang digunakan dalam PME berupa pernyataan, deklarasi, permintaan, pemberitahuan atau permohonan, konfirmasi, penawaran atau penerimaan terhadap penawaran, yang memuat kesepakatan para pihak untuk pembentukan atau pelaksanaan suatu perjanjian.

[222] Pasal 1 Angka 11 PP PMSE

[223] Pasal 1 Angka 12 PP PMSE

[224] Pasal 1 Angka 17 PP PMSE

dan terhadap kegiatan 'Perdagangan Melalui Sistem Elektronik' diamanatkan untuk membuat pengaturan lebih lanjut dalam Peraturan Pemerintah yang mengatur aktivitas perniagaan secara elektronik tersebut demi terselenggaranya sistem perdagangan yang *fair* dan terpercaya serta melindungi kepentingan nasional. Berbeda dengan pengaturan dalam Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaski Elektronik maka Pengaturan Pemerintah tentang Perdagangan Melalui Sistem Elektronik mengatur aspek hukum perdagangan dalam penyelenggaraan dan pemanfaatan 'Sistem Elektronik' yang ditujukan khusus untuk perdagangan[225].

Ruang lingkup pengaturan PMSE meliputi: a. pihak yang melakukan PMSE[226]; b. persyaratan dalam PMSE; c. penyelenggaraan PMSE; d. kewajiban Pelaku Usaha; e. bukti transaksi PMSE; f. Iklan Elektronik; g. Penawaran Secara Elektronik, Penerimaan Secara Elektronik, dan Konfirmasi Elektronik; h. Kontrak Elektronik; **i. perlindungan terhadap data pribadi;** j. pembayaran dalam PMSE; k. pengiriman Barang dan Jasa dalam PMSE; l. penukaran Barang atau Jasa dan pembatalan pembelian dalam PMSE; m. penyelesaian sengketa dalam PMSE; dan n. pembinaan dan pengawasan.

PMSE dilaksanakan berdasarkan asas *pacta sunt servanda* dan atas dasar perjanjian. Berdasarkan Pasal 4 ayat (2) PP

[225] Penjelasan bagian Umum PP PMSE paragraf ke-4.

[226] Berdasarkan Pasal 4 ayat (1) PP PMSE "PMSE dapat dilakukan oleh Pelaku Usaha, Konsumen, Pribadi, dan instansi penyelenggara negara sesuai dengan ketentuan peraturan perundang-undangan yang selanjutnya disebut para pihak." Pelaku Usaha pada PMSE dibedakan menjadi: 1. Pelaku Usaha Dalam Negeri (a. pedagang dalam negeri; b. Penyelenggara Perdagangan Melalui Sistem Elektronik/ PPMSE; c. Penyelenggara Sarana Perantara dalam negeri) yang dapat berbentuk orang perorangan, badan usaha, instansi penyelenggara Negara. dan 2. Pelaku Usaha Luar Negeri (a. pedangan luar negeri; b. Peyelenggara Perdagangan Melalui Sistem Elektronik/PPMSE Luar Negeri; c. Penyelenggara Sarana Perantara Luar Negeri. Lihat lebih lanjut Pasal 5 *jo.* Pasal 6 PP PMSE

PMSE bahwa "PMSE merupakan hubungan hukum privat yang dapat dilakukan antara: a. Pelaku Usaha dengan Pelaku Usaha; b. Pelaku Usaha dengan Konsumen; c. Pribadi dengan Pribadi, sesuai dengan ketentuan peraturan perundang-undangan; dan d. instansi penyelenggara negara dengan Pelaku Usaha, sesuai dengan ketentuan peraturan perundang-undangan."

Sebagaimana diamanatkan dalam Pasal 3 PP PMSE, bahwa PMSE dilaksanakan dengan memperhatikan prinsip-prinsip sebagai berikut:

1) Itikad baik; Prinsip Itikad baik yaitu Pelaku Usaha dan Konsumen dalam melakukan Perdagangan Melalui Sistem Elektronik wajib memiliki Itikad baik, di mana pelanggaran atas asas ini berakibat batalnya kesepakatan diantara para pihak, dengan tidak mengurangi atau mengabaikan hak-hak dari pihak yang memiliki iktikad baik dalam melakukan Perdagangan Melalui Sistem Elektronik (PMSE)[227].
2) Kehati-hatian; Prinsip kehati-hatian yaitu Pelaku Usaha dan Konsumen wajib bersikap hati-hati dalam melakukan Perdagangan Melalui Sistem Elektronik (PMSE), di mana segala informasi elektronik sehubungan dengan Pelaku Usaha, Konsumen, Barang dan/atau Jasa yang menjadi obyek Perdagangan serta syarat dan kondisi dari Perdagangan Barang atau Jasa melalui Sistem Elektronik wajib dipahami dengan baik;[228]
3) Transparansi; Prinsip transparansi yaitu Pelaku Usaha dan Konsumen wajib secara transparan menyampaikan segala informasi elektronik sehubungan dengan Pelaku

[227] Penjelasan Pasal 3 Huruf a PP PMSE
[228] Penjelasan Pasal 3 Huruf b PP PMSE

Usaha, Konsumen, Barang atau Jasa yang menjadi obyek Perdagangan serta persyaratan dan ketentuan dari Perdagangan Barang dan/atau Jasa melalui Sistem Elektronik wajib dipahami dengan baik[229];

4) Keterpercayaan; Prinsip keterpercayaan yaitu Pelaku Usaha wajib membangun Sistem Elektronik dengan baik yang layak dipercaya demi menjaga kepercayaan pengguna sistem terhadap Sistem Elektronik yang diselenggarakannya[230];
5) Akuntabilitas; Prinsip akuntabilitas yaitu Perdagangan Melalui Sistem Elektronik (PMSE) wajib dilakukan oleh para Pelaku Usaha dan Konsumen secara akuntabel dengan memperhatikan ketentuan peraturan perundang-undangan dan etika yang berlaku umum[231];
6) Keseimbangan; Prinsip keseimbangan yaitu Pelaku Usaha dan Konsumen wajib menjamin bahwa hubungan hukum yang dilakukan dilandasi oleh semangat untuk saling menguntungkan sesuai dengan harapan dan pengorbanan yang diberikan oleh masing-masing pihak[232];
7) Adil dan sehat; Prinsip adil dan sehat yaitu adanya kesetaraan kesempatan dan kedudukan dalam kegiatan usaha antar Pelaku Usaha PMSE untuk mewujudkan iklim usaha yang kondusif sehingga menjamin adanya kepastian dan kesempatan berusaha yang sama[233].

PP PMSE mengatur tentang 'perlindungan terhadap data pribadi' dalam Bab XI, Pasal 58 sampai dengan Pasal 59 PP PMSE. PP PMSE mengatur tentang perlindungan terhadap data

[229] Penjelasan Pasal 3 Huruf c PP PMSE
[230] Penjelasan Pasal 3 Huruf d PP PMSE
[231] Penjelasan Pasal 3 Huruf e PP PMSE
[232] Penjelasan Pasal 3 Huruf f PP PMSE
[233] Penjelasan Pasal 3 Huruf g PP PMSE

pribadi dalam Perdagangan Melalui Sistem Elektronik, dalam norma-norma sebagai berikut:

1) Pengaturan terhadap hal iklan elektronik sebagaiman diatur dalam Pasal 33 ayat (2) PP PMSE "Dalam hal Iklan Elektronik[234] disampaikan melalui sarana PPMSE dalam negeri dan/atau PPMSE luar negeri, PPMSE dalam negeri dan/atau PPMSE luar negeri wajib mematuhi ketentuan peraturan perundang-undangan di bidang penyiaran, perlindungan atas privasi dan data pribadi, perlindungan Konsumen, dan tidak bertentangan dengan prinsip persaingan usaha yang sehat."[235];
2) Berdasarkan Pasal 58 ayat (1) PP PMSE bahwa "Setiap data pribadi diberlakukan sebagai hak milik pribadi dari orang atau Pelaku Usaha yang bersangkutan";
3) Berdasarkan Pasal 58 ayat (2) PP PMSE bahwa "Setiap Pelaku Usaha yang memperoleh data pribadi sebagaimana dimaksud pada ayat (1) wajib bertindak sebagai pengemban amanat[236] dalam menyimpan dan menguasai data pribadi sesuai dengan ketentuan peraturan perundang-undangan."

---

[234] Definisi dari Iklan Elektronik sebagaimana diatur dalam Pasal 1 Angka 13 PP PMSE ialah "informasi untuk kepentingan komersial atas Barang dan/atau Jasa melalui Komunikasi Elektronik yang dimuat dan disebarluaskan kepada pihak tertentu baik yang dilakukan secara berbayar maupun yang tidak berbayar".

[235] Berdasarkan Penjelasan Pasal 33 ayat (2) PP PMSE bahwa "Yang dimaksud dengan "privasi dan data pribadi" tidak hanya mencakup aspek keamanan privasi dan data pribadi konsumen melainkan juga mencakup setiap aspek yang menyangkut kenyamanan konsumen sebagaimana telah diatur dalam Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen dan Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik serta peraturan pelaksanaannya."

[236] Berdasarkan Penjelasan Pasal 58 ayat (2) PP PMSE "Yang dimaksud dengan "pengemban amanat" adalah pengendali data pribadi sesuai dengan peruntukannya. Dalam mengemban amanat penyimpanan dan penggunaan data pribadi mengacu kepada standar perlindungan data pribadi sesuai kepatutan dan praktik bisnis yang berkembang."

4) Kewajiban pelaku usaha untuk menyimpan data pribadi sesuai standar perlindungan data pribadi atau kelaziman praktik bisnis yang berkembang sebagaimana diatur dalam Pasal 59 ayat (1) PP PMSE. PP PMSE telah dengan tegas mengatur perlindungan data pribadi dan telah memberikan beberapa standar perlindungan data pribadi yang dapat digunakan oleh pelaku usaha[237].
5) PP PMSE memberikan hak kepada pemilik data pribadi untuk meminta kepada pelaku usaha untuk menghapus seluruh data pribadi yang bersangkutan apabila pemilik data pribadi tersebut menyatakan keluar, berhenti berlangganan atau berhenti menggunakan jasa dan sarana PMSE[238] dan Pelaku Usaha harus menghapus seluruh data pribadi tersebut;

VIII. Data Pribadi dan Blockchain

Penulis pernah melakukan penelitian tentang *blockchain* dengan judul "Urgensi Pembentukan Peraturan Hukum tenang Pemanfaatan Teknologi *Blockchain* di Indonesia". Penelitian ini didukung oleh Lembaga Penelitian dan Pengabdian Masyarakat Universitas Pelita Harapan (LPPM UPH) pada tahun 2019. Pada kesempatan ini, **Penulis** akan membahas sedikit, dan jika diberikan rahmat-Nya suatu saat **Penulis** akan mengulasnya lebih dalam lagi.

Kesimpulan penelitian ini adalah pertama, pembentukan peraturan ataupun pembaharuan hukum yang berkaitan dengan sistem teknologi seyogyanya menyesuaikan dengan perkembangan teknologi *blockchain*, pembaharuan hukum

[237] Penulis telah jabarkan dalam sub bab "standar perlindungan data pribadi"
[238] Pasal 59 ayat (3) PP PMSE

tersebut wajib berisikan keadilan bermartabat, keadilan bagi konsumen ataupun pelaku usaha untuk terciptanya kelancaran dalam berbisnis dan keamanan dalam bertransaksi keuangan. Kedua, bahwa bentuk perlindungan hukum terhadap perkembangan teknologi *blockchain* kurang terintegrasi dengan baik, diperlukan sinergitas dan harmonisasi peraturan perundang-undangan terkait teknologi *blockchain* dan teknologi finansial antara otoritas yang berwenang (Otoritas Jasa Keuangan, Bank Indonesia, PPATK, Kementerian Komunikasi dan Informatika)[239].

1. Tinjauan Umum tentang *Blockchain*

The popularity of blockchain technology is rapidly rising, as many new applications for blockchain technology are being developed and deployed. These applications include new payment options, ways of asset and identity management, and the use of smart contracts. Perhaps the best-known application of blockchain technology is the cryptocurrency as it enables cheap, fast and straightforward international money transfers. Paying with cryptocurrencies for regular products and services is becoming more and more common, as they are easy to buy and sell on online exchange-platforms[240].

The data contained in a blockchain can be different in nature. For example: the blockchain of Bitcoin, a virtual currency, or cryptocurrency to be more precise, is a ledger with information about bitcoin transactions. Cryptocurrencies are probably the most

[239] Teguh Prasetyo, Rizky Karo Karo, Vena Pricilia, "Urgensi Pembentukan Peraturan Hukum tenang Pemanfaatan Teknologi *Blockchain* di Indonesia", Laporan Hasil Penelitian, Lembaga Penelitian dan Pengabdian Masyarakat (LPPM) Universitas Pelita Harapan (UPH), Juli 2019. Hlm. 1.

[240] Bart Custers *and* Lara Overwater, "*Regulating Initial Coin Offerings an Cryptocurrencies: A Comparison of Different Approaches Nine Jurisdictions Worldwide", (European Journal of Law and Technology, Vol 10, Issue 3, 2019)* hlm.2, diakses dari http://ejlt.org/article/view/718/981 tanggal 19 Mei 2020

familiar application of blockchain technology. However, that is just one of the many applications blockchain technology can have. Other applications can be the execution of cadastral registrations, decentralized voting, notarial actions, and other property registrations and transfers, such as supply chain monitoring and peer-to-peer insurance[241].

Teknologi *blockchain* telah banyak dimanfaatkan di berbagai negara di dunia, khususnya di Indonesia. Penggunaan *blockchain* membawa dampak positif bagi pengembangan dunia bisnis di Indonesia, namun juga memiliki dampak negatif jika tidak diawasi oleh baik oleh Pemerintah Indonesia. Dampak positif penggunaan *blockchain* dapat meningkatkan efisiensi waktu, biaya lalu lintas transaksi keuangan. Namun disatu sisi, *blockchain* menimbulkan dampak negatif yakni membuka peluang munculnya kejahatan dunia maya (*cybercrime)* misalnya pencurian data privasi, data keuangan nasabah[242].

Blockchain berasal dari 2 kata yakni *block (*blok) dan *chain (*rantai). Jika ditranslasi ke dalam Bahasa Indonesia berarti rantai blok. *Blockchain* adalah komponen utama dalam sistem mata uang kripto. *Blockchain* dapat diibaratkan sebagai sebuah sistem basis data terdesentralisasi. Basis data ini sangat unik karena dapat diduplikasi oleh pihak manapun. Sementara penambahan metode penambahan informasi baru yang diterapkan pada *blockchain* juga istimewa karena memperbolehkan siapapun berkompetisi untuk membuat data baru asalkan memenuhi semua kriteria yang telah ditetapkan

[241] *Ibid*. hlm.4.

[242] Teguh Prasetyo, Rizky Karo Karo, Vena Pricilia, "Urgensi Pembentukan Peraturan Hukum tenang Pemanfaatan Teknologi *Blockchain* di Indonesia", Laporan Hasil Penelitian, Lembaga Penelitian dan Pengabdian Masyarakat (LPPM) Universitas Pelita Harapan (UPH), Juli 2019. Hlm. 1.

oleh protocol. Meskipun memperbolehkan penambahan data baru namun pengubahan data tidak diperbolehkan dalam sistem *blockchain*. Hal ini dimaksudkan untuk menjaga integritas data agar tetap konsisten[243].

Menurut Iansiti & Lakhani, Konsep *blockchain* mempunyai lima kata kunci: 1. Basis data yang tersebar (*decentralized*); 2. Transmisi *peer-to-peer* ; 3. Transparansi melalui enkripsi ; 4. Perekaman data secara permanen ; 5. Berbasis pemrograman digital.

Gambar 1. Ilustrasi Konsep Blockchain

Sumber gambar: *Centre for Innovation Policy and Governance, Big Data, Kecerdasan Buatan, Blockchain, dan Teknologi Finansial di Indonesia, Usulan Desain, Prinsip dan Rekomendasi Kebijakan,* (Jakarta: CIPG, 2018), hlm. 26.

Blockchain adalah suatu sistem transaksi dan manajemen data digital yang tersebar dimana semua pengguna sistem tersebut mempunyai satu konsensus bersama. Dengan membuat sistem secara tersebar, *blockchain* menghilangkan peran perantara sehingga bisa membuat biaya transaksi lebih murah. Perbincangan *blockchain* tidak bisa dilepaskan dari fenomena Bitcoin Popularitas salah satu mata uang virtual tersebut sering kali membuat masyarakat umum mengasosiasikan *blockchain* dengan Bitcoin (Crosby et al., 2016, Nakamoto, 2008). Bitcoin

[243] *Op.Cit,* Dimaz Ankaa Wijaya, hlm.14.

hanyalah salah satu produk yang berbasis pada *blockchain*. Saat ini, *blockchain* telah dimanfaatkan di luar bidang finansial atau sekuritas keuangan, seperti ketahanan pangan, tata kelola lingkungan, dan perencanaan kota[244].

Blockchain telah berkembangan menjadi *Blockchain 4.0.*

1. ***Blockchain* 1.0: Mata Uang.**
   Implementasi teknologi buku besar terdistribusi (DLT) menyebabkan aplikasi pertama dan jelas: *cryptocurrency.* Hal ini memungkinkan transaksi keuangan berdasarkan teknologi *blockchain* atau DLT (demi kesederhanaan yang sering dilihat sebagai sinonim) untuk dieksekusi dengan **Bitcoin** menjadi contoh paling menonjol di segmen ini. Ini digunakan sebagai «uang tunai untuk Internet», sebuah sistem pembayaran digital dan dapat dilihat sebagai pendukung «*Internet of Money*".[245]
2. **Blockchain 2.0: Kontrak Cerdas**
   Konsep kuncinya adalah *Smart Contracts,* program komputer kecil yang "hidup" di *blockchain*. Mereka adalah program komputer otonom yang mengeksekusi secara otomatis dan kondisi yang ditentukan sebelumnya seperti fasilitasi, verifikasi atau penegakan kinerja kontrak. Satu keuntungan besar yang ditawarkan teknologi ini, adalah *blockchain* yang membuatnya tidak mungkin untuk merusak atau meretas Kontrak Cerdas. Jadi Kontrak Cerdas mengurangi biaya verifikasi, *exceution*, arbitrasi dan pencegahan penipuan dan memungkinkan definisi kontrak transparan mengatasi

[244] *Centre for Innovation Policy and Governance, Big Data, Kecerdasan Buatan, Blockchain, dan Teknologi Finansial di Indonesia, Usulan Desain, Prinsip dan Rekomendasi Kebijakan, (*Jakarta: CIPG, 2018) *H.27.*

[245] https://medium.com/@UnibrightIO/blockchain-evolution-from-1-0-to-4-0-3fbdbccfc666 diakses tanggal 10 Januari 2019

masalah moral hazard. Yang paling menonjol di bidang ini adalah ***Ethereum*** Blockchain yang bertujuan untuk memungkinkan pelaksanaan Kontrak Cerdas[246].

3. ***Blockchain* 3.0: DApps**

   DApp adalah bentuk disingkat untuk *aplikasi desentralisasi yang* menghindari infrastruktur terpusat. Ini menggunakan penyimpanan terdesentralisasi dan komunikasi terdesentralisasi, sehingga sebagian besar DApps menjalankan kode backend mereka pada jaringan *peer-to-peer* terdesentralisasi, sebuah *blockchain*. Sebaliknya, aplikasi tradisional memiliki kode backend yang berjalan di server terpusat. DApp dapat memiliki kode frontend dan antarmuka pengguna yang ditulis dalam bahasa apa pun yang dapat melakukan panggilan ke backendnya, seperti App tradisional. Tapi Dapp dapat memiliki frontend-nya di-host pada penyimpanan terdesentralisasi seperti Ethereums Swarm. **DApp = DApp = frontend + contracts (**running i.e. on Ethereum**) (**berjalan yaitu pada Ethereum **)**[247]

4. ***Blockchain* 4.0: Membuat *blockchain* dapat digunakan di industri (4.0)**

   Dengan fondasi yang diletakkan oleh versi sebelumnya, bagi kami *Blockchain* 4.0 menjelaskan solusi dan pendekatan yang membuat teknologi *blockchain* dapat digunakan untuk tuntutan bisnis. Terutama **tuntutan Industri 4.0**. Industri 4.0 artinya dalam otomatisasi jangka pendek, perencanaan sumber daya perusahaan, dan integrasi sistem eksekusi yang berbeda. Namun, revolusi industri ini

[246] *Ibid.*
[247] *Ibid.*

menuntut tingkat kepercayaan dan perlindungan privasi yang meningkat pada tahap di sinilah *blockchain* masuk. Ketika menambahkan *blockchain* ke sistem TI, orang akan berakhir dengan integrasi bisnis, memungkinkan proses bisnis *Cross-System/Cross-Blockchain*, yaitu mesin yang secara aman dan mandiri menempatkan pesanan untuk suku cadang pengganti mereka. Manajemen rantai pasokan, alur kerja persetujuan, transaksi keuangan dan pembayaran berbasis kondisi, pengumpulan data IoT, manajemen kesehatan dan manajemen aset hanyalah beberapa contoh area yang dapat diberdayakan oleh teknologi *blockchain*. *Blockchain* 4.0 berarti, membuat *Blockchain* 3.0 dapat digunakan dalam skenario bisnis kehidupan nyata. Memenuhi tuntutan Industri 4.0 dengan membuat janji-janji *blockchain* terwujud[248].

Menurut Prof. Sulistiowati (Guru Besar Hukum Dagang Fakultas Hukum UGM), pengawasan terhadap sistem *blockchain* wajib dilakukan oleh seluruh pihak, khususnya, Kementerian Komunikasi dan Informatika, Bank Indonesia, Otoritas Jasa Keuangan, Kepolisian Negara Republik Indonesia (Polri), Pusat Pelaporan dan Analisis Transaksi Keuangan (PPATK)[249]. Kerjasama antara lembaga ini sangat dibutuhkan untuk mecengah kejahatan siber perbankan menggunakan teknologi *blockchain*. OJK pun wajib mengawal konsumen yang mengalami kerugian konsumen untuk mendapatkan uangnya kembali secara gugatan keperdataan[250].

[248] *Ibid.*

[249] Hasil wawancara dengan Prof. Dr Sulistiowati, S.H., M.Hum selaku Guru Besar Hukum Dagang Fakultas Hukum Universitas Gadjah Mada (FH UGM), di Fakultas Hukum UGM, tanggal 23 Maret 2019

[250] Rizky Karo Karo, *A*rtikel "Kejahatan Siber Perbankan", Kolom Opini Harian Kompas tanggal 27 Juli 2018.

BAB V

PENEGAKAN HUKUM PERLINDUNGAN DATA PRIBADI MELALUI SARANA HUKUM ADMINISTRASI NEGARA, HUKUM PERDATA, HUKUM PIDANA

Kebocoran data pribadi wajib diselesaikan secara hukum dan dengan pendekatan keadilan bermartabat. Pelaku harus diproses secara hukum dengan hukuman yang sesuai dengan perbuatannya. Korban kebocoran data di suatu sistem elektronik juga harus diberikan perlindungan dan keadilan dan penyelenggara sistem elektronik wajib meningkatkan sistem keamanan mereka dengan lebih baik lagi.

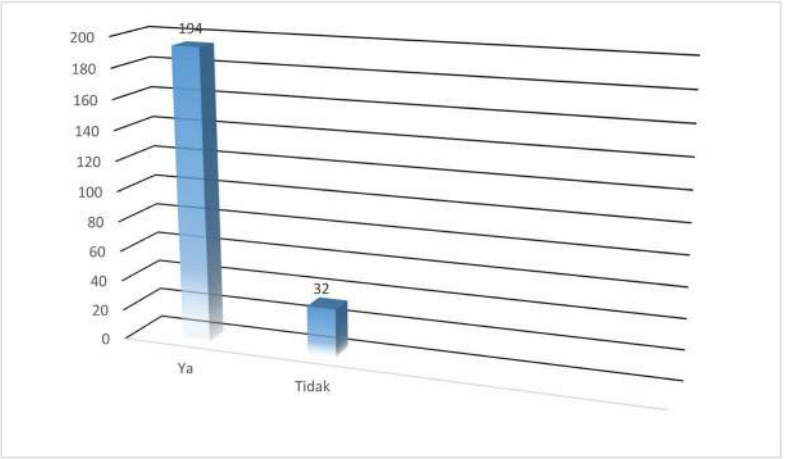
Penegakan hukum terhadap perlindungan data pribadi dapat dilakukan melalui 3 (tiga) sarana hukum, pertama, hukum administrasi negara (HAN); kedua, melalui hukum perdata; ketiga, melalui hukum pidana sebagai *ultimum remidium*. Namun tidak menutup kemungkinan diselesaikan secara mediasi atau dengan alternatif penyelesaian sengketa di luar pengadilan lainnya.

I. Sengketa/Kasus Hukum Perlindungan Data Pribadi di Indonesia

Dalam sub-bab ini, **Penulis** akan membahas kasus-kasus penyalahgunaan data pribadi di Indonesia dan akan

menganalisisnya menggunakan peraturan perundang-undangan yang ada. Untuk menghormati dan menjunjung tinggi etika penulisan, **Penulis** akan menyamarkan identitas yang ada.

Penulis menganalisis data yang diperoleh dari 226 responden. Adapun **Penulis** mendapatkan bahwa 86% atau 194 respoden pernah mendapatkan telepon dari suatu usaha yang menawarkan, menjual (marketing) suatu barang atau layanan kartu kredit dan 14% atau 32 responden tidak pernah mendapatkan telepon terhadap usaha tersebut.



Grafik 26. Pertanyaan tentang Apakah Saudara/i pernah mendapatkan telepon dari suatu usaha yang menawarkan, menjual (marketing) suatu barang atau layanan kartu kredit?

Sumber: Dokumen pribadi.

Pertama, Seorang teman **Penulis,** FS juga pernah mengalami dugaan tindak pidana penyalahgunaan data pribadi. Kronologis kasusnya sebagai berikut: pada malam hari di Desember tahun 2019, FS menerima telepon oleh orang yang tidak dikenal meminta nomor OTP (*One Time Password)* yang

dikirim ke nomor ponsel HP melalui SMS (*short message service)* karena pelaku sedang bertransaksi *online* disuatu *platform (e-commerce)*, FS tidak mengindahkanya dan beberapa menit kemudian, FS menerima telpon dari orang yang mengaku sebagai *customer service* suatu bank swasta di Indonesia yang mengatakan bahwa telah ada transaksi melalui kartu kredit FS dan FS harus memberitahukan angka terakhir pada kartu kredit tersebut. Atas kejadian tersebut, FS tidak menuruti penelpon tersebut, dan FS langsung menghubungi *CS* bank swasta tersebut di *website* yang resmi.

Menurut hemat **Penulis,** langkah yang diambil oleh FS sudah benar. FS tidak memberikan *OTP,* menelpon CS untuk memberitahukan dugaan tindak pidana tersebut dan FS meminta untuk memblokir kartu kredit yang telah diretas. FS pun seyogyanya dapat juga melaporkannya kepada Polisi atau melaporkan nomor ponsel tersebut ke layanan Otoritas Jasa Keuangan (OJK) melalui layanan *email* (konsumen@ojk.go.id) atau hubungi 157[251]. *OTP* adalah salah satu cara untuk meningkatkan keamanan dalam suatu sistem elektronik dengan 2 (dua) kali otentifikasi (*two-factor authentication)* dengan menggunakan proses algoritma, pada umumnya *OTP* akan diberikan melalui pesan singkat (*SMS)* ke nomor ponsel pengguna/konsumen yang dimasukan ke sistem tersebut berbentuk kombinasi huruf besar, huruf kecil, angka dengan sistem acak dan *OTP* umumnya hanya berlaku dalam hitungan menit sehingga si pengguna harus segera memasukan *OTP* tersebut. *OTPs are difficult for human beings to memorize. Therefore they require additional technology to work. So we need*

[251] OJK, "SMS Palsu Mengganggu? Laporkan Saja!, https://sikapiuangmu.ojk.go.id/FrontEnd/CMS/Article/375 diakses tanggal 9 Februari 2020

to generate OTP. OTP generation algorithms typically make use of pseudo randomness or randomness[252]*. Static OTP is a password that is valid for only one login session or transaction, on a computer system or other digital device. A one-time PIN code is a code that is valid for only one login session or transaction using a mobile phone*[253]*.*

Berdasarkan penelusuran **Penulis,** jika konsumen perbankan ingin melakukan pengaduan, maka dapat menyampaikan pengaduan ke Bank Indonesia secara *online* di *website* berikut: https://www.bi.go.id/id/edukasi-perlindungan-konsumen/formpengaduan/Pages/formulirPengaduanKonsumen.aspx atau selain di *website* di Bank Indonesia, konsumen perbankan/jasa keuangan lainnya dapat mengadu di *website* Otoritas Jasa Keuangan (OJK) di *website* https://konsumen.ojk.go.id/FormPengaduan

Kasus Kedua, data penumpang suatu maskapai berinisial (LA) diduga bocor pada awal September 2019. Kebocoran tersebut diungkapkan oleh perusahaan keamanan siber *Kaspersky Lab,* setidaknya sebayak 21 (dua puluh satu) juta data penumpang LA bocor dan diunggah ke forum daring *(online)*. Pada 23 September 2019, Pejabat di Kementerian Komunikasi dan Informatika (Kominfo) telah melakukan pertemuan dengan pihak perusahaan maskapai LA untuk melakukan penanganan dan pengamanan data penumpang. Langkah yang diambil oleh perusahaan maskapai LA ialah mengambil aksi pelaporan dan tuntutan hukum bagi pelaku pencurian dan pembocoran

[252] K. Mohan Kumar *and* G. BalaMurugan "*Comparative Study on One Time Password Algirthms*" (*International Journal of Computer Science and Mobile Computing, Vol. 7, Issue 8, Aug 2018, pg. 37-52)* hlm.38., dapat diakses di https://ijcsmc.com/docs/papers/August2018/V7I8201811.pdf, diakses tanggal 4 April 2020

[253] *Ibid*

data penumpang serta melakukan *legal action* kepada otoritas berwenang di Malaysia[254].

Kominfo mengatakan bahwa lebih dari 150.000 Warga Negara Indonesia menjadi korban skandal dalam kebocoran data penumpang maskapai berinisial MA, anggota dari LA group. Pada tanggal 25 September 2019 MA menjelaskan bahwa investigasi awal oleh pihak independen, ditemukan sekitar 7,8 juta penumpang menjadi korban kegagalan perlindungan data pribadi. Dari jumlah itu, sebanyak 66 persen warga Malaysia, 4 persen warga India, dan 2 persen atau sekitar 156.000 warga Indonesia. Sementara dari hasil pertemuan dengan Direktur Jenderal Jabatan Perlindungan Data Pribadi (JPDP), Kementerian Komunikasi dan Multimedia Malaysia di Putrajaya diketahui bahwa korban kebocoran data Malindo Air berasal dari 18 negara. Dari jumlah itu, enam di antaranya berada di Asia Tenggara. Mereka adalah Malaysia, Indonesia, Singapura, Vietnam, Myanmar, dan Kamboja. Dalam kasus maskapai MA, Dirjen JPDP Malaysia menyampaikan bahwa investigasi difokuskan pada maskapai MA sebagai Badan Hukum Malaysia, sedangkan untuk PT Lion Air Indonesia tidak dapat dikaitkan dengan kasus ini karena tidak berkedudukan di wilayah hukum Malaysia[255].

Menurut hemat **Penulis,** payung hukum yang dapat digunakan dalam kasus ini ialah: 1. Undang-undang

[254] Fitri N.H., artikel tanggal 24 September 2019 berjudul "Data Penumpang Lion Air Bocor, UU Perlindungan Data Pribadi Dibutuhkan", https://www.hukumonline.com/berita/baca/lt5d8947d7aa783/data-penumpang-lion-air-bocor--uu-perlindungan-data-pribadi-dibutuhkan/ diakses tanggal 9 Februari 2020

[255] Liberty Jemadu, artikel tanggal 26 September 2019, "Kominfo: 150.000 WNI jadi Korban Kasus Kebocoran Data Lion Air Group", https://www.suara.com/tekno/2019/09/26/194122/kominfo-150000-wni-jadi-korban-kasus-kebocoran-data-lion-air-group diakses tanggal 9 Februari 2020

Perlindungan Data Pribadi Malaysia 2010 (*Malaysian Personal Data Protection Act 2010)*; 2. UU ITE; UU Penerbangan; 3. PP PSTE

Kasus Ketiga, di dunia internasional, kebocoran data pribadi yang dialami oleh *facebook (FB)* sehingga *FB* harus membayar denda Rp.70 Triliun. Berdasarkan liputan kompas. com bahwa Komisi Perdagangan Federal AS memberikan sanksi ke *FB* atas skandal *Cambridge Analytica* dan kasus-kasus kebocoran data serupa. Alasan Komisi memberikan sanski denda karena FB terbukti lalai melindungi privasi dan data pribadi pengguna yang kemudian bocor&dimanfaatkan oleh pihak ketiga. FB juga terbukti memanfaatkan nomor telepon pengguna untuk kepentingan iklan dan menyalagunakan sistem pengenalan wajah (*face recognition)* dalam *platform FB*. Selain denda, *FB* diwajibkan untuk memperbaiki sistem keamanan&mekanismen privasi terbaru yang lebih transparan, salah satunya dengan menciptakan mekanisme untuk mengulas dan menelisik sisi privasi penggunan di seluruh produk yang diciptakan *FB* baik perangkat lunak, kebijakan layanan ataupun sistem terbaru di *FB*. Produk tersebut harus diuji kelayakan dalam sistem perlindungan data pengguna oleh pihak internal *FB* bersama dengan para asesor pihak ketiga. Penilaian tersebut wajib dilakukan rutin empat kali dalam setahun[256].

Kasus **Keempat,** dunia pada awal tahun 2020 termasuk Indonesia dilanda oleh pandemic virus corona. Berdasarkan Pedoman Pencegahan dan Pengendalian *Coronavirus Disease (COVID-19)* yang dirilis oleh Kementerian Kesehatan RI bahwa ada awal tahun 2020, COVID-19 menjadi masalah kesehatan

[256] Bill Clinten "*Facebook* Resmi Didenda Rp 70 Triliun, Terbesar Dalam Sejarah" diakses dari https://tekno.kompas.com/read/2019/07/25/06510077/facebook-resmi-didenda-rp-70-triliun-terbesar-dalam-sejarah?page=all#page3 diakses tanggal 2 Februari 2020

dunia. Kasus ini diawali dengan informasi dari Badan Kesehatan Dunia/World Health Organization (WHO) pada tanggal 31 Desember 2019 yang menyebutkan adanya kasus kluster pneumonia dengan etiologi yang tidak jelas di Kota Wuhan, Provinsi Hubei, China. Kasus ini terus berkembang hingga adanya laporan kematian dan terjadi importasi di luar China. Pada tanggal 30 Januari 2020, WHO menetapkan COVID-19 sebagai Public Health Emergency of International Concern (PHEIC)/ Kedaruratan Kesehatan Masyarakat Yang Meresahkan Dunia (KKMMD). Pada tanggal 12 Februari 2020, WHO resmi menetapkan penyakit novel coronavirus pada manusia ini dengan sebutan Coronavirus Disease (COVID19). Pada tanggal 2 Maret 2020 Indonesia telah melaporkan 2 kasus konfirmasi COVID-19. Pada tanggal 11 Maret 2020, WHO sudah menetapkan COVID-19 sebagai pandemi[257].

Presiden (masa jabatan 2019-2024) Joko Widodo (Jokowi) juga telah menyampaikan pada Maret 2020 di Istana Bogor bahwa untuk menghadapi dan menghindari penyebaran corona adalah 'kebijakan belajar dari rumah, bekerja dari rumah dan ibadah di rumah'[258]. Masyarakat Indonesia, pekerja yang bekerja dari rumah, *work from home*, belajar dari rumah/*study from home* baik menggunakan pelbagai aplikasi/*platform,* termasuk namun tidak terbatas pada aplikasi *zoom, Microsoft teams, Google Meet, Skype, WebEx,* aplikasi media daring dari Kementerian Pendidikan dan Kebudayaan (*'Rumah Belajar', 'Meja Kita')*, ataupun ibadah dari rumah menggunakan layanan *youtube*.

[257] Kementerian Kesehatan RI, Direktorat Jenderal Pencegahan dan Pengendalian Penyakit (P2P), Maret 2020, hlm. 4

[258] Ihsanuddin, 16 Maret 2020, "Jokowi: Kerja dari Rumah, Belajar dari Rumah, Ibadah di Rumah Perlu Digencarkan", https://nasional.kompas.com/read/2020/03/16/15454571/jokowi-kerja-dari-rumah-belajar-dari-rumah-ibadah-di-rumah-perlu-digencarkan dakses tanggal 5 April 2020

Pada bulan April 2020, aplikasi *zoom* menjadi perhatian dunia karena dianggap berpotensi melakukan pelanggaran privasi data dan perlindungan data pribadi. Menurut Pratama Persadha, pakar keamanan siber dari *CISSRec* sebagaimana dikutip oleh cnnindonesia.com bahwa data yang paling dikhawatirkan untuk disalahgunakan ialah data pemetaan wajah para pengguna. "Pemetaan wajah pengguna ini berbahaya karena sejumlah perangkat kini membuka kata sandi dengan wajah. Bisa diartikan bila ada penyalahgunaan atau bocornya data wajah pemakai akan berakibat risiko keamanan yang besar".[259]

Menurut media *"The Intercept"* sebagaimana dikutip oleh tekno.kompas.com (2 April 2020) melaporkan bahwa aplikasi *zoom* ternyata tidak melakukan enkripsi untuk panggilan video yang dilakukan pengguna. Menurut juru bicara zoom sebagaimana dikutip oleh tekno.kompas.com (2 April 2020) bahwa saat ini tidak memungkinkan untuk menghadrikan enkripsi *end-to-end* untuk panggilan video *Zoom Zoom* menggunakan kombinasi *TCP* dan *UDP* sebagai pengamanan. *TCP* dibuat berdasarkan protokol *TLS. TLS* adalah protokol yang digunakan untuk memperkuat keamanan *website* dengan protokol komunikasi berupa *HTTPS*. Protokol ini berbeda dengan sistem keamanan enkripsi *end-to-end* yang membuat komunikasi tidak dapat diintip oleh peretas[260].

Kasus terakhir yang sempat heboh di Indonesia pada bulan Mei 2020 adalah suatu *platform e-commerce* di Indonesia diduga

[259] CNN Indonesia, 3 April 2020 "Celah Aplikasi Zoom Disebut Rawan Curi Data Wajah Pengguna" https://www.cnnindonesia.com/teknologi/20200403073335-185-489837/celah-aplikasi-zoom-disebut-rawan-curi-data-wajah-pengguna diakses tanggal 5 April 2020

[260] Putri Zakia S, "Bahaya yang Mengintai di Balik Penggunaan Zoom", artikel tanggal 2 April 2020, diakses dari https://tekno.kompas.com/read/2020/04/02/20340017/bahaya-yang-mengintai-di-balik-penggunaan-zoom diakses tanggal 22 Mei 2020

diretas oleh *hacker* dan data pribadi pengguna *e-commerce* tersebut dijual di *darkweb* (pasar gelap). Menurut liputan *kompas.com* bahwa situs *e-commerce* berinisial T dilaporkan mengalami usaha peretasan. Data pengguna T diduga telah diretas dan bocor di dunia maya. Peretasan terjadi pada Maret 2020 dan peretas disebutkan memiliki lebih banyak data lagi, di luar 15 juta pengguna yang telah tersebar datanya. Data yang dikumpulkan termasuk nama pengguna, *e-mail*, dan *hash password* yang tersimpan di dalam sebuah *file database PostgreSQL*. Selain *hash password*, nama, dan alamat e-mail, data yang diretas juga mencakup tanggal lahir, kode aktivasi *e-mail*, kode *reset password*, detail lokasi, *ID messenger*, hobi, pendidikan, waktu pembuatan akun hingga waktu terakhir *log-in*. Namun, dalam daftar akun yang terkumpul di database berjenis *PostgreSQL* itu, disinyalir tidak disertakan dengan kode spesifik atau biasa disebut "*salt*". Rangkaian kode *salt* ini berguna untuk melindungi kata sandi pengguna dengan algoritma. Dengan demikian, diperlukan waktu bagi peretas untuk menebak serta membobol akun pengguna[261].

Menurut Nuraini, *VP of Corporate Communications Tokopedia* sebagaimana dimuat dalam *website* kominfo.go.id membantah bahwa telah kebocoran data penggunanya dan terjadinya transaksi jual beli data tersebut. Data pengguna tetap aman. Nuraini menjelaskan bahwa jika data-data yang beredar luas dan dianggap merupakan data pengguna T yang bocor itu berasal dari data yang sengaja dipublikasikan oleh pengguna[262].

[261] Yudha Pratomo, "Kebocoran Data 15juta Pengguna, Pengakuan Tokopedia, dan analisis ahli, artikel tanggal 3 Mei 2020 diakses dari https://tekno.kompas.com/read/2020/05/03/03330087/kebocoran-data-15-juta-pengguna-pengakuan-tokopedia-dan-analisis-ahli?page=all#page4 diakses tanggal 20 Mei 2020

[262] https://www.kominfo.go.id/content/detail/16657/disinformasi-4-juta-data-pengguna-tokopedia-disebut-bocor-dan-dijual/0/laporan_isu_hoaks diakses tanggal

Nuraini mengatakan, password milik pengguna telah terlindungi dan dienkripsi. Selain itu, Tokopedia mengklaim telah menerapkan sistem kode *OTP (one-time password*) yang hanya bisa diakses secara *real time* oleh pemilik akun. Meskipun begitu, Nuraini mengimbau agar pengguna tetap mengganti *password* akun secara berkala agar tetap aman. T mengaku sedang menindak lanjuti masalah ini[263].

Kementerian Komunikasi dan Informatika langsung bertindak cepat untuk mengatasi dugaan kebocoran data di pada *e-commerce T*. Menurut Menteri Komunikasi dan Informatika (periode pemerintahan 2019), Johny G. Plate menyatakan pada 3 Mei 2020 bahwa "Tim teknis Kominfo sudah bersurat dan melakukan koordinasi teknis untuk menindaklanjuti adanya isu pembobolan data pengguna tersebut. Kami juga telah meminta T melakukan tiga hal untuk menjamin keamanan data pengguna," Menurut Menteri Johnny hal pertama yang harus dilakukan T ialah segera melakukan pengamanan sistem. Hal tersebut penting guna mencegah meluasnya kebocoran data. Kedua, T harus memberitahu pemilik akun, baik yang data pribadinya bocor maupun yang tidak. Ketiga, Kementerian Kominfo meminta Tokopedia untuk melakukan investigasi internal untuk memastikan dugaan kebocoran data, serta mencari tahu penyebab kebocoran data tersebut jika memang benar ditemukan[264].

---

20 Mei 2020

[263] Yudha Pratomo, "Kebocoran Data 15juta Pengguna, Pengakuan Tokopedia, dan analisis ahli, artikel tanggal 3 Mei 2020 diakses dari https://tekno.kompas.com/read/2020/05/03/03330087/kebocoran-data-15-juta-pengguna-pengakuan-tokopedia-dan-analisis-ahli?page=all#page4 diakses tanggal 20 Mei 2020

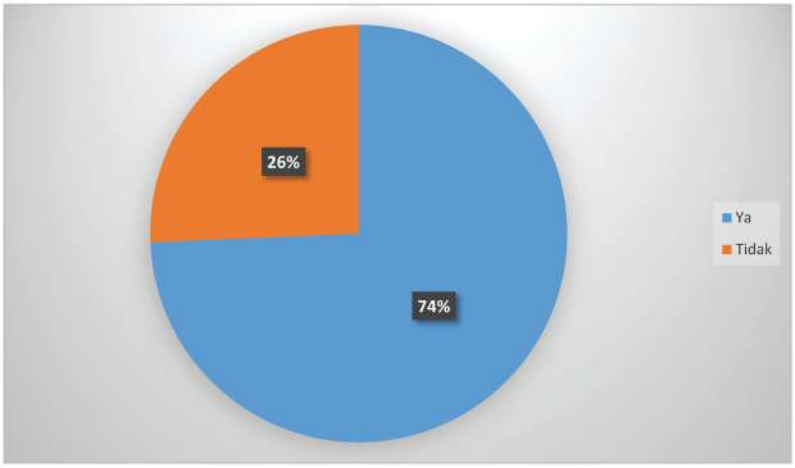
[264] Leski R "Ada Indikasi Kebocoran Data, Kominfo Minta Tokopedia Lakukkan Tiga Hal Ini", artikel tanggal 4 Mei 2020, diakses di https://aptika.kominfo.go.id/2020/05/ada-indikasi-kebocoran-data-kominfo-minta-tokopedia-lakukan-tiga-hal-ini/ diakses tanggal 22 Mei 2020

Selain *e-commerce* T, *e-commerce* BL juga diduga mengalami peretasan sehingga data pengguna bocor. Berdasarkan berita yang dimuat di cnnindonesia.com bahwa Data 13 juta akun BL yang bocor kembali diperjualbelikan di forum *hacker* RaidForums. Data ini dijual oleh dua akun penjual di forum yang sebelumnya menjadi tempat penjualan 91 juta pengguna. Berdasarkan pantauan CNNIndonesia.com, Rabu (6/5), penjual dengan nama akun Asian Boy menyebut data yang ia jual tertanggal tahun 2017. "Saya menjual basis data Bukalapak.com, 12.960.526 pengguna," tulis Asian Boy dalam *thread* di forum itu. Data yang ditampilkan mulai dari email, nama pengguna, *password*, *salt*, *last login*, *email Facebook* dengan *hash*, alamat pengguna, tanggal ulang tahun, hingga nomor telepon. Ia mengeposkan jualan ini sekitar pukul 01.00 WIB. Penjual pertama ini baru bergabung di forum tersebut bulan April 2020 dan baru mengeposkan 3 *thread*. Ketiga *thread* tersebut berupa jualan data dari beberapa situs lain yaitu *Classpass* dan *Reverbnation*. Pengguna ini belum memiliki reputasi. Sementara penjual yang lain dengan nama akun *Tryhard User* juga menawarkan 12 juta data BL. Dalam contoh data yang ia tampilkan, tampak beberapa data pendiri BL seperti Fajrin Rasyid hingga Ahmad Zaky. "Menjual basis data Bukalapak.com," tulisnya[265]. Kementerian Komunikasi dan Informatika langsung bertindak cepat untuk mengatasi dugaan kebocoran data di pada *e-commerce* BL.

Menurut hemat **Penulis,** walaupun sistem penyelenggara dijebol/diretas oleh pihak ketiga yang tidak memiliki hak

[265] CNN Indonesia "13 Juta Data Bocor Bukalapak Dijual di Forum *Hacker*" artikel tanggal 6 Mei 2020, diakses dari https://www.cnnindonesia.com/teknologi/20200506065657-185-500477/13-juta-data-bocor-bukalapak-dijual-di-forum-hacker? Diakes tanggal 22 Mei 2020

hukum, maka tidak serta merta menghilangkan tanggungjawab penyelenggara. Hal ini juga sesuai dengan pendapat mayoritas responden penelitian bahwa 184 atau 82% responden berpendapat bahwa Penyelenggara Sistem Elektronik (penyedia jasa layanan aplikasi *Online*) memiliki kemampuan bertanggung jawab apabila terbukti telah terjadi kebocoran data dalam sistem mereka yang disebabkan oleh pihak ketiga (misalnya peretas/*hacker*) sedangkan 41 responden atau 18% berpendapat bahwa Penyelenggara tidak memiliki kemampuan bertanggungjawab.

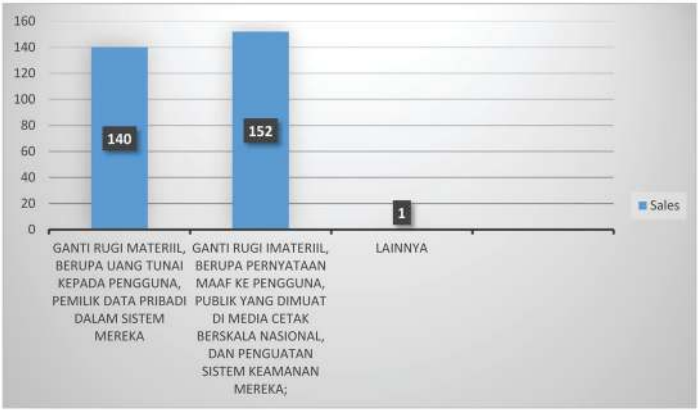


Grafik 27. Pertanyaan tentang Apakah Penyelenggara memiliki kemampuan bertanggungjawab jika diretas oleh pihak ketiga?

Sumber: Dokumen Pribadi.

Adapun bentuk tanggung jawab yang dapat dibebani kepada Penyelenggara Sistem Elektronik (penyedia jasa layanan aplikasi *Online*) yang dapat dibebani ialah pertama, Ganti Rugi Materiil, berupa uang tunai kepada pengguna, pemilik data pribadi dalam sistem mereka dan/atau kedua, Ganti Rugi Imateriil, berupa pernyataan maaf ke pengguna, publik yang

dimuat di media cetak berskala nasional, dan penguatan sistem keamanan mereka. Dan berdasarkan kuisioner yang disebar dan responden dapat memilih salah satu atau kedua opsi tersebut maka didapatkan bahwa 140 responden memiliih opsi pertama, dan 152 responden memilih opsi kedua. Sedangkan yang memilih opsi lainnya berjumlah 1 orang dan berpendapat bahwa korporasi dapat dimintai "Tanggungjawab pidana. Korporasi tersebut harus dipidana karena telah membocorkan data pribadi seseorang. Mungkin saja beberapa orang tidak memerlukan ganti rugi materiil, tapi bukan berarti dengan pernyataan maaf saja cukup atas kejahatan yang telah dilakukan korporasi tersebut. Selain meminta maaf. Tentu memperbaiki sistem pengelolaan nya dan dapat menjelaskan bagaimana hal tersebut bisa terjadi. Dan menjaminkan bahwa pengguna tidak perlu khawatir lagi menggunakan nya, dan menjaminkan bahwa data nya tidak diretas. Supaya tidak terjadi lagi bagi pihak lain."



Grafik 28. Pertanyaan tentang Apakah Jika Saudara menjawab Ya, bentuk tanggung jawab seperti apa yang dapat dibebani kepada Penyelenggara Sistem Elektronik (penyedia jasa layanan aplikasi Online)? (*dapat isi lebih dari 1)

Sumber: Dokumen Pribadi.

II. Modus Pencurian Data Pribadi

Pencurian data pribadi dilakukan dengan pelbagai modus. Pencurian data pribadi merupakan salah satu bentuk tindak pidana siber (*cybercrime)*. *Cybercrime* merupakan salah satu bentuk atau dimensi baru dari kejahatan masa kini yang mendapat perhatian luas dunia internasional[266]. Dalam arti sempit *cybercrime* adalah *computer crime* yang ditujukan terhadap sistem atau jaringan komputer, sedangkan dalam arti luas, cybercrime mencakup seluruh bentuk baru kejahatan yang ditujukan pada komputer, jaringan komputer dan penggunaanya serta bentuk-bentuk kejahatan tradisional yang sekarang dilakukan dengan menggunakan atau dengan bantuan peralatan komputer (*computer related crime*)[267]. Kejahatan dunia maya adalah tindakan perbuatan melawan hukum dan tanpa hak yang dilakukan oleh seseorang ataupun badan hukum dengan memanfaatkan instrument teknologi, komputer, internet untuk menguntungkan diri sendiri baik perbuatan yang dilarang oleh undang-undang ataupun perbuatan yang dianggap tercela di masyarakat[268].

Adapun modus-modus pencurian data pribadi yang berhasil **Penulis** telusuri yakni:

1. Modus dengan *"Social Engineering"*. Definsi *social engineering* ialah Social *engineering refers to all techniques aimed at talking a target into revealing specific information*

[266] Barda Nawawi Arief, Tindak Pidana Mayantara Perkembangan Kajian Cyber Crime di Indonesia, (Jakarta: PT Raja Grafindo Persada, 2007), hal.1

[267] Barda Nawawi Arief, Masalah Penegakan Hukum & Kebijakan Penanggulangan Kejahatan, (Bandung: Citra Aditya Bakti, 2001), hal. 249-250.

[268] Rizky Karo Karo, *Penegakan Hukum Kejahatan Dunia Maya (Cybercrime) Melalui Hukum Pidana,* (Karawaci: Penerbit Fakultas Hukum Universitas Pelita Harapan, 2019), hlm. 46

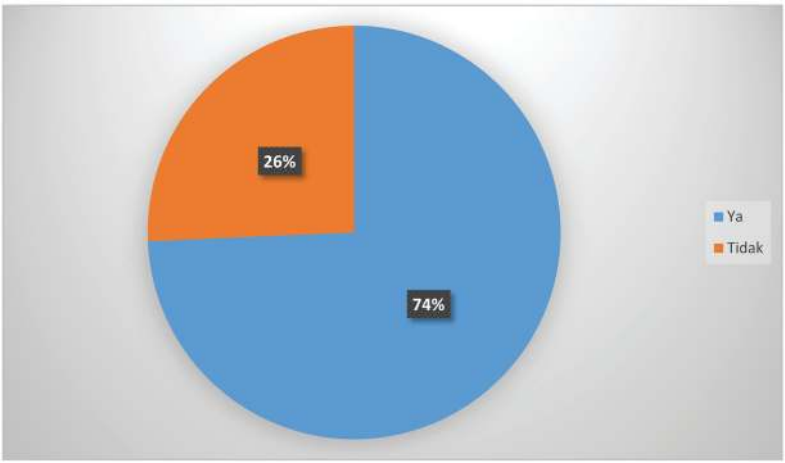
or performing a specific action for illegitimate reasons[269]. Menurut hemat **Penulis,** *social engineering* adalah perbuatan untuk mencari pelbagai informasi pribadi calon korban, berusaha meyakinkannya dengan pelbagai trik dengan tujuan untuk mendapatkan informasi rahasia tersebut. Berdasarkan otoritas keamanan siber Uni Eropa. Teknik *social engineering* ialah: a. *pretexting: this technique the use of a pretext – a false justification for a specific course of action – to gain trust and trick the vaid victim*, misalnya; penyerang mengklaim dirinya berasal dari staff IT dan meminta *password* yang bertujuan untuk perawatan sistem; *b. baiting – baiting involves luring the victim into performing a specific task by providing easy access to something the victim wants.* Misalnya: *a USB flash drive infected with a keylogger and labelled "My private pics" left on the victim's doorstep; c. Quid Pro Quo (*Bahasa Latin) atau *something for something, involves a request for information in exchantge for a compensation, example: the attacker asks the victim's password claiming to be a researcher doing an experiment, in exchange for money; d. Taligating. Taligatinng is the act of following ac authorized person into a restricted area or system. Example: the attacker, dressed as an employee, carries a large box and convinces the victim. Who is an authorized employee entering at the same time*[270].

2. Modus kedua, modus yang menggunakan *email*. **Penulis** mendapatkan bahwa 74% atau 168 responden pernah mendapatkan email dari suatu usaha yang menawarkan,

[269] https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/what-is-social-engineering diakses tanggal 22 Mei 2020

[270] https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/what-is-social-engineering diakses tanggal 22 Mei 2020

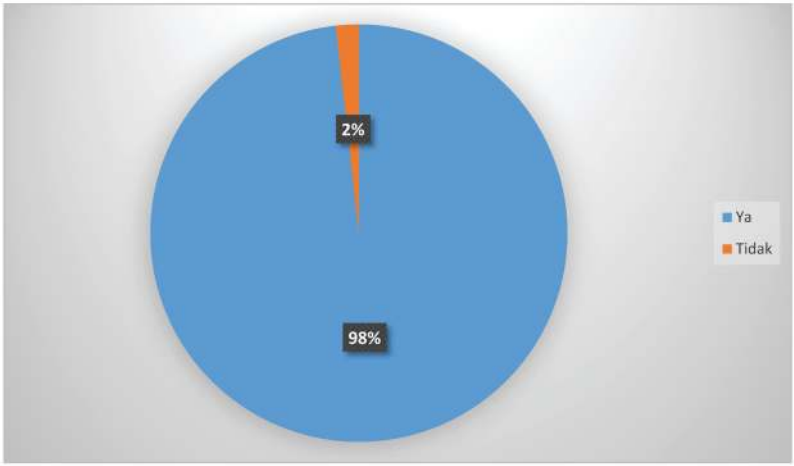
menjual (*marketing*) suatu barang atau layanan kartu kredit namun 26% atau 58 responden tidak pernah mendapatkan email dari suatu usaha yang menawarkan, menjual (marketing) suatu barang atau layanan kartu kredit sebagaimana digambarkan pada grafik ini. Modus seperti ini biasanya dalam *email* yang tidak resmi menawarkan pembukaan kartu kredit yang sangat mudah, limit yang besar dengan cicilan yang sangat ringan.



Grafik 29. Pertanyaan tentang Apakah Saudara/i pernah mendapatkan email dari suatu usaha yang menawarkan, menjual (marketing) suatu barang atau layanan kartu kredit?

Sumber: Dokumen pribadi.

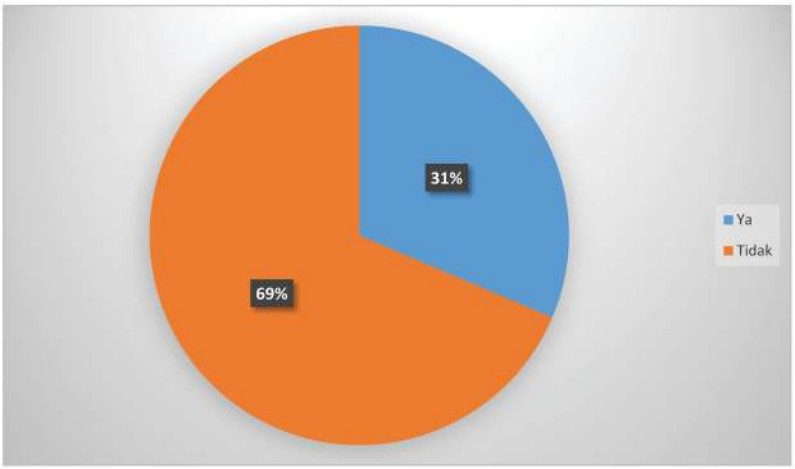
3. **Modus ketiga, modus dengan iming-iming memenangkan hadiah. Penulis** mendapatkan bahwa 98% atau 222 responden pernah mendapatkan email atau SMS (pesan singkat), atau telepon dari bahwa saudara/i memenangkan suatu hadiah dan 2% atau 4 responden tidak pernah mendapatkan email atau SMS (pesan singkat), atau telepon dari bahwa saudara/i memenangkan suatu hadiah.



Grafik 30. Pertanyaan tentang Apakah Saudara/i pernah mendapatkan email atau SMS (pesan singkat), atau telepon dari bahwa saudara/i memenangkan suatu hadiah?

Sumber: Dokumen pribadi.

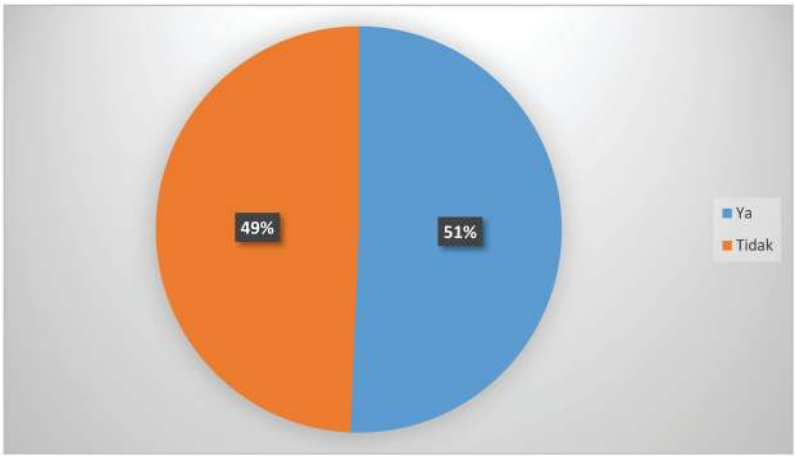
4. **Modus keempat adalah dengan meng-klik/menekan *e-mail* yang tidak resmi.** Bahwa 155 responden atau 69% pernah pernah menekan, meng-klik link/tautan email yang dikirim ke e-mail Saudara/i yang berisikan pemberitahuan untuk mengubah *password* atau berisikan informasi bahwa Saudara/i memenangkan suatu hadiah sedangkan 71 responden atau 31% tidak pernah menekan, meng-klik link/tautan email yang dikirim ke e-mail Saudara/i yang berisikan pemberitahuan untuk mengubah password atau berisikan informasi bahwa Saudara/i memenangkan suatu hadiah. Hal tersebut dapat terlihat pada grafik dibawah ini:



Grafik 31. Pertanyaan tentang Apakah Saudara/i pernah menekan, meng-klik link/tautan email yang dikirim ke e-mail Saudara/i yang berisikan pemberitahuan untuk mengubah password atau berisikan informasi bahwa Saudara/i memenangkan suatu hadiah?

Sumber: Dokumen pribadi.

Dan terkait pemberitahuan *e-mail* tersebut didapatkan bahwa 114 responden atau 51% mengecek kembali alamat email pengirim ke alamat *website* resmi pengirim email terkait pemberitahuan untuk mengubah *password* atau berisikan informasi bahwa Saudara/i memenangkan suatu hadiah sedangkan 48% atau 111 responden tidak mengecek kembali ke website resmi pengirim. Hal tersebut digambarkan pada grafik dibawah ini:



Grafik 32. Pertanyaan tentang Apakah Saudara/i mengecek kembali alamat email pengirim pada pertanyaan no.11 (Apakah Saudara/i pernah menekan, meng-klik link/tautan email yang dikirim ke e-mail Saudara/i yang berisikan pemberitahuan untuk mengubah password atau berisikan informasi bahwa Saudara/i memenangkan suatu hadiah?) ke alamat website resmi pengirim email pada pertanyaan no.11?

Sumber: Dokumen pribadi.

5. **Modus** dengan melakukan serangan *hacker*. Pada prinsipnya, *hacker* memiliki perbedaan dengan *cracker,* perbedaan yang mendasar ialah bahwa *hacker* belum tentu merusak (bisa saja hanya 'mengintip' sistem elektronik) seperti *cracker* melainkan *cracker* sudah pasti merusak – *cracker* memiliki nama lain sebagai *black hat hacker.* Definsi *hacking* yakni *Hacking is the process of attempting to gain or successfully gaining, unauthorized access to computer resources. Computer hacking is the practice of modifying computer hardware and software to accomplish a goal outside of the creator's original purpose*[271].

[271] Sova Pal (Bera) "*Overview of Hacking*" (IOSR Journal of Computer Engineering (IOSR-JCE), Volume 18, Issue 4, Ver. IV (Jul.-Aug. 2016)), hlm. 90. Dapat diakses di http://www.iosrjournals.org/iosr-jce/papers/Vol18-issue4/Version-4/

Hacking terbagi menjadi 2 (dua) yakni: *Physical hacking* dan *logically hacking*. *Physically hacking* adalah melakuan peretasan dengan bantuan alat. Misalnya, memasukan virus ke dalam *Flashdisk* (alat penyimpanan eksternal) atau seorang penyerang masuk ke dalam ruangan server dan memasang alat perusak atau alat penangkap data yang bersifat rahasia[272]. Kedua, *logically hacking,* metode dengan menggunakan alat yang abstrak namun memiliki efek untuk merusak ataupun meretas. Metode *logically hacking* terbagi menjadi 5 yakni: 1. *Reconnaissance (*tahap mengumpulkan data dimana hacker akan mengumpulkan semua data sebanyak– banyaknya mengenai target)*; 2. Scanning (hacker* akan mencari berbagai kemungkinan yang dapat digunakan untuk mengambil alih komputer korban.)*; 3. Gaining access; 4. Maintaning Access* (Para *hacker* biasanya melakukan penanaman berbagai aksesoris tambahan seperti *backdoor, rootkit, Trojan* untuk mempertahankan kekuasaannya terhadap jaringan target)*; 5. Covering Tracks* (Untuk melindungi diri *hacker* dari tuntutan pidana maka *hacker* harus menutupi jejak dalam sebuah penerobosan. Biasanya para *hacker* melakukan penghapusan *log file*)[273].

Selain itu, *hacking* juga memiliki bentuk yakni:

a. Website Hacking – Website hacking means taking control from the website owner to a person who hacks the website.

N1804049092.pdf, diakses tanggal 23 Mei 2020

[272] https://www.resolver.com/resource/physical-and-cybersecurity-defense-how-hybrid-attacks-are-raising-the-stakes/ diakses tanggal 22 Mei 2020

[273] S'to, Certified Ethical Hacker 100% Illegal, (Jakarta: Penerbit Jasakom;.2009). hal 7-8

b. Network Hacking – Network hacking is generally means gathering information about domain by using tools like Telnet, Netstat, etc. over the network.
c. Ethical Hacking – Ethical hacking is where a person hacks to find weakness in a system and then usually patches them.
d. Email Hacking – Email hacking is illicit access to an email account or email correspondence.
e. Password Hacking – Password hacking or password cracking is the process of recovering secret passwords from data that has been stored in or transmitted by a computer system.
f. Online Banking Hacking – Online banking hacking is unauthorized accessing bank accounts without knowing the password or without permission of account holder.
g. Computer Hacking – Computer hacking is when files on your computer are viewed, created, or edited without your authorization[274].

III. Yurisdiksi Sengketa Kejahatan Dunia Maya (Pembocoran Data Pribadi)

UU ITE telah dengan tegas mengatur tentang yurisdiksi jika terjadi dugaan kejahatan dunia maya (*cybercrime)*. Berdasarkan Pasal 2 UU ITE bahwa "Undang-Undang ini berlaku untuk setiap Orang yang melakukan perbuatan hukum sebagaimana diatur dalam Undang-Undang ini, baik yang berada di wilayah hukum Indonesia maupun di luar wilayah hukum Indonesia, yang memiliki akibat hukum di wilayah hukum Indonesia

[274] Sova Pal (Bera). *Loc. Cit.*

dan/atau di luar wilayah hukum Indonesia dan merugikan kepentingan Indonesia"

Berdasarkan Penjelasan Pasal 2 UU ITE bahwa "Undang-Undang ini memiliki jangkauan yurisdiksi tidak semata-mata untuk perbuatan hukum yang berlaku di Indonesia dan/atau dilakukan oleh warga negara Indonesia, tetapi juga berlaku untuk perbuatan hukum yang dilakukan di luar wilayah hukum (yurisdiksi) Indonesia baik oleh warga negara Indonesia maupun warga negara asing atau badan hukum Indonesia maupun badan hukum asing yang memiliki akibat hukum di Indonesia, mengingat pemanfaatan Teknologi Informasi untuk Informasi Elektronik dan Transaksi Elektronik dapat bersifat lintas teritorial atau universal. Yang dimaksud dengan "merugikan kepentingan Indonesia" adalah meliputi tetapi tidak terbatas pada merugikan kepentingan ekonomi nasional, perlindungan data strategis, harkat dan martabat bangsa, pertahanan dan keamanan negara, kedaulatan negara, warga negara, serta badan hukum Indonesia".

PP PMSE juga telah mengatur tentang penyelesaian sengketa dalam perdagangan melalui sistem elektronik dalam Bab XV (Pasal 72 sampai dengan Pasal 75). Salah satu pengaturannya ialah penyelesaian sengketa dengan PMSE internasional.

Para pihak memiliki kewenangan untuk memilih hukum yang berlaku bagi PMSE internasional yang dibuatnya[275]. Dalam hal para pihak tidak melakukan pilihan hukum dalam PMSE internasional, hukum yang berlaku didasarkan pada asas Hukum Perdata Internasional[276]. Para pihak memiliki kewenangan untuk menetapkan forum pengadilan, arbitrase,

[275] Pasal 73 ayat (1) PP PMSE
[276] Pasal 73 ayat (2) PP PMSE

atau lembaga penyelesaian sengketa alternatif lainnya yang berwenang menangani sengketa yang mungkin timbul dari PMSE internasional yang dibuatnya[277]. Dalam hal para pihak tidak melakukan pilihan forum sebagaimana dimaksud pada ayat (1), penetapan kewenangan pengadilan, arbitrase, atau lembaga penyelesaian sengketa alternatif lainnya yang berwenang menangani sengketa yang mungkin timbul dari transaksi tersebut, didasarkan pada asas Hukum Perdata lnternasional[278].

Dalam hal para pihak memilih menyelesaikan sengketa PMSE internasional melalui forum penyelesaian sengketa yang ada di Indonesia, maka lembaga yang berwenang menyelesaikan sengketa tersebut yaitu: a. Pengadilan Negeri Jakarta Pusat; atau b. lembaga arbitrase atau alternatif penyelesaian sengketa lainnya, sesuai dengan ketentuan peraturan perundang-undangan[279].

Pasal 75 PP PMSE mengatur apabila pelaku usaha luar negeri yang melakukan transaksi dengan konsumen Indonesia tidak menentukan pilihan hukum. Dalam hal para pihak merupakan Pelaku Usaha Luar Negeri yang melakukan transaksi dengan Konsumen Indonesia dan tidak melakukan pilihan hukum dan pilihan forum penyelesaian sengketa, maka penyelesaian sengketa dilakukan melalui: a. lembaga yang bertugas menyelesaikan sengketa antara Konsumen dan pelaku usaha; atau b. peradilan yang berada di lingkungan peradilan umum, sesuai dengan ketentuan peraturan perundang-undangan di bidang perlindungan Konsumen.

RUU Perlindungan Data Pribadi juga mengatur tentang yurisdiksi, yakni "Undang-Undang ini berlaku untuk Setiap

[277] Pasal 74 ayat (1) PP PMSE
[278] Pasal 74 ayat (2) PP PMSE
[279] Pasal 74 ayat (3) PP PMSE

Orang, Badan Publik, dan organisasi/institusi yang melakukan perbuatan hukum sebagaimana diatur dalam Undang-Undang ini, baik yang berada di wilayah hukum Negara Kesatuan Republik Indonesia maupun di luar wilayah hukum Negara Kesatuan Republik Indonesia, yang memiliki akibat hukum di wilayah hukum Negara Kesatuan Republik Indonesia dan/atau bagi Pemilik Data Pribadi Warga Negara Indonesia di luar wilayah hukum Negara Kesatuan Republik Indonesia[280]."

IV. Penyelesaian Sengketa Data Pribadi Melalui Alternatif Penyelesaian Sengketa

Upaya penyelesaian sengketa melalui alternatif penyelesaian sengketa (APS) / *Alternative Dispute Resolutin (ADR)*. **Penulis** akan paparkan dasar hukum APS apabila terjadi sengketa terhadap data pribadi atau sengketa dalam aplikasi *online*.

UU ITE	PP PMSE	Permenkominfo PDPSE
Pasal 39 ayat (2) "Selain penyelesaian gugatan perdata sebagaimana dimaksud pada ayat (1), para pihak dapat menyelesaikan sengketa melalui arbitrase, atau lembaga penyelesaian sengketa alternatif lainnya sesuai dengan ketentuan Peraturan Perundang-undangan".	Pasal 72 ayat (1) "Dalam hal terjadi sengketa dalam PMSE, para pihak dapat menyelesaikan sengketa melalui pengadilan atau melalui mekanisme penyelesaian sengketa lainnya."	Pasal 29 ayat (1) "Setiap Pemilik Data Pribadi dan Penyelenggara Sistem Elektronik dapat mengajukan pengaduan kepada Menteri atas kegagalan perlindungan kerahasiaan Data Pribadi."

[280] Pasal 2 RUU PDP

UU ITE	PP PMSE	Permenkominfo PDPSE
		Pasal 29 ayat (2) "Pengaduan sebagaimana dimaksud pada ayat (1) dimaksudkan sebagai upaya penyelesaian sengketa secara musyawarah atau melalui upaya penyelesaian alternatif lainnya."
		Pasal 30 ayat (2) "Direktur Jenderal dapat membentuk panel penyelesaian sengketa Data Pribadi."
Tabel 1. Upaya penyelesaian sengketa melalui alternatif penyelesaian sengketa (APS) Sumber: Dokumen Pribadi		

Tabel 1. Upaya penyelesaian sengketa melalui alternatif penyelesaian sengketa (APS)

Sumber: Dokumen Pribadi

V. Penegakan Hukum Perlindungan Data Pribadi Melalui Sarana Hukum Administrasi Negara

1. Tinjauan Singkat Definisi Hukum Administrasi Negara

Hukum Administrasi Negara mengandung dua aspek yaitu pertama, aturan-aturan hukum yang mengatur dengan cara bagaimana alat-alat perlengkapan Negara

itu melakukan tugasnya, kedua, aturan aturan hukum yang mengatur hubungan antara alat perlengkapan administrasi negara dengan para warga negaranya[281]. Hukum Administrasi Negara adalah hukum yang berkenaan dengan pemerintahan (dalam arti sempit) *Bestuursrecht of administratief Recht omvat regels, die betrekking hebben op de administratie* yaitu hukum yang cakupannya secara garis besar mengatur: 1. Perbuatan Pemerintahan (pusat dan daerah) dalam bidang politik; 2. Kewenangan Pemerintahan (dalam melakukan perbuatan dibidang publik tersebut) di dalamnya diatur mengenai dari mana, dengan cara apa, dan bagaimana Pemerintah menggunakan kewenangannya; pengguna kewenangan ini dituangkan dalam bentuk instrumen hukum, karena itu di atur pula tentang pembuatan dan penggunaan instrument hukum; 3. Akibat-akibat hukum yang lahir dari perbuatan atau penggunaan kewenangan pemerintahan itu; 4. Penegakan hukum dan penerapan sanksi-sanksi dalam bidang pemerintahan[282].

2. Tinjauan Singkat Perizinan

Menurut **W.F. Prins** sebagaimana dikutip oleh **Soehino** memberikan definisi izin yakni: "Pernyataan yang biasanya dikeluarkan sehubungan dengan suatu perbuatan yang pada hakekatnya harus dilarang tetapi hal yang menjadi objek dan perbuatan tersebut menurut sifatnya tidak merugikan dan perbuatan itu dapat dilaksanakan asal saja di bawah pengawasan alat-alat perlengkapan Administrasi Negara[283]". Izin dalam arti luas berarti suatu peristiwa dari

[281] Ridwan HR, *Hukum Administrasi Negara* (Yogyakarta: UII Press, 2003), hlm.26.

[282] *Ibid*, hlm.33

[283] Soehino, *Ilmu Negara,* (Yogyakarta, Liberty, 1984, edisi ketiga), hlm.94.

penguasa berdasarkan Peraturan Perundang-undangan untuk memperbolehkan melakukan tindakan atau perbuatan tertentu yang secara umum dilarang[284].

Menurut hemat **Penulis,** dalam suatu izin yang dikeluarkan oleh Pejabat Publik yang berwenang, izin memiliki substansi untuk mengatur, untuk melengkapi persyaratan yang dibutuhkan untuk melakukan perbuatan hukum, untuk perizinan untuk menyelenggarakan aplikasi *online (platform), e-commerce* dan apabila orang yang telah diberikan izin terbukti melanggar maka wajib siap diberikan sanksi menurut ketentuan hukum administrasi Negara.

Apabila berpedoman pada Undang-undang No. 30 Tahun 2014 tentang Administrasi Pemerintahan (UU Admin Pemerintahan). Definisi izin adalah Keputusan Pejabat Pemerintahan yang berwenang sebagai wujud persetujuan atas permohonan Warga Masyarakat sesuai dengan ketentuan peraturan perundang-undangan. Berdasarkan Pasal 39 ayat (2) UU Admin Pemerintahan bahwa Keputusan Badan dan/atau Pejabat Pemerintahan berbentuk Izin apabila: a. diterbitkan persetujuan sebelum kegiatan dilaksanakan; dan b. kegiatan yang akan dilaksanakan merupakan kegiatan yang memerlukan perhatian khusus dan/atau memenuhi ketentuan peraturan perundang-undangan. Berdasarkan Pasal 39 ayat (6) UU Admin Pemerintahan bahwa izin, dispensasi, atau konsesi tidak boleh menyebabkan kerugian Negara.

Apabila dikaitkan dengan penyelenggara sistem elektronik. Bahwa setiap penyelenggara sistem elektronik

[284] Ridwan HR, *Hukum Administrasi Negara* (Jakarta: Rajagrafindo Persada, 2006), hlm.207.

sebagaimana dimaksud dalam Pasal 2 ayat (2)[285] wajib melakukan pendaftaran[286]. Pendaftaran tersebut diajukan kepada Menteri melalui pelayanan perizinan berusaha terintegrasi secara elektronik sesuai dengan ketentuan peraturan perundang-undangan[287].

Menurut **Sjachrab Basah,** izin memiliki unsur sebagai berikut: 1. Alat kekuasaan (*machsmiddelen);* 2. Bersifat hukum publik (*publiekerchtlijke);* 3. Digunakan oleh penguasa (*overhead);* 4. Sebagai reaksi ketidakpatuhan (*recht eop niet naleving)*[288]. Menurut **Andrian Sutedi,** pada dasarnya izin adalah keputusan pejabat/badan tata usaha Negara yang berwenang, yang memiliki sifat diataranya: a) Izin bersifat bebas, adalah izin sebagai keputusan tata usaha negara yang penerbitannya tidak terikat pada aturan dalam hukum tertulis serta organ yang berwenang dalam izin memiliki kadar kebebasan yang besar dalam memutuskan pemberian izin. b) Izin bersifat berikat, adalah izin sebagai keputusan tata usaha negara yang penerbitannya terikat pada aturan dan hukum tertulis serta organ yang berwenang dalam izin kadar kebebasannya dan wewenangnya tergantung pada kadar sejauhmana peraturan perundang-undangan mengaturnya. c) Izin yang bersifat menguntungkan, adalah izin yang mempunyai sifat menguntungkan pada yang bersangkutan, yang berarti yang bersangkutan diberikan hak-hak atau pemenuhan

[285] Pasal 2 ayat (2) PP PSTE "penyelenggara sistem elektronik sebagaimana dimaksud pada ayat (1) meliputi: a. Penyelenggara Sistem Elektronik Lingkup Publik; dan b. Penyelenggara Sistem Elektronik Lingkup Privat.

[286] Pasal 6 ayat (1) PP PSTE

[287] Pasal 6 ayat (4) PP PSTE

[288] Sjachrab Basah, *Eksistensi dan Tolak Ukur Badan Peradilan Administrasi di Indonesia* (Yogyakarta; Pustaka Pelajar, 1998), hlm.58.

tuntutan yang tidak akan ada tanpa keputusan tersebut. d) Izin yang bersifat memberatkan, adalah izin yang memberikan beban kepada orang lain atau masyarakat di sekitarnya dan mengandung unsur-unsur memberatkan dalam bentuk ketentuan-ketentuan yang berkaitan padanya. e) Izin yang segera berakhir, adalah izin yang menyangkut tindakan-tindakan yang akan segera berakhir atau izin yang masa berlakunya relatif pendek. f) Izin yang berlangsung lama, adalah izin yang menyangkut tindakan-tindakan yang berakhirnya/masa berlakunya relatif lebih lama. g) Izin yang bersifat pribadi adalah, izin yang isinya tergantung pada sifat/kualitas pribadi dan pemohon izin. h) Izin yang bersifat kebendaan, adalah izin yang isinya tergantung pada sifat dan objek izin[289].

Penulis melakukan survei dan dari 226 responden yang terlibat dengan pertanyaan "media hukum administratif berupa pemberian sanksi administratif termasuk namun tidak terbatas pada peringatan lisan, peringatan tertulis, penghentian sementara kegiatan dapat diberikan kepada Penyelenggara Sistem Elektronik (penyedia jasa layanan aplikasi *Online*) yang terbukti tidak dapat melindungi data pribadi dalam sistem sehingga mengakibatkan kebocoran data?" dan didapatkan data bahwa 161 responden atau 73% mengatakan bahwa sanksi administratif dapat diberikan jika penyelenggara tidak dapat melindungi data pribadi, 10 responden atau 4.5% mengatakan tidak dapat sedangkan 23% atau 50 responden menjawab tidak tahu, dan 4 responden tidak memberikan jawaban apapun.

[289] Andrian Sutedi, *Hukum Perizinan dalam Sektor Pelyanan Publik* (Jakarta; Sinargrafika, 2010) hlm.173-175

Grafik 33. Sanksi Administratif
Sumber: Dokumen Pribadi

3. Bentuk Sanksi Administratif dalam Hukum Administrasi Negara

Sanksi dalam Hukum Administrasi yaitu "alat kekekuasaan yang bersifat hukum publik yang dapat digunakan oleh pemerintah sebagai reaksi atas ketidakpatuhan terhadap kewajiban yang terdapat dalam norma Hukum Administrasi Negara." Berdasarkan definisi ini tampak ada empat unsur sanksi dalam hukum administrasi Negara, yaitu alat kekuasaan (*machtmiddelen*), bersifat hukum publik (*publiekrechtlijke*), digunakan oleh pemerintah (*overheid*), sebagai reaksi atas ketidakpatuhan (*reactive op niet-naleving*)[290].

Jenis Sanksi Administrasi dapat dilihat dari segi sasarannya yaitu: a. Sanksi reparatoir, artinya sanksi yang diterapkan sebagai reaksi atas pelanggaran norma, yang ditujukan untuk mengembalikan pada kondisi semula

[290] Ridwan H.R., *Op.cit.* hlm. 315.

sebelum terjadinya pelanggaran, misalnya *bestuursdwang*, *dwangsom*; b. Sanksi punitif, artinya sanksi yang ditujukan untuk memberikan hukuman pada seseorang, misalnya adalah berupa denda administratif; c. Sanksi regresif, adalah sanksi yang diterapkan sebagai reaksi atas ketidakpatuhan terhadap ketentuan yang terdapat pada ketetapan yang diterbitkan[291].

4. Bentuk Sanksi Administratif dalam PP PSTE, PP PMSE, Permenkominfo PDPSE

Penulis akan paparkan bentuk sanksi adminstratif bagi penyelenggara yang termasuk namun tidak terbatas pada tidak dapat menjaga kerahasiaan data pribadi yang diatur dalam PP PSTE, dan PP PMSE serta yang akan diatur dalam RUU PDP.

PP PSTE	PP PMSE	Permenkominfo PDPSE	RUU PDP
Dasar Hukum: Pasal 100. Terdiri dari 5 sanksi.	**Dasar Hukum: Pasal 80 PPMSE. Terdiri dari 5 Sanksi**	**Dasar Hukum: Pasal 36. Terdiri dari 4 sanksi.**	**Sejauh ini diatur dalam Pasal 50. Terdiri dari 5 sanksi**
Teguran Tertulis	Peringatan Tertulis	Peringatan Lisan	Peringatan Tertulis
Denda Administratif	Dimaksukkan ke dalam daftar prioritas pengawasan	Peringatan Tertulis	Penghentian Sementara kegiatan Pemroses Data Pribadi
Penghentian Sementara	Dimasukkan dalam daftar hitam	Penghentian Sementara kegiatan; dan/ atau	Penghapusan atau Pemusnahan Data Pribadi

[291] *Ibid.* hlm.319.

PP PSTE	PP PMSE	Permenkominfo PDPSE	RUU PDP
Pemutusan Akses	Pemblokiran sementara layanan PPMSE dalam negeri dan/atau PPMSE luar negeri oleh instansi terkait yang berwenang; dan/atau	Pengumuman di situs dalam jaringan *(website online)*	Ganti Kerugian
Dikeluarkan dari Daftar	Pencabutan Izin Usaha	-	Denda Administratif
Pengenaan sanksi administratif diberikan oleh Menteri (yang menyelenggarkan urusan pemerintahan di bidang komunikasi dan informatika)	Pengenanaan sanksi diberikan oleh Menteri (yang menyelenggarakan urusan pemerintahan di bidang Perdagangan	Sanksi administratif diberikan oleh menteri atau pimpinan instansi pengawas dan pengatur sektor terkait sesuai dengan ketentuan peraturan perundang-undangan.	Sanksi administratif diberikan oleh Menteri (yang menyelenggarkan urusan pemerintahan di bidang komunikasi dan informatika)

Tabel 2. Bentuk Sanksi Adminstratif.

Sumber: Dokumen Pribadi

VI. Penegakan Hukum Perlindungan Data Pribadi Melalui Sarana Hukum Perdata

1. Tinjauan Umum Hukum Perdata

Menurut **Subekti**, Hukum Perdata dalam arti luas meliputi semua hukum privat materiil, yaitu segala hukum pokok yang mengatur kepentingan-kepentingan perseorangan[292]. Hukum perdata di Indonesia telah berhasil di-kodifikasikan (disusun menjadi satu bagian dari aturan-

[292] Subekti, *Pokok-pokok Hukum Perdata* (Jakarta: PT Intermasa, 1980(, hlm. 9.

aturan yang tersebar dan merupakan satu buku) ke dalam Kitab Undang-Undang Hukum Perdata (Kuh.Perdata). Kodifikasi hukum bertujuan untuk lebih menjamin kepastian hukum, memudahkan masyarakat dalam memperoleh, memiliki dan mempelajari hukum perdata karena lebih sistematis. **Penulis** tidak akan memaparkan sejarah hukum perdata di Indonesia. Kodifikasi hukum perdata di Indonesia diumumumkan dengan maklumat tanggal 30 April 1847 *Staatsblad* Tahun 1847 No.23 dan berdasarkan Pasal II Aturan Peralihan Undang-undang Dasar 1945 yang menyatakan bahwa "segala badan Negara dan peraturan yang ada masih langsung berlaku, selama belum diadakan yang baru menurut Undang-undang Dasar ini".

Isi Kuh.Perdata terbagi menjadi 4 (empat) bagian: 1. Buku I tentang orang (*van personnenrecht)*; 2. Buku II tentang Benda (*van zaken);* 3. Buku III tentang Perikatan (*Van Verbitenessenrech)*; 4. Buku IV tentang Pembuktian dan Daluwarsa (*Van Bewijs en Vejaring)*. Sebagaimana kita tahu bahwa beberpa ketentuan di Kuh.Perdata di Indonesia sudah diatur dalam *lex specialis,* salah satunya Undang-undang No. 5 Tahun 1960 tentang Peraturan Dasar Pokok-Pokok Agraria (UUPA) mencabut semua ketentuan-ketentuan mengenai hak-hak kebendaan yang bertalian dengan tanah dari buku II Kuh.Perdata.

2. Tinjauan Umum Perbuatan Melawan Hukum dan Wanprestasi serta Gugatan

Wanprestasi atau dalam bahasa Belanda *'wanprestastie'*. Menurut hemat **Penulis,** wanprestasi (ingkar janji) sangat berkaitan dengan perikatan yang memiliki tujuan yang diatur dalam perikatan tersebut sebagaimana yang diatur

dalam Pasal 1233 bahwa "perikatan lahir karena suatu persetujuan atau karena undang-undang" *juncto*. Pasal 1234 Kuh.Perdata "Perikatan ditujukan untuk memberikan sesuatu, untuk berbuat sesuatu, atau untuk tidak berbuat sesuatu" namun salah satu pihak tidak mampu untuk melakukan ketentuan Pasal 1234 Kuh.Perdata. Menurut **Wirjono Prodjodikoro "**wanprestasi adalah ketiadaan suatu prestasi di dalam hukum perjanjian, berarti suatu hal yang harus dilaksanakan sebagai isi dari suatu perjanjian. Barangkali dalam bahasa Indonesia dapat dipakai istilah "pelaksanaan janji untuk prestasi dan ketiadaan pelaksanaannya janji untuk wanprestasi[293]".

Wanprestasi harus diawali terlebih dahulu dengan somasi oleh satu pihak yang dianggap lalai. Somasi (surat teguran) diatur dalam Pasal 1238 Kuh.Perdata "Debitur dinyatakan Ialai dengan surat perintah, atau dengan akta sejenis itu, atau berdasarkan kekuatan dari perikatan sendiri, yaitu bila perikatan ini mengakibatkan debitur harus dianggap Ialai dengan lewatnya waktu yang ditentukan." Pada umumnya somasi diberikan sebanyak 3 (tiga) kali.

Apabila seseorang terbukti melakukan maka berdasarkan Pasal 1243 Kuh. Perdata "Penggantian biaya (*kosten)*, kerugian (*schaden)* dan bunga (*interesten)* karena tak dipenuhinya suatu perikatan mulai diwajibkan, bila debitur, walaupun telah dinyatakan Ialai, tetap Ialai untuk memenuhi perikatan itu, atau jika sesuatu yang harus diberikan atau dilakukannya hanya dapat diberikan atau

[293] Wirjono Prodjodikoro, *Asas-asas Hukum Perjanjian* (Bandung: Sumut Pustaka, 2012), hlm.17.

dilakukannya dalam waktu yang melampaui waktu yang telah ditentukan."

Menurut **Yahya Harahap,** Hukuman atau akibat-akibat yang diterima oleh debitur yang lalai ada empat macam, yaitu: a. Membayar kerugian yang diderita oleh kreditur atau dengan singkat dinamakan ganti-rugi. b. Pembatalan perjanjian atau juga dinamakan pemecahan perjanjian. c. Peralihan risiko. d. Membayar biaya perkara, kalau sampai diperkarakan didepan hakim[294].

Perbuatan Melawan Hukum (PMH) atau dalam bahasa Belanda "*Onrechmatige daad*". Dasar Hukum PMH diatur dalam Pasal 1365 Kuh.Perdata "Tiap perbuatan yang melanggar hukum dan membawa kerugian kepada orang lain, mewajibkan orang yang menimbulkan kerugian itu karena kesalahannya untuk menggantikan kerugian tersebut."

Menurut **Subekti,** Pasal 1365 Kuh.Perdata tidak membedakan kesalahan dalam bentuk kesengajaan (*opzet-dolus*) dan kesalahan dalam bentuk kurang hati-hati (*culpa*), dengan demikian hakim harus dapat menilai dan mempertimbangkan berat ringannya kesalahan yang dilakukan sesorang dalam hubungannnya dengan perbuatan melawan hukum ini, sehingga dapat ditentukan ganti kerugian yang seadil-adilnya[295].

Gugatan adalah hak hukum yang dimiliki oleh warga Negara apabila kepentingannya 'diganggu' atau dirugikan – untuk menuntut haknya kembali seperti semula. Seseorang mengajukan gugatan sesuai dengan hukum acara perdata

[294] Yahya Harahap, *Segi-segi Hukum Perjanjian* (Bandung: Alumni, Cetakan Kedua, 1986), hlm. 56.

[295] Subekti, *Pokok-pokok Hukum Perdata,* (Jakarta: Intermasa, 1979), hlm.56.

(hukum perdata formil). Hukum acara perdata yang berlaku di Indonesia yakni: a. Undang-undang No. 48 Tahun 2009 tentang Kekuasan Kehakiman: b. Kitab Undang-undang Hukum Perdata (khususnya Bab IV); c. *Het Herziene Indonesisch Reglement (HIR* atau Reglement Indonesia yang diperbaharui: S. 1848 No. 16, S. 1941 No. 44) untuk daerah Jawa dan Madura, dan d. *Rechtsglement Buitengewesten (Rbg. atau Reglement* daerah seberang: S. 1927 No. 227) untuk luar Jawa dan Madura. Dan berdasarkan Surat Edaran Mahkamah Agung No. 19 Tahun 1964 perihal Pemeriksaan dan memutus perkara Negeri. "Menurut kenyataan berhubung dengan keadaan di beberapa Pengadilan Negeri belum dapat ditempatkan 3 (tiga) orang hakim, maka di Pengadilan Negeri – dimana hanya ada seorang atau dua orang hakim – Mahkamah Agung mengizinkan melakukan pemeriksaan dan memutus perkara oleh hanya seorang Hakim saja, oleh karena resminya Reglemen Indonesia yang diperbaharui (*Herziene Indonesisch Reglement)* dan Reglemen Indonesia yang berlaku untuk daerah seberang (*Recht-sreglement Buitengewsten)* masih berlaku".

Dasar suatu gugatan adalah gugatan atas dasar wanprestasi atau gugatan atas dasar perbuatan melawan hukum. Berdasarkan yurisprudensi Mahkamah Agung Nomor 1875 K/Pdt/1984 tanggal 24 April 1986 yang menyebutkan bahwa Kumulasi/penggabungan gugatan perbuatan melawan hukum dengan perbuatan ingkar janji/wanprestasi tidak dapat dibenarkan dalam tertib beracara dan harus diselesaikan masing-masing. Gugatan harus disampaikan lengkap secara tertulis, kronologis/dasar gugatan yang jelas – dan permohonan/tuntutan (*petitum)*

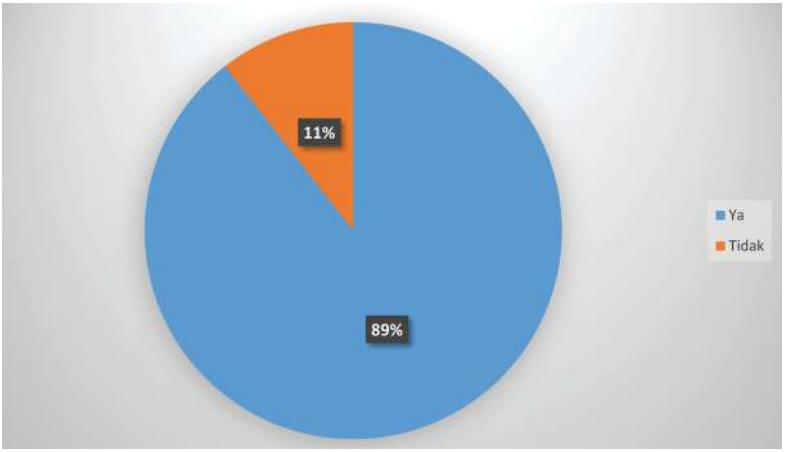
harus sesuai dengan dasar gugatan (*fundamentum petendi)*, agar tidak kabur (*obscuur libel)*.

Beberapa prinsip pokok dalam mengajukan gugatan yakni:

1. Asas *Actor Sequitor Forum Rei*. Gugatan dimasukkan di Pengadilan Negeri tempat diam si tergugat; (Pasal 118 ayat (1) *HIR)*;
2. Asas *audi et altera partem* bahwa hakim mendengar pernyataan/kepentingan Pengguggat/Tergugat;
3. Asas *affirmandi incumbit probatio*. Hal ini sebagaimana diatur dalam Pasal 164 *HIR jo*. Pasal 284 *RBg jo*. Pasal 1865 Kuh.Perdata "Setiap orang yang mengaku mempunyai suatu hak, atau menunjuk suatu peristiwa untuk meneguhkan haknya itu atau untuk membantah suatu hak orang lain, wajib membuktikan adanya hak itu atau kejadian yang dikemukakan itu."

Manusia memiliki hak dan kedudukan yang sama di depan hukum (*equality before the law)*. Hak hukum ini diamanatkan dan dilindungi oleh konstitusi. Konsumen, pengguna aplikasi *online* memiliki hak hukum agar data pribadinya dilindungi oleh penyelenggara dan memiliki hak hukum untuk mengajukan gugatan sebagaimana diatur dalam UU ITE untuk mengajukan gugatan ganti rugi terhadap 'kebocoran data' namun berdasarkan kuisioner penelitian yang **Penulis** dapatkan, bahwa 89% (delapan puluh sembilan per seratus) yang mengetahui bahwa konsumen memiliki hak hukum untuk mengajukan gugatan kepada Penyelenggara Sistem Elektronik (penyedia jasa layanan aplikasi Online) yang lalai dalam melindungi

data pribadi dalam sistem mereka sedangkan 11% (sebelas per seratus) tidak mengetahui.



Grafik 34. Pertanyaan Apakah Saudara mengetahui bahwa pengguna/pemilik data pribadi/konsumen memiliki hak hukum untuk mengajukan gugatan kepada Penyelenggara Sistem Elektronik (penyedia jasa layanan aplikasi Online) yang lalai dalam melindungi data pribadi dalam sistem mereka?

Sumber: Dokumen Pribadi.

Apabila merujuk pada UU Perlinkos memang mengakomodir tentang penyelesaian sengketa baik didalam pengadilan maupun luar pengadilan[296]. Namun,

[296] Berdasarkan Pasal 45 sampai dengan Pasal 48 UU Perlinkos diatur tentang penyelesaian sengketa. Berdasarkan Pasal 45 ayat (1) sampai dengan ayat (4) bahwa: (1) Setiap konsumen yang dirugikan dapat menggugat pelaku usaha melalui lembaga yang bertugas menyelesaikan sengketa antara konsumen dan pelaku usaha atau melalui peradilan yang berada di lingkungan peradilan umum. (2) Penyelesaian sengketa konsumen dapat ditempuh melalui pengadilan atau di luar pengadilan berdasarkan pilihan sukarela para pihak yang bersengketa. (3) Penyelesaian sengketa di luar pengadilan sebagaimana dimaksud pada ayat (2) tidak menghilangkan tanggung jawab pidana sebagaimana diatur dalam Undang-undang. (4) Apabila telah dipilih upaya penyelesaian sengketa konsumen di luar pengadilan, gugatan melalui pengadilan hanya dapat ditempuh apabila upaya tersebut dinyatakan tidak berhasil oleh salah satu pihak atau oleh para pihak yang bersengketa.

Sedangkan apabila para pihak menempuh jalur di luar pengadilan, maka berdasarkan Pasal 47 UU Perlinkos bahwa "Penyelesaian sengketa konsumen di luar pengadilan diselenggarakan untuk mencapai kesepakatan mengenai bentuk

UU Perlinkos kita saat ini tidak mendukung tentang perlindungan data pribadi dalam sistem elektronik oleh karena itu penegakan hukum perlindungan data pribadi melalui hukum perdata beralaskan peraturan sektoral namun menurut hemat **Penulis,** dasar hukumnya tetap berpegang teguh pada UU ITE, PP PSTE, PP PMSE, dan Permenkominfo PDPSE.

Penulis akan uraikan dalam bentuk tabel dasar hukum gugatan apabila terjadi dugaan perbuatan melawan hukum berupa kebocoran data pribadi.

UU ITE	PP PMSE	PERMENKOMINFO PDPSE
Pasal 26 ayat (2): Setiap Orang yang dilanggar haknya sebagaimana dimaksud pada ayat (1)[297] dapat mengajukan gugatan atas kerugian yang ditimbulkan berdasarkan Undang-Undang ini.	Pasal 72 ayat (3): "Dalam hal terjadi sengketa antara Pelaku Usaha Dalam Negeri dan Konsumen, Konsumen dapat menggugat Pelaku Usaha melalui badan penyelesaian sengketa Konsumen atau mengajukan ke lembaga peradilan di tempat kedudukan Konsumen."	Pasal 32 ayat (1) "Dalam upaya penyelesaian sengketa secara musyawarah atau melalui upaya penyelesaian alternatif lainnya belum mampu menyelesaikan sengketa atas kegagalan perlindungan kerahasiaan Data Pribadi, setiap Pemilik Data Pribadi dan Penyelenggara Sistem Elektronik dapat mengajukan gugatan atas terjadinya kegagalan perlindungan rahasia Data Pribadi."

dan besamya ganti rugi dan/atau mengenai tindakan tertentu untuk menjamin tidak akan terjadi kembali atau tidak akan terulang kembali kerugian yang diderita oleh konsumen."

[297] Pasal 26 ayat (1) UU ITE "Kecuali ditentukan lain oleh peraturan perundangundangan, penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan Orang yang bersangkutan."

UU ITE	PP PMSE	PERMENKOMINFO PDPSE
		Pasal 32 ayat (2) "Gugatan sebagaimana dimaksud pada ayat (1) hanya berupa gugatan perdata dan diajukan sesuai dengan ketentuan peraturan perundang-undangan."

Tabel 3. Dasar hukum gugatan apabila terjadi dugaan perbuatan melawan hukum berupa kebocoran data pribadi.

Sumber: Dokumen Pribadi.

3. Contoh Gugatan Perbuatan Melawan Hukum Dalam Penegakan Perlindungan Data Pribadi

Penulis akan paparkan contoh gugatan dengan membuat kasus posisi fiktif, apabila terdapat kesamaan termasuk namun tidak terbatas pada nama, alamat, e-mail dan sebagainya adalah 'kebetulan' belaka.

1.1.1. Kasus Posisi

Pada tanggal 3 bulan Agustus tahun 2020, PT 'Belanja Hingga Habis' (selanjutnya disebut BHB) yang berkedudukan hukum di Jakarta Selatan memiliki *platform e-commerce* bernama 'tukumeneh' mengalami kebocoran data pelanggan, *user* dalam sistem mereka. BHB memiliki izin usaha dari Kementerian Perdagangan dan masih berlaku dan memiliki izin dari Bank Indonesia terkait 'uang elektronik'. *E-commerce* 'tukumeneh' sudah bediri di Indonesia sejak bulan Januari tahun 2018 namun telah memiliki *user* yang sangat banyak hingga tahun 2020 yakni sebanyak 3.000.000 (tiga juta) pelanggan/*user*.

Kebocoran data diketahui dilakukan oleh 3 karyawan I.T. BHB (Aque, Cury, Datamu). Aque, Cury, Datamu

membocorkan data *user* 'tukumeneh' dan menjual data pelanggan dengan harga berebeda. Data *user* yang berisikan nama, nomor hp, alamat *email* dijual seharga Rp.10.000 (sepuluh rupiah) per data, dan data berisikan *profil* lengkap hingga data transaksi keuangan dijual seharga Rp.50.000 (lima puluh ribu rupiah). Aque, Cury, Datamu menjual data-data ini ke satu Perusahaan *marketing* bernama PT 'DatamuDataku' yang biasanya menawarkan promo, kartu kredit, dan lainnnya dengan cara menelpon si pengguna nomor *handphone* tersebut. Berdasarkan investigasi BHB, data yang bocor tersebut berjumlah 2.000.000 (duta juta) pengguna. BHB tidak dapat menyelematkan data yang telah dijual tersebut dan hanya bisa mengadukan Aque, Cury, Datamu kepada Penyidik.

Setelah penjualan data tersebut, 1 (satu) *user* 'tukumeneh' yang berperan sebagai pembeli dan penjual barang kebutuhan pokok dan kebutuhan listrik merasa mengalami kerugian dan selalu diganggu oleh *marketer* yang menawarkan produk rumah, kartu kredit, dan produk lainnya setiap hari hingga pernah ditelepon di malam hari. Salah 1 (satu) *user* tersebut menempuh langkah hukum karena merasa datanya diperjualbelikan dan tidak dijaga.

1.1.2. Gugatan Perbuatan Melawan Hukum

*Contoh Jakarta, 18 Agustus 2020

GUGATAN PERBUATAN MELAWAN HUKUM TERHADAP PEMBOCORAN DATA PRIBADI

Kepada Yth.
Ketua Pengadilan Negeri Jakarta Pusat,
Di Pengadilan Negeri Jakarta Pusat

Dengan hormat,

Yang bertanda tangan dibawah ini Dr. Putra, S.H., M.H. pekerjaan Advokat di Putra&Associates berkedudukan hukum di Jalan ABC No.11, Jakarta Pusat, bertindak untuk dan atas nama klien-klien kami (**Surat Kuasa Khusus Terlampir):**

Nama	: Balikandata
Tempat/Tanggal Lahir	: Jakarta, 20 Juni 1988
Agama	: Kristen Protestan
Domisili	: Jl. R, Jakarta Pusat, DKI Jakarta
Pekerjaan	: Wiraswasta **(selanjutnya disebut Penggugat)**

Dalam hal ini telah memilih domisili hukum di kantor Kuasa Hukum diatas.

Dengan ini Penggugat mengajukan gugatan "Perbuatan Melawan Hukum" (PMH) terhadap:

I. Nama : PT 'Belanja Hingga Habis' (BHB)
Alamat : Jalan Belanja No.12, Jakarta Selatan
(**selanjutnya disebut Tergugat I)**

II. Nama : Pemerintah Republik Indonesia *c.q*. Kementerian Komunikasi dan Informatika Republik Indonesia
Alamat : Jl. Medan Merdeka Barat No. 9, Kec. Gambir, Jakarta Pusat, DKI Jakarta
(**selanjutnya disebut Tergugat II)**

III. Nama : Pemerintah Republik Indonesia *c.q*. Kementerian Perdagangan Republik Indonesia
Alamat : Jl. M. Ridwan Rais No.5, Kec. Gambir, Jakarta Pusat, DKI Jakarta
(**selanjutnya disebut Tergugat III)**

Adapun pokok-pokok perkara yang menjadi dasar Gugatan PMH ini ialah sebagai berikut:

4. Bahwa Penggugat adalah salah 1 (satu) *user*/pengguna aplikasi *online* (*platform) e-commerce* (layanan toko *online)* milik PT BHB (**selanjutnya disebut BHB)** atau Tergugat I sejak tanggal 1 Februari tahun 2019. *Platform* tersebut bernama 'tukumeneh'. Adapun nama Penggugat sebagai identitas pengguna *online* dalam sistem tersebut

ialah balikandata_2019 dan menggunakan layanan *e-mail* (surat elektronik) bernama balikandata@gmail.com, serta nomor ponsel milik Penguggat di nomor 0852xxxxxxxxxx2 (**Bukti P1: *Screenshot/* hasil cetak Profil Penggugat sebagai Pengguna dalam layanan 'tukumeneh')**

5. Bahwa Penggugat sangat yakin akan kredibilitas 'tukumeneh' sehingga Penguggat meningkatkan performa penggunaan dalam aplikasi *online* tersebut dengan menggunggah (*upload)* Kartu Tanda Penduduk (KTP) milik Penggugat untuk dapat digunakan sebagai penjual dan Penggugat tidak memiliki akun di *platform e-commerce* lainnya. Pengugat menjual barang-barang berupa kebutuhan pokok, kebutuhan listrik di akun toko *online* Tergugat I (**Bukti P2: *Screenshot/* hasil cetak layar KTP di sistem 'tukumeneh'**)
6. Bahwa Penggugat sangat menikmati berbelanja di 'tukumeneh' karena mudah dan banyak memberikan promo potongan harga berbelanja;
7. Bahwa Penggugat mengetahui dari berita *online (***Bukti P3: *Screenshot* 3 Berita *Online* – Terlampir)** bahwa pada 3 Agustus tahun 2020 'tukumeneh' mengalami kebocoran data pelanggan dalam sistem mereka. Berdasarkan berita tersebut "Kebocoran data diketahui dilakukan oleh 3 karyawan I.T. Tergugat I (Aque, Cury, Datamu). Aque, Cury, Datamu membocorkan data *user* 'tukumeneh' dan menjual data pelanggan dengan harga berbeda. Data *user* yang berisikan nama, nomor hp, alamat *email* dijual seharga Rp.10.000 (sepuluh ribu rupiah) per data,

dan data berisikan *profil* lengkap hingga data transaksi keuangan dijual seharga Rp.50.000 (lima puluh ribu rupiah). Tiga Mantan Karyawan Tergugat I bernama Aque, Cury, Datamu menjual data-data ini ke satu Perusahaan *marketing* bernama PT 'Datamu Dataku' yang biasanya menawarkan promo, kartu kredit, dan lainnnya dengan cara menelpon si pengguna nomor *handphone* tersebut. Berdasarkan investigasi Tergugat I, data yang bocor tersebut berjumlah 2.000.000 (dua juta) pengguna. Tergugat I tidak dapat menyelamatkan data yang telah dijual tersebut dan hanya bisa mengadukan Aque, Cury, Datamu kepada Penyidik.";

8. Bahwa 30 (tiga puluh) menit setelah berita kebocoran data tersebut, Penggugat menjadi panik dan segera mengganti *password* (kata sandi) akun layanan milik Penggugat di sistem 'tukumeneh' dan Penggugat mengirim keluhan ke *email* (surat elektronik) *customer service* menanyakan apakah data Penggugat juga menjadi salah satu data yang dibocorkan namun saat itu, *customer service* tersebut mengatakan bahwa pihak 'tukumeneh' sedang melakukan investigasi dan memastikan data&*password* seluruh akun pengguna dalam sistem dalam keadaan aman (**Bukti P4: *Bukti screenshot*/hasil cetak layar riwayat telepon Penggugat yang menelpon *customer service* 'tukumeneh');**
9. Bahwa pada Rabu, 5 Agustus 2020 jam 15.00 WIB, jam 18.00 WIB Penguggat mendapat telepon dari seseorang tidak dikenal yang menawari kartu kredit dari Bank 'bingbung' padahal Penggugat bukan salah satu nasabah

dari Bank 'bingbung' dan Penggugat menolak dan langsung mematikan nomor *handphone* (**Bukti P5: *Bukti screenshot*/hasil cetak layar riwayat telepon Penggugat yang ditelpon seseorang yang menawarkan kartu kredit dari Bank 'bingbung' pada tanggal 5 Agustus 2020)**

10. Bahwa pada Jumat, 7 Agustus 2020 jam 13.00 WIB dan jam 16.32 WIB Penguggat mendapat telepon dari seseorang tidak dikenal yang menawari kartu kredit dari Bank 'bingbung' padahal Penggugat bukan salah satu nasabah dari Bank 'bingbung' namun dengan nomor ponsel yang berbeda dan Penggugat menolak dan langsung mematikan nomor *handphone* (**Bukti P6: *Bukti screenshot*/hasil cetak layar riwayat telepon Penggugat yang ditelpon seseorang yang menawarkan kartu kredit dari Bank 'bingbung' namun dengan nomor ponsel berbeda pada tanggal 7 Agustus 2020);**
11. Bahwa pada tanggal 8 Agustus 2020, di jam 07.35WIB, 12.35WIB; 15.21WIB, Penguggat mendapat telepon dari orang yang tidak dikenal yang menawari pinjaman tunai secara *online* dan Penggugat menolak dan langsung mematikan nomor *handphone* (**Bukti P6: *Bukti screenshot*/hasil cetak layar riwayat telepon Penggugat yang ditelpon seseorang yang menawarkan kartu kredit dari Bank 'bingbung' namun dengan nomor ponsel berbeda pada tanggal 5 Agustus 2020);**
12. Bahwa pada tanggal 8 Agustus 2020 di jam 16.32 WIB, Penggugat mendapatkan *e-mail* dari suatu perusahaan toko *online* yang menginformasikan katalog berisikan barang-barang yang pernah Penggugat beli

di *e-commerce* 'tukumeneh' padahal Penggugat tidak pernah berbelanjan di *online shop* tersebut (**Bukti P6: *Bukti screenshot*/hasil cetak layar *e-mail* pada tanggal 8 Agustus 2020)**

13. Bahwa pada tanggal 9 Agustus 2020, Penggugat lagi-lagi mendapatkan tawaran produk dari seseorang yang mana Penggugat tidak membutuhkan produk tersebut dan saat Penggugat bertanya darimana si penelepon mendapatkan nomor ponsel Penggugat, si penelpon menjawab dari suatu *online shop* ((**Bukti P7: *Bukti screenshot*/hasil cetak riwayat telepon Penggugat pada tanggal 9 Agustus 2020);**
14. Bahwa pada tanggal 11 Agustus 2020, Penggugat ditelpon oleh orang yang mengaku sebagai petugas dari layananan pinjaman *online* dan mengatakan bahwa Penggugat telah meminjam uang dengan utang pokok sebesar Rp5.000.000,00 (lima juta rupiah) dan telah jatuh tempo pada tanggal 10 Agustus 2020 sehingga Penggugat diharuskan membayar denda Rp250.000,00 (dua ratus lima puluh ribu rupiah) per hari. Bahwa karena Penggugat tidak mau repot maka Penggugat mentransfer Rp5.250.000,00 (lima juta dua ratus lima puluh ribu rupiah) dan setelah Penggugat mengecek di situs resmi Otoritas Jasa Keuangan dan menemukan bahwa Pinjaman *Online* tersebut tidak terdaftar di OJK;
15. Bahwa Penggugat merasa terganggu, tidak nyaman ditelepon oleh pihak yang menawarkan produk-produk tersebut dan hal tersebut telah terjadi setelah berita kebocoran data dari 'tukumeneh';

16. Bahwa *e-commerce* 'tukumeneh' yang dijalankan oleh Tergugat I memiliki kewajiban hukum untuk menjaga dan melindungi data pribadi pengguna sebagaimana diatur dalam Pasal 31 Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik **(selanjutnya disebut PP PSTE)** bahwa Penyelenggara Sistem Elektronik wajib melindungi penggunanya dan masyarakat luas dari kerugian yang ditimbulkan oleh sistem elektronik yang diselenggarakanya *juncto* Pasal 27 Peraturan Menteri Komunikasi dan Informatika No. 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik (selanjutnya disebut Permenkominfo PDPSE) bahwa Pengguna (dalam hal ini penyelenggara *e-commerce* 'tukumeneh') wajib melindungi data pribadi beserta dokumen yang memuat data pribadi tersebut dari tindakan penyalahgunaan.
17. Bahwa Tergugat I juga wajib memastikan pekerjanya bekerja juga melindungi data pribadi dalam sistem *e-ommerce* 'tukumeneh' sebagiamana diatur dalam Pasal 32 ayat (1) PP PSTE bahwa 'setiap orang yang bekerja di lingkungan penyelenggaraan sistem elektronik wajib mengamankan dan melindungi sarana dan prasarana sistem elektronik atau informasi yang disalurkan melalui sistem elektronik".
18. Bahwa kebocoran data pribadi tersebut telah melanggar hak pemilik data pribadi sebagaimana diamanatkan dalam Pasal 26 Permenkominfo PDPSE;
19. Bahwa kebocoran data pribadi tersebut juga telah melawan hukum sebagaimana diatur dalam Pasal 59

ayat (1) Peraturan Pemerintah No. 80 Tahun 2019 tentang Perdagangan Melalui Sistem Elektronik (PP PMSE) yang mengatur bahwa "pelaku usaha wajib menyimpan data pribadi sesuai standar perlindungan data pribadi atau kelaziman praktik bisnis yang berkembang";

20. Bahwa berdasarkan Pasal 58 ayat (1) PP PMSE mengatur bahwa Setiap data pribadi diberlakukan sebagai hak milik pribadi dari orang atau Pelaku Usaha yang bersangkutan *juncto*. Pasal 58 ayat (2) PP PMSE mengatur bahwa Setiap Pelaku Usaha yang memperoleh data pribadi sebagaimana dimaksud pada ayat (1) wajib bertindak sebagai pengemban amanat dalam menyimpan dan menguasai data pribadi sesuai dengan ketentuan peraturan perundang-undangan.
21. Bahwa Penggugat memiliki *legal standing* dan kewenangan hukum untuk mengajukan gugatan perbuatan melawan hukum (PMH) terhadap perlindungan rahasia data pribadi sebagaimana diatur dalam Pasal 26 ayat (2) Undang-undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik *juncto*. Undang-undang No. 19 Tahun 2016 (UU ITE) *juncto*. Pasal 32 ayat (2) Permenkominfo PDPSE *junctis*. Pasal 72 ayat (3) PP PMSE
22. Bahwa Tergugat II adalah Kementerian yang dibentuk atas Peraturan Presiden. Bahwa berdasarkan Pasal 2 Peraturan Presiden Republik Indonesia No. 54 Tahun 2015 tentang Kementerian Komunkasi dan Informatika (Perpres Kominfo) bahwa Kementerian Komunikasi dan Informatika (Selanjutnya disebut Kominfo) mempunyai tugas menyelenggarakan urusan pemerintahan di

bidang komunikasi dan informatika untuk membantu Presiden dalam menyelenggarakan pemerintahan negara *juncto*. Pasal 100 ayat (2) PP 71/2019 bahwa Menteri (yang membidangi komunikasi dan informatika) dapat memberikan sanksi administratif sesuai dengan ketentuan peraturan perundang-undangan;

23. Bahwa berdasarkan Pasal 100 ayat (1) PP 71/2019 apabila pelaku usaha/penyelenggara melakukan pelanggaran terhadap ketentuan-ketentuan Pasal 4, Pasal 5 ayat (1) dan ayat (2), Pasal 6 ayat (1), Pasal 9 ayat (1) dan ayat (4), Pasal 14 ayat (1) dan ayat (5), Pasal 15 ayat (1), Pasal 17 ayat (4), Pasal 18 ayat (1), Pasal 21 ayat (2) dan ayat (3), Pasal 22 ayat (1), Pasal 23, Pasal 24 ayat (1), ayat (2), dan ayat (3), Pasal 25, Pasal 26 ayat (1), Pasal 28 ayat (1), Pasal 29, Pasal 30 ayat (1), Pasal 31, Pasal 32 ayat (1) dan ayal(21, Pasal 33, Pasal 34 ayat (1), Pasal 37 ayat (1) dan ayat(2), Pasal 38 ayat (3), Pasal 39 ayat (2), Pasal 40 ayat (1) dan ayat (2), Pasal 42 ayat (1) dan ayat (3), Pasal 51 ayat (1), Pasal 53 ayat (3), Pasal 55 ayat (2), Pasal 63 ayat (3), Pasal 64 ayat (1), Pasal 69 ayat (1), Pasal 82 ayat (7), Pasal 84 ayat (1) dan ayat (2), Pasal 87 ayat (2), dan Pasal 98 ayat (1), dikenai sanksi administratif.
24. Bahwa berdasarkan Pasal 100 ayat (2) PP 71/2019 bahwa Sanksi administratif sebagaimana dimaksud pada ayat (1) dapat berupa: a. teguran tertulis; b. denda administratif; c. penghentian sementara; d. pemutusan Akses; dan/atau e. dikeluarkan dari daftar.
25. Bahwa Tergugat III adalah Kementerian yang dibentuk atas Peraturan Presiden. Bahwa berdasarkan Pasal

2 Peraturan Presiden No. 48 Tahun 2015 tentang Kementerian Perdagangan (Perpres 48/2015) bahwa Kementerian Perdagangan mempunyai tugas menyelenggarakan urusan pemerintahan di bidang perdagangan untuk membantu Presiden dalam menyelenggarakan pemerintahan Negara *juncto.* Pasal 100 ayat (1) PP 80/2019 Menteri (yang menyelenggarakan urusan pemerintahan di bidang Perdagangan) dapat memberikan sanksi administratif.

26. Bahwa berdasarkan Pasal 100 ayat (1) PP 80/2019 "Pelanggaran terhadap ketentuan Pasal 4, Pasal 5 ayat (1) dan ayat (2), Pasal 6 ayat (1), Pasal 9 ayat (1) dan ayat (4), Pasal 14 ayat (1) dan ayat (5), Pasal 15 ayat (1), Pasal 17 ayat (4), Pasal 18 ayat (1), Pasal 21 ayat (2) dan ayat (3), Pasal 22 ayat (1), Pasal 23, Pasal 24 ayat (1), ayat (2), dan ayat (3), Pasal 25, Pasal 26 ayat (1), Pasal 28 ayat (1), Pasal 29, Pasal 30 ayat (1), Pasal 31, Pasal 32 ayat (1) dan ayat (2), Pasal 33, Pasal 34 ayat (1), Pasal 37 ayat (1) dan ayat (2), Pasal 38 ayat (3), Pasal 39 ayat (2), Pasal 40 ayat (1) dan ayat (2), Pasal 42 ayat (1) dan ayat (3), Pasal 51 ayat (1), Pasal 53 ayat (3), Pasal 55 ayat (2), Pasal 63 ayat (3), Pasal 64 ayat (1), Pasal 69 ayat (1), Pasal 82 ayat (7), Pasal 84 ayat (1) dan ayat (2), Pasal 87 ayat (2), dan Pasal 98 ayat (1), dikenai sanksi administratif oleh Menteri.
27. Bahwa berdasarkan Pasal 100 ayat (2) PP 80/2019 "Sanksi administratif sebagaimana dimaksud pada ayat (1) dapat berupa: a. teguran tertulis; b. denda administratif; c. penghentian sementara; d. pemutusan Akses; dan/atau e. dikeluarkan dari daftar."

28. Bahwa atas perbuatan Tergugat I yang tidak dapat menyimpan, melindungi data pribadi dengan baik maka mendatangkan kerugian bagi 2.000.000 (dua juta) *user/* penggunan aplikasi *online, e-commerce* 'tukumeneh' khususnya menimbulkan kerugian waktu kepada Penggugat dan berpotensi menimbulkan kerugian lain jika tidak diantisipasi lebih lanjut;
29. Bahwa Penggugat menunggu itikad baik (*good faith)* dari Tergugat I untuk meminta maaf kepada Penggugat dan kepada 1.999.999 (satu juta sembilan ratus sembilan puluh sembilan) *user/*pelanggan Tergugat I *dan* memberikan kompensasi kepada Penggugat atas kebocoran data pribadi sehingga data pribadi Penggugat dimiliki oleh Pihak lain yang tidak berwenang;
30. Bahwa Tergugat II, dan Tergugat III adalah Kementerian yang berwenang untuk melakukan investigasi kepada *e-commerce* 'tukumeneh' dan memberikan sanksi administratif kepada Tergugat I agar meningkatkan kemanan mereka;
31. Bahwa adapun kerugian yang diderita Penggugat jika dinilai berupa uang adalah sebagai berikut:
    1. Kerugian materiil sebesar Rp55.250.000,00 (lima puluh juta rupiah) yang terdiri dari Rp2.250.000 (lima juta dua ratus lima puluh ribu rupiah) dan harga data pribadi Penggugat dalam sistem tersebut mengurangi omset Penggugat karena pelanggan Penggugat yang beraluh ke toko *onine* lainnya yang ditotal mengalami kerugian yakni bernilai Rp50.000.000,00 (lima puluh juta rupiah);

2. Kerugian imateriil akibat perbuatan kebocoran data sehingga Penggugat dihubungi oleh Penelpon yang akhirnya merugikan waktu, dan membuat Penggugat cemas, tidak bisa tidur, takut kalau data pribadinya disalahgunakan untuk hal-hal melawan hukum sehinga menimbulkan kerugian imateriil sebesar Rp1.000.000.000,00 (satu miliar Rupiah)

32. Bahwa agar Tergugat I menjalankan itikad baik dan agar tidak membuang waktu memenuhi kewajibannya untuk membayar ganti rugi sesuai dengan putusan majelis hakim pemeriksa perkara *a quo* maka Penggugat mohon agar Tergugat dihukum untuk membayar uang paksa (*dwangsom)* atas setiap hari keterlambatan Tergugat dalam melaksanakan isi putusan yakni sebesar Rp1.000.000,00 (satu juta rupiah) terhitung sejak putusan perkara *a quo* memiliki kekuatan hukum tetap;
33. Bahwa mengingat usaha Tergugat I adalah usaha yang sangat penting bagi *user*/pengguna *platform* 'tukumeneh' maka Penggugat mohon agar Majelis Hakim memberikan Penetapan Sementara Pengadilan agar sistem *platform* 'tukumeneh' diberhentikan sementara untuk jangka waktu 7 (tujuh) hari kalender atau hingga Tergugat I mampu untuk memperbaiki sistem pengamanan kembali dengan baik atau memerintahkan Tergugat II untuk memberhentikan sementara koneksi atau jaringan sistem elektronik milik Tergugat I;
34. Bahwa Tergugat III juga memiliki kewenangan dalam bidang *e-commerce*, maka Tergugat III juga seyogyanya mengawasi, melakukan investigasi dan memberikan

sanksi administratif bagi Tergugat I karena lalai, tidak dapat menjaga keamanan data pribadi dalam sistem mereka;

35. Bahwa memperhatikan gugatan dalam perkara *a quo* memiliki fakta hukum yang tidak dapat dibantah kebenarannya, maka adalah wajar bilmana nantinya Tergugat I dihukum untuk membayar biaya perkara dalam perkara ini.

Berdasarkan seluruh uraian dalam gugatan diatas, maka dengan ini Penggugat mohon kepada Ketua Pengadilan Negeri Jakarta Pusat *c.q.* Majelis Hakim pemeriksa perkara *a quo* berkenan memeriksa, mengadili dan memutus dengan amar putusan sebagai berikut:

1. Mengabulkan gugatan Penggugat untuk seluruhnya;
2. Menyatakan Tergugat I telah melakukan Perbuatan Melawan Hukum, khususnya dalam hal tidak berhasil menjaga keamanan data pribadi;
3. Memerintahkan kepada Tergugat II untuk memberikan sanksi administratif sesuai dengan peraturan perundang-undangan;
4. Memerintahkan kepada Tergugat II untuk segera memanggil Tergugat I, melakukan investigasi mendalam terhadap Tergugat I;
5. Memerintahkan kepada Tergugat III untuk melakukan investigasi mendalam terhadap Tergugat I;
6. Memerintahkan kepada Tergugat III untuk memberikan sanksi administratif kepada Tergugat I sesuai dengan ketentuan peraturan perundang-undangan;

7. Menghukum Tergugat I untuk menghentikan sementara jaringan koneksi sistem elektronik milik Tergugat I selama 7 (tujuh) hari kalender atau sampai dengan Tergugat I mampu memperbaiki sistem keamanan;
8. Menghukum Tergugat membayar kerugian materiil kepada Penggugat sebesar Rp55.250.000,00 (lima puluh lima juta dua ratus lima puluh ribu rupiah) yang terdiri dari Rp2.250.000 (dua juta dua ratus lima puluh ribu rupiah) dan harga data pribadi Penggugat dalam sistem tersebut mengurangi omset Penggugat karena pelanggan Penggugat yang beralih ke toko *onine* lainnya yang ditotal mengalami kerugian yakni bernilai Rp50.000.000,00 (lima puluh juta rupiah);
9. Menghukum Tergugat untuk membayar Kerugian imateriil akibat perbuatan kebocoran data sehingga Penggugat dihubungi oleh Penelepon yang akhirnya merugikan waktu, dan membuat Penggugat cemas, tidak bisa tidur, takut kalau data pribadinya disalahgunakan untuk hal-hal melawan hukum sehinga menimbulkan kerugian imaterril sebesar Rp1.000.000.000,00 (satu miliar Rupiah);
10. Menghukum Tergugat untuk membuat pernyataan maaf kepada seluruh *user,* pengguna 'tukumeneh' *dalam* minimal 3 harian surat kabar berskala nasional dengan ukuran setengah halaman selama 3 (tiga) hari secara berturut-turut;
11. Menyatakan putusan dapat dilaksanakan terlebih dahulu walaupun ada upaya hukum terhadap gugatan ini (*Uit Voerbaar Bij Voorrad)*;

12. Menghukum Tergugat I untuk membayar perkara *a quo* ini.

Atau
Apabila Ketua Pengadilan Negeri Jakarta Pusat *c.q.* Majels Hakim Pemeriksa perkara *a quo* berpendapat lain, mohon putusan seadil-adilnya (***Ex Aequo et Bono)*.**

Hormat Kami,
Kuasa Hukum Penggugat

TTD,
Dr. Putra, S.H, M.H.

VII. Penegakan Hukum Perlindungan Data Pribadi Melalui Sarana Hukum Pidana

Penulis melakukan survei dan dari 226 responden yang terlibat dengan pertanyaan "Apakah menurut Saudara, media hukum pidana berupa pemberian sanksi pidana penjara dalam kurun waktu tertentu dan/atau denda dengan nominial tertentu dapat diberikan kepada Penyelenggara Sistem Elektronik (penyedia jasa layanan aplikasi Online) yang terbukti tidak dapat melindungi data pribadi dalam sistem sehingga mengakibatkan kebocoran data?" dan didapatkan bahwa 71% menjawab ya, 10% menjawab tidak dan 19% menjawab tidak tahu.

Di dalam pembagian hukum konvensional, hukum pidana termasuk bidang hukum publik, artinya bahwa hukum pidana mengatur hubungan antara warga Negara dengan Negara dan menitikberatkan kepada kepentingan umum atau kepentingan publik. Secara historis, hubungan hukum yang ada pada awalnya adalah hubungan pribadi/hubungan privat, namun dalam perjalanan waktu terdapat hal-hal yang diambil alih kelompok atau suku dan akhirnya setelah berdirinya Negara diambil alih oleh Negara dan dijadikan kepentingan umum. Bukti yang jelas dapat kita lihat di dalam Kitab Undang-undang Hukum Pidana (KUHP) Pasal 344 "Barangsiapa merampas nyawa orang lain atas permintaan orang itu sendiri yang jelas dinyatakan dengan kesungguhan hati diancam dengan pidana penjara paling lama 12 tahun". Hak penuntutan terhadap perbuatan yang dilarang dan diancam hukuman terletak pada alat perlengkapan Negara yakni Jaksa Penuntut Umum[298].

[298] Teguh Prasetyo, *Hukum Pidana, Op.Cit,* hlm. 2.

Hukum pidana adalah hukum yang memiliki sifat khusus, yaitu dalam hal sanksinya. Setiap kita berhadapan dengan hukum, pikiran kita menuju ke arah sesuatu yang mengikat perilaku seseorang di dalam masyarakatnya. Di dalamnya terdapat ketentuan tentang apa yang harus dilakukan dan apa yang tidak boleh dilakukan, serta akibatnya. Hal yang pertama diatas disebut sebagai 'norma' sedang akibatnya dinamakan 'sanksi'. Yang membedakan hukum pidana dengan hukum yang lainnya, diantaranya adalah bentuk sanksinya, yang bersifat negative yang disebut sebagai 'pidana' (hukuman). Bentuknya bermacam-macam dari dipaksa diambil hartanya karena harus membayar 'denda', dirampas kebebasanya karena dipidana 'kurungan atau penjara', bahkan dapat pula 'dirampas nyawanya' apabila diputuskan dijatuhi 'pidana mati'.[299]

1. Tinjauan Singkat Definsi Hukum Pidana

   Hukum pidana itu merupakan suatu sistem norma-norma yang menentukan terhadap tindakan-tindakan yang mana (hal melakukan sesuatu atau tidak melakukan sesuatu di mana terdapat suatu keharusan untuk melakukan sesuatu) dan dalam keadaaan-keadaan bagaimana yang dapat dijatuhkan bagi tindakan-tindakan tersebut[300].

   Banyak ahli telah merumuskan definisi hukum pidana dalam pelbagai literatur. Salah satunya ialah menurut **Wirjono Prodjodikoro** sebagaimana dikutip oleh **Laden Marpaung** menjelaskan bahwa hukum pidana materiil dan hukum pidana formil ialah a. Penunjuk dan gambaran dari perbuatan-perbuatan yang diancam

[299] *Ibid.*

[300] P.A.F. Lamintang, *Dasar-Dasar Hukum Pidana Indonesia*, (Bandung: Sinar Baru,1984), hlm.1-2.

dengan hukum pidana. b. Penunjukan syarat umum yang harus dipenuhi agar perbuatan itu merupakan perbuatan yang membuatnya dapat dihukum pidana. c. Penunjuk jenis hukuman pidana yang dapat dijatuhkan hukum acara pidana berhubungan erat dengan diadakannya hukum pidana, oleh karena itu merupakan suatu rangkaian yang memuat cara bagaimana badan-badan pemerintah yang berkuasa, yaitu kepolisian, kejaksaan dan pengadilan bertindak guna mencapai tujuan Negara dengan mengadakan hukum pidana[301].

Hukum pidana adalah sekumpulan peraturan hukum yang dibuat oleh Negara, yang isinya berupa larangan ataupun keharusan sedang bagi pelanggar terhadap larangan dan keharusan tersebut dikenakan sanksi yang dapat dipaksakan oleh Negara[302].

Hukum pidana merupakan bagian dari hukum publik yang berisi ketentuan tentang:

a. Aturan hukum pidana dan larangan melakukan perbuatan – perbuatan tertentu yang disertai dengan ancaman berupa sanksi pidana bagi yang melanggar larangan itu. Aturan umum hukum pidana dapat dilihat dalam KUHP ataupun peraturan perundang-undangan lainnya diluar KUHP;
b. Syarat-syarat tertentu yang harus dipenuhi bagi si pelanggar untuk dapat dijatuhkannya sanksi pidana, dan berisi tentang: pertama, kesalahan/*schuld*; kedua, pertanggungjawaban pidana pada diri si pembuat/*toerekeningsvadbaarheid*. Dalam hukum

[301] Laden Marpaung, *Asas-Teori-Praktik Hukum Pidana*, (Jakarta: Sinar Grafika, 2005), hlm. 21.

[302] Teguh Prasetyo, *Hukum Pidana*, *Op. Cit,* hlm. 9-10.

pidana dikenal asas *geen straf zonder schuld* (tiada pidana tanpa kesalahan), artinya seseorang dapat dipidana apabila perbuatanya nyata melanggar larangan hukum pidana. Hal tersebut diatur dalam Pasal 44 KUHP tentang tidak mampu bertanggung jawab bagi si pembuat atas perbuatanya dan Pasal 48 KUHP tentang 'tidak dapat dipidananya' si pembuat karena dalam keadaan daya paksa (*overmacht),* kedua keadaan ini termasuk dalam 'alasan penghapus pidana', merupakan sebagian dari Bab II Buku II KUHP;

c. Tindakan dan upaya yang harus dilakukan Negara melalui hukum terhadap tersangka / terdakwa sebagai pelanggar hukum pidana dalam rangka menentukan menjatuhkan dan melaksanakan sanksi pidana terhadap dirinya serta upaya – upaya yang dapat dilakukan oleh tersangka / terdakwa dalam usaha mempertahankan hak-haknya. Dikatakan sebagai hukum pidana dalam arti bergerak (formal) memuat aturan tentang bagaimana Negara harus berbuat dalam rangka menegakkan hukum pidana dalam arti diam (materiil).

2. Fungsi dan Tujuan Hukum Pidana

2 (dua) aliran mengenai tujuan hukum pidana, yakni: pertama, untuk menakut-nakuti setiap orang jangan sampai melakukan perbuatan yang tidak baik (aliran klasik); kedua, untuk mendidik orang yang telah pernah melakukan perbuatan tidak baik menjadi baik dan dapat diterima kembali dalam kehidupan lingkunganya (aliran modern). Tujuan hukum pidana mengandung makna pencegahan terhadap gejala-gejala sosial yang kurang

sehat di samping pengobatan bagi yang sudah terlanjur tidak berbuat baik[303].

Menurut **Bambang Poernomo,** seseorang yang terbukti dan telah dijatuhi putusan pidana penjara berkedudukan sebagai 'narapidana'. Narapidana adalah 'seseorang manusia atau anggota masyarakat yang dipisahkan dari induknya dan selama waktu tertentu itu diproses dalam lingkungan tempat tertentu dengan tujuan, metode, dan sistem pemasyarakatan. Pada suatu saat narapidana itu akan kembali menjadi manusia anggota masyarakat yang lebih baik dan taat terhadap hukum'.[304]

Menurut **Roeslan Saleh,** hukum pidana dan sanksi pidana masih diperlukan karena 3 (tiga) alasan dibawah ini, yakni:

1. Perlu tidaknya hukum pidana terletak pada persoalan tujuan-tujuan yang hendak dicapai, namun terletak pada persoalan seberapa jauh untuk mencapai tujuan itu boleh menggunakan paksaan. Persoalan bukan terletak pada hasil yang akan dicapai, namun dalam perimbangan antara nilai dari hasil itu dan nilai dari batas-batas kebebasan pribadi masing-masing;
2. Ada usaha-usaha perbaikan atau perawatan yang tidak mempunyai arti sama sekali bagi si terhukum; dan di samping itu harus tetap ada suatu reaksi atas pelanggaran-pelanggaran norma yang telah dilakukannya itu dan tidaklah dapat dibiarkan begitu saja;

[303] *Ibid*, hlm. 14-15

[304] Bambang Poernomo, *Pelaksanaan Pidana Penjara dengan Sistem Pemasyarakatan,* (Yogyakarta: Liberty Yogyakarta, 1986), hlm. 92.

3. Pengaruh pidana atau hukum pidana bukan semata-mata ditujukan pada si penjahat, namun juga untuk mempengaruhi oang yang tidak jahat, yakni warga masyarakat yang mentaati norma-norma masyarakat[305].

Menurut **Van Bemmelen,** pendekatan dari sudut politik mengapa hukum pidana diperlukan, ialah sebagai berikut:

*"Jika kita mendekati hukum pidana bukan dari sudut pidananannya namun dari sudut ketentuan-ketentuan perintah dan larangan serta dari sudut penegakan ketentuan-ketentuan itu (***Pen-***yakni penegakan hukum), dan khususnya dari sudut hukum acara pidana, maka tidak lagi begitu condong untuk membuang hukum pidana."*

"Apabila kita mendekati hukum pidana dari sudut ketentuan-ketentuan perintah dan larangan, kita sadar bahwa ada perbuatan-perbuatan tertentu melawan hukum yang tidak mungkin diterima oleh masyarakat. Makar terhadap Kepala Negara tidak mungkin diterima oleh Negara. Begitupun masyarakat tidak mungkin menerima bahwa manusia yang satu secara bebas membunuh orang lain atau dengan sengaja merusak, menghilangkan atau mengambil suatu benda milik orang lain tanpa izin pemiliknya".

"Oleh karena itu selalu perlu ada ketentuan atau larangan dan selalu ada pelanggaran-pelanggaran terhadap ketentuan dan larangan tersebut di mana tidak mungkin Pemerintah membiarkan perlindungan terhadap pelanggaran itu berada di tengah individu. Apabila A membunuh tetangganya B, maka mungkin sekali Negara membiarkan keluarga B untuk menuntut ganti rugi pada A. Namun, apabila keluarga B juga membiarkan untuk membunuh A, maka kita kembali kepada pembalasan berdarah dan pada suatu keadaan hukum yang kacau seperti juga terdahulu. Suatu alasan sebab apa hukum pidana tidak dapat dihapuskan ialah bahwa hukum pidana dengan teliti menunjuk dalam hal-hal mana Negara berhak

[305] Roeslan Saleh, *Mencari Asas-Asas Umum yang Sesuai untuk Hukum Pidana Nasional,* Kumpulan Bahan *Upgrading* Hukum Pidana, Jilid 2, 1971, hlm.15-16; Lihat pula Barda Nawawi Arief, "Pemidanaan", *Masalah-Masalah Hukum,* No. 16, 1974, hlm. 14-16

untuk bertindak terhadap seorang penduduk lewan jalan hukum acara pidana."[306]

Berdasarkan **Rancangan Undang-undang tentang Kitab Undang-undang Hukum Pidana (September 2019),** selanjutnya disebut RKUHP**,** berdasarkan Pasal 51 bahwa pemidanaan bertujuan untuk:

1. mencegah dilakukannya Tindak Pidana dengan menegakkan norma hukum demi pelindungan dan pengayoman masyarakat;
2. memasyarakatkan terpidana dengan mengadakan pembinaan dan pembimbingan agar menjadi orang yang baik dan berguna;
3. menyelesaikan konflik yang ditimbulkan akibat Tindak Pidana, memulihkan keseimbangan, serta mendatangkan rasa aman dan damai dalam masyarakat; dan
4. menumbuhkan rasa penyesalan dan membebaskan rasa bersalah pada terpidana.

Dan berdasarkan Pasal 52 RKUHP, bahwa pemidanaan tidak dimaksudkan untuk merendahkan martabat manusia. Hal ini serupa dengan tujuan 'Keadilan Bermartabat' bahwa hukum pidana dimaksudkan untuk memberikan pemulihan dan sanksi yang diberikan ditujukan untuk tetap memanusiakan manusia tersebut.

3. Ketentuan Pidana dalam RKUHP terhadap Perlindungan Data Pribadi

[306] Van Bemmelen, *Ons Strafrecht I, het matierele strafrecht algemeen deel, zesde herzien druk, H.D. Tjeenk Willink,* Gronengen, 1979, hlm. 21-22; Lihat Pula, Teguh Prasetyo, *Kriminalisasi dalam Hukum Pidana,* (Bandung: Penerbit Nusa Media, 2010).

RKUHP (pembahasan per September 2019) dibentuk dengan pertimbangan sebagai berikut: **pertama**, bahwa untuk mewujudkan hukum pidana nasional Negara Kesatuan Republik Indonesia yang berdasarkan Pancasila dan Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 serta asas hukum umum yang diakui masyarakat beradab, perlu disusun hukum pidana nasional untuk mengganti Kitab Undang-Undang Hukum Pidana warisan pemerintah kolonial Hindia Belanda; **kedua**, bahwa hukum pidana nasional tersebut harus disesuaikan dengan politik hukum, keadaan, dan perkembangan kehidupan bermasyarakat, berbangsa, dan bernegara yang bertujuan menghormati dan menjunjung tinggi hak asasi manusia, berdasarkan Ketuhanan Yang Maha Esa, kemanusiaan yang adil dan beradab, persatuan Indonesia, kerakyatan yang dipimpin oleh hikmat kebijaksanaan dalam permusyawaratan/perwakilan, dan keadilan sosial bagi seluruh rakyat Indonesia; **ketiga**, bahwa materi hukum pidana nasional juga harus mengatur keseimbangan antara kepentingan umum atau negara dan kepentingan individu, antara pelindungan terhadap pelaku tindak pidana dan korban tindak pidana, antara unsur perbuatan dan sikap batin, antara kepastian hukum dan keadilan, antara hukum tertulis dan hukum yang hidup dalam masyarakat, antara nilai nasional dan nilai universal, serta antara hak asasi manusia dan kewajiban asasi manusia.

Penulis tidak menemukan satu delik yang mengatur tentang tindak pidana pembocoran data pribadi, penyalahgunaan data pribadi. Namun, dalam **RKUHP** terdapat delik yang mengatur tentang 'tindak pidana

terhadap informatika dan elektronika'. **Penulis** akan memaparkannya sebagai berikut[307]:

1) **Tindak Pidana Penggunaan dan Perusakan Informasi Elektronik sebagaimana diatur dalam RKUHP Pasal 336** "Setiap Orang yang menggunakan atau mengakses Komputer atau sistem elektronik dengan cara apapun tanpa hak dengan maksud untuk memperoleh, mengubah, merusak, atau menghilangkan informasi dalam Komputer atau sistem elektronik dipidana dengan pidana penjara paling lama 4 (empat) tahun atau pidana denda paling banyak kategori V";
2) **Tindak Pidana Tanpa Hak Mengakses Komputer dan Sistem Elektronik sebagaimana diatur dalam Pasal 337 RKUHP** "Dipidana dengan pidana penjara paling lama 7 (tujuh) tahun atau pidana denda paling banyak kategori VI, Setiap Orang yang:
   a. tanpa hak menggunakan, mengakses Komputer, atau sistem elektronik dengan cara apapun, dengan maksud memperoleh, mengubah, merusak, atau menghilangkan informasi pertahanan nasional atau hubungan internasional yang dapat menyebabkan

[307] Dalam RKUHP (pembahasan per September 2019) diatur tentang pidana denda dengan kategori I-VIII yakni sebagai berikut: berdasarkan Pasal 79 ayat (1) RKUHP "Pidana denda paling banyak ditetapkan berdasarkan:
a. kategori I, Rp1.000.000,00 (satu juta rupiah);
b. kategori II, Rp10.000.000,00 (sepuluh juta rupiah);
c. kategori III, Rp50.000.000,00 (lima puluh juta rupiah);
d. kategori IV, Rp200.000.000,00 (dua ratus juta rupiah);
e. kategori V, Rp500.000.000,00 (lima ratus juta rupiah);
f. kategori VI, Rp2.000.000.000,00 (dua miliar rupiah);
g. kategori VII, Rp5.000.000.000,00 (lima miliar rupiah); dan
h. kategori VIII, Rp50.000.000.000,00 (lima pul[uh miliar rupiah)".

Berdasarkan Pasal 79 ayat (2) RKUHP (pembahasan per September 2019) bahwa "Dalam hal terjadi perubahan nilai uang, ketentuan besarnya pidana denda ditetapkan dengan Peraturan Pemerintah."

gangguan atau bahaya terhadap negara atau hubungan dengan subjek hukum internasional;

b. tanpa hak melakukan tindakan yang menyebabkan transmisi dari program, informasi, kode atau perintah Komputer atau sistem elektronik yang dilindungi negara menjadi rusak;

c. tanpa hak atau melampaui wewenangnya menggunakan atau mengakses Komputer atau sistem elektronik, baik dari dalam maupun luar negeri untuk memperoleh informasi dari Komputer atau sistem elektronik yang dilindungi oleh negara;

d. tanpa hak menggunakan atau mengakses Komputer atau sistem elektronik milik pemerintah;

e. tanpa hak atau melampaui wewenangnya menggunakan atau mengakses Komputer atau sistem elektronik yang dilindungi oleh negara, yang mengakibatkan Komputer atau sistem elektronik tersebut menjadi rusak;

f. tanpa hak atau melampaui wewenangnya menggunakan atau mengakses Komputer atau sistem elektronik yang dilindungi oleh masyarakat, yang mengakibatkan Komputer atau sistem elektronik tersebut menjadi rusak;

g. mempengaruhi atau mengakibatkan terganggunya Komputer atau sistem elektronik yang digunakan oleh pemerintah;

h. menyebarkan, memperdagangkan, atau memanfaatkan Kode Akses atau informasi yang serupa dengan hal tersebut, yang dapat digunakan menerobos Komputer atau sistem elektronik

dengan tujuan menyalahgunakan Komputer atau sistem elektronik yang digunakan atau dilindungi oleh pemerintah;

i. melakukan perbuatan dalam rangka hubungan internasional dengan maksud merusak Komputer atau sistem elektronik lainnya yang dilindungi negara dan berada di wilayah yurisdiksi Indonesia dan ditujukan kepada siapa pun; atau

j. melakukan perbuatan dalam rangka hubungan internasional dengan maksud merusak Komputer atau sistem elektronik lainnya yang dilindungi negara dan berada di wilayah yurisdiksi Indonesia dan ditujukan kepada siapa pun.

3) **Tindak Pidana sebagaimana diatur dalam Pasal 338 RKUP** yang mengatur demikian "Dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun atau pidana denda paling banyak kategori VI, Setiap Orang yang:

a. tanpa hak atau melampaui wewenangnya menggunakan atau mengakses Komputer atau sistem elektronik dengan maksud memperoleh keuntungan atau memperoleh informasi keuangan dari bank sentral, lembaga perbankan atau lembaga keuangan, penerbit kartu kredit, atau kartu pembayaran atau yang mengandung data laporan nasabahnya;

b. tanpa hak menggunakan data atau mengakses dengan cara apapun kartu kredit atau kartu pembayaran milik orang lain dalam transaksi elektronik untuk memperoleh keuntungan;

c. tanpa hak atau melampaui wewenangnya menggunakan atau mengakses Komputer atau

sistem elektronik bank sentral, lembaga perbankan atau lembaga keuangan yang dilindungi, dengan maksud menyalahgunakan, atau untuk mendapatkan keuntungan daripadanya; atau

d. menyebarkan, memperdagangkan, atau memanfaatkan Kode Akses atau informasi yang serupa dengan hal tersebut yang dapat digunakan menerobos Komputer atau sistem elektronik dengan maksud menyalahgunakan yang akibatnya dapat mempengaruhi sistem elektronik bank sentral, lembaga perbankan atau lembaga keuangan, serta perniagaan di dalam dan luar negeri".

4) Tindak Pidana sebagaimana diatur dalam Pasal 339 RKUP yang mengatur demikian "Setiap Orang yang tanpa hak menggunakan atau mengakses Komputer atau sistem elektronik dengan cara apapun, dengan maksud memperoleh, mengubah, merusak, atau menghilangkan informasi milik pemerintah yang karena statusnya harus dirahasiakan atau dilindungi dipidana dengan pidana penjara paling lama 12 (dua belas) tahun atau pidana denda paling banyak kategori VII".

4. Ketentuan Pidana dalam UU ITE terhadap Perlindungan Data Pribadi

Ketentuan pidana hanya dimuat dalam Undang-Undang, Peraturan Daerah Provinsi, dan Peraturan Daerah Kabupaten/Kota. Ketentuan pidana memuat rumusan yang menyatakan penjatuhan pidana atas pelanggaraan ataupun kejahatan terhadap ketentuan yang berisi norma larangan atau norma perintah. Dalam menentukan lamanya

pidana atau banyaknya denda perlu dipertimbangkan mengenai dampak yang ditimbulkan oleh tindak pidana dalam masyarakat serta unsur kesalahan pelaku[308]. Dalam merumuskan ketentuan pidana yang terdapat dalam Buku Kesatu Kitab Undang-undang Hukum Pidana (KUHP) karena ketentuan dalam Buku Kesatu juga berlaku bagi perbuatan yang dapat dipidana menurut peraturan perundang-undangan lain, kecuali jika oleh undang-undang ditentukan lain.[309]

UU ITE belum mengatur dengan tegas terkait delik penyalahgunanaan data pribadi secara melawan hukum. Namun, UU ITE mengatur tentang kesengajaan dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain

1) Pasal 29 UU ITE: "Setiap Orang dengan sengaja dan tanpa hak mengirimkan Informasi Elektronik dan/atau Dokumen Elektronik yang berisi ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi". Apabila terduga pelaku terbukti melakukan kejahatan sebagaimana dalam ketentuan Pasal 29 maka berdasarkan Pasal 45B UU ITE dapat dipidana dengan pidana penjara paling lama 4 (empat) tahun dan/atau denda paling banyak Rp750.000.000,00 (tujuh ratus lima puluh juta rupiah)".
2) Pasal 30 ayat (1) UU ITE: "Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses

[308] Teguh Prasetyo, *SIstem Hukum Pancasila.... Op.Cit,* hlm. 167

[309] Pasal 103 KUHP yang mengatur bahwa "Ketentuan-ketentuan dalam Bab I sampai Bab VIII buku ini juga berlaku bagi perbuatanperbuatan yang oleh ketentuan perundang-undangan lainnya diancam dengan pidana, kecuali jika oleh undang-undang ditentukan lain."

Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apa pun". Apabila terduga pelaku terbukti melakukan kejahatan sebagaimana dalam ketentuan Pasal 30 ayat (1) maka berdasarkan Pasal 46 ayat (1) dapat dipidana dengan penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp600.000.000,00 (enam ratus juta rupiah);

3) Pasal 30 ayat (2) UU ITE: "Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik". Apabila terduga pelaku terbukti melakukan kejahatan sebagaimana dalam ketentuan Pasal 30 ayat (2) maka berdasarkan Pasal 46 ayat (2) dapat dipidana dengan penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp700.000.000,00 (tujuh ratus juta rupiah).
4) Pasal 30 ayat (3) UU ITE: "Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan". Apabila terduga pelaku terbukti melakukan kejahatan sebagaimana dalam ketentuan Pasal 30 ayat (3) maka berdasarkan Pasal 46 ayat (3) dapat dipidana dengan penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp800.000.000,00 (delapan ratus juta rupiah).
5) Pasal 32 ayat (1) UU ITE: "Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun mengubah, menambah, mengurangi, melakukan

transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik publik". Apabila terduga pelaku terbukti melakukan perbuatan yang dilarang dalam Pasal 32 ayat (1) maka berdasarkan Pasal 48 ayat (1) dapat diancam dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp2.000.000.000,00 (dua miliar rupiah);

6) Pasal 32 ayat (2) UU ITE: "Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun memindahkan atau mentransfer Informasi Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik Orang lain yang tidak berhak". Apabila terduga pelaku terbukti melakukan perbuatan yang dilarang dalam Pasal 32 ayat (2) maka berdasarkan Pasal 48 ayat (2) dapat diancam dengan pidana penjara paling lama 9 (sembilan) tahun dan/atau denda paling banyak Rp3.000.000.000,00 (tiga miliar rupiah);
7) Pasal 32 ayat (3) UU ITE: "Terhadap perbuatan sebagaimana dimaksud pada ayat (1) yang mengakibatkan terbukanya suatu Informasi Elektronik dan/atau Dokumen Elektronik yang bersifat rahasia menjadi dapat diakses oleh publik dengan keutuhan data yang tidak sebagaimana mestinya."
8) Pasal 34 ayat (1) UU ITE: "Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum memproduksi, menjual, mengadakan untuk digunakan, mengimpor, mendistribusikan, menyediakan, atau memiliki: a. perangkat keras atau perangkat lunak Komputer yang

dirancang atau secara khusus dikembangkan untuk memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 33; b. sandi lewat Komputer, Kode Akses, atau hal yang sejenis dengan itu yang ditujukan agar Sistem Elektronik menjadi dapat diakses dengan tujuan memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 33. Namun terdapat **'pengecualian' (*exception clause)*** yakni yang diatur dalam Pasal 34 ayat (2) UU ITE "Tindakan sebagaimana dimaksud pada ayat (1) bukan tindak pidana jika ditujukan untuk melakukan kegiatan penelitian, pengujian Sistem Elektronik, untuk perlindungan Sistem Elektronik itu sendiri secara sah dan tidak melawan hukum." Apabila terduga pelaku terbukti melakukan perbuatan yang dilarang dalam Pasal 34 ayat (1) maka berdasarkan Pasal 50 dapat diancam dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp10.000.000.000,00 (sepuluh miliar rupiah).

5. Ketentuan Pidana yang Tersebar tentang Delik yang Dapat dikategorikan sebagai Penyalahgunaan Data Pribadi
   A. UU ADMINDUK terhadap Perlindungan Data Pribadi
      1) **Perbuatan manipulasi data.** Pasal 77 UU ADMINDUK (perubahan - tahun 2013) "Setiap orang dilarang memerintahkan dan/atau memfasilitasi dan/atau melakukan manipulasi Data Kependudukan dan/atau elemen data Penduduk". Apabila terbukti melawan Pasal 77 UU ADMINDUK (perubahan - tahun 2013) tersebut maka berdasar Pasal 94 UU ADMINIDUK (perubahan - tahun 2013) "Setiap orang

yang memerintahkan dan/atau memfasilitasi dan/atau melakukan manipulasi Data Kependudukan dan/atau elemen data Penduduk sebagaimana dimaksud dalam Pasal 77 dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp75.000.000,00 (tujuh puluh lima juta rupiah)";

2) **Pasal 79 ayat (1) UU ADMINDUK (perubahan-tahun 2013) tentang kewajiban Negara menyimpan dan melindungi data kependudukan[310] dan Pasal 86 ayat (1) UU ADMINDUK (perubahan-tahun 2013) tentang pemberian hak akses data pribadi kepada petugas.** Apabila terbukti melawan norma tersebut maka berdasarkan Pasal 95 UU ADMINDUK (tahun 2006) "Setiap orang yang tanpa hak mengakses database kependudukan sebagaimana dimaksud dalam Pasal 79 ayat (1), Pasal 86 ayat (1) dipidana dengan pidana penjara paling lama 2 (dua) tahun dan/atau denda paling banyak Rp 25.000.000,00 (dua puluh lima juta rupiah)".

3) **Pasal 79 ayat (3) UU ADMINDUK (perubahan - tahun 2013)[311] tentang larangan petugas dan pengguna untuk menyebarluaskan data dan**

[310] Pasal 79 ayat (1) UU ADMINDUK (perubahan-tahun 2013) "Data Perseorangan dan dokumen kependudukan wajib disimpan dan dilindungi kerahasiaannya oleh Negara" dan Pasal 86 ayat (1) UU ADMINDUK (perubahan-tahun 2013) "Menteri sebagai penanggung jawab memberikan hak akses Data Pribadi kepada petugas provinsi dan petugas Instansi Pelaksana"

[311] Pasal 79 ayat (3) UU ADMINDUK (perubahan - tahun 2013) "Petugas dan pengguna sebagaimana dimaksud pada ayat (2) dilarang menyebarluaskan Data Kependudukan yang tidak sesuai dengan kewenangannya". Dan Pasal 79 ayat (2) UU ADMINDUK (perubahan - tahun 2013 "Menteri sebagai penanggung jawab memberikan hak akses Data Kependudukan kepada petugas provinsi dan petugas Instansi Pelaksana serta pengguna".

Pasal 86 ayat (1a) UU ADMINDUK (perubahan - tahun 2013)[312] tentang larangan bagi petugas provinsi untuk menyebarluaskan data pribadi. Apabila terbukti melawan ketentuan tersebut maka berdasarkan Pasal 95A UU ADMINDUK (perubahan-tahun 2013) "Setiap orang yang tanpa hak menyebarluaskan Data Kependudukan sebagaimana dimaksud dalam Pasal 79 ayat (3) dan Data Pribadi sebagaimana dimaksud dalam Pasal 86 ayat (1a) dipidana dengan pidana penjara paling lama 2 (dua) tahun dan/atau denda paling banyak Rp25.000.000,00 (dua puluh lima juta rupiah)".

6. Pembocoran Rahasia Nasabah

Pasal 40 ayat (1) UU Perbankan dengan tegas mengatur bahwa "Bank Wajib merahasiakan keterangan mengenai Nasabah Penyimpan dan simpanannya, kecuali dalam hal sebagaimana dimaksud dalam Pasal 41[313], Pasal 41A,[314] Pasal 42[315], Pasal 44[316], dan Pasal 44A[317]".

Apabila melanggar maka dapat dikenakan ancaman pidana, misalnya: Barang siapa tanpa membawa perintah tertulis atau izin dari Pimpinan Bank Indonesia

[312] Pasal 86 ayat (1a) UU ADMINDUK (perubahan - tahun 2013) "Petugas sebagaimana dimaksud pada ayat (1) dilarang menyebarluaskan Data Pribadi yang tidak sesuai dengan kewenangannya". Dan Pasal 86 ayat (1) UU ADMINDUK (perubahan-tahun 2013) "Menteri sebagai penanggung jawab memberikan hak akses Data Pribadi kepada petugas provinsi dan petugas Instansi Pelaksana."

[313] Untuk Kepentingan Perpajakan

[314] Untuk penyelesaian piutang bank yang sudah diserahkan kepada Badan Urusan Piutang dan Lelang Negara

[315] Untuk kepentingan peradilan dalam perkara pidana

[316] Dalam tukar menukar informasi antar bank, Direksi bank dapat memberitahukan keadaan keuangan nasabahnya kepada bank lain.

[317] Atas permintaan, persetujuan atau kuasa dari Nasabah Penyimpan yang dibuat secara tertulis, bank wajib memberikan keterangan mengenai simpan Nasabah Penyimpan

sebagaimana dimaksud dalam Pasal 41, Pasal 41A, dan Pasal 42, dengan sengaja memaksa bank atau Pihak Terafiliasi untuk memberikan keterangan sebagaimana dimaksud dalam Pasal 40, diancam dengan pidana penjara sekurang-kurangnya 2 (dua) tahun dan paling lama 4 (empat) tahun serta denda sekurang-kurangnya Rp 10.000.000.000,00 (sepuluh miliar rupiah) dan paling banyak Rp 200.000.000.000,00 (dua ratus miliar rupiah)[318].

7. Pembocoran Rahasia Pasien

Berdasarkan UU No. 29 Tahun 2004 tentang praktik kedokteran (UU Praktik Kedokteran) bahwa berdasarkan Pasal 51 UU Praktik Kedokteran "Dokter atau dokter gigi dalam melaksanakan praktik kedokteran mempunyai kewajiban : a. memberikan pelayanan medis sesuai dengan standar profesi dan standar prosedur operasional serta kebutuhan medis pasien; b. merujuk pasien ke dokter atau dokter gigi lain yang mempunyai keahlian atau kemampuan yang lebih baik, apabila tidak mampu melakukan suatu pemeriksaan atau pengobatan; c. merahasiakan segala sesuatu yang diketahuinya tentang pasien, bahkan juga setelah pasien itu meninggal dunia; d. melakukan pertolongan darurat atas dasar perikemanusiaan, kecuali bila ia yakin ada orang lain yang bertugas dan mampu melakukannya; dan e. menambah ilmu pengetahuan dan mengikuti perkembangan ilmu kedokteran atau kedokteran gigi." Berdasarkan Pasal 79 UU Praktik Kedoketeran *jo.* Putusan Mahkamah Konstitusi No. 4/PUU-V/2007 bahwa "Pasal 79 Dipidana dengan pidana kurungan paling lama 1 (satu) tahun atau denda paling banyak Rp 50.000.000,00

[318] Pasal 47 ayat (1) UU Perbankan

(lima puluh juta rupiah), setiap dokter atau dokter gigi yang : a. dengan sengaja tidak memasang papan nama sebagaimana dimaksud dalam Pasal 41 ayat (1); b. dengan sengaja tidak membuat rekam medis sebagaimana dimaksud dalam Pasal 46 ayat (1); atau c. dengan sengaja tidak memenuhi kewajiban sebagaimana dimaksud dalam Pasal 51 huruf a, huruf b, huruf c, huruf d, atau huruf e."

8. Ketentuan Pidana dalam KUHP
    1. **Membuka Rahasia Jabatan.** Barang siapa dengan sengaja membuka rahasia yang wajib disimpannya karena jabatan atau pencariannya, baik yang sekarang maupun yang dahulu, diancam dengan pidana penjara paling lama sembilan bulan atau pidana denda paling banyak sembilan ribu rupiah – Pasal 322 ayat (1) KUHP. Dan berdasarkan Pasal 322 ayat (2) KUHP bahwa "Jika kejahatan dilakukan terhadap seorang tertentu, maka perbuatan itu hanya dapat dituntut atas pengaduan orang itu."
    2. **Penggelapan dalam Jabatan apabila pelaku adalah karyawanan bidang IT dalam perusahaan.** Pasal 374 KUHP "Penggelapan yang dilakukan oleh orang yang penguasaannya terhadap barang disebabkan karena ada hubungan kerja atau karena pencarian atau karena mendapat upah untuk itu, diancam dengan pidana penjara paling lama lima tahun."
9. Apabila Pelaku Tindak Pidana Adalah Korporasi

    Apabila pelaku tindak pidana penyalahgunaan data pribadi adalah korporasi maka penyelesaiannya melalui Peraturan Mahkamah Agung Republik Indonesia No. 13 Tahun 2016 tentang Tata Cara Penangananan Perkara Tindak

Pidana oleh Korprorasi (Perma 13/2016). **Penulis** akan menguraikan beberapa norma yang mengatur:

1. Penilaian kesalahan korporasi dengan: a. Korporasi dapat memperoleh keuntungan atau manfaat dari tindak pidana tersebut atau tindak pidana tersebut dilakukan untuk kepentingan Korporasi; b. Korporasi membiarkan terjadinya tindak pidana; atau c. Korporasi tidak melakukan langkah-langkah yang diperlukan untuk melakukan pencegahan, mencegah dampak yang lebih besar dan memastikan kepatuhan terhadap ketentuan hukum yang berlaku guna menghindari terjadinya tindak pidana[319].
2. Keterangan korporasi merupakan alat bukti yang sah[320]. Sistem pembuktian dalam penanganan tindak pidana yang dilakukan oleh Korporasi mengikuti Kitab Undang-Undang Hukum Acara Pidana (KUHAP) dan ketentuan hukum acara yang diatur khusus dalam undang-undang lainnya[321].
3. Hakim dapat menjatuhkan pidana terhadap korporasi berupa pidana pokok yakni denda dan/atau pidana tambahan[322].

Penulis menganalisis dengan menyebarkan kuisioner dengan pertanyaan Berdasarkan media hukum diatas, menurut Saudara/i, media hukum apa yang paling efektif, dan pantas diberikan kepada Penyelenggara Sistem Elektronik (penyedia jasa layanan aplikasi *Online*) yang terbukti tidak

[319] Pasal 4 ayat (2) Perma 13/2016.
[320] Pasal 14 ayat (1) Perma 13/2016
[321] Pasal 14 ayat (2) Perma 13/2016
[322] Pasal 25 ayat (1), (2), (3) Perma 13/2016

dapat melindungi data pribadi dalam sistem sehingga mengakibatkan kebocoran data? Hasil yang didapatkan adalah 107 responden (47%) menjawab penegakan melalui hukum pidana; 53 responden (24%) menjawab penegakan melalui hukum administratif; 66 responden (29%) menjawab penegakan melalui hukum perdata.

Grafik 35. Pertanyaan media hukum apa yang paling efektif, dan pantas diberikan kepada Penyelenggara Sistem Elektronik (penyedia jasa layanan aplikasi *Online*) yang terbukti tidak dapat melindungi data pribadi dalam sistem sehingga mengakibatkan kebocoran data?

Sumber: Dokumen Pribadi.

BAB VI

CATATAN KRITIS TERHADAP RUU PELINDUNGAN DATA PRIBADI

RUU Pelindungan Data Pribadi (RUU PDP) hasil pembahasan per Desember 2019 terdiri dari 15 Bab.

a. BAB I KETENTUAN UMUM terdiri dari 2 Pasal . Pada Pasal 1 menjelaskan tentang terminologi-terminologi yang dipergunakan, misalnya terminolgi data pribadi. Pasal 2 menjelaskan tentang pemberlakuan UU PDP, yurisdikis.
b. BAB II JENIS DATA PRIBADI terdiri dari 1 Pasal yang membahas tentang pembagian data pribadi (data pribadi yang bersifat umum dan yang bersifat spesifik);
c. BAB III HAK PEMILIK DATA PRIBADI. Dalam Bab III terdiri dari 12 Pasal. Salah satu hak pemilik data pribadi yakni dalam Pasal 13 RUU PDP Pemilik Data Pribadi berhak menuntut dan menerima ganti rugi atas pelanggaran Data Pribadi miliknya sesuai dengan ketentuan peraturan perundang-undangan.
d. BAB IV PEMROSESAN DATA PRIBADI. Dalam Bab IV ini terdiri dari 5 Pasal. Berdasarkan Pasal 17 ayat (1) pemrosesan data pribadi meliputi: a. perolehan dan pengumpulan; b. pengolahan dan penganalisisan; c. penyimpanan; d. perbaikan dan pembaruan; e. penampilan, pengumuman,

transfer, penyebarluasan, atau pengungkapan; dan/atau f. penghapusan atau pemusnahan.

e. BAB V KEWAJIBAN PENGENDALI DATA PRIBADI DAN PROSESOR DATA PRIBADI DALAM PEMROSESAN DATA PRIBADI. Dalam Bab V ini terdiri dari 23 Pasal. Salah satu pengaturannya yakni, pengendali data pribadi dan prosesor data pribadi meliputi: a. setiap orang; b. Badan Publik; c. Organisasi/Institusi;
f. BAB VI TRANSFER DATA PRIBADI terdiri dari 2 Pasal dan 2 bagian. Bagian Kesatu tentang Transfer Data Pribadi dalam Wilayah Hukum Negara Kesatuan Republik Indonesia dan Bagian Kedua tentang Transfer Data Pribadi Ke Luar Wilayah Hukum Negara Kesatuan Republik Indonesia
g. BAB VII SANKSI ADMINISTRATIF. Bab VII terdiri dari 1 Pasal. Salah satu pengaturannya yakni sanksi administratif berupa: a. peringatan tertulis; b. penghentian sementara kegiatan pemrosesan Data Pribadi; c. penghapusan atau pemusnahan Data Pribadi; d. ganti kerugian; dan/atau e. denda administratif;
h. BAB VIII LARANGAN DALAM PENGGUNAAN DATA PRIBADI. Bab VIII terdiri dari 4 Pasal. Salah satu larangannya yakni "setiap orang dilarang menjual atau membeli data pribadi";
i. BAB IX PEMBENTUKAN PEDOMAN PERILAKU PENGENDALI DATA PRIBADI. Bab IX ini terdiri dari 1 Pasal. Salah satu pengaturannya yakni bahwa "Asosiasi pelaku usaha dapat membentuk pedoman perilaku Pengendali Data Pribadi";
j. BAB X PENYELESAIAN SENGKETA DAN HUKUM ACARA. Bab X ini terdiri dari 1 Pasal. Salah satu pengaturannya yakni Penyelesaian sengketa perlindungan Data Pribadi dilakukan melalui arbitrase, pengadilan, atau lembaga

penyelesaian sengketa alternatif lainnya sesuai dengan ketentuan peraturan perundang-undangan;

k. BAB XI KERJA SAMA INTERNASIONAL. Bab XI terdiri dari 1 Pasal;
l. BAB XII PERAN PEMERINTAH DAN MASYARAKAT. Bab XII terdiri dari 3 Pasal;
m. BAB XIII KETENTUAN PIDANA. Bab XIII terdiri dari 9 Pasal. Salah satu pengaturannya yakni "Setiap Orang yang dengan sengaja menjual atau membeli Data Pribadi sebagaimana dimaksud dalam Pasal 54 ayat (2) dipidana dengan pidana penjara paling lama 5 (lima) tahun atau pidana denda paling banyak Rp50.000.000.000,00 (lima puluh miliar rupiah)."
n. BAB XIV KETENTUAN PERALIHAN. Bab XIV terdiri dari 1 Pasal;
o. BAB XV KETENTUAN PENUTUP. Bab XV terdiri dari 2 Pasal.

Menurut hemat **Penulis,** Indonesia, rakyat Indonesia, pelaku usaha di Indonesia, konsumen baik konsumen Indonesia ataupun konsumen yang menggunakan *marketplace*, penyelenggara sistem elektronik lainnya dalam kehidupan sehari-hari wajib dilindungi baik diberikan terhadap data pribadi yang telah dimasukan/di-*submit* ke dalam sistem elektronik.

Menurut **Setyawati F. Anngraeni** bahwa Peraturan perundang-undangan yang tersedia di Indonesia saat ini tentang perlindungan data pribadi tidak secara komprehensif memberikan perlindungan yang cukup pada data pribadi. Undang-Undang tentang Informasi Elektronik dan Transaksi Elektronik (UU ITE) hanya menyentuh subjek perlindungan data pribadi tanpa adanya ketentuan lebih lanjut tentang rincian pelaksanaan perlindungan tersebut. Selanjutnya, fakta bahwa peraturan tentang perlindungan data diatur

dalam peraturan sektoral juga mengimplikasikan bahwa perlindungan data masih dianggap sebagai masalah minor di Indonesia. Kurangnya rincian tentang pengaturan perlindungan data pribadi menjadikan permasalahan mengenai kepemilikan data menjadi lebih kompleks. Dalam prakteknya, perusahaan teknologi biasanya mengekstrak data dari pengguna sebagai bentuk pertukaran atas layanan gratis yang mereka sediakan[323].

Namun, satu data pribadi tidak banyak bermanfaat bagi perusahaan. Agar data yang dikumpulkan ini memiliki nilai ekonomi, data-data ini perlu diproses, dianalisis dan disempurnakan menjadi big data. Untuk mencapai tujuan ini, perusahaan akan mengklaim kepemilikan atas data pribadi. Sebagai pemilik, perusahaan kemudian akan memiliki hak mutlak untuk mengeksploitasi data pribadi yang dikumpulkan tersebut.

Menurut Menteri Komunikasi dan Informatika (Menkominfo) pada Kabinet Indonesia Maju (2019-sekarang) **Johny G. Plate** sebagaimana dikutip oleh ccn.indonesia.com pada 26-02-2020 berpendapat bahwa banyak kasus pelanggaran data pribadi yang tidak terdeteksi di Indonesia. RUU Perlindungan Data Pribadi merupakan instrumen hukum yang disusun untuk melindungi data pribadi warga Negara dari praktik penyalahgunaan data dan merupakan perwujudan kehadiran Negara dalam melaksanakan amanat konstitusi untuk memberikan perlindungan data pribadi bagi warga Negara[324].

---

[323] Setyawati F. Anggraeni, "Polemik Pengaturan Kepemilkan Data Pribadi: Urgensi Untuk Harmonisasi dan Reformasi Hukum di Indonesia", Jurnal Hukum & Pembangunan 48, No. 4 (2018), hlm. 823-824.

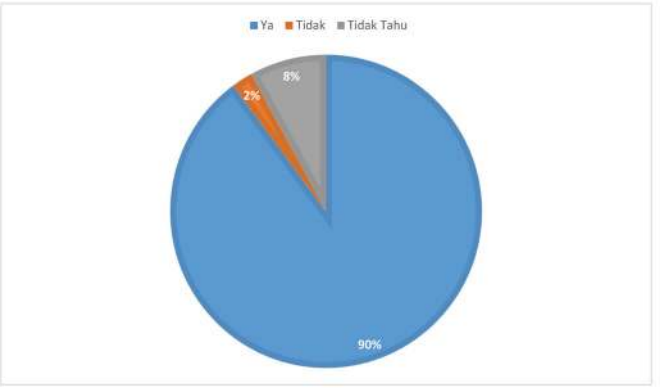
[324] CNN Indonesia, artikel tangal 26-02-2020 "Menkominfo: Kasus Pelanggaran Data Pribadi Sulit Terdeteksi" https://www.cnnindonesia.com/teknologi/20200225204935-185-478090/menkominfo-kasus-pelanggaran-data-pribadi-sulit-terdeteksi diakses tanggal 5 April 2020

Pengaturan perlindungan data pribadi yang bersifat khusus hingga penulisan buku ini disusun (Januari 2020) barulah diatur dalam bentuk Peraturan Menteri, Peraturan Menteri Republik Indonesia No. 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik (Permenkominfo PDPSE). Permenkominfo PDPSE dibentuk untuk melaksanakan ketentuan Pasal 15 ayat (3) Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik[325] (PP tersebut telah dicabut dan diubah dengan PP 71 tahun 2016).

Hingga penulisan buku disusun (Februari 2020), Rancangan Undang-undang tentang Perlindungan Data Pribadi (RUU PDP) masih belum disahkan namun masuk dalam Program Legislasi Nasional.

Berdasarkan pertanyaan yang **Penulis** ajukan kepada responden melalui kuisioner tentang Apakah menurut Saudara, pengaturan pelindungan data pribadi seyogyanya diatur dalam bentuk Undang-undang, bukan hanya dalam bentuk Peraturan Menteri Komunikasi dan Informatika? Hasil yang didapatkan bahwa 203 responden (89%) menjawab ya, 5 responden (2,2%) menjawab tidak dan 18 responden (8%) menjawab tidak tahu.

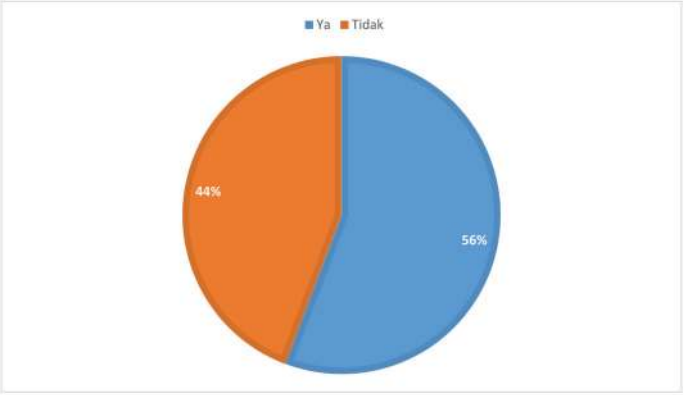
[325] Pasal 15 ayat (3) Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik mengatur bahwa "Ketentuan lebih lanjut mengenai pedoman perlindungan Data Pribadi dalam Sistem Elektronik sebagaimana dimaksud pada ayat (2) diatur dalam Peraturan Menteri."



Grafik 36. Pertanyaan Apakah menurut Saudara, pengaturan pelindungan data pribadi seyogyanya diatur dalam bentuk Undang-undang, bukan hanya dalam bentuk Peraturan Menteri Komunikasi dan Informatika?

Sumber: Dokumen Pribadi.

Penulis juga menanyakan pertanyaan tentang Apakah Saudara/i mengetahui bahwa saat ini Pemerintah (Lembaga Legislatif) sedang menyusun Rancangan Undang-undang Pelindungan Data Pribadi dan telah masuk ke dalam Program Legislasi Nasional Prioritas? Dan hasil yang didapatkan bahwa 126 responden (56%) menjawab tidak tahu sedangkan 100 responden (44%) mennjawab ya.



Grafik 37. Pertanyaan tentang Apakah Saudara/i mengetahui bahwa saat ini Pemerintah (Lembaga Legislatif) sedang menyusun Rancangan Undang-undang Pelindungan Data Pribadi dan telah masuk ke dalam Program Legislasi Nasional Prioritas?

Sumber: Dokumen Pribadi.

I. Catatan Kritis RUU Perlindungan Data Pribadi

Pembentukan perundang-undangan yang baik wajib disertai dengan naskah akademik (NA)[326] yang disusun pula dengan berprinsipkan 'Sistem Hukum Pancasila'[327]. Pada pokoknya, identifikasi masalah dalam suatu NA mencakup empat pokok masalah:

1. Permasalahan yang dihadapi dalam kehidupan berbangsa, bernegara dan bermasyarakat;
2. Mengapa perlu RUU atau Rancangan Peraturan Daerah yang menjadi dasar atau pembenar bagi pemecahan masalah tersebut;

[326] NA dapat diunduh / di-*download* di https://www.bphn.go.id/data/documents/na_perlindungan_data_pribadi.pdf, Penulis mengakses pada tanggal 29 Maret 2020

[327] Teguh Prasetyo, *SIstem Hukum Pancasila..... Op.Cit,* hlm.80.

3. Apa yang menjadi pertimbangan/landasan filosofis, sosiologis, yuridis pembentukan RUU atau Rancangan Perda tersebut?;
4. Apa sasaran yang akan diwujudkan, ruang lingkup, cakupan atau *scope* pengaturan, jangkauan, dan arah pengaturan[328].

Tujuan Naskah Akademik Rancangan Undang-undang Pelindungan Data Pribadi (NA RUU PDP) yakni: a. Merumuskan permasalahan yang dihadapi bangsa Indonesia dalam kehidupan bermasyarakat, berbangsa dan bernegara terkait dengan perlindungan data pribadi serta cara mengatasi permasalahan tersebut. b. Merumuskan permasalahan hukum yang dihadapi sebagai dasar pembentukan Rancangan UndangUndang sebagai dasar hukum penyelesaian atau solusi permasalahan hukum dalam kehidupan bermasyarakat, berbangsa dan bernegara. c. Merumuskan pertimbangan atau landasan filosofis, sosiologis, yuridis pembentukan RUU Pelindungan Data Pribadi. d. Merumuskan sasaran yang akan diwujudkan, ruang lingkup pengaturan, jangkauan, dan arah pengaturan dalam pengaturan, dalam Rancangan Undang-Undang Pelindungan Data Pribadi.

1. **Asas dan Prinsip serta Tujuan.** RUU Pelindungan Data Pribadi (RUU PDP) membedakan asas dan prinsip pelindungan data pribadi. Namun, menurut **Penulis,** walaupun dipisahkan namun keduanya memilki satu kesatuan. Asas yang akan diberlakukan yakni: a. asas pelindungan[329]; b. asas kepentingan umum[330]; c. asas

[328] *Ibid,* hlm. 84-85

[329] Berdasarkan Penjelasan RUU PDP, Yang dimaksud dengan "Asas Pelindungan" adalah pemerintah wajib memberikan pelindungan data pribadi warga negaranya baik di dalam maupun di luar negeri.

[330] Berdasarkan Penjelasan RUU PDP, Yang dimaksud dengan "Asas Kepentingan Umum" adalah bahwa Undang-Undang ini disusun untuk melindungi kepentingan

keseimbangan[331]; d. dan asas pertanggungjawaban[332]. Sedangkan, prinsip pelindungan dan penyelenggaraan data pribadi terdiri dari 9 (sembilan) prinsip. Menurut hemat **Penulis,** kesembilan prinsip ini mencerminkan bahwasanya penyelenggaran data pribadi wajib dilaksanakan secara hati-hati, tepat guna dan *platform*/pengusaha dilarang untuk menyalahgunakan data pribadi tersebut. Dan tujuan pengaturan pelindungan data pribadi terdiri dari 4 (empat) tujuan, menurut hemat **Penulis,** keempat tujuan itu memiliki esensi yang berlandaskan keadilan bermartabat, bahwasnya tujuan RUU PDP untuk memberikan keadilan bemartabat baik bagi konsumen/pengguna ataupun pengusaha/penghimpun data.

2. **Pembagian Data Pribadi**. RUU PDP membagi data pribadi kedalam 2 (dua) bentuk sebagaimana **Penulis** paparkan pada tabel berikut:

No	Data Pribadi yang bersifat Umum	Jenis Data Pribadi yang bersifat umum	Catatan Kritis
1	**Definisi:** data yang berkenaan dengan subyek data sehingga orang lain dapat	1. Nama; 2. Tempat&tanggal lahir; 3. Nomor Kartu Tanda Penduduk, Surat Izin Mengemudi, atau nomor pengenal lainnya;	Menurut hemat **Penulis,** suatu peraturan perundang-undangan 'wajib' memiliki harmonisasi

masyarakat secara luas

[331] Berdasarkan Penjelasan RUU PDP, Yang dimaksud dengan "Asas Keseimbangan" adalah keseimbangan antara hak Privasi dengan hak negara yang sah berdasarkan kepentingan umum.

[332] Berdasarkan Penjelasan RUU PDP, Yang dimaksud dengan "Asas Pertanggungjawaban" adalah Penyelenggaraan Data Pribadi harus dapat dipertanggungjawabkan oleh penyelenggara data pribadi.

No	Data Pribadi yang bersifat Umum	Jenis Data Pribadi yang bersifat umum	Catatan Kritis
	mengetahui identitas seseorang dengan menggunakan salah satu atau kombinasi	4. Data biometric seperti: sidik jari, foto digital atau pindaian retina; atau Data lainnya yang terkait dengan penyelenggaraan data pribadi	terhadap peraturan perundang-undangan lainnya.

Tabel 4. Data Pribadi yang bersifat umum dalam RUU PDP

Sumber: Dokumen Pribadi

No	Data Pribadi yang bersifat Khusus	Jenis
1	Tidak diberikan definisi. Namun menurut hemat **Penulis,** data sensitif adalah data khusus tentang suatu perbuatan hukum atau kondisi seseorang yang diatur dalam peraturan perundang-undangan lainnya.	1. Agama/keyakinan; 2. Kesehatan; 3. Kondisi fisik dan kondisi mental; 4. Biometric; 5. Kebiasaan pribadi; 6. Kehidupan seksual; 7. Pandangan politik; 8. Catatan kejahatan; 9. Data anak; 10. Data keuangan pribadi; dan/atau 11. Data lainnya sesuai dengan ketentuan peraturan perundang-undangan

Tabel 5. Data Pribadi yang bersifat khusus dalam RUU PDP

Sumber: Dokumen Pribadi.

3. **Subyek Hukum/Pihak-Pihak pada RUU PDP. Penulis** akan paparkan pihak-pihak dalam RUU PDP yang mana para pihak tersebut berbeda dengan yang ada di UU ITE.

Pihak-pihak dalam RUU PDP yakni: a. pengendali data pribadi; b. prosesor data pribadi; c. pihak ketiga; d. orang; e. pemilik data pribadi; Instansi Pengawas dan Pengatur Sektor; f. badan publik; g. korporasi; h. pelaku usaha; i. Menteri. **Penulis** akan sandingkan dengan para pihak sebagaimana yang diatur dalam UU ITE *jo.* PP PSTE. Adapun para pihak dalam UU ITE *jo.* PP PSTE yakni: a. penyelenggara sistem elektronik; b. penyelenggara sertifikasi elektronik; c. Lembaga Sertifikasi Keandalan; d. Penanda Tangan; e. Pengirim; f. Penerima; g. Orang; h. Badan Usaha; i. Pemerintah.

No	Para Pihak dalam RUU PDP	Para Pihak dalam UU ITE	Para Pihak dalam PP PSTE
1	**Pengendali data pribadi** adalah pihak yang menentukan tujuan dan melakukan kendali pemrosesan data pribadi.	Tidak mengenal pembagian pengendali data pribadi, prosesor data pribadi. Namun yang diatur ialah **Penyelenggara Sistem Elektronik (PSE)** "setiap Orang, penyelenggara negara, Badan Usaha, dan masyarakat yang menyediakan, mengelola, dan/atau mengoperasikan Sistem Elektronik, baik secara sendiri-sendiri maupun bersama-sama kepada pengguna	Tidak mengenal pembaguan pengendali data pribadi, prosesor data pribadi. Namun yang diatur ialah **Penyelenggara Sistem Elektronik (PSE)** yakni: "setiap Orang, penyelenggara negara, Badan Usaha, dan masyarakat yang menyediakan, mengelola, dan/atau mengoperasikan Sistem Elektronik secara sendiri-sendiri maupun bersama-sama

No	Para Pihak dalam RUU PDP	Para Pihak dalam UU ITE	Para Pihak dalam PP PSTE
		Sistem Elektronik untuk keperluan dirinya dan/atau keperluan pihak lain." (Pasal 1 Angka 6a)	kepada Pengguna Sistem Elektronik untuk keperluair dirinya dan/ atau keperluan pihak lain." (Pasal 1 Angka 4 PP PSTE)
2	**Prosesor Data Pribadi** adalah pihak yang melakukan pemrosesan Data Pribadi atas nama Pengendali Data Pribadi.	Tidak mengenal pembagian pengendali data pribadi, prosesor data pribadi. Namun yang diatur ialah tentang **PSE**.	Tidak mengenal pembaguan pengendali data pribadi, prosesor data pribadi. Namun yang diatur ialah tentang **PSE**. **PP PSTE membagi kedalam 2 jenis PSE yakni: 1. PSE Lingkup Publik dan 2. PSE Lingkup Privat**
3	**Pihak Ketiga** adalah setiap Orang, Badan Publik, dan badan lain selain Pemilik Data Pribadi, Pengendali Data Pribadi, Prosesor Data Pribadi, dan pihak lain yang berada di bawah kendali Pengendali Data Pribadi atau Prosesor Data Pribadi yang memperoleh otorisasi dari Pengendali Data Pribadi atau Prosesor Data	Tidak memberikan definisi Pihak Ketiga. Namun, pengaturan Pihak Ketiga ditemukan pada Pasal 21 ayat (3) UU ITE "Jika kerugian Transaksi Elektronik disebabkan gagal beroperasinya Agen Elektronik akibat tindakan pihak ketiga secara langsung terhadap Sistem Elektronik, segala akibat hukum menjadi tanggung jawab penyelenggara Agen Elektronik."	Definisi Pihak Ketiga Terpercaya dapat ditemukan pada Penjelasan Pasal 9 ayat (3) PP PSTE yakni: "Yang dimaksud dengan "pihak ketiga terpercaya penyimpan kode sumber (*source code escrou*)" adalah profesi atau pihak independen yang berkompeten menyelenggarakan jasa penyimpanan kode sumber program komputer atau Perangkat Lunak untuk

No	Para Pihak dalam RUU PDP	Para Pihak dalam UU ITE	Para Pihak dalam PP PSTE
	Pribadi untuk melakukan pemrosesan Data Pribadi.		kepentingan dapat diakses, diperoleh, atau diserahkan kode sumber oleh penyedia kepada pihak pengguna."
4	**Orang** adalah orang perseorangan, baik warga negara Indonesia, warga negara asing, maupun korporasi.	**Orang** adalah orang perseorangan, baik warga negara Indonesia, warga negara asing, maupun badan hukum (Pasal 1 Angka 21 UU ITE)	**Orang** adalah orang perseorangan, baik warga negara Indonesia, warga negara asing, maupun badan hukum (Pasal 1 Angka 36 PP PSTE)
5	**Pemilik Data Pribadi** adalah orang perseorangan selaku subyek data yang memiliki Data Pribadi secara sah.	Tidak mengenal terminologi pemilik data pribadi, namun yang diatur ialah terminologi **Pengirim. Pengirim** adalah subjek hukum yang mengirimkan Informasi Elektronik dan/ atau Dokumen Elektronik. (Pasal 1 Angka 18)	Tidak mengenal terminologi pemilik data pribadi, namun yang diatur ialah terminologi **Pengirim. Pengirim** adalah subjek hukum yang mengirimkan Informasi Elektronik dan/ atau Dokumen Elektronik. (Pasal 1 Angka 18)
6	**Instansi Pengawas dan Pengatur Sektor** adalah Instansi yang bertugas mengawasi pelaksanaan tugas sektor dan mengeluarkan pengaturan terhadap sektor tersebut.	Tidak mengenal terminologi **Instansi Pengawas dan Pengatur Sektor.** Namun berdasarkan Pasal 40 ayat (3) bahwa Pemerintah menetapkan instansi atau institusi yang memiliki data	Tidak mengenal terminologi **Instansi Pengawas dan Pengatur Sektor.**

No	Para Pihak dalam RUU PDP	Para Pihak dalam UU ITE	Para Pihak dalam PP PSTE
		elektronik strategis yan wajib dilindungi.	
7	**Badan Publik** adalah lembaga eksekutif, legislatif, yudikatif, dan badan lain yang fungsi dan tugas pokoknya berkaitan dengan penyelenggaraan negara, yang sebagian atau seluruh dananya bersumber dari Anggaran Pendapatan dan Belanja Negara dan/atau Anggaran Pendapatan dan Belanja Daerah, atau organisasi nonpemerintah sepanjang sebagian atau seluruh dananya bersumber dari Anggaran Pendapatan dan Belanja Negara dan/atau Anggaran Pendapatan dan Belanja Daerah, sumbangan masyarakat dan/ atau luar negeri.	**Tidak mengenal definisi Badan Publik**	**Tidak mengenal definisi Badan Publik,** Badan Publik sebagaimana diatur dalam Pasal 24 huruf b RUU PDP dengan **Penyelenggara Sistem Elektronik Lingkup Publik**. Misalnya: PSE lingkup Publik wajib melakukan pengelokaan, pemrosesan, dan/ atau penyimpanan sistem elektronik dan data elektronik di wilayah Indonesia (Pasal 20 ayat (2) PP PSTE) sama dengan Pasal 24 huruf b RUU PDP bahwa Pengedali data pribadi dan prosesor data pribadi meliputi a. orang; b. 'badan publik'.
8	**Korporasi** adalah kumpulan terorganisasi dari orang dan/atau kekayaan, baik	**Badan Usaha** adalah perusahaan perseorangan atau perusahaan persekutuan, baik	**Badan Usaha** adalah perusahaan perseorangan atau perusahaan persekutuan, baik

No	Para Pihak dalam RUU PDP	Para Pihak dalam UU ITE	Para Pihak dalam PP PSTE
	badan hukum maupun bukan badan hukum.	yang berbadan hukum maupun yang tidak berbadan hukum. Pasal 1 Angka 22	yang berbadan hukum maupun yang tidak berbadan hukum. Pasal 1 Angka 37.
9	**Pelaku Usaha** adalah orang perseorangan, badan usaha, yang didirikan dan berkedudukan atau melakukan kegiatan dalam wilayah hukum Negara Republik Indonesia, baik sendiri maupun bersama-sama melalui perjanjian menyelenggarakan kegiatan usaha dalam berbagai bidang ekonomi.	**Tidak memberikan definisi Pelaku Usaha.**	**Pelaku Usaha** adalah setiap orang perseorangan atau Badan Usaha, baik berbentuk badan hukum maupun bukan badan hukum, yang didirikan dan berkedudukan atau melakukan kegiatan dalam wilayah hukum Negara Republik Indonesia, secara sendiri-sendiri maupun bersama-sama, melalui perjanjian penyelenggaraan kegiatan usaha dalam berbagai bidang ekonomi. Pasal 1 Angka 28
10	**Menteri** adalah menteri yang menyelenggarakan urusan pemerintahan di bidang komunikasi dan informatika.	Menggunakan terminologi Pemerintah. Namun **Pemerintah** yang dimaksud adalah Menteri atau pejabat lainnya yang ditunjuk oleh Presiden. (Pasal 1 Angka 23)	**Menteri** adalah menteri yang menyelenggarakan urusan pemerintahan di bidang komunikasi dan informatika. (Pasal 1 Angka 39 PP PSTE). Selain Menteri, PP PSTE juga mengatur tentang terminologi

No	Para Pihak dalam RUU PDP	Para Pihak dalam UU ITE	Para Pihak dalam PP PSTE
			"Kementerian" yakni: Kementerian atau Lembaga adalah Instansi Penyelenggara Negara yang bertugas mengawasi dan mengeluarkan pengaturan terhadap sektornya (Pasal 1 Angka 7 PP PSTE)
11	**Tidak Mengatur Terminologi Pengirim dan Penerima**	**Mengatur terminologi Pengirim dan Penerima. Terminologi Pengirim** adalah subjek hukum yang mengirimkan informasi elektronik dan/ atau dokumen elektronik (Pasal 1 Angka 18). **Terminologi Penerima** adalah subjek hukum yang menerima informasi elektronik dan/ atau dokumen elektronik dari Pengirim. (Pasal 1 Angka 19).	**Terminologi Pengirim** adalah subjek hukum yang mengirimkan informasi elektronik dan/ atau dokumen elektronik (Pasal 1 Angka 18). **Terminologi Penerima** adalah subjek hukum yang menerima informasi elektronik dan/ atau dokumen elektronik dari Pengirim. (Pasal 1 Angka 19).
12	**Tidak Mengatur lagi Sertifikasi Elektronik** karena telah diatur dalam UU ITE *jo.* PP PSTE	**Terminologi Penyelenggara Sertifikasi Elektronik** adalah badan hukum	**Terminologi Penyelenggara Sertifikasi Elektronik** adalah badan hukum

No	Para Pihak dalam RUU PDP	Para Pihak dalam UU ITE	Para Pihak dalam PP PSTE
		yang berfungsi sebagai pihak yang layak dipercaya, yang memberikan dan mengaudit Sertifikat Eletkronik. Pasal 1 Angka 10.	yang berfungsi sebagai pihak yang layak dipercaya, yang memberikan dan mengaudit Sertifikat Eletkronik. Pasal 1 Angka 21.
13	**Tidak Mengatur lagi Penanda Tangan** karena telah diatur dalam UU ITE *jo.* PP PSTE	**Terminologi Penanda Tangan** adalah subjek hukum yang terasosiasikan atau terkait dengan tanda tangan elektronik. Pasal 1 Angka 13.	**Terminologi Penanda Tangan** adalah subjek hukum yang terasosiasikan atau terkait dengan tanda tangan elektronik. Pasal 1 Angka 23.
		Tidak mengatur lebih rinci tentang pembuat tanda tangan elektronik.	**Terminologi Perangkat Pembuat Tanda Tangan Elektronik** adalah Perangkat Lunak atau Perangkat Keras yang di-konfigurasi dan digunakan untuk membuat tanda tangan elektronik. Pasal 1 Angka 24.
14	**Tidak Mengatur lagi Lembaga Sertifikasi Keandalan** karena telah diatur dalam UU ITE *jo.* PP PSTE	**Terminologi Lembaga Sertifikasi Keandalan** adalah lembaga independen yang dibentuk oleh professional yang diakui, disahkan dan diawasi oleh Pemerintah dengan kewenangan	**Terminologi Lembaga Sertifikasi Keandalan** adalah lembaga independen yang dibentuk oleh professional yang diakui, disahkan dan diawasi oleh Pemerintah dengan kewenangan

No	Para Pihak dalam RUU PDP	Para Pihak dalam UU ITE	Para Pihak dalam PP PSTE
		mengaudit dan mengeluarkan Sertifikat Keandalan dalam Transaksi Elektronik. Pasal 1 Angka 11.	mengaudit dan mengeluarkan Sertifikat Keandalan dalam Transaksi Elektronik. Pasal 1 Angka 27.
15	**Tidak Mengatur lagi Registri Nama Domain** karena telah diatur dalam UU ITE *jo.* PP PSTE	Tidak memberikan terminologi registri nama domain melainkan hanya memberikan terminologi nama domain. **Terminologi nama domain** adalah alamat internet penyelenggara Negara, orang, badan usaha dan/ atau masyarakat yang dapat digunakan dalam berkomunikasi melalui internet, yang berupa kode atau susunan karakter yang bersifat unik untuk menunjukkan lokasi tertentu dalam internet. Pasal 1 Angka 20.	**Terminologi Registri Nama Domain** adalah penyelenggara yang bertanggung jawab dalam melakukan pengelolaan, pengoperasian, dan pemeliharaan penyelenggaraaan sistem elektronik nama domain. Pasal 1 Angka 32.

No	Para Pihak dalam RUU PDP	Para Pihak dalam UU ITE	Para Pihak dalam PP PSTE
16	**Tidak Mengatur lagi Registrar Nama Domain** karena telah diatur dalam UU ITE *jo.* PP PSTE	**Hanya memberikan terminologi nama domain**	**Terminologi Registrar Nama Domain** adalah orang, badan usaha, atau masyarakat yang menyediakan jasa pendaftaran nama domain.

Tabel 6. Para Pihak dalam RUU PDP, UU ITE, PP PSTE

Sumber: Dokumen Pribadi.

4. Perbuatan yang Dilarang

RUU PDP (naskah pembahasan per Desember 2019) mengatur perbuatan yang dilarang, yakni:

a. Larangan memperoleh atau mengumpulkan Data Pribadi yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum atau dapat mengakibatkan kerugian Pemilik Data Pribadi[333].
b. dilarang secara melawan hukum mengungkapkan Data Pribadi yang bukan miliknya[334].
c. Setiap Orang dilarang secara melawan hukum menggunakan Data Pribadi yang bukan miliknya[335];
d. Setiap Orang dilarang secara melawan hukum memasang dan/atau mengoperasikan alat pemroses atau pengolah data visual di tempat umum atau

[333] Pasal 51 ayat (1) RUU PDP
[334] Pasal 51 ayat (2) RUU PDP
[335] Pasal 51 ayat (3) RUU PDP

fasilitas pelayanan publik yang dapat mengancam dan/atau melanggar pelindungan Data Pribadi[336].

e. Setiap Orang dilarang secara melawan hukum menggunakan alat pemroses atau pengolah data visual yang dipasang di tempat umum dan/atau fasilitas pelayanan publik yang digunakan untuk mengidentifikasi seseorang[337];

f. Setiap Orang dilarang memalsukan Data Pribadi dengan maksud untuk menguntungkan diri sendiri atau orang lain atau yang dapat mengakibatkan kerugian bagi orang lain[338].

g. Setiap Orang dilarang menjual atau membeli Data Pribadi[339].

5. Ketentuan Sanksi

RUU PDP (Naskah pembahasan per Desember 2019) mengatur ketentuan pidana. Pengaturan ini adalah sebagai bentuk pengejawantahan asas legalitas bahwa: 1. Tiada kejahatan tanpa ketentuan pidana dalam peraturan perundang-undangan (*nullum crimen sine lege)*; 2. Tiada pidana/penghukuman tanpa undang-undang (*nulla poena sine lege)*; 3. Tiada pidana/penghukuman tanpa tindak pidana menurut undang-undang (*nulla poena sine cremen)*. Ketentuan pidana dalam RUU PDP sebagai berikut:

a. Ancaman Pidana Penjara dan/atau Pidana Denda

1. Setiap Orang yang dengan sengaja memperoleh atau mengumpulkan Data Pribadi yang bukan

[336] Pasal 52 RUU PDP
[337] Pasal 53 RUU PDP
[338] Pasal 54 ayat (1) RUU PDP
[339] Pasal 54 ayat (2) RUU PDP

miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum atau dapat mengakibatkan kerugian Pemilik Data Pribadi sebagaimana dimaksud dalam Pasal 51 ayat (1) dipidana dengan pidana penjara paling lama 5 (lima) tahun atau pidana denda paling banyak Rp50.000.000.000,00 (lima puluh miliar rupiah)[340];

2. Setiap Orang yang dengan sengaja dan melawan hukum mengungkapkan Data Pribadi yang bukan miliknya sebagaimana dimaksud dalam Pasal 51 ayat (2) dipidana dengan pidana penjara paling lama 2 (dua) tahun atau pidana denda paling banyak Rp20.000.000.000,00 (dua puluh miliar rupiah)[341];
3. Setiap Orang yang dengan sengaja dan melawan hukum menggunakan Data Pribadi yang bukan miliknya sebagaimana dimaksud dalam Pasal 51 ayat (3) dipidana dengan pidana penjara paling lama 7 (tujuh) tahun atau pidana denda paling banyak Rp70.000.000.000,00 (tujuh puluh miliar rupiah)[342].
4. Setiap Orang yang dengan sengaja dan melawan hukum memasang dan/atau mengoperasikan alat pemroses atau pengolah data visual di tempat umum atau fasilitas pelayanan publik yang dapat mengancam atau melanggar pelindungan Data Pribadi sebagaimana dimaksud dalam

[340] Pasal 61 ayat (1) RUU PDP
[341] Pasal 61 ayat (2) RUU PDP
[342] Pasal 61 ayat (3) RUU PDP

Pasal 52, dipidana dengan pidana penjara paling lama 1 (satu) tahun atau pidana denda paling banyak Rp10.000.000.000,00 (sepuluh miliar rupiah)[343];

5. Setiap Orang yang dengan sengaja dan melawan hukum menggunakan alat pemroses atau pengolah data visual yang dipasang di tempat umum dan/atau fasilitas pelayanan publik yang digunakan untuk mengidentifikasi seseorang sebagaimana dimaksud dalam Pasal 53 dipidana dengan pidana penjara paling lama 1 (satu) tahun atau pidana denda paling banyak Rp10.000.000.000,00 (sepuluh miliar rupiah)[344];
6. Setiap Orang yang dengan sengaja memalsukan Data Pribadi dengan maksud untuk menguntungkan diri sendiri atau orang lain atau yang dapat mengakibatkan kerugian bagi orang lain sebagaimana dimaksud dalam Pasal 54 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun atau pidana denda paling banyak Rp60.000.000.000,00 (enam puluh miliar rupiah)[345];
7. Setiap Orang yang dengan sengaja menjual atau membeli Data Pribadi sebagaimana dimaksud dalam Pasal 54 ayat (2) dipidana dengan pidana penjara paling lama 5 (lima) tahun atau pidana denda paling banyak Rp50.000.000.000,00 (lima puluh miliar rupiah)[346].

[343] Pasal 62 RUU PDP
[344] Pasal 63 RUU PDP
[345] Pasal 64 ayat (1) RUU PDP
[346] Pasal 64 ayat (2) RUU PDP

b. Pidana Tambahan

RUU PDP mengatur tentang pidana tambahan berupa perampasan keuntungan dan/atau harta kekayaan yang diperoleh atau hasil dari tindak pidana dan pembayaran ganti kerugian.

Apabila pelaku adalah korporasi maka juga dapat dijatuhi pidana tambahan berupa:

1. perampasan keuntungan dan/atau harta kekayaan yang diperoleh atau hasil dari tindak pidana;
2. pembekuan seluruh atau sebagian usaha Korporasi;
3. pelarangan permanen melakukan perbuatan tertentu;
4. penutupan seluruh atau sebagian tempat usaha dan/atau kegiatan Korporasi;
5. melaksanakan kewajiban yang telah dilalaikan; dan
6. pembayaran ganti kerugian[347].

c. Apabila Pelaku Adalah Korporasi

RUU PDP mengatur tentang apabila pelaku penyalahgunaan data pribadi adalah korporasi maka pidana dapat dijatuhkan kepada pengurus, pemegang kendali, pemberi perintah, pemilik manfaat, dan/atau Korporasi[348]. Pidana yang dapat dijatuhkan terhadap Korporasi hanya pidana denda[349].

d. Ketentuan Pelaksanaan Pidana Denda & Pidana Tambahan Berupa Ganti Kerugian

Penulis akan menguraikan ketentuan pelaksanaan pidana denda & pidana tambahan berupa ganti

[347] Pasal 66 ayat (4) RUU PDP
[348] Pasal 66 ayat (1) RUU PDP
[349] Pasal 66 ayat (2) RUU PDP

kerugian. Jika pengadilan menjatuhkan putusan pidana denda, terpidana diberikan jangka waktu 1 (satu) bulan sejak putusan telah memperoleh kekuatan hukum tetap untuk membayar denda tersebut[350]. Dalam hal terdapat alasan kuat, jangka waktu sebagaimana dimaksud pada ayat (1) dapat diperpanjang untuk waktu paling lama 1 (satu) bulan[351]. Jika terpidana tidak membayar pidana denda dalam jangka waktu sebagaimana dimaksud pada ayat (1) atau ayat (2) maka harta kekayaan atau pendapatan terpidana dapat disita dan dilelang oleh Jaksa untuk melunasi pidana denda yang tidak dibayar[352]. Jika penyitaan dan pelelangan harta kekayaan atau pendapatan sebagaimana dimaksud pada ayat (3) tidak cukup atau tidak memungkinkan untuk dilaksanakan, pidana denda yang tidak dibayar diganti dengan pidana penjara paling lama sebagaimana diancamkan untuk tindak pidana yang bersangkutan[353]. Lamanya pidana penjara sebagaimana dimaksud pada ayat (4) yang ditentukan oleh hakim, dicantumkan dalam putusan pengadilan[354].

Ketentuan diatas juga berlaku dalam hal terdakwa dijatuhi pidana tambahan berupa pembayaran ganti kerugian. Berdasarkan ketentuan peralihan bahwa pada saat RUU PDP ini nantinya berlaku, pihak yang telah melakukan pemrosesan data pribadi, wajib menyesuaikan dengan ketentuan pemrosesan data

[350] Pasal 67 ayat (1) RUU PDP
[351] Pasal 67 ayat (2) RUU PDP
[352] Pasal 67 ayat (3) RUU PDP
[353] Pasal 67 ayat (4) RUU PDP
[354] Pasal 67 ayat (5) RUU PDP

pribadi berdasarkan UU PDP paling lama 2 (dua) tahun sejaka UU PDP diundangkan.

6. Catatan Kritis Pengaturan Perlindungan Data Pribadi Perspektif Keadilan Bermartabat

Data pribadi dalam sistem elektronik adalah "barang seksi" pada abad ke-21. Berbagai perusahaan berlomba-lomba menciptakan aplikasi online yang mewajibkan pengguna memasukkan data pribadinya, seperti nama lengkap, alamat surat elektronik, nomor telepon seluler, dan tanggal lahir. Konsumen pun hanya memiliki dua pilihan: setuju atau tidak. Pada umumnya, konsumen hanya akan memberikan persetujuan tanpa membaca *disclaimer* yang diberikan[355].

Pengaturan perlindungan data pribadi perspektif keadilan bermartabat bertujuan untuk menciptakan suatu pengaturan yang komprehensif, holistik, dan bermanfaat bagi pelaku usaha, konsumen, Negara dan kerjasama antara Negara. Walaupun penyusunan RUU PDP mengacu pada beberapa prinsip internasional dan pada *GDPR* namun menurut hemat **Penulis,** RUU PDP wajib berlandaskan pada nilai *wisdom* nasional, yakni Pancasila. Mengambil beberapa prinsip ataupun nilai internasional adalah baik namun wajib ditekankan bahwasanya nilai luhur Indonesia adalah nilai Pancasila.

Keadilan bermartabat tidak anti dengan *wisdom* internasional. Apabila ada pertentangan dengan nilai internasional dengan nilai-nilai nasional, maka fungsi nilai lokal yakni untuk menyaring nilai internasional tersebut dan

[355] Rizky Karo Karo, "Perkara Kebocoran Data *E-Commerce*", Harian Tempo tanggal 6 Mei 2020, dapat juga diakses dari https://kolom.tempo.co/read/1339150/perkara-kebocoran-data-e-commerce/full&view=ok

mengadaptasinya sesuai dengan nilai-nilai luhur Pancasila (dasar Negara&*way of life)*. Apabila ada pertentangan antara norma di ketentuan internasional dengan hukum positif nasional maka diselesaikan dengan asas-asas hukum dan berpandangan pada keadilan bermartabat.

Pengaturan perlindungan data pribadi yang berperspektif keadilan bermartabat yakni memiliki materi, muatan yang mencerminkan sifat&watak Bangsa Indonesia, menjunjung prinsip *pluralism* dengan tetap menjaga prinsip Negara Kesatuan Republik Indonesia. Selain itu, wajib memiliki nilai keadilan, keadilan yang bermartabat bagi para pihak dalam teknologi, data pribadi, dalam hal ini wajib adil bagi perlindungan konsumen, penyelenggara. Konsumen dalam data pribadi memiliki posisi yang lemah jika menjadi korban karena konsumen harus melawan perusahaan besar/ multinasional sehingga perspektif keadilan bermarabat bertujuan agar RUU PDP nantinya memiliki nilai *equilibrium, harmony* antara peraturan perundang-undangan nasional dan pengaturan internasional. Dan **Penulis** berharap dalam RUU PDP juga diatur tentang panduan dalam menyusun *disclaimer,* klausula baku, perjanjian baku yang tidak menyimpang pada peraturan perundang-undangan lainnya (*harmonized system)*.

Pemerintah, melalui Kementerian yang berwenang juga harus menjadi garda terdepan perlindungan konsumen/pengguna dalam sistem elektronik yang umumnya milik asing, *server*-nya tidak di Indonesia, caranya misalnya memberi *warning* kepada penyelenggara untuk memperbaharui keamanananya atau memberi *warning letters, notice* apabila tidak dapat menjaga data

pribadi sehingga merugikan kepentingan warga Negara Indonesia atau bahkan merugikan keamanan Negara, maka sistem elektornik tersebut, aplikasi *online* dilarang untuk beroperasi lagi di Indonesia (*banned)*. Apabila sudah sampai di tahap itu, maka sudah dapat dipastikan reputasi *(trust)* aplikasi *online* menjadi turun dan kepentingan/keuntungan bisnis dari aplikasi *online* juga akan menurun.

7. Catatan Kritis Penegakan Hukum Perlindungan Data Pribadi Perspektif Keadilan Bermartabat (Hulu-Hilir, Preventif-Kuratif)

Penegakan hukum (*law enforcement)* yang berlandaskan pada hukum positif adalah hal penting dalam sistem penegakan hukum di Indonesia. Amanat Pasal 1 ayat (3) UUD 1945 bahwa Negara Indonesia adalah Negara hukum. Dalam amanat ini mengandung makna penting bahwa perlindungan hukum, perlindungan konsumen, perlindungan pelaku usaha, perlindungan Negara wajib berlandaskan pada hukum dan bermuatan keadilan bermartabat.

Penegakan hukum perlindungan data pribadi wajib 'diselenggarakan dari hulu (awal) hingga hilir (akhir)'. Dimulai dari sisi preventif (pencegahan), pencegahan penyalahgunaan data pribadi dimulai dari sisi perizinan, pendaftaran maka otoritas yang berenang wajib dengan baik melakukan seleksi sesuai standar nasional, standar internasional terhadap penyelenggaraan perlidungan data pribadi. Misalnya, Otoritas Jasa Keuangan menyelenggarakan *Regulatory Sandbox*[356] untuk memastikan Inovasi Keuangan

[356] Berdasarkan Pasal 1 Angka 4 POJK 13/2018. *Regulatory Sandbox* adalah mekanisme pengujian yang dilakukan oleh Otoritas Jasa Keuangan untuk menilai keandalan proses bisnis, model bisnis, instrumen keuangan, dan tata kelola Penyelenggara.

Digital yang sesuai dengan kriteria sebagaimana telah diatur dalam Pasal 4 POJK No. 13/POJK.02/2018 tentang Inovasi Keuangan Digital di Sektor Jasa Keuangan.

Selain itu, penyelenggara sistem elektronik juga wajib menerapkan *self regulatory, self assessment, compliance principle* dan mentaati Peraturan Menteri Komunikasi dan Informatika No. 4 Tahun 2016 tentang Sistem Manejemen Pengamanan Informasi (Permenkominfo 4/2016). Salah satu pengaturannya yakni berdasarkan a. Pasal 10 ayat (1) Permenkominfo 4/2016 bahwa Penyelenggara Sistem Elektronik strategis[357] dan Penyelenggara Sistem Elektronik tinggi[358] wajib memiliki Sertifikat Sistem Manajemen Pengamanan Informasi[359]; b. Pasal 10 ayat (2) Permenkominfo 4/2016 bahwa Penyelenggara Sistem Elektronik rendah[360] dapat memiliki Sertifikat Sistem Manajemen Pengamanan Informasi. Apabila ketentuan Pasal 10 ayat (1) dilanggar maka Menteri[361] dapat memberikan sanksi administratif meliputi: a. teguran tertulis; b. penghentian sementara Nama Domain Indonesia[362].

[357] Berdasarkan Pasal 4 ayat (2) Permenkominfo 4/2016, sistem elektornik strategis merupakan Sistem Elektronik yang berdampak serius terhadap kepentingan umum, Pelayanan Publik, kelancaran penyelenggaraan negara, atau pertahanan dan keamanan negara.

[358] Berdasarkan Pasal 4 ayat (3) Permenkominfo 4/2016, Sistem Elektronik tinggi merupakan Sistem Elektronik yang berdampak terbatas pada kepentingan sektor dan/atau daerah tertentu.

[359] Berdasarkan Pasal 1 Angka 11 Permenkominfo 4/2016, Sertifikat Sistem Manajemen Pengamanan Informasi adalah bukti tertulis yang diberikan oleh Lembaga Sertifikasi kepada Penyelenggara Sistem Elektronik yang telah memenuhi persyaratan.

[360] Berdasarkan Pasal 4 ayat (4) Permenkominfo 4/2016, Sistem Elektronik rendah merupakan Sistem Elektronik lainnya yang tidak termasuk pada ayat (2) dan ayat (3).

[361] Berdasarkan Pasal 1 Angka 19 Permenkominfo 4/2016, Menteri adalah menteri yang menyelnggarakan urusan pemerintahan di bidang komunikasi dan informatika

[362] Pasal 25 ayat (1) Permenkominfo 4/2016

Penegakan hukum (*politie*-Bahasa Belanda) perlindungan data pribadi juga dilakukan pada tahap pelaksanaan, bahwasanya pelaksanaan penegakan hukum juga harus dilakukan dalam pelbagai sudut, jika ada filosofi kuno yang mengatakan, apabila hukumnya (*recht)* baik namun penegak hukumnya tidak maka hukum yang baik tersebut menjadi buruk dan sebaliknya apabila hukumnya dikatakan tidak baik namun apabila penegak hukum baik maka hasil penegakan hukum juga baik. Penegakan hukum yang bermartabat dilandaskan pada sikap professional, penegak hukum menjalankan tugas pokok dan fungsi (tupoksi) sesuai kode etik profesi yang berlaku.

Apabila penegak hukum sudah baik dan professional, namun apabila masyarakat tidak memiliki kesadaran hukum yang baik (*awareness* atau *jurisdisch bewustzjin)* maka data pribadi memiliki potensi bocor karena kecerobohan masyarakat, misalnya: masyarakat yang mudah 'tergoda', percaya terhadap iklan di *SMS*, masyarakat yang bangga meng-*upload* (menggunggah) foto diri dengan KTP atau Kartu Keluarga ke dalam media sosial mereka namun tidak memikirkan akibatnya, apabila foto diri dengan KTP/KK tersebut disalahgunakan. Oleh karena itu, peran penegakan hukum, peran Lembaga Swadaya Masyarakat (LSM), peran Universitas maupun peran otoritas yang berwenang untuk lebih sering lagi melakukan sosialisasi untuk menjaga data pribadi.

Kebocoran data pribadi merupakan perbuatan melawan hukum yang sengaja dilakukan oleh peretas (*hacker/cracker)* ataupun disebabkan oleh kelalaian penyelenggara sistem elektronik yang tidak menjaga sistem keamanan mereka.

konsumen/pengguna berada di sisi lemah. Walapun penyelenggara sistem elektronik telah diberikan sanksi administratif namun hal tersebut tidak menghapuskan tanggung jawab pidana dan perdata[363].

Keadilan bermartabat tidak *vis a vis* tentang menghukum pelaku dan selesai. Keadilan bermartabat berpandangan bahwa penghukuman tidak hanya pada 'sanksi dan tindakan' (*double track system)* namun berpandangan untuk memberikan pendekatan kuratif (*curative approach)*. Konsumen/pengguna aplikasi *online* perlu kepastian bahwa data pribadi dalam sistem aplikasi *online* dijaga dan apabila sudah 'terlanjur' bocor, maka konsumen/pengguna seyogyanya diberikan kompensasi.

Sanksi pemidanaan diberikan untuk membuat efek jera dan wajib diberikan sesuai prinsip keadilan bermartabat. **Penulis** mengapresiasi ketentuan sanksi yang telah disusun dalam RUU PDP pembahasan per Desember 2019 yang bersifat represif tersebut. **Penulis** ingin memberi catatan kritis bahwasanya seyogyanya diatur juga ketentuan yang bersifat **'kuratif',** tindakan untuk memberikan penyadaran kepada pelaku penyalahgunaan data pribadi tersebut untuk memperbaiki kehidupannya. Adapun tindakan tersebut yakni berupa pemberian **'kompensasi'** bagi seluruh penggunan *platform e-commerce,* aplikasi *online*. Kompensasi ini adalah hak pengguna *platform* tersebut. Penghitungan kompensasi berupa uang dihitung oleh lembaga yang berwenang dan diberikan kepada pengguna. Kompensasi dapat berupa apapun yang dapat dinilai dengan uang selama sekian waktu, misalnya

[363] Pasal 100 ayat (5) PP PSTE

konsumen/pengguna mendapatkan potongan harga selama 12 (dua belas) bulan berturut-turut atau kompensasi berupa bebas akses pengurangan paket data internet untuk mengakses aplikasi tersebut atau mendapatkan jaminan keamanan data dengan pembaharuan sistem keamanan.

Apabila dalam ilmu hukum pidana dikenal dengan ***double track system*** yang berarti penggabungan model antara sanksi pidana dengan sanksi tindakan (*maatregel)* dan bertujuan untuk mengakomodasi penggabungan sifat hukum pidana yang berupa pencelaan dengan pembinaan melalui tindakan sama-sama dilaksanakan dan bersifat sementara. Misal, contoh sanksi tindakan sebagaimana dalam Undang-undang No. 11 Tahun 2012 tentang Sistem Peradilan Pidana Anak (UU SPPA) yakni: a. pengembalian kepada orang tua/wali; b. penyerahan kepada seseorang; c. perawatan di rumah sakit jiwa; d. perawatan di LPKS (Lembaga Penyelenggaraan Kesejahteraan Sosial) ; e. kewajiban mengikuti pendidikan formal dan/atau pelatihan yang diadakan oleh pemerintah atau badan swasta; f. pencabutan surat izin mengemudi; dan/atau g. perbaikan akibat tindak pidana.

Oleh karenanya, dalam RUU PDP juga seyogyanya diatur ketentuan mengenai tindakan dan ketentuan yang bersifat koeratif sehingga menjadi kebaharuan (*novelty)* yakni UU yang menganut *triple track system*. Sanksi pemidanaan, tindakan dan perbuatan kuratif berupa pemulihan/kompensasi bagi pengguna yang menjadi korban pencurian data.

Ketentuan tindakan ini juga dapat digabungkan dengan ketentuan koeratif, misalnya apabila pelaku penyalahgunaan

data pribadi berupa kebocoran data pribadi dihukum untuk menghentikan sementara layanan sistem mereka untuk diperbaiki dan selama penghentian (*undermaintenance)* tersebut pengguna diberikan kompensasi karena dalam toko *online* tersebut terdapat penjual yang usaha penjualanya terhenti sementara waktu.

BAB VII
TIPS PELINDUNGAN DATA PRIBADI

Penulis akan paparkan tips kepada pembaca untuk melindungi data pribadinya dalam sistem elektronik.

1) Berikan *PIN (Personal Identification Number*) atau cara mengunci lainnya pada ponsel / laptop / gawai (*gadget)* Saudara/i.
2) Pergunakan kombinasi kata sandi/*password* yang sulit, misalkan dengan kombinasi huruf besar, simbol, angka. Jangan pergunakan, nama lengkap, tanggal lahir. Penulis dapatkan data dari pertanyaan kuisioner (apakah saudara/I menggunakan *password (*kata sandi) yang mudah diingat?) yang **Penulis** sebar *online* dan hasilnya bahwa 51% (115 responden) telah menggunakan kata sandi *(password)* yang sangat sulit,berupa kombinasi huruf besar,huruf kecil, simbol, angka namun 49% (111 responden) menggunakan kata sandi yang mudah diingat.

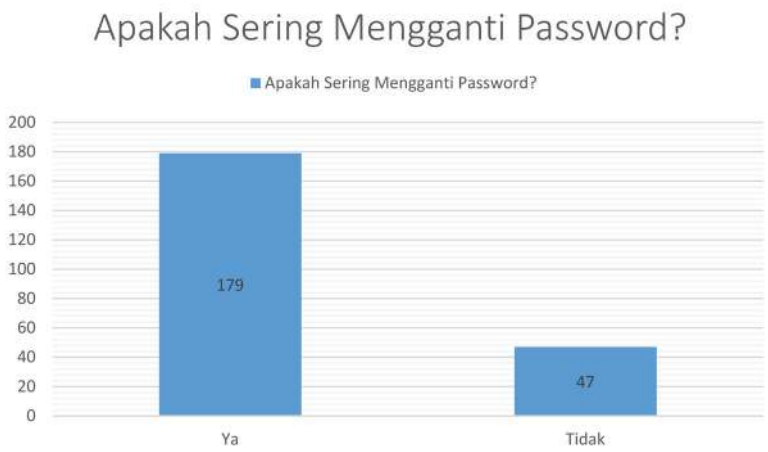
Grafik 38. Penggunaan *Password*
Sumber: Dokumen Pribadi.

3) Perbaharui *password/*kata sandi aplikasi *online*-mu secara berkala. **Penulis** dapatkan data dari pertanyaan kuisioner

(Apakah saudara/i sering mengganti Password (kata sandi) pada seluruh aplikasi online yang saudara/I gunakan secara berkala?) yang **Penulis** sebar *online* dan hasilnya bahwa 79% (179 responden) menjawab tidak sedangkan 21% (47 responden) menjawab ya.

Grafik 39. pertanyaan 'apakah sering mengganti *password*?'
Sumber: Dokumen pribadi.

Berdasaran pertanyaan **Penulis** tentang 'setiap berapa lama Saudara/I mengganti *password* (kata sandi) pada seluruh aplikasi *online* yang Saudara/I gunakan? Dan hasilnya adalah 111 responden(49%) Tidak Pernah Dari WaktuMembuat Password Pertama kali; sedangkan 73 responden (32%) menjawab mengganti *password* lebih dari 6 bulan; 28 responden menjawab dalam waktu 4-6 bulan; 14 responden (6%) menjawab dalam rentang 2-3 bulan.



Grafik 40. Skala Waktu Penggantian *Password*.
Sumber: Dokumen Pribadi.

4) Hindari menuliskan *password* dan menempelnya di kartu *ATM/Debit Card atau Credit Card*. Hal ini untuk menghindari apabila dompet terjatuh maka kartu *ATM* tersebut tidak disalagunakan. Dan apabila kehilangan segeralah telepon *call center* yang resmi untuk menonaktifkan kartu tersebut;
5) Pergunakan *anti-virus* pada perangkat ponsel atau laptop Saudara/I;
6) Jangan mengakses situs internet yang tidak jelas, tidak valid, atau mencurigakan;
7) Jangan meng-klik tautan/link yang diberikan di *e-mail,* nomor telepon yang umumnya berisi penipuan 'selamat Anda memenangkan hadiah maka silahkan klik link berikut;
8) Apabila Saudara/i mendapatkan link dari oknum yang mengatasnamankan instansi resmi, pastikan bahwa link tersebut adalah valid, resmi. Pada umumnya, link bank yang resmi diawali dengan https:// dan memiliki simbol gembok/kunci di bagian paling kiri.

9) Jangan menggunakan free-WIFI, internet publik untuk melakukan transaksi elektronik;

10) *Install* aplikasi yang resmi, atau banyak diunduh/*downloads* oleh *user*.

11) Dilarang untuk menggunggah data pribadi berupa foto Kartu Tanda Penduduk (KTP), Kartu Keluarga (KK), Paspport, Tiket Pesawat ke media sosial Saudara/i untuk menghindari penyalahgunaan dari oknum yang jahat.

DAFTAR PUSTAKA

BUKU

Basah, Sjachrab, *Eksistensi dan Tolak Ukur Badan Peradilan Administrasi di Indonesia* (Yogyakarta; Pustaka Pelajar, 1998).

Bemmelen, Van, *Ons Strafrecht 1, het matierele strafrecht algemeen deel, zesde herzien druk, H.D. Tjeenk Willink,* Gronengen, 1979.

*Centre for Innovation Policy and Governance, Big Data, Kecerdasan Buatan, Blockchain, dan Teknologi Finansial di Indonesia, Usulan Desain, Prinsip dan Rekomendasi Kebijakan, (*Jakarta: CIPG, 2018),

Darus Badrulzaman, Mariam, *Perjanjian Kredit Bank,* (Bandung: Alumni Bandung, 1989).

E. Gindin, Susan, *"Lost and Found in Cyberspace: Informational Privacy in the Age of the Internet," San Diego Law Review* 1153 (1997).

Fuster, G G, Fuster *The Emergence of Personal Data Protecton as a Fundamental Right of the EU (Cham: Springer Internatonal Publishing,* 2014*).*

Harahap, Yahya *Segi-segi Hukum Perjanjian* (Bandung: Alumni, Cetakan Kedua, 1986)

HR, Ridwan, *Hukum Administrasi Negara* (Jakarta: Rajagrafindo Persada, 2006).

HR, Ridwan, *Hukum Administrasi Negara* (Yogyakarta: UII Press, 2003).

Karo Karo, Rizky, *Penegakan Hukum Kejahatan Dunia Maya (Cybercrime) Melalui Hukum Pidana,* (Karawaci: Penerbit Fakultas Hukum Universitas Pelita Harapan, 2019).

Kementerian Kesehatan RI, Direktorat Jenderal Pencegahan dan Pengendalian Penyakit (P2P), Maret 2020.

Kementerian Perindustrian, "Making Indonesia 4.0." yang telah disampaikan pada Seminar Nasional Standardisasi Badan Standardisasi Nasional (BSN), Surabaya 25 Oktober 2018.

Laden Marpaung, Leden*, Asas-Teori-Praktik Hukum Pidana*, (Jakarta: Sinar Grafika, 2005).

Lamintang, P.A.F, *Dasar-Dasar Hukum Pidana Indonesia*, (Bandung: Sinar Baru,1984).

Makarim, Edmon, *Pengantar Hukum Telematika Suatu Kompilasi Kajian* (Jakarta: PT RajaGrafindo Persada, 2005)

Mertokusumo, Sudikno,, *Mengenal Hukum Suatu Pengantar*, edisi keempat, Cetakan Peratama (Yogyakarta: Liberty, 1996)

Nawawi Arief, Barda "Pemidanaan", *Masalah-Masalah Hukum,* No. 16, 1974.

Nawawi Arief, Barda, Masalah Penegakan Hukum & Kebijakan Penanggulangan Kejahatan, (Bandung: Citra Aditya Bakti, 2001).

Nawawi Arief, Barda, Tindak Pidana Mayantara Perkembangan Kajian Cyber Crime di Indonesia, (Jakarta: PT Raja Grafindo Persada, 2007).

OECD, "OECD dan Indonesia", Oktober 2018, Perancis: Global Relations Secretariat.

Paterson, Moira *and* McDonagh, Maeve, "*Data Protection in an Era of Big Data: The Challenges Posed by Big Personal Data".* Monash University Law Review (Vol 44, No 1).

Poernomo, Bambang, *Pelaksanaan Pidana Penjara dengan Sistem Pemasyarakatan,* (Yogyakarta: Liberty Yogyakarta, 1986).

Prasetyo, Teguh, *Hukum Pidana*, Edisi Revisi, Cetakan ke-9, (Depok: PT RajaGrafindo Persada, 2018).

Prasetyo, Teguh, *Keadilan Bermartabat: Perspektif Teori Hukum,* Edisi Pertama, Cetakan ke-I, (Bandung: Nusa Media, 2015).

Prasetyo, Teguh, *Kriminalisasi dalam Hukum Pidana,* (Bandung: Penerbit Nusa Media, 2010).

Prasetyo, Teguh, *Pengantar Ilmu Hukum,* Edisi Pertama, Cetakan ke-I, (Depok: PT RajaGrafindo Persada, 2018),

Prasetyo, Teguh, *Sistem Hukum Pancasila (Sistem, Sistem Hukum, dan Pembentukan Peraturan Perundang-undangan di Indonesia) Perspektif Teori Keadilan Bermartabat*, (Bandung: Penerbit Nusa Media, 2016),

Prodjodikoro, Wirjono, *Asas-asas Hukum Perjanjian* (Bandung: Sumut Pustaka, 2012).

Purbacaraka, Purnadi, & Soekanto, Soerjono, *Perihal Kaidah Hukum*, Cetaka Pertama (Bandung: Alumni, 1978)

Rahardjo, Budi, *Keamanan Sistem Informasi Berbasis Internet,* (Bandung: PT Insan Komunikasi Indonesia, 2002).

S'to, Certified Ethical Hacker 100% Illegal, (Jakarta: Penerbit Jasakom;.2009).

Saleh, Roeslan, *Mencari Asas-Asas Umum yang Sesuai untuk Hukum Pidana Nasional,* Kumpulan Bahan *Upgrading* Hukum Pidana, Jiid 2, 1971,

Soehino, *Ilmu Negara,* (Yogyakarta, Liberty, 1984, edisi ketiga),

Subekti, *Pokok-pokok Hukum Perdata* (Jakarta: PT Intermasa, 1980

Sutedi, Andrian, *Hukum Perizinan dalam Sektor Pelyanan Publik* (Jakarta; Sinargrafika, 2010).

JURNAL

Anggraeni, Setyawati F., "Polemik Pengaturan Kepemilkan Data Pribadi: Urgensi Untuk Harmonisasi dan Reformasi Hukum di Indonesia", Jurnal Hukum & Pembangunan 48, No. 4 (2018). Dapat juga diakses di http://jhp.ui.ac.id/index.php/home/article/view/1804

Custers, Bart *and* Overwater, Lara, "*Regulating Initial Coin Offerings an Cryptocurrencies: A Comparison of Different Approaches Nine Jurisdictions Worldwide",* (*European Journal of Law and Technology, Vol 10, Issue 3, 2019)*, diakses dari http://ejlt.org/article/view/718/981 tanggal 19 Mei 2020

Devins, Caryn, Fellin, Teppi, Kauffman, Stuart & Koppl, Rogel, "*The Law and Big Data" (*CORNELL JOURNAL OF LAW AND PUBLIC POLICY [Vol. 27:357]), diakses dari https://scholarship.law.cornell.edu/cjlpp/vol27/iss2/3/

Froomkin, A. Michael, "Big Data: Destroyer of Informed Consent", (YALE JOURNAL OF LAW AND TECHNOLOGY 21:3 (2019)), diakses dari https://yjolt.org/big-data-destroyer-informed-consent

Inggarwati, M. P., Celia, O., & Arthanti, B. D. (2020). Online Single Submission For Cyber Defense and Security in Indonesia. *Lex Scientia Law Review*, *4*(1), 89-102. https://journal.unnes.ac.id/sju/index.php/lslr/article/view/37709/16023

Jenkins, Jonathan, *"What Can Information Technology Do for Law?", Harvard Journal of Law&Technology, Vol. 21, No. 2, (Harvard University, Massachusetts,* 2008 diakses dari http://jolt.law.harvard.edu/articles/pdf/v21/21HarvJLTech589.pdf

Kumar, K. Mohan, *and* BalaMurugan, G. "*Comparative Study on One Time Password Algirthms"* (*Interntional Journal of Computer Science and Mobile Computing, Vol. 7, Issue 8, Aug 2018, pg. 37-52),* dapat diakses di https://ijcsmc.com/docs/papers/August2018/V7I8201811.pdf, diakses tanggal 4 April 2020

Laney, Doug,, '3D Data Management: Controlling Data Volume, Velocity, and Variety' on Gartner Blog Network (6 February 2001) dapat diakses dari https://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf

M. H,Muaziz., & Busro, A. (2015). Pengaturan Klausula baku dalam hukum perjanjian untuk mencapai keadilan berkontrak. *Law Reform*, *11*(1), Dapat diakses di https://ejournal.undip.ac.id/index.php/lawreform/article/view/15757/11772

Maltzan, Stephanie von, *"No Contradiction between Cyber-Security and Data Protection? Designing a Data Protection compliant Incident Response System" (United Kingdom: European Journal of Law and Technology, Vo.10,Issue 1, 2019)* dapat diakses di http://ejlt.org/article/view/665/893, diakses tanggal 17 April 2020

Manheim, Karl *and* Kaplan, Lyric*, "Artificial Intelligence: Risks to Privacy and Democracy",* (The Yale Journal of Law&Technology, Vol. 21) diakses dari https://yjolt.org/sites/default/files/21_yale_j.l._tech._106_0.pdf

Mostert, Menno,. Bredenoord, Annelien, Sloot, L.Bart van der, Delden, Johannes J.M. van, "From Privacy to Data Protection in the EU: Implications for Big Data Health Research", european Journal of health law 25 (2018) 43-55 diakses dari https://brill.com/view/journals/ejhl/25/1/article-p43_43.xml?language=en&body=citedBy-29618

Prasetyo, Teguh, "Kejahatan Pertambangan Dalam Perspektif Keadilan

Bermartabat", Jurnal PERSPEKTIF Vol XXI No. 1 Tahun 2016 Edisi Januari, Nomor ISSN Cetak 1410- 3648 dan ISSN Online 2406-7385. Dapat diakses di http://oaji.net/articles/2017/4674-1495772027.pdf

Rusell and Norvig (2009, *Artificil Intelligence: A Modern Approach (3rd edition).* http://ejlt.org/article/view/675/915

Sova Pal (Bera) "*Overview of Hacking"* (IOSR Journal of Computer Engineering (IOSR-JCE), Volume 18, Issue 4, Ver. IV (Jul.-Aug. 2016)), hlm. 90. Dapat diakses di http://www.iosrjournals.org/iosr-jce/papers/Vol18-issue4/Version-4/N1804049092.pdf

Vetterman, Oliver, "*Self-made data protection – is it enough? Prevention and after care of identity theft" (United Kindgom:* European Journal of Law and Technology, Vol.10, Issue 1, 2019) diakses dari http://ejlt.org/article/view/673/911 tanggal 5 Mei 2020

Wardoyo, Siswo, Fahrizal,Rian, Imanullah, Zaldi, "Aplikasi Teknik Enkripsi dan Dekripsi *File* dengan Algoritma *Blowfish* pada Perangkat *Mobile* berbasis *Android",* Jurnal Setrum Vol. 3, No. 1 Juni 2014, Universitas Sultan Ageng Tirtayasa Cilegon, dapat diakses di http://jnte.ft.unand.ac.id/index.php/jnte/article/view/199

Zarsky, Tal Z, *'Desperately Seeking Solutions: Using Implementation Based Solutions for the Troubles of Information Privacy in the Age of Data Mining and the Internet Society' (2004)* 56 Maine Law Review 13 . dapat diakses dari https://digitalcommons.mainelaw.maine.edu/mlr/vol56/iss1/3/

PUTUSAN HAKIM

Putusan Mahkamah Konstitusi RI No. 20 / PUU – XIV / 2016

Putusan Mahkamah Konstitusi No. 4/PUU-V/2007

NASKAH AKADEMIK

Naskah Akademik Rancangan Undang-undang Pelindungan Data Pribadi dapat diunduh / di-*download* di https://www.bphn.go.id/data/documents/na_perlindungan_data_pribadi.pdf

RANCANGAN PERATURAN

Rancangan Surat Edaran OJK Nomor .. /SEOJK.05/2017 tentang Pendaftaran, Perizinan Usaha dan Kelembagaan Penyelenggara Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi (**PEN-**Hingga penyusunan buku ini, April 2020, SE ini masih dalam bentuk Rancangan). Diakses dari https://www.ojk.go.id/id/regulasi/otoritas-jasa-keuangan/rancangan-regulasi/Documents/LAMPIRAN%20%20RSEOJK%20Pendaftaran%20dan%20Perizinan%20v3%20(Dengar%20%20Pendapat).pdf

Rancangan Undang-undang tentang Kitab Undang-undang Hukum Pidana (Pembahasan September 2019)

Rancangan Undang-undang tentang Pelindungan Data Pribadi (Pembahasan per Desember 2019)

KAMUS

Black's Law Dictonary 9th edition

Kamus Besar Bahasa Indonesia (KBBI)

LAPORAN HASIL PENELITIAN

Teguh Prasetyo, Rizky Karo Karo, Vena Pricilia, "Urgensi Pembentukan Peraturan Hukum tenang Pemanfaatan Teknologi *Blockchain* di Indonesia", Laporan Hasil Penelitian, Lembaga Penelitian dan Pengabdian Masyarakat (LPPM) Universitas Pelita Harapan (UPH), Juli 2019. Hlm. 1.

ARTIKEL SURAT KABAR

Karo Karo, Rizky, Artikel "Kejahatan Siber Perbankan", Kolom Opini Harian di Kompas tanggal 27 Juli 2018, dapat juga diakses dari https://kompas.id/baca/opini/2018/07/27/kejahatan-siber-perbankan/

Karo Karo, Rizky, "Perkara Kebocoran Data *E-Commerce"*, Kolom Pendapat di Harian Tempo tanggal 6 Mei 2020, dapat juga diakses dari https://kolom.tempo.co/read/1339150/perkara-kebocoran-data-e-commerce/full&view=ok

Harian Kompas, edisi cetak, tanggal 11 Mei 2019 “Data Pribadi Dijual Bebas”.

Harian Kompas, edisi cetak, tanggal 11 Mei 2019 “Dari Alamat hingga Nama Ibu Kandung”

SUMBER INTERNET

Adiya Jaya, “ Data 91 juta Pengguna Tokopedia Diduga Bocor, Media Asing Ikut Soroti” artikel tanggal 3-5-2020 https://www.kompas.com/global/read/2020/05/03/133257970/data-91-juta-pengguna-tokopedia-diduga-bocor-media-asing-ikut-soroti?page=all diakses tanggal 8 Mei 2020

Ahmad Naufal, “ Jalan Panjang Brexit, Keluarnya Inggris dari Uni Eropa” artikel tanggal 1-Februari 2020, https://www.kompas.com/tren/read/2020/02/01/165308965/jalan-panjang-brexit-keluarnya-inggris-dari-uni-eropa?page=all diakses tanggal 10 Februari 2020

Bill Clinten “*Facebook* Resmi Didenda Rp 70 Triliun, Terbesar Dalam Sejarah” diakses dari https://tekno.kompas.com/read/2019/07/25/06510077/facebook-resmi-didenda-rp-70-triliun-terbesar-dalam-sejarah?page=all#page3 diakses tanggal 2 Februari 2020

Bill Clinten “Lebih dari 500.000 Akun *Zoom* Curian Dijual di Pasar Gelap Internet, diakses dari https://tekno.kompas.com/read/2020/04/15/10240047/lebih-dari-500.000-akun-zoom-curian-dijual-di-pasar-gelap-internet?page=all#page3 diakses tanggal 8 Mei 2020

CNN Indonesia “13 Juta Data Bocor Bukalapak Dijual di Forum *Hacker”* artikel tanggal 6 Mei 2020, diakses dari https://www.cnnindonesia.com/teknologi/20200506065657-185-500477/13-juta-data-bocor-bukalapak-dijual-di-forum-hacker? Diakes tanggal 22 Mei 2020

CNN Indonesia “Risiko Ketika Data Prbadi Dicuri” artikel tanggal 27 Desember 2018, diakses dari https://www.cnnindonesia.com/teknologi/20181226210103-185-356593/risiko-ketika-data-pribadi-dicuri diakses tanggal 1 Maret 2020

CNN Indonesia, 3 April 2020 “Celah Aplikasi Zoom Disebut Rawan Curi Data Wajah Pengguna “ https://www.cnnindonesia.com/teknologi/20200403073335-185-489837/celah-aplikasi-zoom-disebut-rawan-curi-data-wajah-pengguna diakses tanggal 5 April 2020

CNN Indonesia, artikel tangal 26-02-2020 “Menkominfo: Kasus Pelanggaran

Data Pribadi Sulit Terdeteksi" https://www.cnnindonesia.com/teknologi/20200225204935-185-478090/menkominfo-kasus-pelanggaran-data-pribadi-sulit-terdeteksi diakses tanggal 5 April 2020

CNN Indonesia, artikel tanggal 10-12-2018, "3,9 Miliar Orang di Dunia Telah Terhubung Internet" diakses dari https://www.cnnindonesia.com/teknologi/20181210094556-192-352374/39-miliar-orang-di-dunia-telah-terhubung-internet diakses tanggal 8 Mei 2020

Devina Halim, "Tersangka Jual Beli Data Kependudukan Raup Untung Rp250.000 per hari", artikel tanggal 15-08-2019, diakses dari https://nasional.kompas.com/read/2019/08/15/21362431/tersangka-jual-beli-data-kependudukan-raup-untung-rp-250000-per-hari tanggal 7 Mei 2020

Devina Halim,, "Polri: Kasus Jual-Beli Data Pribadi di *WEB* berbeda dengan di *Grup Facebook* diakses dari https://nasional.kompas.com/read/2019/08/16/08272631/polri-kasus-jual-beli-data-pribadi-di-web-berbeda-dengan-di-grup-facebook tanggal 7 Mei 2020

Dwi H, "Indonesia Peringkat Kelima Dunia dalam Jumlah Pengguna Internet", artikel tanggal 11-09-2019 diakses dari https://databoks.katadata.co.id/datapublish/2019/09/11/indonesia-peringkat-kelima-dunia-dalam-jumlah-pengguna-internet diakses tanggal 8 Mei 2020

FAQ: Kategori Pengguna/Konsumen. Otoritas Jasa Keuangan, dapat diakses di https://www.ojk.go.id/id/berita-dan-kegiatan/publikasi/Documents/Pages/-FAQ-Terkait-Layanan-Pinjam-Meminjam-Uang-Berbasis-Teknologi-Informasi---Kategori-Konsumen/FAQ%20LPMUBTI%20-%20Kategori%20Konsumen.pdf

Fitri N.H., artikel tanggal 24 September 2019 berjudul "Data Penumpang Lion Air Bocor, UU Perlindungan Data Pribadi Dibutuhkan", https://www.hukumonline.com/berita/baca/lt5d8947d7aa783/data-penumpang-lion-air-bocor--uu-perlindungan-data-pribadi-dibutuhkan/ diakses tanggal 9 Februari 2020

https://en-gb.facebook.com/about/privacy diakses tanggal 11 Mei 2020

https://europa.eu/european-union/about-eu/countries_en diakses tanggal 10 Februari 2020

https://faq.whatsapp.com/id/android/28030015/ diakses tanggal 11 Mei 2020

https://medium.com/@UnibrightIO/blockchain-evolution-from-1-0-to-4-0-3fbdbccfc666 diakses tanggal 10 Januari 2019

https://www.afpi.or.id/about diakses tanggal 4 Februari 2020

https://www.britannica.com/event/Industrial-Revolution diakses tanggal 1 Maret 2020

https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/what-is-social-engineering diakses tanggal 22 Mei 2020

https://www.isms.online/iso-27001/ diakses tanggal 2 Januari 2020

https://www.its.ac.id/news/2019/06/13/bagaimana-industri-4-0-dan-society-5-0-bantu-ciptakan-kesejahteraan/, diakses tanggal 20 Maret 2020

https://www.kominfo.go.id/content/detail/16657/disinformasi-4-juta-data-pengguna-tokopedia-disebut-bocor-dan-dijual/0/laporan_isu_hoaks diakses tanggal 20 Mei 2020

https://www.oecd.org/about/ diakses tanggal 24 Maret 2020

https://www.oecd.org/about/members-and-partners/ diakses tanggal 25 Maret 2020

https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotection-ofprivacyandtransborderflowsofpersonaldata.htm diakses tanggal 25 Maret 2020

https://www.resolver.com/resource/physical-and-cybersecurity-defense-how-hybrid-attacks-are-raising-the-stakes/ diakses tanggal 22 Mei 2020

Ihsanuddin, 16 Maret 2020, "Jokowi: Kerja dari Rumah, Belajar dari Rumah, Ibadah di Rumah Perlu Digencarkan", https://nasional.kompas.com/read/2020/03/16/15454571/jokowi-kerja-dari-rumah-belajar-dari-rumah-ibadah-di-rumah-perlu-digencarkan dakses tanggal 5 April 2020

Implementation Guidline ISO/IEC 27001: 2013. A Practical guideline for Implementing an ISMS in Accordance with The International Standard ISO/ IEC 27001: 2013, hlm. 19

Kevin Rizky, "Tuntut Skandal *Cambridge Analytica, Autralia Tuntut Facebook Rp 7 Triliun",* artikel tanggal 14-03-2020 diakses dari https://tekno.kompas.com/read/2020/03/14/12090007/buntut-skandal-cambridge-analytica-australia-tuntut-facebook-rp-7-triliun diakses tanggal 8 Mei 2020

Leski R “Ada Indikasi Kebocoran Data, Kominfo Minta Tokopedia Lakukkan Tiga Hal Ini”, artikel tanggal 4 Mei 2020, diakses di https://aptika.kominfo.go.id/2020/05/ada-indikasi-kebocoran-data-kominfo-minta-tokopedia-lakukan-tiga-hal-ini/ diakses tanggal 22 Mei 2020

Liberty Jemadu, artikel tanggal 26 September 2019, “Kominfo: 150.000 WNI jadi Korban Kasus Kebocoran Data Lion Air Group”, https://www.suara.com/tekno/2019/09/26/194122/kominfo-150000-wni-jadi-korban-kasus-kebocoran-data-lion-air-group diakses tanggal 9 Februaru 2020

M. Khiry Alfarizi “Begini Cara Kerja Enkripsi End-to-end Whatsapp” artikel tanggal 11 Januari 2019 https://tekno.tempo.co/read/1163636/begini-cara-kerja-enkripsi-end-to-end-whatsapp/full&view=ok diakses tanggal 11 Mei 2020

Maizal W (Reproter) “Penggunaan Data Pribadi Pengguna P2P lending diatur oleh OJK dan AFPI” artikel tanggal 22 Juli 2019, diakses di https://keuangan.kontan.co.id/news/penggunaan-data-pribadi-pengguna-p2p-lending-diatur-oleh-ojk-dan-afpi diakses tanggal 3 Februari 2020

OJK, “SMS Palsu Mengganggu? Laporkan Saja!, https://sikapiuangmu.ojk.go.id/FrontEnd/CMS/Article/375 diakses tanggal 9 Februari 2020

Putri Zakia S, “Bahaya yang Mengintai di Balik Penggunaan Zoom”, artikel tanggal 2 April 2020, diakses dari https://tekno.kompas.com/read/2020/04/02/20340017/bahaya-yang-mengintai-di-balik-penggunaan-zoom diakses tanggal 22 Mei 2020

Tim CNN Indonesia, “Waspada Aksi Jual Beli Data Pribadi Lewat Aplikai Fintech”, artikel tanggal 29 Juli 2019 diakses di https://www.cnnindonesia.com/teknologi/20190729082602-185-416323/waspada-aksi-jual-beli-data-pribadi-lewat-aplikasi-fintech diakses tanggal 4 Februari 2020

Yudha Pratomo, “Kebocoran Data 15juta Pengguna, Pengakuan Tokopedia, dan analisis ahli, artikel tanggal 3 Mei 2020 diakses dari https://tekno.kompas.com/read/2020/05/03/03330087/kebocoran-data-15-juta-pengguna-pengakuan-tokopedia-dan-analisis-ahli?page=all#page4 diakses tanggal 20 Mei 2020

Yudha Pratomo, “Kebocoran Data 15juta Pengguna, Pengakuan Tokopedia, dan analisis ahli, artikel tanggal 3 Mei 2020 diakses dari https://tekno.kompas.com/read/2020/05/03/03330087/kebocoran-data-15-juta-

pengguna-pengakuan-tokopedia-dan-analisis-ahli?page=all#page4 diakses tanggal 20 Mei 2020

INDEKS

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

Y

Z

LAMPIRAN
(Daftar Pertanyaan Kuisioner)

Kuisioner_Buku dengan tema 'data pribadi'

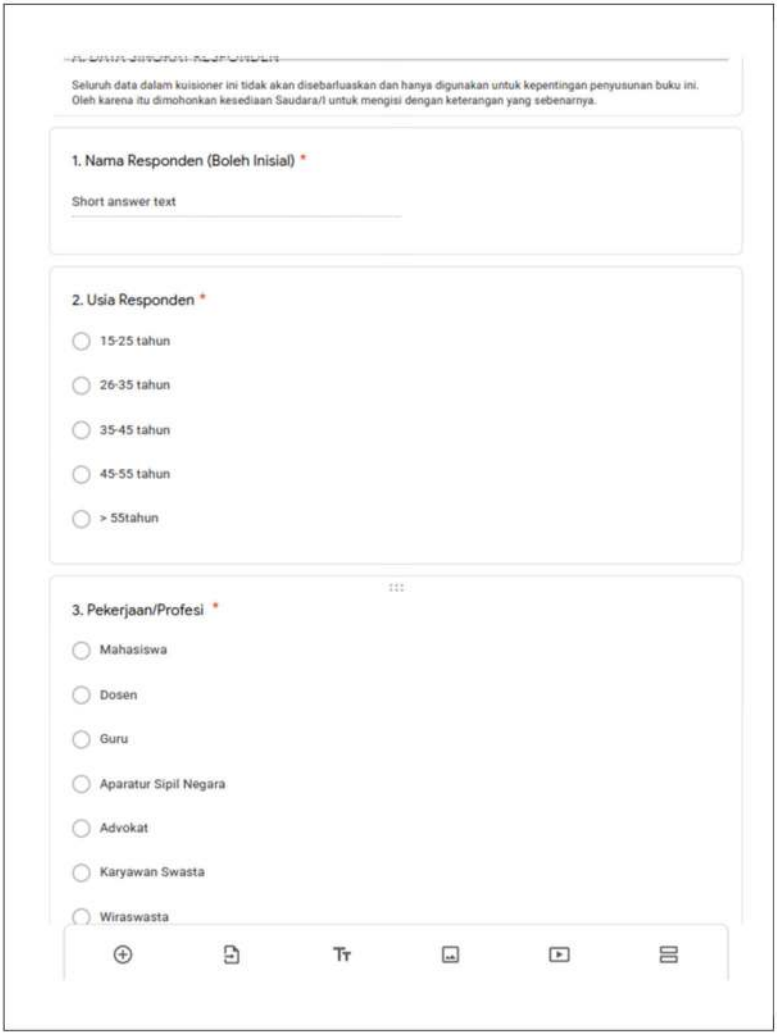
Questions Responses 226

Kuisioner Penyusunan Buku tentang "Pelindungan Data Pribadi Berdasarkan Perspektif Keadilan Bermartabat".

Kuisioner ini disusun dalam rangka penyusunan Buku tentang "Pelindungan Data Pribadi Berdasarkan Perspektif Keadilan Bermartabat". Penyusunan buku ini digagas oleh Prof. Dr. Teguh Prasetyo, S.H.,M.Si (Guru Besar Fakultas Hukum Universitas Pelita Harapan) dan Rizky Karo Karo, S.H., M.H. (Dosen Fakultas Hukum Universitas Pelita Harapan).

Pada abad ke-21 ini, khususnya di masyarakat perkotaan data pribadi dalam sistem elektronik sudah dapat disamakan dengan barang kebutuhan pokok. Apabila tidak waspada dari konsumen/pengguna dalam menggunakan aplikasi dan Penyelenggara juga tidak meningkatkan keamanan sistem mereka maka akan memberi celah 'perbuatan melawan hukum' termasuk namun tidak terbatas pada dugaan 'penjualan data pribadi'. Oleh karena itu, selain konsumen, Penyelenggara (platform aplikasi online/daring) juga harus meningkatkan keamanan sistem mereka dan Pemerintah melalui Kementerian yang berwenang, salah satunya ialah Kementerian Komunikasi dan Informatika juga harus memberikan pengawasan lebih intens agar Penyelenggara menjalankan prinsip kehati-hatian dan kepatuhan (compliance) sehingga pengolahan, penggunaan dan pemrosesan data pribadi nantinya ialah berlandaskan keadilan bermartabat, keadilan yang memanusiakan manusia dan apabila terjadi sengketa maka penyelesaiannya dapat win-win solution (keadilan bermartabat ialah konsep yang digagas oleh Prof. Dr. Teguh Prasetyo, S.H.,M.Si).

Seluruh data dalam kuisioner ini tidak akan disebarluaskan dan hanya digunakan untuk kepentingan penyusunan buku ini. Oleh karena itu dimohonkan kesediaan Saudara/I untuk mengisi dengan keterangan yang sebenarnya.



Seluruh data dalam kuisioner ini tidak akan disebarluaskan dan hanya digunakan untuk kepentingan penyusunan buku ini. Oleh karena itu dimohonkan kesediaan Saudara/I untuk mengisi dengan keterangan yang sebenarnya.

1. Nama Responden (Boleh Inisial) *

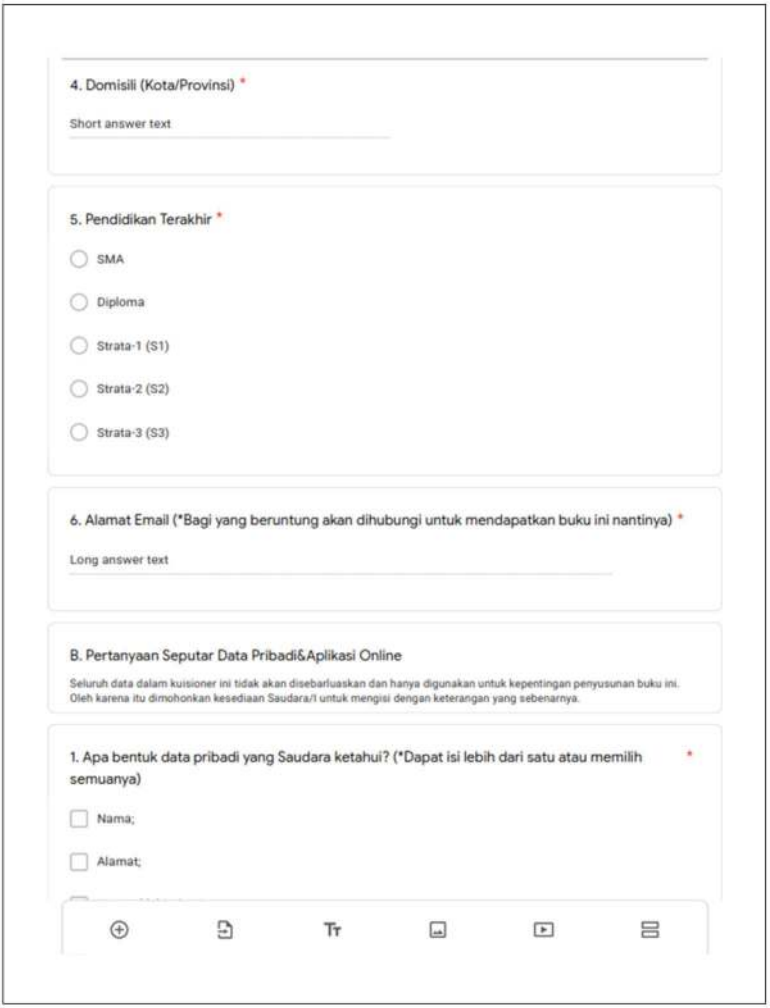
Short answer text

2. Usia Responden *

- 15-25 tahun
- 26-35 tahun
- 35-45 tahun
- 45-55 tahun
- > 55tahun

3. Pekerjaan/Profesi *

- Mahasiswa
- Dosen
- Guru
- Aparatur Sipil Negara
- Advokat
- Karyawan Swasta
- Wiraswasta



4. Domisili (Kota/Provinsi) *

Short answer text

5. Pendidikan Terakhir *

- SMA
- Diploma
- Strata-1 (S1)
- Strata-2 (S2)
- Strata-3 (S3)

6. Alamat Email (*Bagi yang beruntung akan dihubungi untuk mendapatkan buku ini nantinya) *

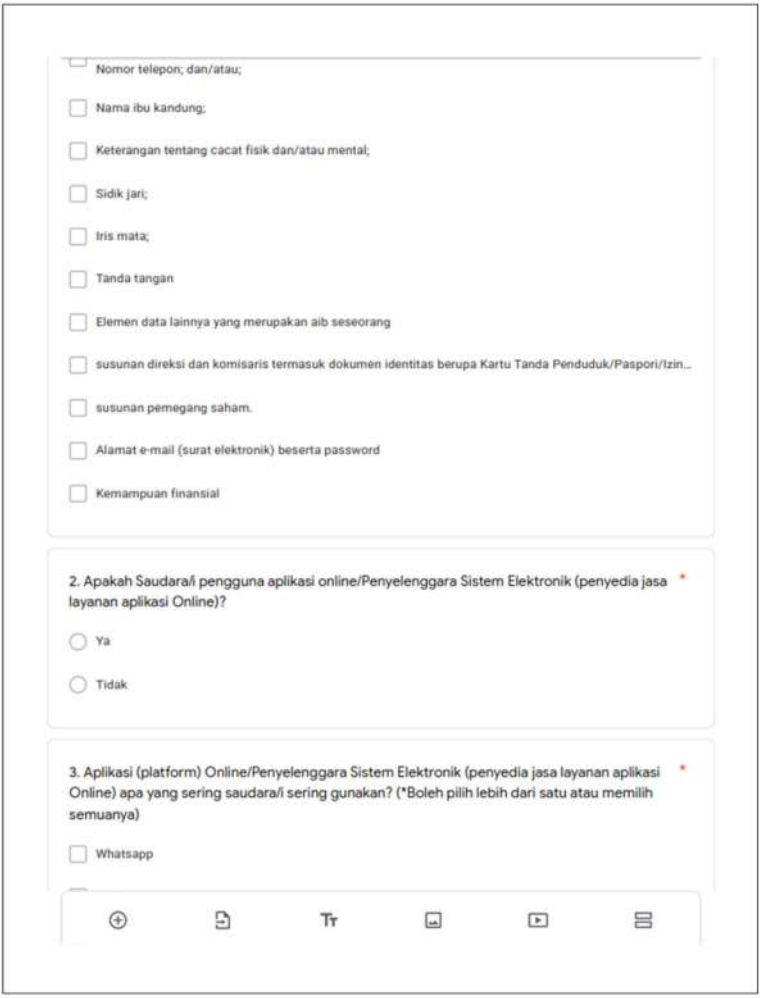
Long answer text

B. Pertanyaan Seputar Data Pribadi&Aplikasi Online

Seluruh data dalam kuisioner ini tidak akan disebarluaskan dan hanya digunakan untuk kepentingan penyusunan buku ini. Oleh karena itu dimohonkan kesediaan Saudara/I untuk mengisi dengan keterangan yang sebenarnya.

1. Apa bentuk data pribadi yang Saudara ketahui? (*Dapat isi lebih dari satu atau memilih semuanya) *

- [ ] Nama;
- [ ] Alamat;



Nomor telepon; dan/atau;

Nama ibu kandung;

Keterangan tentang cacat fisik dan/atau mental;

Sidik jari;

Iris mata;

Tanda tangan

Elemen data lainnya yang merupakan aib seseorang

susunan direksi dan komisaris termasuk dokumen identitas berupa Kartu Tanda Penduduk/Paspori/Izin...

susunan pemegang saham.

Alamat e-mail (surat elektronik) beserta password

Kemampuan finansial

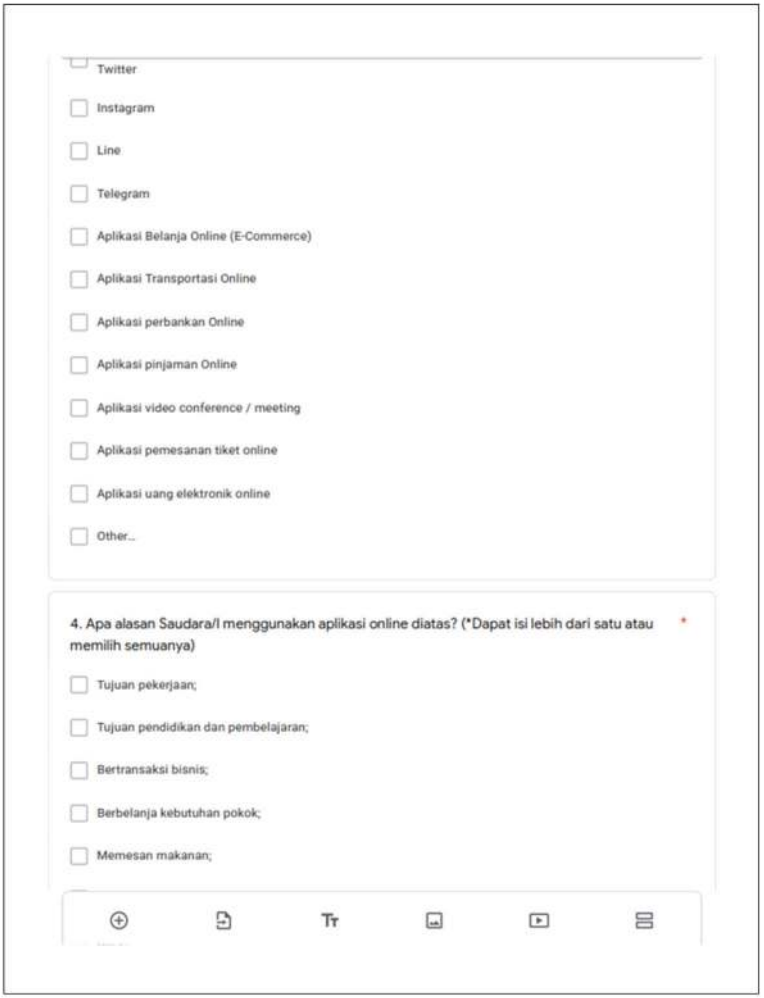
2. Apakah Saudara/i pengguna aplikasi online/Penyelenggara Sistem Elektronik (penyedia jasa layanan aplikasi Online)? *

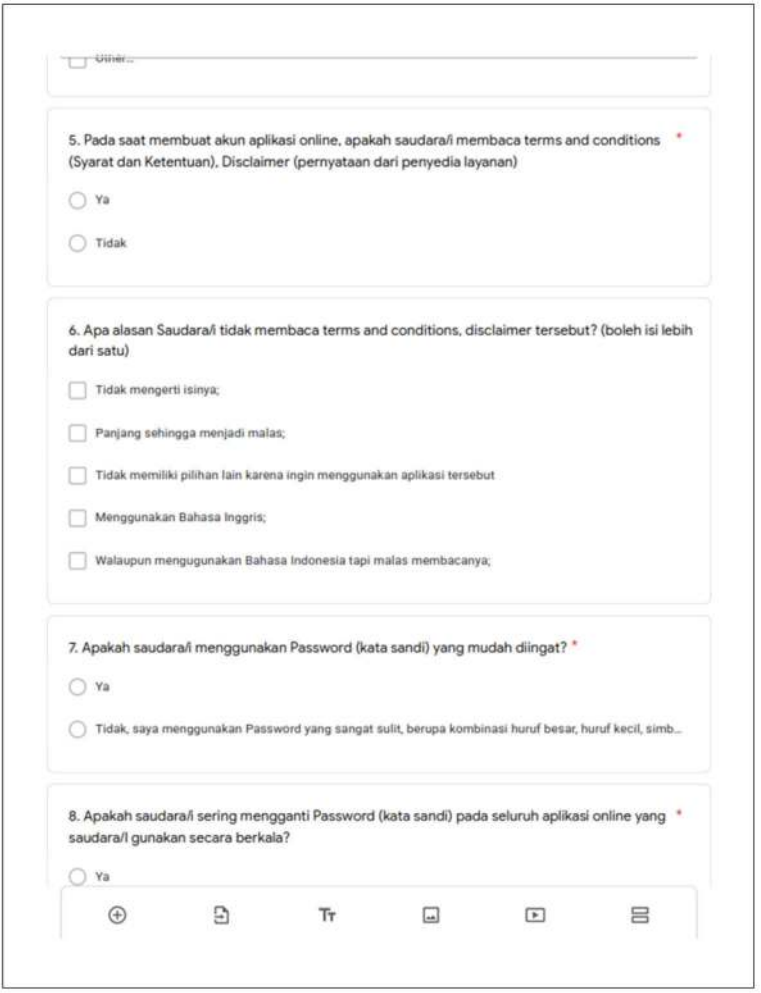
Ya

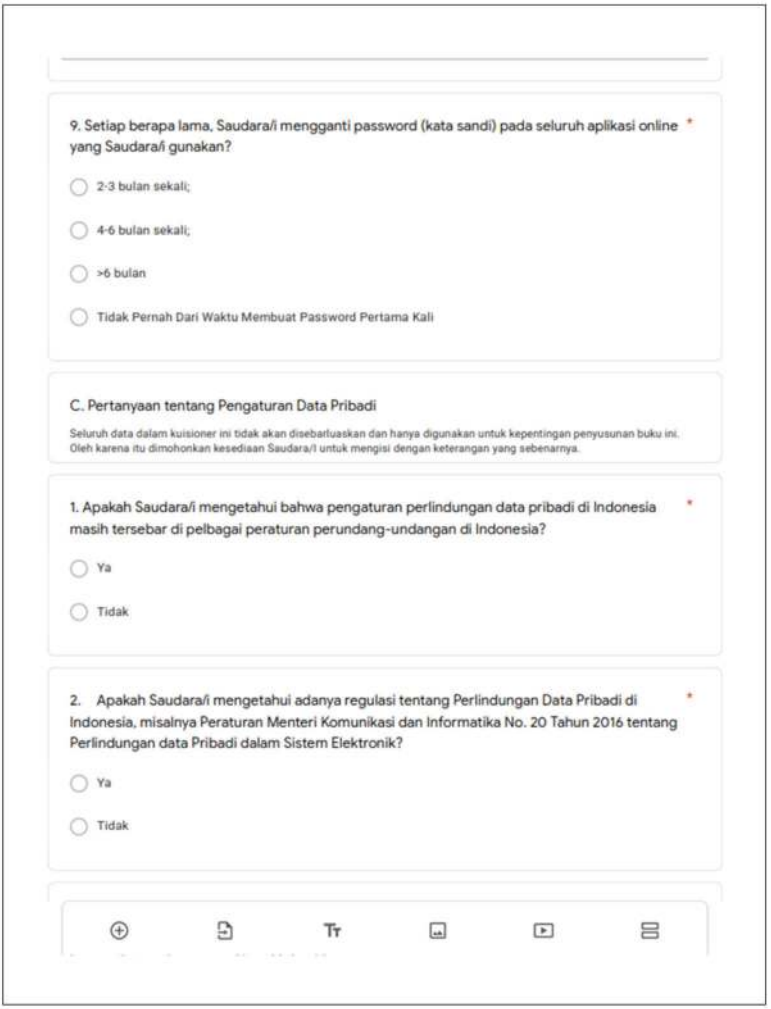
Tidak

3. Aplikasi (platform) Online/Penyelenggara Sistem Elektronik (penyedia jasa layanan aplikasi Online) apa yang sering saudara/i sering gunakan? (*Boleh pilih lebih dari satu atau memilih semuanya) *

Whatsapp


Twitter
Instagram
Line
Telegram
Aplikasi Belanja Online (E-Commerce)
Aplikasi Transportasi Online
Aplikasi perbankan Online
Aplikasi pinjaman Online
Aplikasi video conference / meeting
Aplikasi pemesanan tiket online
Aplikasi uang elektronik online
Other...
4. Apa alasan Saudara/I menggunakan aplikasi online diatas? (*Dapat isi lebih dari satu atau memilih semuanya) *
Tujuan pekerjaan;
Tujuan pendidikan dan pembelajaran;
Bertransaksi bisnis;
Berbelanja kebutuhan pokok;
Memesan makanan;


Other...
5. Pada saat membuat akun aplikasi online, apakah saudara/i membaca terms and conditions (Syarat dan Ketentuan), Disclaimer (pernyataan dari penyedia layanan) *
Ya
Tidak
6. Apa alasan Saudara/i tidak membaca terms and conditions, disclaimer tersebut? (boleh isi lebih dari satu)
Tidak mengerti isinya;
Panjang sehingga menjadi malas;
Tidak memiliki pilihan lain karena ingin menggunakan aplikasi tersebut
Menggunakan Bahasa Inggris;
Walaupun mengugunakan Bahasa Indonesia tapi malas membacanya;
7. Apakah saudara/i menggunakan Password (kata sandi) yang mudah diingat? *
Ya
Tidak, saya menggunakan Password yang sangat sulit, berupa kombinasi huruf besar, huruf kecil, simb...
8. Apakah saudara/i sering mengganti Password (kata sandi) pada seluruh aplikasi online yang saudara/I gunakan secara berkala? *
Ya



9. Setiap berapa lama, Saudara/i mengganti password (kata sandi) pada seluruh aplikasi online yang Saudara/i gunakan? *

- 2-3 bulan sekali;
- 4-6 bulan sekali;
- >6 bulan
- Tidak Pernah Dari Waktu Membuat Password Pertama Kali

C. Pertanyaan tentang Pengaturan Data Pribadi

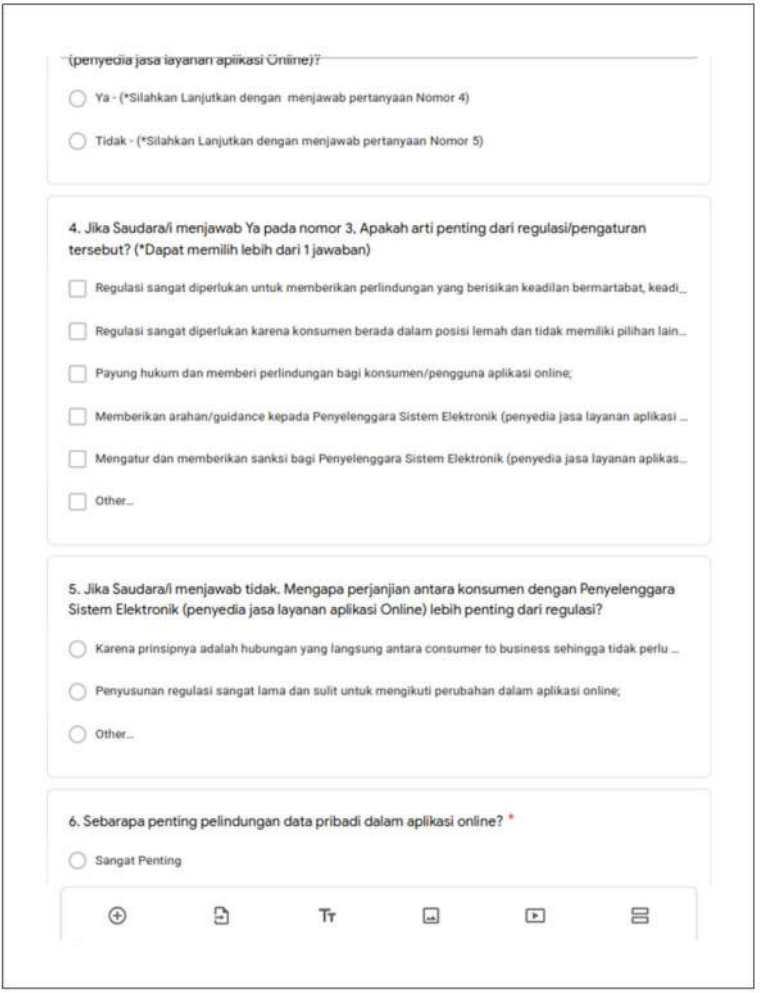
Seluruh data dalam kuisioner ini tidak akan disebarluaskan dan hanya digunakan untuk kepentingan penyusunan buku ini. Oleh karena itu dimohonkan kesediaan Saudara/i untuk mengisi dengan keterangan yang sebenarnya.

1. Apakah Saudara/i mengetahui bahwa pengaturan perlindungan data pribadi di Indonesia masih tersebar di pelbagai peraturan perundang-undangan di Indonesia? *

- Ya
- Tidak

2. Apakah Saudara/i mengetahui adanya regulasi tentang Perlindungan Data Pribadi di Indonesia, misalnya Peraturan Menteri Komunikasi dan Informatika No. 20 Tahun 2016 tentang Perlindungan data Pribadi dalam Sistem Elektronik? *

- Ya
- Tidak



(penyedia jasa layanan aplikasi Online)?

- ◯ Ya - (*Silahkan Lanjutkan dengan menjawab pertanyaan Nomor 4)
- ◯ Tidak - (*Silahkan Lanjutkan dengan menjawab pertanyaan Nomor 5)

4. Jika Saudara/i menjawab Ya pada nomor 3, Apakah arti penting dari regulasi/pengaturan tersebut? (*Dapat memilih lebih dari 1 jawaban)

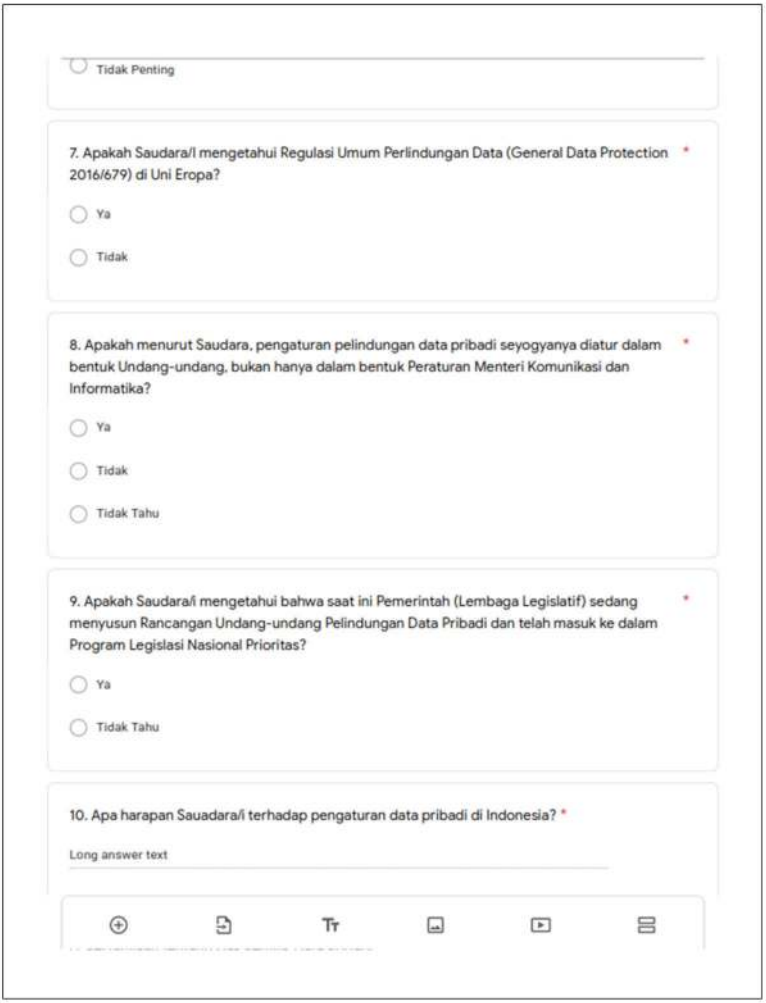
- ☐ Regulasi sangat diperlukan untuk memberikan perlindungan yang berisikan keadilan bermartabat, keadi...
- ☐ Regulasi sangat diperlukan karena konsumen berada dalam posisi lemah dan tidak memiliki pilihan lain...
- ☐ Payung hukum dan memberi perlindungan bagi konsumen/pengguna aplikasi online;
- ☐ Memberikan arahan/guidance kepada Penyelenggara Sistem Elektronik (penyedia jasa layanan aplikasi ...
- ☐ Mengatur dan memberikan sanksi bagi Penyelenggara Sistem Elektronik (penyedia jasa layanan aplikas...
- ☐ Other...

5. Jika Saudara/i menjawab tidak. Mengapa perjanjian antara konsumen dengan Penyelenggara Sistem Elektronik (penyedia jasa layanan aplikasi Online) lebih penting dari regulasi?

- ◯ Karena prinsipnya adalah hubungan yang langsung antara consumer to business sehingga tidak perlu ...
- ◯ Penyusunan regulasi sangat lama dan sulit untuk mengikuti perubahan dalam aplikasi online;
- ◯ Other...

6. Sebarapa penting pelindungan data pribadi dalam aplikasi online? *

- ◯ Sangat Penting



Tidak Penting

7. Apakah Saudara/I mengetahui Regulasi Umum Perlindungan Data (General Data Protection 2016/679) di Uni Eropa? *

- Ya
- Tidak

8. Apakah menurut Saudara, pengaturan pelindungan data pribadi seyogyanya diatur dalam bentuk Undang-undang, bukan hanya dalam bentuk Peraturan Menteri Komunikasi dan Informatika? *

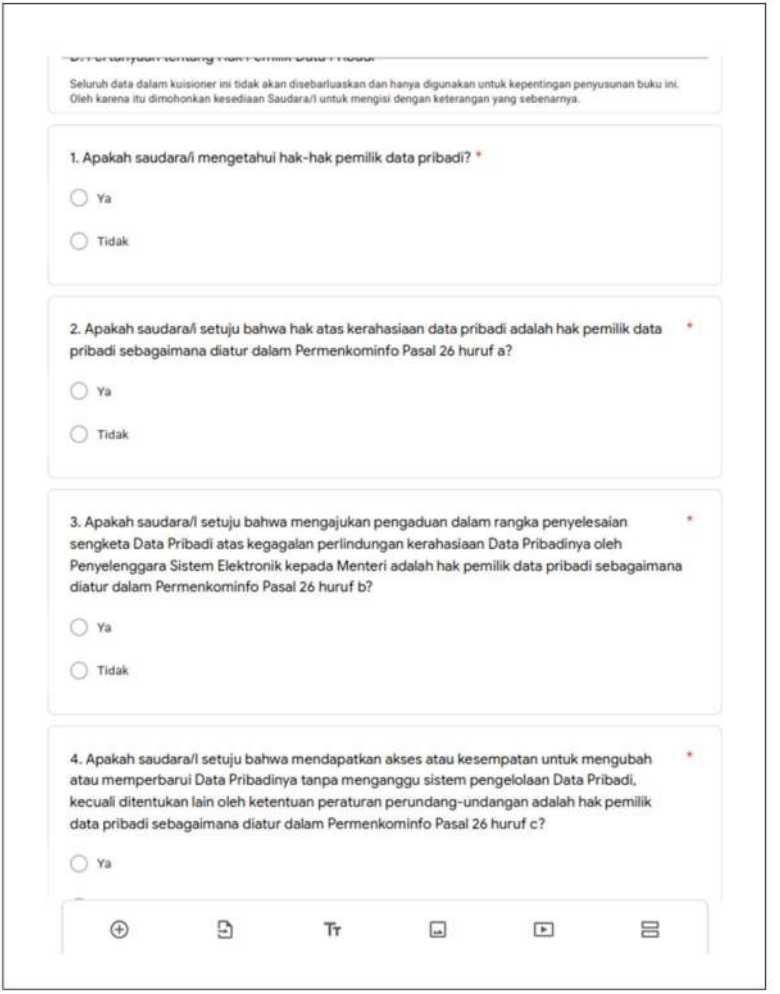
- Ya
- Tidak
- Tidak Tahu

9. Apakah Saudara/I mengetahui bahwa saat ini Pemerintah (Lembaga Legislatif) sedang menyusun Rancangan Undang-undang Pelindungan Data Pribadi dan telah masuk ke dalam Program Legislasi Nasional Prioritas? *

- Ya
- Tidak Tahu

10. Apa harapan Sauadara/i terhadap pengaturan data pribadi di Indonesia? *

Long answer text



Seluruh data dalam kuisioner ini tidak akan disebarluaskan dan hanya digunakan untuk kepentingan penyusunan buku ini. Oleh karena itu dimohonkan kesediaan Saudara/I untuk mengisi dengan keterangan yang sebenarnya.

1. Apakah saudara/i mengetahui hak-hak pemilik data pribadi? *

- Ya
- Tidak

2. Apakah saudara/i setuju bahwa hak atas kerahasiaan data pribadi adalah hak pemilik data pribadi sebagaimana diatur dalam Permenkominfo Pasal 26 huruf a? *

- Ya
- Tidak

3. Apakah saudara/I setuju bahwa mengajukan pengaduan dalam rangka penyelesaian sengketa Data Pribadi atas kegagalan perlindungan kerahasiaan Data Pribadinya oleh Penyelenggara Sistem Elektronik kepada Menteri adalah hak pemilik data pribadi sebagaimana diatur dalam Permenkominfo Pasal 26 huruf b? *

- Ya
- Tidak

4. Apakah saudara/I setuju bahwa mendapatkan akses atau kesempatan untuk mengubah atau memperbarui Data Pribadinya tanpa menganggu sistem pengelolaan Data Pribadi, kecuali ditentukan lain oleh ketentuan peraturan perundang-undangan adalah hak pemilik data pribadi sebagaimana diatur dalam Permenkominfo Pasal 26 huruf c? *

- Ya

5. Apakah saudara/I setuju bahwa mendapatkan akses atau kesempatan untuk memperoleh historis Data Pribadinya yang pernah diserahkan kepada Penyelenggara Sistem Elektronik sepanjang masih sesuai dengan ketentuan peraturan perundang-undangan adalah hak pemilik data pribadi sebagaimana diatur dalam Permenkominfo Pasal 26 huruf d? *

- ○ Ya
- ○ Tidak

6. Apakah saudara/I setuju bahwa meminta pemusnahan Data Perseorangan Tertentu miliknya dalam Sistem Elektronik yang dikelola oleh Penyelenggara Sistem Elektronik, kecuali ditentukan lain oleh ketentuan peraturan perundang-undangan adalah hak pemilik data pribadi sebagaimana diatur dalam Permenkominfo Pasal 26 huruf e? *

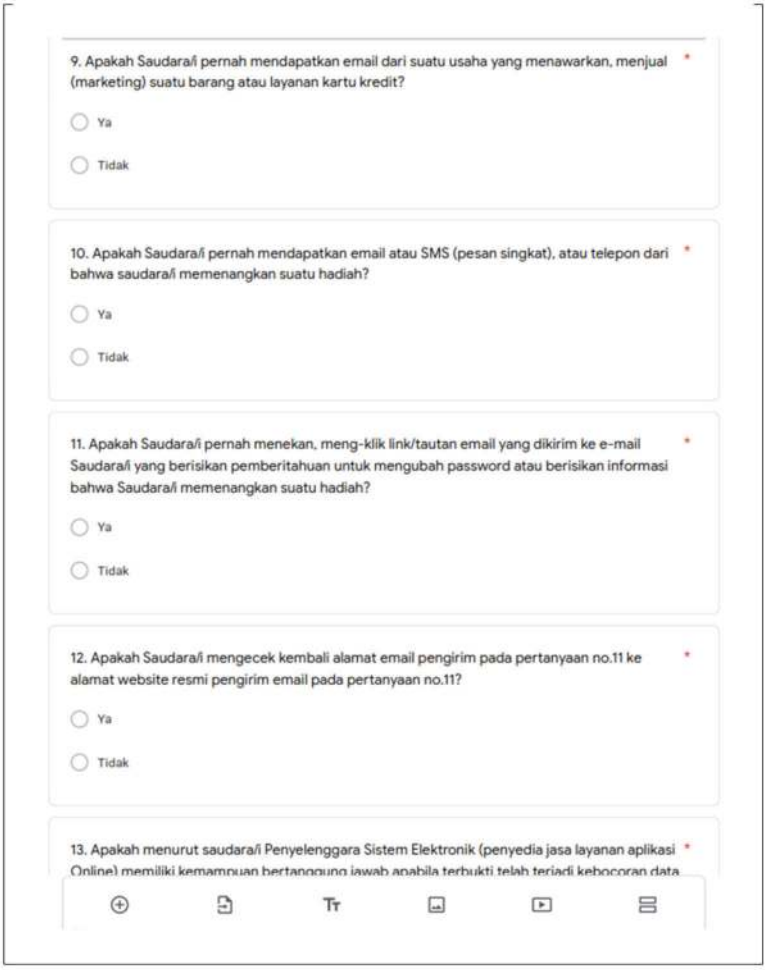
- ○ Ya
- ○ Tidak

7.Apakah Saudara mengetahui bahwa pengguna/pemilik data pribadi/konsumen memiliki hak hukum untuk mengajukan gugatan kepada Penyelenggara Sistem Elektronik (penyedia jasa layanan aplikasi Online) yang lalai dalam melindungi data pribadi dalam sistem mereka? *

- ○ Ya
- ○ Tidak

8. Apakah Saudara/i pernah mendapatkan telepon dari suatu usaha yang menawarkan, menjual (marketing) suatu barang atau layanan kartu kredit? *

- ○ Ya
- ○ Tidak



9. Apakah Saudara/i pernah mendapatkan email dari suatu usaha yang menawarkan, menjual (marketing) suatu barang atau layanan kartu kredit? *

- Ya
- Tidak

10. Apakah Saudara/i pernah mendapatkan email atau SMS (pesan singkat), atau telepon dari bahwa saudara/i memenangkan suatu hadiah? *

- Ya
- Tidak

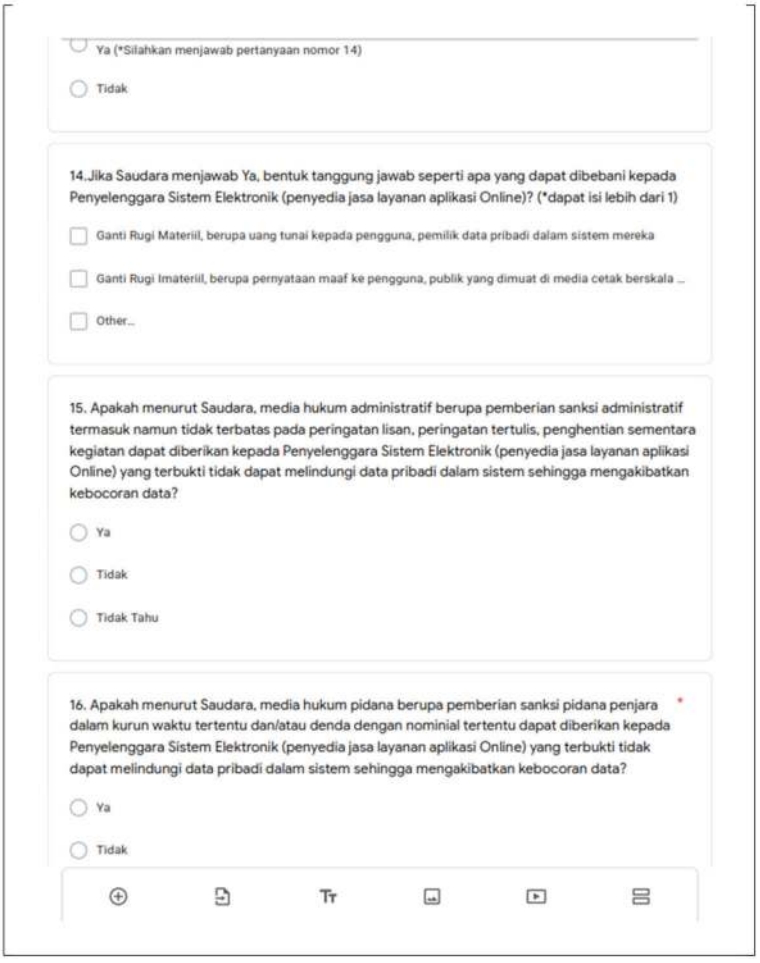
11. Apakah Saudara/i pernah menekan, meng-klik link/tautan email yang dikirim ke e-mail Saudara/i yang berisikan pemberitahuan untuk mengubah password atau berisikan informasi bahwa Saudara/i memenangkan suatu hadiah? *

- Ya
- Tidak

12. Apakah Saudara/i mengecek kembali alamat email pengirim pada pertanyaan no.11 ke alamat website resmi pengirim email pada pertanyaan no.11? *

- Ya
- Tidak

13. Apakah menurut saudara/i Penyelenggara Sistem Elektronik (penyedia jasa layanan aplikasi Online) memiliki kemampuan bertanggung jawab apabila terbukti telah terjadi kebocoran data *



Ya (*Silahkan menjawab pertanyaan nomor 14)

Tidak

14.Jika Saudara menjawab Ya, bentuk tanggung jawab seperti apa yang dapat dibebani kepada Penyelenggara Sistem Elektronik (penyedia jasa layanan aplikasi Online)? (*dapat isi lebih dari 1)

Ganti Rugi Materiil, berupa uang tunai kepada pengguna, pemilik data pribadi dalam sistem mereka

Ganti Rugi Imateriil, berupa pernyataan maaf ke pengguna, publik yang dimuat di media cetak berskala ...

Other...

15. Apakah menurut Saudara, media hukum administratif berupa pemberian sanksi administratif termasuk namun tidak terbatas pada peringatan lisan, peringatan tertulis, penghentian sementara kegiatan dapat diberikan kepada Penyelenggara Sistem Elektronik (penyedia jasa layanan aplikasi Online) yang terbukti tidak dapat melindungi data pribadi dalam sistem sehingga mengakibatkan kebocoran data?

Ya

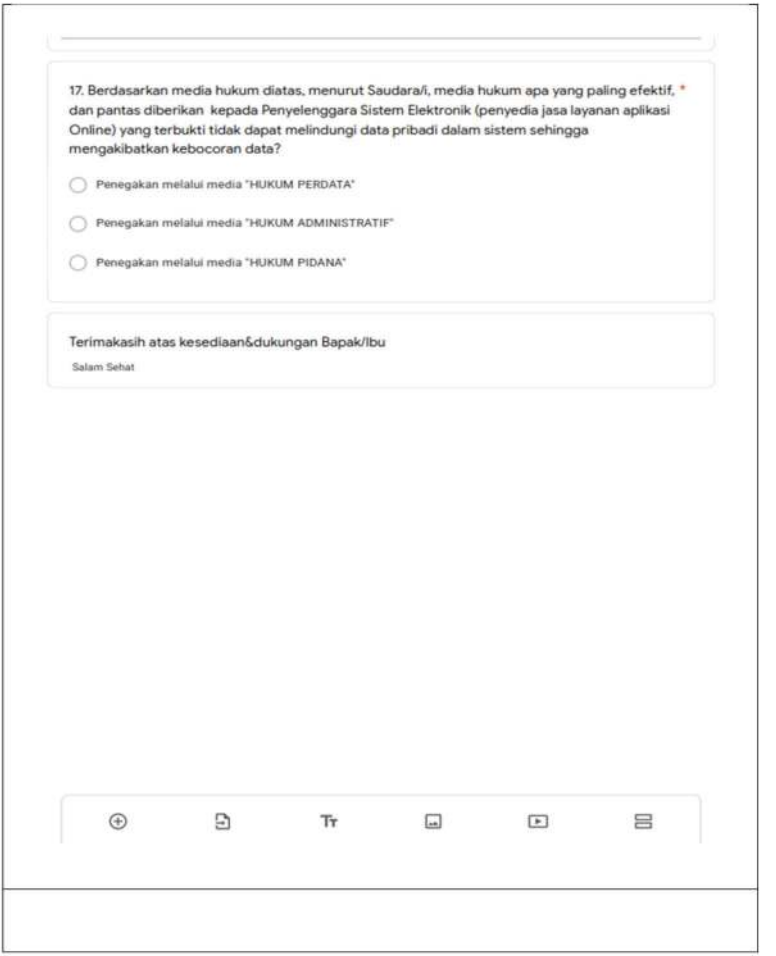
Tidak

Tidak Tahu

16. Apakah menurut Saudara, media hukum pidana berupa pemberian sanksi pidana penjara dalam kurun waktu tertentu dan/atau denda dengan nominal tertentu dapat diberikan kepada Penyelenggara Sistem Elektronik (penyedia jasa layanan aplikasi Online) yang terbukti tidak dapat melindungi data pribadi dalam sistem sehingga mengakibatkan kebocoran data? *

Ya

Tidak



17. Berdasarkan media hukum diatas, menurut Saudara/i, media hukum apa yang paling efektif, * dan pantas diberikan kepada Penyelenggara Sistem Elektronik (penyedia jasa layanan aplikasi Online) yang terbukti tidak dapat melindungi data pribadi dalam sistem sehingga mengakibatkan kebocoran data?

- Penegakan melalui media "HUKUM PERDATA"
- Penegakan melalui media "HUKUM ADMINISTRATIF"
- Penegakan melalui media "HUKUM PIDANA"

Terimakasih atas kesediaan&dukungan Bapak/Ibu

Salam Sehat

BIODATA PENULIS

Prof. Dr. Teguh Prasetyo, S.H, M.Si. lahir di Pati Juli 1961. Memperoleh gelar Sarjana Hukum dari FH UNKRIS Jakarta (1986), Magister di UGM Yogyakarta (1994), Doktor Ilmu Hukum dari FH UII Yogyakarta (2006).

Anggota Dewan Kehormatan Penyelenggara Pemilu Republik Indonesia (DKPP RI) Periode 2017-2022. Dosen Tetap dan Guru Besar di Fakultas Hukum Universitas Pelita Harapan Karawaci dan juga mengajar di FH UKSW Salatiga, DIH dan MH UNTAG Surabaya, DIH UNISSULA Semarang, DIH UNTAG Semarang, DIE di FE UII Yogya, MMP ISTIPER Yogya, STAK Marturia Yogya, STT NAZAREN Yogya, STT KADESI Yogya, MH UNSA Surakarta, MH UPS Tegal, FH JAYABAYA Jakarta.

Karya buku yang sudah diterbitkan sebanyak 40 (empat puluh) buku antara lain: Keadilan Bermartabat; Hukum dan Sistem Hukum Berdasarkan Pancasila; Filsafat Pemilu; Hukum Pidana; Hukum Acara Pidana; Kriminologi; Pembaharuan Hukum dalam Perspektif Teori Keadilan Bermartabat; Kriminalisasi dalam Hukum Pidana; Hukum Islam Menjawab Tantangan Zaman yang Berkembang Dinamis; Membangun Hukum Pancasila; Politik Hukum Pidana; Tindak Pidana Anak; Pengantar Ilmu Hukum; Pengantar Hukum Indonesia; Penelitian Hukum Suatu Perspektif Teori Keadilan Bermartabat. Serta aktif dalam menulis jurnal baik nasional maupun internasional.

Rizky P.P. Karo Karo, S.H, M.H. memperoleh gelar Sarjana Hukum dan Magister Hukum di Fakultas Hukum Universitas Gadjah Mada Yogyakarta.

Dosen Tetap di Fakultas Hukum Universitas Pelita Harapan (FH UPH) dan aktif pelayanan hukum sebagai Sekretaris Pelaksana Harian di Lembaga Konsultasi dan Bantuan Hukum FH UPH (LKBH FH UPH).

Aktif dalam pelbagai publikasi, beberapa diantaranya: buku "Penegakan Hukum Kejahatan Dunia Maya (Cybercrime) Melalui Hukum Pidana" yang diterbitkan oleh Fakultas Hukum UPH (Karawaci), artikel di surat kabar " "Kejahatan Siber Perbankan", Kolom Opini Harian di Kompas; Artikel "Perkara Kebocoran Data E-Commerce", Kolom Pendapat di Harian Tempo. Dan aktif dalam menulis jurnal nasional. Rizky Karo Karo dapat dihubungi di rizky. karokaro@uph.edu

PENGATURAN PERLINDUNGAN DATA PRIBADI DI INDONESIA

PERSPEKTIF TEORI KEADILAN BERMARTABAT

Perkembangan teknologi, internet berkembang dengan pesat. Perkembangan tersebut membawa dampak negatif dan positif. Teknologi memudahkan manusia untuk bekerja, bertransaksi elektronik, berkomunikasi, menjaga hubungan/relasi dengan keluarga tetap berjaga, bahkan juga dipergunakan untuk keperluan penegakan hukum (e-litigation, memeriksa saksi menggunakan video conference, melakukan perizinan online). Namun, apabila oknum tidak memiliki martabat yang baik maka oknum tersebut menggunakan otak/ilmu yang dimiliki untuk melakukan perbuatan melawan hukum, misalnya melakukan peretasan, penipuan menggunakan layanan teknologi.

Manusia, korporasi sebagai subyek hukum pada abad ke-21 tidak dapat tidak dilepaskan dari aplikasi online, sistem elektronik yang dikembangkan oleh penyelenggara sistem elektronik (penyelenggara/aplikator). Syarat untuk menggunakan aplikasi online adalah pengguna/konsumen wajib memasukan data pribadi ke dalam sistem tersebut dan apabila ingin menggunakan layanan ekstra/tambahan dari aplikasi tersebut, pengguna diwajibkan menggunggah foto diri sambil memegang Kartu Tanda Penduduk (KTP) ke dalam sistem tersebut. Konsumen/pengguna tidak memiliki pilihan dalam aplikasi online pada saat harus mengisi disclaimer, karena pilihannya hanya yes or no, agree or disagree. Jika tidak memilih yes/agree maka konsumen/pengguna tidak dapat menggunakan aplikasi online tersebut.

Data pribadi merupakan wujud/personifikasi perpanjangan diri manusia/badan hukum dalam sistem elektronik. Manusia/badan hukum cukup dengan memasukan data pribadi termasuk namun tidak terbatas pada nama, nomor ponsel, e-mail (surat elektronik), nomor rekening setelah memasukan data pribadi tersebut maka konsumen/pengguna dapat melakukan perbuatan hukum melalui aplikasi online. Penyelenggara wajib menjaga, melindungi data pribadi pengguna/konsumen dari oknum yang tidak bertanggung jawab. Namun, dugaan kebocoran data pribadi, praktik jual beli data pribadi marak terjadi di Negara di dunia, khususnya di Indonesia. Data pribadi dijual dengan harga tertentu, dan diberi harga tinggi jika data yang dijual memiliki riwayat tabungan/riwayat keuangan. Kebocoran data pribadi akan menimbulkan dugaan tindak pidana lainnya, misalnya penipuan, diganggu oleh telemarketer yang menawarkan pelbagai produk di sektor jasa keuangan.

NUSAMEDIA

PENELITIAN

ISBN 978-602-6913-88-3