FEBRUARY 2021

ALSA INDONESIA

SPECIALIZED RESEARCH TEAM

Doctrinal Research

Perlindungan Data Pribadi Pada Sektor *E-Commerce* di Negara-Negara ASEAN

alsa-indonesia.org

REDACTIONAL BOARD
AISRT FEBRUARY 2021

Nikolaus Baptista Ruma
VP of Academic Activities & Training
(Leading Researcher)

Ratu Tasya Adawiyah
CO of Academic Research & Publication
(Leading Researcher)

Mario Jon Jordi
ALSA LC UGM
(Researcher)

Nisrina Olivia J
ALSA LC UB
(Researcher)

Agung Kurniawan S
ALSA LC UNPAD
(Researcher)

NARASUMBER

1. Tim Subdit Tata Kelola Perlindungan Data Pribadi Direktorat Jenderal Aplikasi Informatika Kementerian Komunikasi dan Informatika Republik Indonesia (Indonesia);
2. Wahyudi Djafar selaku Direktur Eksekutif ELSAM Periode 2021-2025 (Indonesia);
3. Ardhanti Nurwidya selaku Senior Manager of Public Policy and Government Relation & Group Data Protection Officer Gojek dan Founder of Asosiasi Praktisi Perlindungan Data Indonesia (APPDI) (Indonesia);
4. Sonny Zulhuda, LL.B. (Honours), MCL., Ph.D. selaku Associate Professor on Cyber Law & Data Protection Law at International Islamic University Malaysia (Malaysia);
5. Maria Francesca Montes, J.D. selaku Head of Artificial Intelligence and Data Policy and Data Protection Officer at Union Bank of The Philippines (Filipina);
6. Jasmine Wong selaku Senior Manager of Legal Department at Authority for Info-communications Technology Industry of Brunei Darussalam (AITI)) dan Pengiran Alias (AITI's Brunei Darussalam Network Information Centre (BNNIC), Cyber Security & Data Protection Office Manager (Brunei Darussalam);
8. Nguyen Dung Mai dan Tu Thien Huynh selaku Lecturer of Law at University of Economics Ho Chi Minh City (Vietnam);
9. Kelvin Chia Partnership Yangon (Myanmar);- Jansen Aw selaku Partner at Donaldson & Burkinshaw LLP, Singapore dan Former Assistant Chief Counsel Personal Data Protection Commission (PDPC) Singapore (Singapura)

MITRA BESTARI

1. Prof. Dr. Abu Bakar Munir, LL.B. (Hons), LL.M. (Profesor Adjung Fakultas Hukum Universitas Indonesia)
2. Dr. Sinta Dewi S.H., LL.M. (Ketua Cyber Law Center Fakultas Hukum Universitas Padjadjaran)

Khalifah Al Kays Yusuf
President 2020-2021

Assalamualaikum Wr. Wb.,
Shalom,
Om Swastiastu,
Namo Buddhaya,
Salam kebajikan.

Puji syukur kita panjatkan kehadirat Allah SWT yang telah memberikan rahmat dan hidayah-Nya sehingga kita selalu diberikan kesehatan dan kenikmatan yang berlipat ganda. Tak luput dari rahmat-Nya untuk kita dapat berkumpul dalam satu organisasi hukum se-indonesia yang kita banggakan, Asian Law Students' Association (ALSA) *National Chapter* Indonesia yang menaungi 14 (empat belas) *Local Chapter* di segala penjuru Indonesia. ALSA Indonesia merupakan organisasi nirlaba dan non-politik, kami penuh akan solidaritas dari segala golongan dimana senantiasa mengedepankan peningkatan kualitas keilmuan hukum dari setiap anggotanya, yang kelak akan menebarkan manfaatnya kepada masyarakat luas.

Dengan bangga kami mempersilahkan para pembaca untuk menikmati dan memahami hasil penelitian dari ALSA Indonesia *Specialized Research Team*. Tim ini dibentuk dengan tujuan utama untuk memberikan edukasi dengan tinjauan akademis yang komprehensif kepada para anggota dan masyarakat luas. Penelitian ini merupakan doctrinal research yang pada kesempatan ini memberikan tinjauan yuridis mengenai perlindungan data pribadi pada sektor *e-commerce* di negara-negara ASEAN. Kami harap penelitian ini dapat memberikan pemahaman yang jelas secara akademis dan objektif, serta bermanfaat bagi berbagai pihak yang berkesempatan untuk membacanya.

Tanpa adanya dukungan dan partisipasi dari teman – teman *Local Chapter*, dan para *Redactional Board* yang telah melakukan penelitian dan penulisan kajian ini, tim ini tidak mungkin berada dalam kondisi yang maju dan berjaya seperti ini. Kami sangat berterima kasih atas seluruh pihak yang telah mendukung dan berpartisipasi dalam mensukseskan berjalannya tim ini dalam melakukan penelitian.

Patut kita pahami bersama, bahwasanya hasil penelitian ini didasari oleh kajian dan analisis hukum melalui tinjauan akademis yang objektif. Kami dan tim ini tidak ditunggangi oleh kepentingan politik manapun dan semata – mata bertujuan untuk memberikan edukasi kepada para anggota ALSA Indonesia dan masyarakat luas.

Akhir kata, semoga kita semua dapat membawa ALSA Indonesia selalu bersifat responsif terhadap isu hukum terkini dan senantiasa memperbaiki tatanan masyarakat ke arah yang lebih baik lagi.

Wassalamualaikum Wr. Wb.,
Shalom,
Om Shanti Shanti Shanti Om,
Namo Buddhaya,
Salam kebajikan bagi kita semua.

ALSA, *Always be One!*

PERLINDUNGAN DATA PRIBADI PADA SEKTOR *E-COMMERCE* DI NEGARA-NEGARA ASEAN

ALSA Indonesia *Specialized Research Team*

BAB I
PENDAHULUAN

1.1 Latar Belakang

Teknologi informasi dan komunikasi (TIK) telah menimbulkan perbedaan signifikan dalam aktivitas hidup masyarakat, dan akan terus menjadi kekuatan penting yang mendorong pembangunan bangsa dalam banyak aspek dalam beberapa dekade mendatang. Saat ini, revolusi TIK telah mengubah lanskap industri dan bisnis di seluruh dunia secara signifikan. Hal ini termasuk mempengaruhi sifat distribusi produk, pemasaran, periklanan, layanan, dan ritel. Perubahan ini menjanjikan percepatan dalam *e-commerce* dan inovasi digital lainnya. Terkhususnya pada *e-commerce,* pertumbuhan tersebut telah menghadirkan banyak manfaat penting bagi konsumen dan bisnis di seluruh dunia. Untuk itu, kita perlu terus beradaptasi, merangkul, dan memahami TIK dan peluang digital diperlukan untuk pembangunan ekonomi di era TIK.[1]

Baru-baru ini, ASEAN telah membawa kemakmuran dan kekayaan ke kawasannya melalui inovasi dan teknologi. Salah satu inovasi yang menunjang ekonomi digital di ASEAN adalah *e-commerce*. Pada studi bersama yang dirilis oleh Facebook dan Bain & Company, diperkirakan bahwa jumlah konsumsi online rata-rata di Asia Tenggara pada tahun 2025 akan mencapai USD390, yang menunjukkan penambahan tiga kali lipat dari tahun 2018 dengan jumlah rata-rata sebesar USD125. Laporan tersebut juga memperkirakan bahwa Asia Tenggara akan menjadi rumah bagi sekitar 310 juta konsumen digital pada tahun 2025, dimana pada tahun 2018 hanya ada 250 juta dan pada tahun 2015 hanya ada hanya 90 juta.[2] Sementara itu, Data Reportal melaporkan bahwa pada tahun 2019 terdapat 6 negara ASEAN yang tercatat dengan penggunaan *e-commerce* tertinggi, yakni Indonesia sebanyak 90%, Thailand sebanyak 85%, Malaysia sebanyak 80%, Vietnam sebanyak 78%, Filipina sebanyak

[1] Phet Sengpunya, 'ASEAN E-Commerce Legal Framework and Alignment of Lao PDR: A Review' (2019) 6 Lentera Hukum 269, [369].
[2] Facebook and Bain & Company, 'Riding the Digital Wave' (Bain & Company, 14 January 2020) <https://www.bain.com/insights/riding-the-digital-wave/>, diakses 24 November 2020.

Faculty of Law Universitas Gadjah Mada
Jl. Sosio Yustisia No. 1, Bulaksumur,
Sleman, D.I. Yogyakarta 55281, Republic of Indonesia
Tel +62-811-1396-565
Mail contact@alsaindonesia.org
Web www.alsaindonesia.org

75%, dan Singapura sebanyak 73%.[3]

E-commerce mengacu pada semua transaksi komersial yang didasarkan pada pemrosesan elektronik dan transmisi data, termasuk teks, suara, dan gambar. Proses ini melibatkan transaksi melalui internet, termasuk transfer dana elektronik dan Electronic Data Interchange (EDI).[4] Dengan semakin banyaknya pilihan yang tersedia, akses internet yang terus berkembang dan tingkat kemakmuran yang meningkat adalah faktor-faktor yang akan terus mendorong lebih banyak belanja *online*. Berdasarkan laporan e-Conomy Asia Tenggara yang dirilis oleh Google, Temasek dan Bain & Company, *e-commerce* juga telah mengungguli jasa layanan makanan dan transportasi, serta *online travel* sebagai sektor terbesar dalam ekonomi digital ASEAN.[5]

Berdasarkan karakteristik hubungan subjeknya, *e-commerce* memiliki beberapa tipe, antara lain *Business to business (B2B)*, *Business to consumer (B2C)*, *Consumer to consumer (C2C)*, dan *Consumer to business (C2B)*.[6] Meski berbeda karakteristik, terdapat satu kesamaan dari setiap tipe dari *e-commerce* tersebut, yakni adanya penggunaan data pribadi pengguna yang disimpan di dalam sistemnya.

Data pribadi dapat didefinisikan sebagai informasi yang dapat diidentifikasikan kepada seseorang seperti nama, tanggal lahir, alamat, dan sebagainya.[7] Ketika kita mendaftarkan akun di *e-commerce*, kita harus mengisi beberapa data pribadi kita untuk dapat menggunakan secara maksimal layanannya. Sebagai upaya meningkatkan pengalaman individu pengguna, pada *e-commerce* terdapat pula upaya-upaya untuk mempersonalisasi pengalaman pengguna, seperti dengan adanya iklan yang dipersonalisasi, seperti lewat *e-mail* tawaran dan rekomendasi produk. Upaya tersebut dilakukan dengan mengandalkan profil yang dibangun dalam sistem *e-commerce* berdasarkan olahan data milik pengguna yang kita berikan secara sadar ataupun tidak sadar.[8]

[3] Simon Kemp & Sarah Moey, 'Digital 2019 Spotlight: E-Commerce in Southeast Asia ' (Data Reportal, 2019) <https://datareportal.com/reports/digital-2019-spotlight-ecommerce-in-southeast-asia>, diakses 24 November 2020.
[4] Alan Davidson, *The Law of Electronic Commerce*, USA: Cambridge University Press, 2009.[1].
[5] Google, Temasek and Bain & Company, 'e-Conomony Sea 2020, At full Velocity: Resilient and Racing Ahead' (e-Conomony Sea, 2020) <https://www.bain.com/globalassets/noindex/2020/e-conomy_sea_2020_report.pdf> diakses 24 November 2020.
[6] Richard L. Sandhusen, *Marketing*, New York: Barron's Educational Series, 2008, [520].
[7] Ida Madieha Azmi, 'E-Commerce and Privacy Issues: An Analysis of the Personal Data Protection Bill' (2002) 16 International Review of Law, Computers & Technology 317, [318].
[8] Horst Treiblmaier, 'The Influence of Privacy Concerns on Perceptions of Web Personalisation' (2011) 1 In. J. Web Science 3. [4].

Faculty of Law Universitas Gadjah Mada
Jl. Sosio Yustisia No. 1, Bulaksumur,
Sleman, D.I. Yogyakarta 55281, Republic of Indonesia
Tel +62-811-1396-565
Mail contact@alsaindonesia.org
Web www.alsaindonesia.org

Kekhawatiran yang timbul dalam penggunaan data pribadi pada *e-commerce* dapat berkaitan dengan tindakan apa saja yang akan dilakukan perusahaan komersial dengan data pribadi konsumen. Hal ini berhubungan erat dengan topik seperti kepemilikan informasi, kontrol hak informasi, dan keamanan data.[9] Dalam dunia perdagangan di internet, kini informasi pelanggan menjadi aset penting di *e-commerce*, sehingga memunculkan bahaya akan data yang digunakan untuk tujuan selain dari yang dikumpulkan tanpa persetujuan pemiliknya,[10] ataupun pengaksesan data secara ilegal.[11] Pada penggunaan *e-commerce*, perlindungan konsumen sendiri merupakan hal yang penting untuk menjaga kepercayaan konsumen dan meningkatkan penggunaannya. Masalah ini pun menjadi sangat penting di kawasan ASEAN.

ASEAN sendiri merupakan organisasi regional negara-negara yang dibentuk pada tahun 1967 untuk memajukan kerjasama regional di antara negara-negara anggotanya, dengan tujuan untuk mempercepat pertumbuhan ekonomi, kemajuan sosial dan perkembangan budaya serta untuk mempromosikan perdamaian dan stabilitas regional di kawasan Asia Tenggara. Saat ini ASEAN beranggotakan 10 negara anggota, termasuk Indonesia, Singapura, Malaysia, Brunei Darussalam, Kamboja, Republik Demokratik Rakyat Laos, Myanmar, Filipina, Thailand, dan Vietnam.[12]

Sejalan dengan tujuannya, ASEAN sendiri telah melaksanakan beberapa program kerjasama dalam meningkatkan keamanan dalam *e-commerce* dan data pribadi. Contohnya, pada November 2017, ASEAN mengadopsi *Work Program on Electronic Commerce* 2017-2025 untuk memperkuat pengembangan *e-commerce* di pasar tunggal ASEAN yang sedang berkembang. Program kerja tersebut bertujuan untuk mengembangkan dan mengimplementasikan pedoman, mekanisme koordinasi, dan inisiatif khusus terkait infrastruktur *broadband*, modernisasi kerangka hukum *e-commerce*, perlindungan konsumen, fasilitasi perdagangan, sistem pembayaran, keamanan transaksi elektronik, persaingan, dan peningkatan logistik. Dalam elemen 'keamanan transaksi elektronik', telah tercantum satu inisiasi yang menganjurkan pelaksanaan praktik terbaik perlindungan data pribadi untuk meningkatkan pengimplementasian *ASEAN Framework on Personal Data Protection*

[9] UNCTAD, 'Review of e-commerce legislation harmonization in ASEAN' (UNCTAD Org, 2013) <https://unctad.org/system/files/official-document/dtlstict2013d1_en.pdf> diakses 24 November 2020.
[10] Mary J. Culnan, '"How Did They Get My Name?": An Exploratory Investigation of Consumer Attitudes toward Secondary Information Use' (1993) 17 MIS Quarterly,[344].
[11] Horst Treiblmaier, *op.cit.*
[12] ASEAN, 'ASEAN Member States' (Association of Southeast Asian Nations) <https://asean.org/asean/asean-member-states/> diakses 24 November 2020

Faculty of Law Universitas Gadjah Mada
Jl. Sosio Yustisia No. 1, Bulaksumur,
Sleman, D.I. Yogyakarta 55281, Republic of Indonesia
Tel +62-811-1396-565
Mail contact@alsaindonesia.org
Web www.alsaindonesia.org

(ASEAN PDP Framework).[13]

Sejalan dengan itu, pengakuan pentingnya perlindungan atas pribadi sebagai bagian dari hak atas privasi di ASEAN dapat ditemukan pada pada pasal 21 *ASEAN Human Rights Declaration*. Pasal tersebut berbunyi:[14]

> *'Every person has the right to be free from arbitrary interference with his or her privacy, family, home or correspondence including personal data, or to attacks upon that person's honor and reputation. Every person has the right to the protection of the law against such interference or attacks.'*

Pada tahun 2016, negara-negara anggota ASEAN juga sepakat untuk membuat ASEAN PDP Framework pada Pertemuan Menteri Telekomunikasi dan Teknologi Informasi (*Telecommunications and Information Technology Ministers Meeting*) ASEAN ke-16,[15] yang mencantumkan tujuh prinsip utama dalam penggunaan data pribadi di ASEAN, yakni:

1. Persetujuan, pemberitahuan, dan tujuan (*consent, notification, and purpose*);
2. Akurasi data pribadi (*Accuracy of personal data*);
3. Pengamanan keamanan (*Security safeguards*);
4. Akses dan koreksi (*Access and correction*);
5. Transfer ke negara bagian atau teritori lain (*Transfers to another state or territory*);
6. Retensi (*Retention*); dan
7. Akuntabilitas (*Accountability*).

Penting untuk diketahui bahwa dengan tujuan utama ASEAN yang berpusat pada perkembangan ekonomi, pembahasan mengenai hak asasi manusia sendiri tergolong baru untuk menjadi perhatian di ASEAN.[16] Sementara itu, ASEAN juga memiliki karakteristik yang kental dengan prinsip ASEAN *way* yang menyatakan tidak bolehnya ada interferensi

[13] ASEAN, 2017-2025 ASEAN Work Programme on Electronic Commerce (diadopsi 7 September 2017).
[14] ASEAN, ASEAN Human Rights Declaration (diadopsi 18 November 2012) (**AHRD**), pasal 21.
[15] ASEAN, 'The 16th ASEAN Telecommunications and Information Technology Ministers Meeting and Related Meetings: Joint Media Statement' (2016).
[16] Graham Greenleaf, *Asian Data Privacy Laws: Trade & Human Rights Perspectives, 1st edn*, UK: Oxford University Press, 2014.[2].

Faculty of Law Universitas Gadjah Mada
Jl. Sosio Yustisia No. 1, Bulaksumur,
Sleman, D.I. Yogyakarta 55281, Republic of Indonesia
Tel +62-811-1396-565
Mail contact@alsaindonesia.org
Web www.alsaindonesia.org

antar sesama negara anggota.[17] Keberadaan badan yang bergerak di bidang hak asasi manusia di dalam ASEAN sendiri lebih kepada badan konsultasi, bukan badan penegakan yang memiliki kekuatan memberikan sanksi.[18]

Sementara itu, apabila dilihat per negara, maka saat ini belum semua negara anggota ASEAN telah memiliki peraturan perlindungan data pribadi yang dapat mencakup perlindungan dalam *e-commerce* secara komprehensif. Dari sepuluh negara ASEAN, hanya 5 negara yang telah memiliki peraturan perlindungan data pribadi, yakni Malaysia, Singapura, Filipina, Laos, dan Thailand. Sedangkan di negara lain seperti Indonesia, Myanmar, Kamboja, Brunei dan Vietnam, perlindungan khusus terhadap data pribadi belum ada, dan peraturan terkait masih bersifat sektoral.[19]

Tentunya hal ini pun berdampak pada penegakan hukum di antara negara-negara tersebut. Di Indonesia, pada awal bulan Mei 2020 dilaporkan telah terjadi kebocoran sebanyak 15 juta data pengguna *unicorn* Tokopedia berupa nama, alamat *e-mail*, dan nomor telepon.[20] Kasus serupa bahkan juga terjadi di Singapura yang telah memiliki peraturan perlindungan data pribadi, tepatnya pada perusahaan RedMart yang telah dibeli oleh Lazada. Dalam kasus tersebut, terdapat 1,1 juta data berupa nama, nomor telepon, alamat tempat tinggal, kata sandi terenkripsi, dan sebagian nomor kartu kredit pelanggan RedMart yang telah diakses secara ilegal.[21]

Melihat perkembangan penggunaan *e-commerce* yang semakin meningkat dan adanya kasus-kasus pelanggaran data pribadi di negara-negara ASEAN, maka tim peneliti dari ALSA Indonesia *Specialized Research Team* telah melaksanakan penelitian mengenai pentingnya perlindungan data pribadi dalam *e-commerce*, kerangka perlindungan data pribadi di negara-negara ASEAN, serta membandingkannya dengan keberadaan perlindungan data pribadi di Indonesia saat ini.

---

[17] Amitav Acharya, 'Culture, Security, Multilateralism: The „ASEAN way" and Regional Order' (2007) 19 Contemporary Security Policy 55, [8].
[18] Graham Greenleaf, *op.cit.*[26].
[19] Nadarashnaraj Sargunaraj, 'Personal Data Protection in ASEAN' (ZICO, April 2019) < https://zico.group/publication/personal-data-protection-in-asean/> accesed 24 November 2020.
[20] Eisya A. Eloksari, 'Tokopedia Data Breach Exposes Vulnerability of Personal Data" (The Jakarta Post, 5 May 2020) <https://www.thejakartapost.com/news/2020/05/04/tokopedia-data-breach-exposes-vulnerability-of-personaldata.html> diakses 24 November 2020.
[21] Saheli Roy Choudhury, 'TECH Alibaba-owned Lazada suffers data breach for its grocery delivery business in Singapore' (CNBC, 1 November 2020) https://www.cnbc.com/2020/11/02/alibaba-owned-lazada-suffers-databreach-on-redmart.html#:~:text=Southeast%20Asian%20e-commerce%20firm,service%20in%20the%20city-state. diakses 24 November 2020.

Faculty of Law Universitas Gadjah Mada
Jl. Sosio Yustisia No. 1, Bulaksumur,
Sleman, D.I. Yogyakarta 55281, Republic of Indonesia
Tel +62-811-1396-565
Mail contact@alsaindonesia.org
Web www.alsaindonesia.org

1.2 Rumusan Masalah

1.2.1 Bagaimana keterkaitan antara data pribadi dan penggunaan *e-commerce*?

1.2.2 Bagaimana perlindungan data pribadi pada penggunaan *e-commerce* di negara-negara ASEAN?

1.2.3 Apa saran yang dapat diberikan dalam upaya penguatan standar perlindungan data pribadi di negara-negara ASEAN?

1.3 Tujuan Penelitian

1.3.1 Mengetahui keterkaitan perlindungan data pribadi dan penggunaan *e-commerce* di ASEAN.

1.3.2 Mengetahui perlindungan data pribadi pada penggunaan *e-commerce* di negara-negara ASEAN

1.3.3 Memberikan saran untuk penguatan standar perlindungan data pribadi di ASEAN.

1.4 Metode Penelitian

Penelitian ini merupakan jenis penelitian doktrinal. Penelitian hukum doktrinal sendiri adalah penelitian-penelitian atas hukum yang dikonsepkan dan dikembangkan atas doktrin-doktrin hukum yang dikembangkan dalam kajian-kajian hukum.[22] Di Indonesia, metode penelitian hukum doktrinal lebih akrab dikenal dengan metode penelitian hukum normatif.[23] Penelitian ini juga didasarkan pada pendekatan peraturan perundang-undangan (*statute approach*), dimana peraturan perundang-undangan di Indonesia akan dibandingkan dengan peraturan perundang-undangan negara-negara ASEAN lainnya, serta dengan pendekatan komparatif (*comparative approach*)[24] yang dilakukan dengan membandingkan keadaan-keadaan serta peraturan terkait masalah dan perkembangan TIK, khususnya di lingkup perlindungan data pribadi dalam sektor *e-commerce* di Indonesia dengan negara-negara ASEAN lainnya. Perbandingan peraturan ini mencakup perbandingan jenis aturan yang ada, prinsip-prinsip, aspek

[22] Soetandyo Wignjosoebroto, HUKUM Paradigma, Metode dan Dinamika Masalahnya, Jakarta: ELSAM dan HUMA, 2002, [47].
[23] Ibid, [48].
[24] Johnny Ibrahim, Teori dan Metodologi Penelitian Hukum Normatif, Malang: Bayumedia Publishing, 2006,[300].

Faculty of Law Universitas Gadjah Mada
Jl. Sosio Yustisia No. 1, Bulaksumur,
Sleman, D.I. Yogyakarta 55281, Republic of Indonesia
Tel +62-811-1396-565
Mail contact@alsaindonesia.org
Web www.alsaindonesia.org

penegakan, dan lembaga yang menegakkan perlindungan data pribadi di negara yang bersangkutan.

Teknik pengumpulan data untuk penelitian ini adalah menggunakan teknik studi pustaka dan teknik wawancara. Studi pustaka sebagai langkah awal pengumpulan data dilakukan dengan pencarian data dan informasi melalui media cetak maupun elektronik yang diarahkan kepada topik yang akan dibahas. Sementara itu melalui wawancara, peneliti menggali data dan informasi berkaitan dengan topik permasalahan yang diteliti. Teknik wawancara yang dilakukan adalah wawancara bebas terpimpin, artinya pertanyaan yang dilontarkan tidak terpaku pada pedoman wawancara dan dapat diperdalam maupun dikembangkan sesuai dengan situasi dan kondisi lapangan. Wawancara tersebut akan dilakukan kepada pihak-pihak yang bersangkutan dengan topik riset yang telah dilakukan, yakni perwakilan akademisi maupun praktisi hukum, yang memiliki keahlian di bidang *cyber law* maupun *data protection law* beberapa negara ASEAN baik secara langsung melalui proses tatap muka melalui media daring maupun secara tidak langsung melalui pemberian *working paper* sebagai jawaban atas poin pertanyaan penelitian yang telah dikirimkan sebelumnya kepada narasumber. Berikut merupakan rincian narasumber penelitian kami:

1. Tim Subdit Tata Kelola Perlindungan Data Pribadi Direktorat Jenderal Aplikasi Informatika Kementerian Komunikasi dan Informatika Republik Indonesia (Indonesia);
2. Wahyudi Djafar selaku Direktur Eksekutif ELSAM Periode 2021-2025 (Indonesia);
3. Ardhanti Nurwidya selaku *Senior Manager of Public Policy and Government Relation* & *Group Data Protection Officer* Gojek dan *Founder of* Asosiasi Praktisi Perlindungan Data Indonesia (APPDI) (Indonesia);
4. Sonny Zulhuda, LL.B. (Honours), MCL., Ph.D. selaku *Associate Professor on Cyber Law & Data Protection Law* at International Islamic University Malaysia (Malaysia);
5. Maria Francesca Montes, J.D. selaku *Head of Artificial Intelligence and Data Policy and Data Protection Officer* at Union Bank of The Philippines (Filipina);

Faculty of Law Universitas Gadjah Mada
Jl. Sosio Yustisia No. 1, Bulaksumur,
Sleman, D.I. Yogyakarta 55281, Republic of Indonesia
Tel +62-811-1396-565
Mail contact@alsaindonesia.org
Web www.alsaindonesia.org

6. Jasmine Wong selaku *Senior Manager of Legal Department* at Authority for Info-communications Technology Industry of Brunei Darussalam (AITI)) dan Pengiran Alias (AITI's Brunei Darussalam Network Information Centre (BNNIC), *Cyber Security & Data Protection Office Manager* (Brunei Darussalam);
7. Nguyen Dung Mai dan Tu Thien Huynh selaku *Lecturer of Law* at University of Economics Ho Chi Minh City (Vietnam);
8. Kelvin Chia Partnership Yangon (Myanmar);
9. Jansen Aw selaku *Partner* at Donaldson & Burkinshaw LLP, Singapore dan *Former Assistant* Chief Counsel Personal Data Protection Commission (PDPC) Singapore (Singapura).

1.5 Dasar Hukum

Brunei Darussalam

1.5.1 Data Protection Policy 2014

1.5.2 The Electronic Transaction Act

Filipina

1.5.3 The Republic Act No. 10173

1.5.4 The Implementing Rules and Regulations of the PDPA

Indonesia

1.5.5 Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

1.5.6 Undang-Undang Republik Indonesia Nomor 7 Tahun 2014 tentang Perdagangan.

1.5.7 Peraturan Pemerintah Nomor 80 Tahun 2019 tentang Perdagangan Melalui Sistem Elektronik.

1.5.8 Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem Elektronik.

1.5.9 Peraturan Menteri Komunikasi dan Informasi Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik.

1.5.10 Rancangan Undang-Undang Perlindungan Data Pribadi.

Faculty of Law Universitas Gadjah Mada
Jl. Sosio Yustisia No. 1, Bulaksumur,
Sleman, D.I. Yogyakarta 55281, Republic of Indonesia
Tel +62-811-1396-565
Mail contact@alsaindonesia.org
Web www.alsaindonesia.org

Kamboja

1.5.11 Cambodia Civil Code

1.5.12 Cambodia Criminal Procedure Law

1.5.13 Cambodia Penal Code

1.5.14 *E-commerce* Law 2019.

Laos

1.5.15 Guidelines on the Implementation of the Law on Electronic Data Protection (No. 2126/MoPTC).

1.5.16 Law on Prevention and Combating Cyber Crime 2015.

Malaysia

1.5.17 Personal Data Protection Act 2010.

Myanmar

1.5.18 Law on Electronic Data Protection No. 25/NA (2017)

1.5.19 Financial Institutional Law 2016.

1.5.20 Private Healthcare Services 2007.

Singapura

1.5.21 Personal Data Protection Act 2012 (No. 26 of 2012)

Thailand

1.5.22 Personal Data Protection Act, B.E. 2562 (2019)

Vietnam

1.5.23 Civil Code 2013

1.5.24 Law on Information Technology (Law 67/2006/QH11)

1.5.25 Law on Consumer Protection (LoCP) 2010

1.5.26 Law on Digital Transaction (LoDT) 2005

1.5.27 Law on Network Information Safety (LoNIS)

1.5.28 Law on Cybersecurity (Law 24/2018/QH14) (CSL) 2018

1.5.29 Peraturan terkait, yakni Decree 52/2013/ND-CP dan Decree 72/2013/ND-CP

Faculty of Law Universitas Gadjah Mada
Jl. Sosio Yustisia No. 1, Bulaksumur,
Sleman, D.I. Yogyakarta 55281, Republic of Indonesia

Tel +62-811-1396-565
Mail contact@alsaindonesia.org
Web www.alsaindonesia.org

BAB II
PEMBAHASAN

2.1 Keterkaitan Perlindungan Data Pribadi dan *E-Commerce*

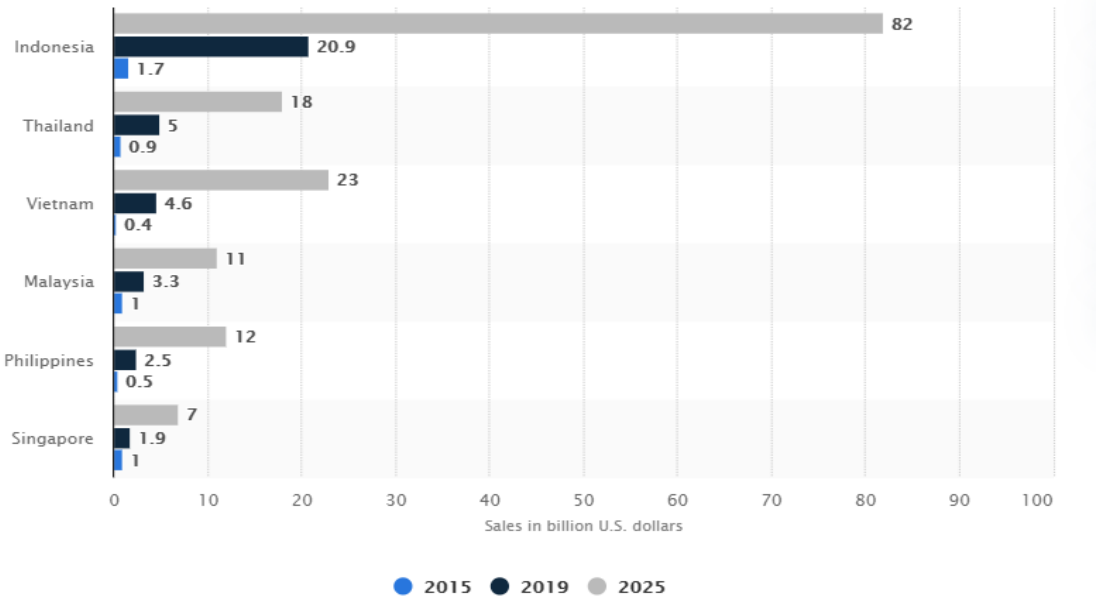
Tidak dapat dipungkiri bahwa internet membawa perubahan besar bagi aktivitas kita sehari-hari. Perkembangan teknologi telah meleburkan garis antara bidang fisik dan digital, yang menyebabkan tidak sedikit aktivitas kita di dunia maya akan mempengaruhi kehidupan di dunia nyata. Salah satu manfaat yang dapat dirasakan dari adanya perkembangan teknologi, khususnya pada penggunaan *e-commerce* di negara-negara ASEAN, adalah adanya inovasi terus menerus, serta bertambahnya pemasukan nasional. Di sisi lain, terdapat pula tantangan bagi kehidupan kita sehari-hari, yang erat kaitannya dengan privasi.

ASEAN sendiri merupakan rumah bagi 672 miliar penduduk,[25] dengan presentasi penetrasi internet rata-rata sebesar 55,1% pada tahun 2020.[26] Jumlah ini akan diperkirakan terus naik setiap tahunnya, sehingga semakin besar pula keterkaitan antara dunia digital dan kehidupan sehari-hari kita. Salah satu inovasi yang sangat relevan dengan aktivitas sehari-hari dan akan terus berkembang ialah industri *e-commerce*, yang memungkinkan kita berbelanja secara online secara lebih efektif dan efisien, dengan berbagai tawaran menarik yang akan ditawarkan setiap periodenya.[27] Pada tahun 2020, perusahaan data statistik Statista melaporkan jumlah Volume Barang Dagangan Bruto (*Gross merchandise volum*e/GMV) pasar *E-commerce* di kawasan ASEAN pada 2015 dan 2019, serta perkiraan untuk tahun 2025 sebagai berikut.[28]

[25] 'South-Eastern Asia Population' (Worldometer) <https://www.worldometers.info/world-population/south-eastern-asia-population/>, diakses pada 20 Januari 2021.
[26] 'Internet penetration rate Asia 2009-2020', (Statista 2020) <https://www.statista.com/statistics/265156/internet-penetration-rate-in-asia/>, diakses 20 Januari 2021.
[27] Dave Chaffey, 'The reasons why consumers shop online instead of in stores', (Smart Insight, 2017) <https://www.smartinsights.com/ecommerce/ecommerce-strategy/the-reasons-why-consumers-shop-online-instead-of-in-stores/>, diakses 20 Januari 2021.
[28] 'Gross merchandise volume (GMV) of the e-commerce market in the ASEAN region in 2015 and 2019 with a forecast for 2025, by country', (Statista, 2019) <https://www.statista.com/statistics/1177826/asean-e-commerce-gross-merchandise-volume-by-country/>, diakses 20 Januari 2021.

Faculty of Law Universitas Gadjah Mada
Jl. Sosio Yustisia No. 1, Bulaksumur,
Sleman, D.I. Yogyakarta 55281, Republic of Indonesia
Tel +62-811-1396-565
Mail contact@alsaindonesia.org
Web www.alsaindonesia.org

Gambar 2.1 *Gross Merchandise Volume* Pasar *E-Commerce* di Kawasan ASEAN Tahun 2015 dan 2019 dan Perkiraan Tahun 2025



Sumber: Statista

Pada data tersebut dapat dilihat bahwa setidaknya ada 6 (enam) negara anggota ASEAN yang memiliki total nilai moneter penjualan terbesar di ASEAN, yakni Indonesia, Thailand, Vietnam, Malaysia, Filipina, dan Singapura. Indonesia sendiri diperkirakan akan meningkat secara drastis pada tahun 2025, di mana GMV *e-commerce* di Indonesia diperkirakan mencapai $82 miliar.[29] Angka tersebut tentunya merupakan berita baik bagi negara-negara ASEAN untuk dapat mengembangkan negaranya melalui ekonomi digital.

Seiring dengan munculnya potensi yang besar tersebut, privasi merupakan aspek yang kerap terkikis dalam aktivitas maya tersebut. Hal ini ditunjukan oleh adanya pelanggaran-pelanggaran yang terjadi dalam pemanfaatan data oleh para penyelenggara layanan elektronik.[30] Secara umum, pelanggaran privasi dapat berupa kebocoran, pengungkapan, atau kesimpulan yang tidak diinginkan atas informasi pribadi atau rahasia. Dari pengertian tersebut, dapat dilihat kaitan erat antara privasi dan data pribadi. Pada praktiknya, data pribadi dikumpulkan untuk membentuk suatu informasi mengenai individu, yang dapat digunakan dalam berbagai kepentingan,

[29] Ibid.
[30] Radi P. Romansky dan Irina S. Noninska, "Challenges of the digital age for privacy and personal data protection' (2020) 17 Mathematical Biosciences and Engineering, [5295].

Faculty of Law Universitas Gadjah Mada
Jl. Sosio Yustisia No. 1, Bulaksumur,
Sleman, D.I. Yogyakarta 55281, Republic of Indonesia
Tel +62-811-1396-565
Mail contact@alsaindonesia.org
Web www.alsaindonesia.org

termasuk kepentingan ekonomi.

Dalam proses *e-commerce*, misalnya, penyelenggara elektronik dapat memanfaatkan informasi pribadi untuk menciptakan 'pembeda' layanan mereka melalui peningkatan hubungan pelanggan, komunikasi langsung, dan layanan yang dipersonalisasi. Salah satu proses yang paling umum dalam mewujudkan hal ini adalah melalui '*cookie*'. *Cookie* adalah kumpulan informasi yang disimpan situs *web* di komputer kita. Biasanya, *cookie* dirancang untuk mengingat dan menginformasikan situs *web* yang kita kunjungi kembali tentang beberapa informasi berguna tentang aktivitas kita di internet. *Cookies* adalah metode paling umum untuk mengidentifikasi dan melacak aktivitas konsumen online.[31]

Selain itu, terdapat pula bentuk-bentuk *software* yang dapat mengutip data-data dari perangkat kita, seperti melalui *web-bugs*, *spywares*, *adwares*, dan sebagainya.[32] Sering kali aktivitas-aktivitas pemrosesan data tersebut terjadi tanpa sepengetahuan kita, demi kepentingan penyedia layanan belanja *online* tersebut. Praktik pemrosesan data yang terjadi di 'balik layar' tersebutlah yang dapat menimbulkan pelanggaran terhadap privasi kita.

Di era digital ini, pelaku bisnis semakin terdorong untuk mengumpulkan dan menggunakan informasi pribadi dalam jumlah besar karena potensinya untuk menghasilkan nilai finansial yang sangat besar. Oleh karenanya muncullah konsep '*data is the new oil*' yang merujuk pada fakta bagaimana data pribadi dapat dimonetisasi.[33] Pelanggaran privasi dapat terjadi dengan cara akuisisi, penyimpanan, penjualan dan penggunaan informasi pribadi tanpa kesadaran dan/ atau persetujuan dari subjek pemilik data.[34] Tindakan ini tidak hanya mengancam hak asasi kita atas privasi, namun juga mengakibatkan kerugian finansial. Berikut merupakan penjelasan mengenai beberapa praktik pelanggaran data tersebut.

2.2.1. Akuisisi Ilegal

Tindakan ini dilakukan dengan mengumpulkan data pribadi

[31] Anthony D. Miyazaki, "Online Privacy and the Disclosure of Cookie Use: Effects on Consumer Trust and Anticipated Patronage", (2008) 27 Online Privacy and the Disclosure of Cookie Use, [20].
[32] Paolo Guarda, "Data Protection, Information Privacy, and Security Measures: An Essay on the European and the Italian Legal Frameworks" (2009) Ciberspazio e diritto.[68].
[33] P Rotella, "Is data the new oil?" (Forbes, 2012) <http://www.forbes.com/sites/perryrotella/2012/04/02/is-data-thenew-oil/.> diakses 20 Januari 2021.
[34] Milena Head dan Yufei Yuan, "Privacy Protection in Electronic Commerce - A Theoretical Framework" (2001) 20 Human Systems Management.[151].

Faculty of Law Universitas Gadjah Mada
Jl. Sosio Yustisia No. 1, Bulaksumur,
Sleman, D.I. Yogyakarta 55281, Republic of Indonesia
Tel +62-811-1396-565
Mail contact@alsaindonesia.org
Web www.alsaindonesia.org

secara tersirat atau terselubung. Hal ini bisa dilakukan setiap hari oleh pelaku bisnis yang mencari keunggulan kompetitif. Tindakan akuisisi dapat menjadi pelanggaran privasi jika dikumpulkan tanpa persetujuan dan identitas subjek tetap dikaitkan dengan informasi pribadi. Akuisisi ilegal juga dapat terjadi karena tindakan seorang '*hacker*' (peretas). Seorang peretas dapat memperoleh informasi langsung dari subjek privasi, namun sering kali mereka mencuri data dari tempat penyimpanan data informasi dari organisasi pengumpul data yang lebih besar, baik karena alasan kesenangan semata maupun alasan politik dan ideologis.[35]

2.2.2. Penyimpanan Ilegal

Pengumpulan informasi dapat dilakukan dalam penggunaan waktu dekat, atau untuk penyimpanan jangka panjang. Sering kali, penyimpanan data pribadi dalam jangka panjang lah yang dapat mengganggu hak atas privasi kita. Penyimpanan tersebut mempengaruhi hak seseorang untuk menentukan informasi apa yang ingin mereka ungkapkan tentang masa lalu mereka. Hal ini dapat mempengaruhi kehidupan seseorang, misalnya berkenaan dengan kesalahan masa lalu seseorang yang tersimpan di internet yang dapat mempengaruhi masa depannya.[36]

2.2.3. Penjualan Ilegal

Penjualan ilegal merupakan salah satu bentuk pelanggaran privasi yang paling besar saat ini. Semakin sering informasi pribadi dibeli dan dijual melalui internet, semakin besar pula kemungkinannya jatuh ke tangan yang salah.[37] Contohnya pernah terjadi pada GeoCities pada tahun 1998. Geocities merupakan layanan pembuatan *website* yang memiliki beberapa juta pengguna. Kasusnya terjadi ketika diketahui bahwa GeoCities menyesatkan penggunanya, di mana informasi pengguna dijual kepada pemasar target tanpa sepengetahuan

[35] Ibid.[156].
[36] Ibid.[156].
[37] Ibid.[156].

Faculty of Law Universitas Gadjah Mada
Jl. Sosio Yustisia No. 1, Bulaksumur,
Sleman, D.I. Yogyakarta 55281, Republic of Indonesia
Tel +62-811-1396-565
Mail contact@alsaindonesia.org
Web www.alsaindonesia.org

pemilik data tersebut.[38]

2.2.4. Penggunaan Ilegal

Penggunaan informasi pribadi dapat mengakibatkan pelanggaran dengan konsekuensi yang signifikan. Data pribadi dapat digunakan untuk tindakan ilegal yang secara langsung mempengaruhi seseorang, misalnya melalui pengiriman *email* "spam" yang mengancam seseorang, atau hal-hal lain yang dapat mengakibatkan kerugian personal dan/atau moneter yang lebih serius. Atas dasar ini, sangat penting bagi pemilik data untuk mengetahui tujuan pengumpulan dan penggunaan data mereka, untuk menjaga dampak yang dapat terjadi nantinya.[39]

2.2.5. Kebocoran Data Pribadi

Kebocoran data pribadi adalah pengungkapan informasi rahasia yang disengaja atau tidak disengaja kepada pihak yang tidak berwenang. Kebocoran data sering kali disebabkan oleh kegagalan dalam menciptakan sistem keamanan yang memadai untuk melindungi penyimpanan data, dan merupakan ancaman serius bagi operasi perusahaan, baik pihak swasta maupun pihak pemerintah. Bocornya informasi sensitif dapat menyebabkan kerusakan reputasi dan kerugian finansial yang signifikan, bahkan mengancam stabilitas jangka panjang suatu organisasi. Jenis-jenis informasi yang bocor ini dapat berupa data pribadi karyawan maupun pelanggan, kekayaan intelektual, hingga catatan medis.[40] Jenis pelanggaran ini sering berkaitan dengan kejahatan akuisisi ilegal, dan merupakan yang paling sering menarik perhatian publik.[41]

---

[38] Rachel Withers, "Before Facebook, There Was GeoCities" (Slate, 2018) <https://slate.com/technology/2018/04/the-ftcs-1998-case-against-geocities-laid-the-groundwork-for-facebook-debates-today.html>, diakses 20 Februari 2021.

[39] Milena Head dan Yufei Yuan, *op.cit.*

[40] Cristina Lago, 'The biggest data breaches in Southeast Asia' (CSO, 2020) <https://www.csoonline.com/article/3532816/the-biggest-data-breaches-in-southeast-asia.html>, diakses 20 Februari 2021.

[41] Long Cheng (et.al), 'Enterprise data breach: causes, challenges, prevention, and future directions' (2017) 7 Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery Publisher: Wiley.[1].

Faculty of Law Universitas Gadjah Mada
Jl. Sosio Yustisia No. 1, Bulaksumur,
Sleman, D.I. Yogyakarta 55281, Republic of Indonesia
Tel +62-811-1396-565
Mail contact@alsaindonesia.org
Web www.alsaindonesia.org

Perlu dicatat bahwa perlindungan data pribadi tidak hanya berbicara soal sistem teknologi saja, melainkan juga perlindungan hukum. Pada praktiknya, teknologi seperti *firewall*, kriptografi kunci-publik (*public key encryption*), lapisan soket aman (*Secure Socket Layer/* SSL) telah digunakan untuk meningkatkan keamanan (*security*) data. Meski demikian, teknologi tersebut belum tentu dapat melindungi privasi konsumen melalui perlindungan data pribadi.[42] Keamanan data berfokus pada perlindungan semua data organisasi dari pencurian atau kerusakan (seperti ketika adanya serangan *ransomware*), sedangkan perlindungan data sifatnya lebih spesifik. Pemenuhan perlindungan data pribadi harus didukung oleh aspek teknologi, hukum, dan sistem administrasi. Oleh karena itu, suatu organisasi harus memahami, melacak, dan mengontrol hal-hal pemanfaatan dan pengelolaan data tersebut.[43]

Dari sisi ketika terjadinya pelanggaran, biaya yang harus dikeluarkan ketika terjadinya kebocoran data dan insiden keamanan *cyber* tidaklah murah, dan akan terus meningkat setiap tahunnya.[44] Berdasarkan laporan *International Business Machines* (IBM) dan *Ponemon Institute*, biaya total rata-rata atas adanya pelanggaran data di ASEAN pada tahun 2019 sendiri mencapai $2.62 juta[45] dan naik hingga $2.71 juta pada tahun 2020.[46] Laporan yang sama juga mengatakan bahwa Informasi Identitas Pribadi (*Personally Identifiable Information*/ PII) pelanggan adalah jenis data tersimpan yang paling sering disusupi, sekaligus paling mahal, dalam kasus pelanggaran data yang diteliti.[47]

Dalam kaitannya dengan *e-commerce*, perlindungan data juga tidak hanya bertujuan untuk melindungi kerahasiaan informasi personal, melainkan untuk menciptakan kepercayaan bagi pengguna dalam transaksi online.[48] Menurut penelitian

[42] Ibid.[151].
[43] Allen Bernard, 'Data privacy and data security are not the same', (Zdnet Austus 2020) <https://www.zdnet.com/article/data-privacy-and-data-security-are-not-the-same/> diakses 20 Februari 2021.
[44] Dan Swinhoe, "What is the cost of a data breach?" (CSO, 2020) <https://www.csoonline.com/article/3434601/what-is-the-cost-of-a-data-breach.html#:~:text=The%20average%20cost%20of%20a,over%20the%20last%20five%20years> diakses 20 Februari 2021.
[45] IBM, "Cost of a Data Breach Report 2019", (IBM Security, 2019) <https://www.ibm.com/downloads/cas/ZBZLY7KL?_ga=2.214883607.1034594978.1579101338-1286175879.1579101338>, diakses 20 Februari 2021.
[46] IBM, "Cost of a Data Breach Report 2020", (IBM Security, 2020) https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/pdf/>, diakses 20 Februari 2021.
[47] Ibid.
[48] A Bakar Munir dan Mohd SH Yasin, *Information and Communication Technology Law: State, Internet and Information, Legal and Regulatory Challenges*, (Sweet and Maxwell Asia, 2018).[40].

Faculty of Law Universitas Gadjah Mada
Jl. Sosio Yustisia No. 1, Bulaksumur,
Sleman, D.I. Yogyakarta 55281, Republic of Indonesia
Tel +62-811-1396-565
Mail contact@alsaindonesia.org
Web www.alsaindonesia.org

Steven Muzatko dan Gaurav Bansal, kasus pelanggaran data berdampak pada pengurangan kepercayaan dari konsumen. Penelitian tersebut juga menemukan kecenderungan pengurangan kepercayaan konsumen ketika adanya penundaan terhadap pengumuman terjadinya pelanggaran data.[49]

Kepercayaan selalu menjadi elemen penting dalam mempengaruhi perilaku konsumen terhadap pedagang, dan telah terbukti sangat penting dalam *e-commerce*. Hal ini juga secara langsung mempengaruhi perilaku pembelian, baik dari segi biaya, preferensi, maupun frekuensi kunjungan. Pada akhirnya, kepercayaan pun akan mempengaruhi tingkat profitabilitas yang dapat diterima oleh pedagang di *e-commerce* dari konsumen.[50] Adanya 'harga' yang harus dibayar ketika terjadinya pelanggaran data menunjukkan signifikansi bagi perlindungan data pribadi dalam penggunaan *e-commerce*.

Adanya peningkatan keamanan sistem dan penguatan kepercayaan konsumen atas perlindungan data pribadi dapat meningkatkan pula pertumbuhan dalam aktivitas jual beli *online*. Tanpa perlindungan tersebut, konsumen tidak akan mengunjungi atau berbelanja pada suatu platform. Sebaliknya, penyelenggaraan platform *e-commerce* juga tidak dapat berfungsi secara efektif. Dalam hal ini, maka teknologi dan hukum harus saling berkoordinasi dalam pendorong laju inovasi dan kepercayaan pengguna terhadap pemanfaatan *e-commerce*.[51]

2.2 Perbandingan Kerangka Pengaturan Perlindungan Data Pribadi di Negara-Negara ASEAN

ASEAN adalah organisasi regional yang dibentuk pada tahun 1967, dan saat ini beranggotakan sepuluh orang: Singapura, Laos, Vietnam, Brunei Darussalam, Thailand, Filipina, Malaysia, Myanmar, Kamboja, dan Indonesia. Kerja sama yang dijalin negara-negara ini tidak hanya mencakup bidang ekonomi saja, melainkan juga

[49] Steven Muzatko dan Gaurav Bansal, 'Timing of Data Breach Announcement and E-Commerce Trust' (2018). MWAIS 2018 Proceedings.[7].
[50] R. Mekovec*and Ž. Hutinski, 'The role of perceived privacy and perceived security in online market' (2012) Proceedings of the 35th International Convention MIPRO 2012/ISS.[1884].
[51] Robert E. Litan, 'Law and policy in the age of the Internet' (2001) 50 Duke Law Journal.[1085].

Faculty of Law Universitas Gadjah Mada
Jl. Sosio Yustisia No. 1, Bulaksumur,
Sleman, D.I. Yogyakarta 55281, Republic of Indonesia
Tel +62-811-1396-565
Mail contact@alsaindonesia.org
Web www.alsaindonesia.org

ilmu pengetahuan dan teknologi, kebudayaan dan informasi, dan kerja sama transnasional lainnya.[52]

Berbeda dengan organisasi regional pada umumnya, ASEAN tidak memiliki sistem pengambilan keputusan dan implementasi yang jelas. Pendekatan yang digunakan oleh negara-negara ASEAN lebih kepada 'dialog' dan 'mekanisme konsultatif'.[53] Hal ini tercermin dalam Pasal 20 Piagam ASEAN yang menguraikan bahwa keputusan akan didasarkan pada konsultasi dan konsensus. Keengganan pembentukan kewajiban yang mengikat atau mekanisme penegakan hukum di dalam ASEAN berakar dalam pada prinsip-prinsip fundamental *non-intervention* dan penghormatan terhadap kedaulatan negara-negara anggotanya.

Meski demikian, secara umum prinsip-prinsip yang telah dicantumkan dalam ASEAN *Framework on Data Protection* juga dapat dilihat dari praktik per negara anggotanya. Adapun data mengenai kerangka perlindungan data pribadi di negara-negara ASEAN adalah sebagai berikut:

Tabel 2.1 Perbandingan Keberadaan Peraturan Perlindungan Data Pribadi dan Lembaga Berwenang di Negara-Negara ASEAN

No.	Nama Negara Anggota	Peraturan Perlindungan Data Pribadi Komprehensif	Lembaga Berwenang
1.	Singapura	Personal Data Protection Act 2012 (No. 26 of 2012)	*Personal Data Protection Commission*
2.	Laos	Law on Electronic Data Protection No. 25/2017	*The Ministry of Post, Telecommunications and Communications*
3.	Vietnam	-	-
4.	Brunei	-	-

[52] "ASEAN Member States" (Association of Southeast Asian Nations) <https://asean.org/asean/asean-member-states/>, diakses 21 Februari 2021.
[53] Amitav Acharya, op.cit,[8].

Faculty of Law Universitas Gadjah Mada
Jl. Sosio Yustisia No. 1, Bulaksumur,
Sleman, D.I. Yogyakarta 55281, Republic of Indonesia
Tel +62-811-1396-565
Mail contact@alsaindonesia.org
Web www.alsaindonesia.org

5.	Thailand	Personal Data Protection Act, B.E. 2562 (2019)	*Thailand Personal Data Protection Committee*
6.	Filipina	The Republic Act No. 10173 (Data Privacy Act of 2012) dan *the Implementing Rules and Regulations of the DPA*	*National Privacy Commission*
7.	Malaysia	Personal Data Protection Act 2010	*Personal Data Protection Commission*
8.	Myanmar	-	-
9.	Kamboja	-	-
10.	Indonesia	-	-

2.2.1 Singapura

Dalam hal perlindungan privasi data, Singapura terhitung lebih maju daripada negara-negara ASEAN lainnya. Sejak 2012, Singapura telah memberlakukan *Personal Data Protection Act* 2012 (No. 26 of 2012) (PDPA), yang kemudian berlaku pada Januari 2013. Ruang lingkup keberlakuan PDPA mencakup semua organisasi yang menggunakan, mengumpulkan, atau menampilkan data pribadi Singapura, baik di dalam atau di luar wilayah Singapura. PDPA ini tidak berlaku terhadap instansi pemerintah serta organisasi yang bekerja untuk pemerintah. Menurut parlemen, hal ini dikarenakan lembaga pemerintah perlu mengumpulkan data ketika dibutuhkan untuk menjalankan fungsi peraturan dan perundang-undangan mereka. Pada PDPA, terdapat 9 prinsip utama sebagai berikut:[54]

2.2.1.1. *Consent Obligation* (*Section* 13-17 PDPA), bahwa sebuah organisasi harus mendapatkan persetujuan individu sebelum

[54] Hasil wawancara dengan Jansen Aw, Partner di Donaldson & Burkinshaw LLP.

Faculty of Law Universitas Gadjah Mada
Jl. Sosio Yustisia No. 1, Bulaksumur,
Sleman, D.I. Yogyakarta 55281, Republic of Indonesia
Tel +62-811-1396-565
Mail contact@alsaindonesia.org
Web www.alsaindonesia.org

mengumpulkan, menggunakan, atau menyingkap data pribadi individu tersebut untuk suatu tujuan.

2.2.1.2. *Purpose Limitation Obligation* (*Section* 18 PDPA), bahwa sebuah organisasi hanya boleh mengumpulkan, menggunakan atau mengungkapkan data pribadi untuk tujuan yang dianggap sesuai oleh orang yang wajar dalam keadaan tersebut.

2.2.1.3. *Notification Obligation* (*Section* 18 dan 20 PDPA), Organisasi harus memberi tahu individu tentang tujuan pengumpulan, penggunaan, atau pengungkapan data pribadinya pada atau sebelum pengumpulan, penggunaan, atau pengungkapan tersebut.

2.2.1.4. *Access and Correction Obligation* (*Section* 21 dan 22 PDPA), Organisasi harus, atas permintaan, mengizinkan seseorang untuk mengakses dan / atau mengoreksi data pribadinya yang dimilikinya atau di bawah kendalinya. Selain itu, organisasi berkewajiban untuk memberikan informasi kepada individu tentang cara-cara penggunaan atau pengungkapan data pribadi selama setahun terakhir.

2.2.1.5. *Accuracy Obligation* (*Section* 23 PDPA), Suatu organisasi harus melakukan upaya yang wajar untuk memastikan bahwa data pribadi yang dikumpulkan olehnya akurat dan lengkap ketika data tersebut akan digunakan dan berdampak pada individu pemilik data

2.2.1.6. *Protection Obligation* (*Section* 24 PDPA), Organisasi harus melindungi data pribadi yang dimilikinya atau di bawah kendalinya dengan membuat pengaturan keamanan yang wajar untuk mencegah akses, pengumpulan, penggunaan, pengungkapan, penyalinan, modifikasi, pembuangan, atau risiko serupa yang tidak sah.

2.2.1.7. *Retention Limitation Obligation* (*Section* 25 PDPA), Suatu organisasi harus segera berhenti menyimpan dokumen yang berisi data pribadi, atau menghapus sarana yang dapat

Faculty of Law Universitas Gadjah Mada
Jl. Sosio Yustisia No. 1, Bulaksumur,
Sleman, D.I. Yogyakarta 55281, Republic of Indonesia
Tel +62-811-1396-565
Mail contact@alsaindonesia.org
Web www.alsaindonesia.org

digunakan untuk menghubungkan data pribadi dengan individu tertentu, setelah penyimpanan data pribadi tersebut tidak lagi sesuai dengan tujuannya.

2.2.1.8. *Transfer Limitation Obligation* (*Section* 26 PDPA), suatu organisasi tidak boleh mentransfer data pribadi ke negara atau wilayah di luar Singapura yang tidak memiliki standar perlindungan yang setidaknya sebanding dengan PDPA.

2.2.1.9. *Accountability Obligation* (*Section* 11 dan 12 PDPA), sebuah organisasi harus menunjuk seseorang untuk bertanggung jawab untuk memastikan kepatuhannya terhadap PDPA, biasanya disebut sebagai petugas perlindungan data ('DPO'). DPO dapat bertugas untuk mengembangkan dan mengimplementasikan kebijakan serta praktik yang perlu dalam melindungi data pribadi, serta menerima komplain dari individu yang dikumpulkan datanya.

Dari prinsip-prinsip tersebut, dapat dilihat bahwa PDPA Singapura telah memiliki peraturan yang cukup jelas terhadap hak dan kewajiban pemilik data serta pemegang data pribadi. Persetujuan (*consent)* merupakan salah satu prinsip paling penting dalam perlindungan data pribadi di Singapura. Meski pada PDPA tidak ditentukan bagaimana cara untuk mendapatkan persetujuan pemilik data, dalam praktiknya sangat dianjurkan untuk menerapkan *opt in consent*, dikarenakan dengan metode *opt out* consent, individu belum tentu sepenuhnya setuju dengan penggunaan datanya. Dalam hal ini, fakta bahwa seorang individu tidak 'menolak' (*opt out*) pengumpulan datanya tidak bisa dianggap sebagai persetujuan dalam setiap situasi.

Selain itu, mengingat transfer data yang dapat terjadi lewat *e-commerce* cukup tidak terbatas, maka penyelenggara harus memperhatikan prinsip '*Transfer Limitation Obligation*' (Kewajiban Batasan Transfer). Dalam hal ini, setiap organisasi yang mentransfer data pribadi ke luar wilayah Singapura harus memastikan bahwa penerima data pribadi tersebut terikat oleh kewajiban standar yang ditetapkan hukum, untuk perlindungan atas data

Faculty of Law Universitas Gadjah Mada
Jl. Sosio Yustisia No. 1, Bulaksumur,
Sleman, D.I. Yogyakarta 55281, Republic of Indonesia
Tel +62-811-1396-565
Mail contact@alsaindonesia.org
Web www.alsaindonesia.org

pribadi yang sepadan dengan PDPA.[55] Selain itu, perusahaan juga sangat disarankan untuk melaksanakan Data Protection Impact Assessment (DPIA) untuk melihat adanya potensi pelanggaran data pribadi dalam suatu pemrosesan yang akan dilakukan suatu organisasi sesuai dengan *Guide to Data Protection Impact Assessments* yang dibuat oleh Komisi Perlindungan Data Pribadi (Personal Data Protection Commission/ PDPC) pada 1 November 2017.

PDPC sendiri adalah lembaga yang berwenang dalam hal perlindungan data pribadi di Singapura, yang dibentuk berdasarkan *section* 8 (1) (a) PDPA. PDPC memiliki kewenangan untuk membuat pedoman ('*guidelines*') sebagai interpretasi terhadap pelaksanaan PDPA, serta menetapkan sanksi bagi pelanggaran yang terjadi atas PDPA. Dalam praktiknya, pedoman-pedoman yang dikeluarkan oleh PDPC sangat penting dalam praktik perlindungan data pribadi di Singapura.

Belum lama ini, Singapura telah memberlakukan amandemen komprehensif pertamanya sejak tahun 2012. Amandemen ini disahkan di Parlemen Singapura pada tanggal 2 November 2020 dan akan mulai berlaku sebagian pada tanggal 1 Februari 2021. Secara garis besar, amandemen ini dilakukan untuk memperkuat perlindungan konsumen serta mendukung inovasi bisnis. Hal ini termasuk dengan memperkuat kepercayaan konsumen melalui akuntabilitas organisasi; meningkatkan efektivitas penegakan; meningkatkan otonomi konsumen; dan meningkatkan penggunaan data untuk inovasi.[56]

Dalam amandemen PDPA, terdapat perluasan konsep mengenai persetujuan, yang mewajibkan organisasi untuk memberitahukan pemilik data mengenai data yang akan digunakan untuk pemenuhan suatu tujuan kontraktual, serta notifikasi atas adanya perubahan dalam tujuan pemanfaatan data. Organisasi juga diwajibkan untuk memberikan pemberitahuan atas adanya kemungkinan atau telah terjadinya pelanggaran data pribadi dengan

[55] PDPC, 'Advisory Guidelines On Key Concepts In The Pdpa (revised 27 July 2017)' (PDPC, 2017).[37].
[56] 'Amendments to the Personal Data Protection Act and Spam Control Act Passed' (Personal Data Protection Commission Singapore, 2020), <https://www.pdpc.gov.sg/news-and-events/announcements/2020/11/amendments-to-the-personal-data-protection-act-and-spam-control-act-passed>, diakses 24 Februari 2021.

Faculty of Law Universitas Gadjah Mada
Jl. Sosio Yustisia No. 1, Bulaksumur,
Sleman, D.I. Yogyakarta 55281, Republic of Indonesia
Tel +62-811-1396-565
Mail contact@alsaindonesia.org
Web www.alsaindonesia.org

'skala besar' kepada individu yang terkait serta PDPC.[57] Selain itu, PDPC nantinya akan dapat memberlakukan sanksi finansial hingga 10% dari omset tahunan organisasi di Singapura, atau SGD 1 juta.[58]

2.2.2. Laos

Perlindungan data pribadi di Laos diatur dalam Undang-Undang Perlindungan Data Elektronik (*Law on Electronic Data Protection*) No. 25 / NA tanggal 12 November 2017 yang lingkup keberlakuannya mencakup untuk individu domestik atau asing, badan hukum atau badan hukum, yang tinggal dan beroperasi di Lao PDR. Undang-undang ini juga berlaku untuk pengguna data asing jika mereka menjalankan bisnis atau beroperasi di Lao PDR.[59] Kemudian, pada bulan Agustus 2018, Kementerian Pos dan Telekomunikasi (*Ministry of Posts and Telecommunications*) selaku otoritas yang mengatur Perlindungan Data Elektronik di Laos juga menerbitkan Pedoman Penerapan UU Perlindungan Data Elektronik (*Guidelines on the Implementation of the Law on Electronic Data Protection*) (No. 2126/MoPTC).

Pasal 8 Undang-Undang ini mengklasifikasikan data elektronik dalam dua kategori besar, yaitu data umum (*general data*) dan data khusus (*specific data*). Berdasarkan pasal 10 UU *a quo*, data pribadi termasuk kepada data khusus. Ada pun prinsip-prinsip yang berlaku dalam perlindungan data elektronik dalam Undang-undang ini adalah:

a. Sesuai dengan kebijakan, undang-undang, rencana strategi, Rencana Pembangunan Sosial Ekonomi Nasional;
b. Menjamin stabilitas bangsa, perdamaian dan ketertiban masyarakat;
c. Menjaga kerahasiaan dan keamanan data negara, individu, badan hukum atau organisasi;
d. Memastikan hak dan manfaat pemilik data; dan
e. Sesuai dengan perjanjian internasional yang diratifikasi Lao PDR.

[57] Pelanggaran dalam 'skala besar' adalah pelanggaran yang mempengaruhi 500 orang atau lebih.
[58] Jonathan Goacher, 'Amendments to Singapore's Personal Data Protection Act' (Hill Dickinson LLP, Desember 2020) <https://www.lexology.com/library/detail.aspx?g=33fcd6d1-e505-4870-991b-f0a46d3bd742>, diakses 24 Februari 2021.
[59] Nadarashnaraj Sargunaraj, 'Personal Data protection in ASEAN' (ASEAN Insider, 2019), <https://zico.group/publication/personal-data-protection-in-asean/> diakses 24 Februari 2021.

Faculty of Law Universitas Gadjah Mada
Jl. Sosio Yustisia No. 1, Bulaksumur,
Sleman, D.I. Yogyakarta 55281, Republic of Indonesia
Tel +62-811-1396-565
Mail contact@alsaindonesia.org
Web www.alsaindonesia.org

Meski tidak tertulis secara eksplisit di dalam undang-undangnya, dalam peraturan ini terdapat pula prinsip-prinsip perlindungan data yang lazim ditemukan dalam perlindungan data pribadi di negara lain. Hal ini mencakup kewajiban untuk memberitahukan pengumpulan dan penggunaan data, menjaga akurasi data yang disimpan dan akan digunakan, memastikan keamanan penyimpanan data, meminta persetujuan pemilik data untuk proses serta transfer data ke luar wilayah Laos, serta kewajiban seperti mengoreksi dan menghapus data yang tidak lagi relevan.

Mengenai kewajiban pengelola data, berdasarkan undang-undang ini "pengelola data" diwajibkan untuk memperhatikan kewajiban-kewajiban yang sudah ada pada undang-undang tersebut. Selain itu, kewajiban ini dijelaskan lebih rinci pada Panduan Perlindungan Data Elektronik. Panduan tersebut memberikan penjelasan lebih rinci mengenai:[60]

(i) pengumpulan data;
(ii) pemeriksaan data elektronik;
(iii) menyimpan / menyimpan data elektronik;
(iv) memelihara data elektronik;
(v) menggunakan dan menyebarkan data elektronik;
(vi) transmisi dan transfer data elektronik;
(vii) akses ke data elektronik;
(viii) mengubah dan memperbarui data elektronik; dan
(ix) penghapusan data elektronik.

Dalam undang-undang tersebut, tidak ada kewajiban untuk menetapkan seorang DPO bagi perusahaan, namun dalam praktiknya pengontrol data memiliki kewajiban untuk menunjuk departemen / petugas internal untuk mengawasi perlindungan data.[61] Selain itu, terkhususnya dalam keamanan data dalam sistem elektronik, Laos menetapkan beberapa kewajiban terkait dalam Undang-Undang Pencegahan dan Pemberantasan Kejahatan Dunia Maya (*Law*

[60] Kunal, "Ministry of Posts and Telecommunications Guidelines Shed Light and Clarity on the Lao PDR's Data Protection Regime", (DFPL) <https://www.ela.law/Templates/media/files/Newsletter_Articles_Clients/AP/October/Ministry_of_Posts_and_Telecommunications_Guidelines_Shed_Light_and_Clarity_on_the_Lao_PDR's_Data_Protection_Regime.pdf>, diakses 21 Februari 2021.
[61] Nadarashnaraj Sargunaraj, op.cit.

Faculty of Law Universitas Gadjah Mada
Jl. Sosio Yustisia No. 1, Bulaksumur,
Sleman, D.I. Yogyakarta 55281, Republic of Indonesia
Tel +62-811-1396-565
Mail contact@alsaindonesia.org
Web www.alsaindonesia.org

on Prevention and Combating Cyber Crime, 2015). Undang-undang tersebut mengatur mengenai kejahatan elektronik, termasuk yang dapat mempengaruhi data. Sanksi terhadap pelanggarannya dapat berupa penjara dan denda. Oleh karena itu, dalam praktiknya sangat penting bagi penyelenggara pengumpulan dan pemrosesan data untuk mendapatkan persetujuan yang valid serta memastikan keamanan sistem.

2.2.3. Vietnam

Sampai saat ini, belum ada peraturan mengenai perlindungan data pribadi yang komprehensif di Vietnam. Meski begitu, pengakuan terhadap privasi dan perlindungan data pribadi dapat ditemukan pada beberapa peraturan perundang-undangan yang berbeda-beda. Khususnya pengakuan terhadap privasi dapat ditemukan dalam Pasal 21 Kode Sipil (*Civil Code*) 2013 yang menyatakan bahwa kehidupan pribadi, rahasia pribadi, dan rahasia keluarga seseorang tidak dapat diganggu gugat dan dilindungi oleh hukum; serta pengumpulan, pelestarian, penggunaan, dan publikasi informasi tentang kehidupan pribadi seseorang harus mendapat persetujuan dari orang tersebut. Selanjutnya, peraturan terkait mengenai perlindungan data pribadi di Vietnam dapat ditemukan pada:[62]

a. *Law on Information Technology* (Law 67/2006/QH11)
b. *Law on Consumer Protection* (LoCP) 2010
c. *Law on Digital Transaction* (LoDT) 2005
d. *Law on Network Information Safety* (LoNIS)
e. *Law on Cybersecurity* (Law 24/2018/QH14) (CSL) 2018
f. Peraturan terkait, yakni *Decree* 52*/2013/ND-CP* dan *Decree 72/2013/ND-CP*

Pada Pasal 21 Law 67/2006, mengatur tentang pengumpulan, pemrosesan dan penggunaan informasi pribadi di jaringan, sedangkan Pasal 22 UU *a quo* mengatur tentang penyimpanan dan penyediaan informasi pribadi di jaringan. Kedua pasal tersebut mengatur secara umum bagaimana kewajiban

[62] Tu Thien Huynh, 'Implementation of the ASEAN Framework on Personal Data Protection as a Personal Data Protection Regulation in ASEAN Countries' 2021.

Faculty of Law Universitas Gadjah Mada
Jl. Sosio Yustisia No. 1, Bulaksumur,
Sleman, D.I. Yogyakarta 55281, Republic of Indonesia
Tel +62-811-1396-565
Mail contact@alsaindonesia.org
Web www.alsaindonesia.org

penyelenggara yang akan mengumpulkan, memproses dan menggunakan data pribadi, beserta hak pemilik data atas kegiatan yang dilakukan oleh organisasi tersebut.

Kemudian, dari segi perlindungan konsumen, LoCP mengatur dalam Pasal 6 yang menyebutkan bahwa data pribadi kosumen harus dilindungi, antara lain berkenaan dengan penyimpanan, penggunaan, pentransferan, pemberitahuan kepada pemilik data, dan sebagainya, yang secara garis besar berkenaan dengan prinsip-prinsip perlindungan data pribadi pada umumnya. Peraturan tersebut secara spesifik relevan terhadap model hubungan transaksi *B2C*, di mana pihak bisnis berkewajiban untuk memastikan kepatuhan setiap aktivitas yang melibatkan data pribadi konsumen dalam kegiatannya terhadap prinsip-prinsip perlindungan tersebut.

Dalam hal transfer data lintas batas negara, Pasal 23 (6) CSL mengatur bahwa data tidak dapat ditransfer keluar dari wilayah Vietnam, melainkan harus disimpan di dalam wilayah Vietnam. Secara khusus terhadap *E-Commerce*, Vietnam memiliki *Decree 52/2013*. Pasal 72 keputusan ini mewajibkan mengenai pelaporan adanya pelanggaran data pribadi dalam waktu 24 jam, sejak ditemukannya pelanggaran tersebut.

Lembaga yang berwenang dalam pengaturan perlindungan data pribadi di Vietnam adalah Menteri Informasi dan Komunikasi (*Ministry of Information and Communications*/ MIC). Di bawah kewenangan MIC, ada pula Departemen Keamanan Informasi (Information Safety Department/ ISD) yang menjalankan fungsi memberi nasihat dan membantu Menteri dalam manajemen keamanan informasi dan penegakan peraturan keamanan informasi. Keberadaan ISD tersebut diatur dalam Keputusan 2036 / QĐ-BTTTT yang dikeluarkan pada tahun 2019.

2.2.4. Brunei Darussalam

Pada tahun 2000, Brunei Darussalam memberlakukan kode komersial untuk transaksi elektronik. Undang-undang Transaksi Elektronik (Bab 196) didasarkan pada UNCITRAL Model Law on Electronic Commerce, 1996. Saat ini tidak ada undang-undang perlindungan data secara umum di Brunei

Faculty of Law Universitas Gadjah Mada
Jl. Sosio Yustisia No. 1, Bulaksumur,
Sleman, D.I. Yogyakarta 55281, Republic of Indonesia
Tel +62-811-1396-565
Mail contact@alsaindonesia.org
Web www.alsaindonesia.org

Darussalam, tetapi negara tersebut telah dipandu oleh Kebijakan Perlindungan Data sejak 2014. Namun hanya badan pemerintah yang tunduk pada ketentuan Kebijakan Perlindungan Data - sektor swasta tetap dikecualikan.

Sekarang ini, masyarakat Brunei Darussalam menjadi semakin sadar akan perlindungan data pribadinya saat diharuskan untuk membagikan data pribadinya sendiri. Salah satu contohnya di masa pandemi Covid-19 ini dimana ada aplikasi untuk mengidentifikasi setiap orangnya yang mengharuskan setiap orang untuk memberikan data pribadinya.

Dalam praktiknya pada sektor *e-commerce* di Brunei sudah muncul beberapa perusahaan, namun masih dalam lingkup nasional dan belum ada kasus ataupun masalah yang terjadi terkait perlindungan data pribadi dalam penggunaan *e-commerce*. Mengenai organisasi ataupun badan yang bertanggung jawab atas pengolahan perlindungan data pribadi pun belum ada dan masih di dalam wewenang Pemerintah. Untuk peraturan mengenai data pribadi Brunei Darussalam sekarang masih dalam tahap *drafting*. Untuk tahap *drafting* pun, salah satu hal yang menjadi fokus mereka adalah memfokuskan pada *crossborder transfer data*.[63]

2.2.5. Thailand

Peraturan perlindungan data pribadi Thailand diatur dalam B.E. 2562 (2019) PDPA Personal Data Protection Act (PDPA 2019). Dalam peraturan tersebut diatur mengenai definisi personal data/data pribadi, yaitu tiap informasi yang berhubungan dengan seseorang yang dapat mengidentifikasi orang tersebut secara langsung maupun tidak langsung, namun tidak mencakup informasi dari orang yang sudah meninggal.[64] PDPA 2019 mengenal beberapa definisi, yaitu personal data ialah segala data yang dimiliki oleh subjek hukum/seseorang yang dapat diidentifikasikan secara langsung ataupun tidak langsung, namun tidak termasuk pada data dari orang yang sudah meninggal. Selanjutnya, disebutkan juga mengenai *data subject*, lalu

[63] Hasil wawancara dengan Ms. Jasmine Wong selaku *Senior Manager of Legal Department* at Authority for Info-communications Technology Industry of Brunei Darussalam (AITI)) dan Pengiran Alias (AITI's Brunei Darussalam Network Information Centre (BNNIC), *Cyber Security & Data Protection Office Manager* (Brunei Darussalam, pada tanggal 22 Desember 2021.
[64] Section 6, B.E. 2562 (2019) PDPA Personal Data Protection Act.

Faculty of Law Universitas Gadjah Mada
Jl. Sosio Yustisia No. 1, Bulaksumur,
Sleman, D.I. Yogyakarta 55281, Republic of Indonesia
Tel +62-811-1396-565
Mail contact@alsaindonesia.org
Web www.alsaindonesia.org

data controller, yaitu seseorang yang mempunyai wewenang untuk membuat keputusan terkait mengumpulkan, memakai, atau menyebarkan data pribadi, serta *data processor* yaitu perseorangan/lebih yang mengoperasikan hubungan dari pengumpulan, pemakaian, dan penyebaran data dengan perintah dari *data controller*.[65]

Di dalam PDPA 2019, diatur bahwa setiap domain bisnis harus patuh terhadap PDPA apabila jika beroperasi dan memegang data subjek dari Thailand, termasuk untuk perusahaan di luar Thailand.[66] Perusahaan juga diwajibkan memiliki izin hukum untuk mengumpulkan, memproses, dan menyebarkan data tersebut. Sama seperti prinsip dalam GDPR, wewenang penggunaan data tersebut harus dengan *consent* antar pihaknya.[67]

Peraturan ini juga mengatur *sensitive personal data*, yaitu data pribadi yang mencakup hal-hal terkait etnis, ras, pandangan politik, doktrin, dan data lainnya yang dapat berpengaruh pada data subject dalam keadaan tertentu. Terdapat kewajiban pengaturan mengenai *notification requirements*, transfer data-data pribadi antar negara, hak dan kewajiban pemilik data, sanksi pidana, dan sanksi administratif.[68] Mengenai limitasi untuk menyimpan, menggunakan, dan menyalurkan data atau yang sering dikenal dengan '*Limitation to Collection, Use, and Disclosure*' juga diatur dalam PDPA 2019 dimana seorang *Data Controller* di Thailand memiliki batas dalam menyimpan, menggunakan, dan menyalurkan data, kecuali dalam keadaan tertentu dan harus dengan *consent* dari *data subject* terkait.[69]

Seorang *data controller* juga memiliki beberapa tugas, yaitu bertanggung jawab atas informasi yang selalu terbarukan untuk menghindari adanya kesalahartian terkait data pribadi yang jenis-jenis informasinya diatur dalam PDPA 2019 *Section* 39 (1). *Data controller* juga harus menyediakan sistem keamanan yang baik untuk perlindungan data pribadi yang disimpannya

[65] Robert Healey, " Thailand's New Data Protection Bill PDPA and It's Affect on Your Business?" (Relentless Data Privacy, 2020) <https://relentlessdataprivacy.com/thailands-new-data-protection-bill-pdpa-and-its-affect-on-your-business/> diakses 18 November 2020.
[66] B.E. 2562 (2019) PDPA Personal Data Protection Act Section 3.
[67] B.E. 2562 (2019) PDPA Personal Data Protection Act Section 19.
[68] Athistha (Nop) Chitranukroh, 'Thailand Personal Data Protection Act', (Tilleke & Gibbins Thailand, 2021) [10-22].
[69] B.E. 2562 (2019) PDPA Personal Data Protection Act Section 37 number (5).

Faculty of Law Universitas Gadjah Mada
Jl. Sosio Yustisia No. 1, Bulaksumur,
Sleman, D.I. Yogyakarta 55281, Republic of Indonesia
Tel +62-811-1396-565
Mail contact@alsaindonesia.org
Web www.alsaindonesia.org

untuk mencegah kebocoran data, data yang dimodifikasi tanpa *consent*, dan masalah-masalah lainnya.[70]

Lembaga yang bertanggung jawab atas perlindungan data pribadi di Thailand adalah Personal Data Protection Committee (PDPC), sebagaimana ketentuan dan strukturnya tercantum dalam PDPA 2019 Section 8, dan mengenai tugas serta wewenangnya diatur dalam Section 16, yang diantaranya ialah memastikan sistem operasi untuk promosi dan perlindungan data pribadi koheren dengan peraturan nasional, strategi nasional, dan relevan dengan rencana nasional, terkait untuk kepentingan ekonomi digital juga harus dipastikan sesuai dengan peraturan pemerintah terkait perkembangan ekonomi digital dan sosial, serta untuk mempromosikan dan membantu badan pemerintah maupun badan privat dalam aktivitas sistem tersebut, termasuk mengorganisir evaluasi dari pengoperasian sistem tersebut.[71]

Dapat dikatakan bahwa Personal Data Protection Act 2019 Thailand ialah salah satu yang cukup komprehensif mengatur tentang perlindungan data pribadi di ASEAN, karena peraturan yang baru berlaku pada tahun 2019 dan proses pengimplementasiannya masih baru berjalan.

2.2.6. Filipina

Peraturan mengenai perlindungan data pribadi di Filipina diatur dalam Data Protection Act 2012. Ada beberapa pengaturan yang diatur didalamnya seperti transparansi, lalu verifikasi umur untuk anak dibawah 16 tahun, serta memperbolehkan adanya pihak di dalam domain/perusahaan untuk melakukan *review* dan *handle* atas data-data *customer*. Untuk membuat sistem internet yang berbasis Data Protection Act, Filipina harus membuat *Data Privacy Impact Assesment* (DPIA) yang berisikan data, prosedur pengumpulan data, proses aktifitas, dan pusat data. Setelah itu, diharuskan untuk menunjuk seorang *Data Protection Officer* (DPO), yaitu orang yang bertanggung jawab agar sistem pengolahan *data protection* yang dilakukan tetap mematuhi peraturan. DPO harus didaftarkan pada *National Privacy Commission* untuk

[70] B.E. 2562 (2019) PDPA Personal Data Protection Act Section 37.
[71] B.E. 2562 (2019) PDPA Personal Data Protection Act Section 16 number (1) & (2).

Faculty of Law Universitas Gadjah Mada
Jl. Sosio Yustisia No. 1, Bulaksumur,
Sleman, D.I. Yogyakarta 55281, Republic of Indonesia
Tel +62-811-1396-565
Mail contact@alsaindonesia.org
Web www.alsaindonesia.org

mendapatkan sertifikasi. Setelah selesai, maka harus dilakukan *testing* untuk pemeriksaan yang dilakukan oleh DPO.[72]

Permasalahan yang kerap terjadi di Filipina adalah peminjaman uang secara *online*, dimana data dikumpulkan dari para peminjam uang seketika mengunduh aplikasi peminjaman uang tersebut dan memilih pilihan sepakat pada *privacy policy* tanpa membaca ketentuan lebih lanjut, kemudian aplikasi tersebut bisa mengumpulkan kontak telepon dari para peminjam uang tersebut tanpa persetujuan yang diketahui sebelumnya. Terkait permasalahan ini dapat diselesaikan oleh *Security Exchange Commision* di Filipina untuk memberikan peringatan agar masalah ini dihentikan. Untuk pelayanan terkait data pribadi sendiri di Filipina dapat dikatakan cukup baik karena *regulator* yang bertugas untuk menyelesaikan masalah-masalah terkait data pribadi dapat dihubungi dengan mudah kapan saja jika memiliki pertanyaan terkait seperti menanyakan adakah hukum negara lain mengenai perlindungan data ribadi yang diterapkan di Filipina.

Terkait dengan *e-commerce* di Filipina, sebagai salah satu pengguna media sosial terbesar dimana pasarnya pun sangat besar, banyak *e-commerce* maupun media sosial yang mendirikan kantor di Filipina seperti Google dan Facebook, yang juga memiliki *partnership* dengan bisnis-bisnis lokal di Filipina. Untuk *e-commerce* seperti Shopee, Grab, dan Lazada juga sudah memiliki DPO dan sudah bekerja sama dengan bank-bank yang ada di Filipina.

Terdapat hal unik di Filipina, yaitu adanya diskusi antar *privacy officer* di dalam *council sector* untuk mendiskusikan terkait permasalahan-permasalahan yang ada di sektor tersebut seperti tentang permasalahan *data privacy compliance,* ataupun masalah-masalah lainnya terkait perlindungan data pribadi beserta cara penyelesaian masalah-masalah tersebut. Perusahaan-perusahaan pun sudah biasa berdiskusi bersama dengan regulator dari Security Exchange Commision, yang berbentuk seperti rapat berkala maupun insidentil

[72] Alex Wall, 'Summary : Philippines Data Privacy Act and Implementing Regulations', (IAPP, 2017) <https://iapp.org/news/a/summary-philippines-data-protection-act-and-implementing-regulations/#:~:text=In%202012%20the%20Philippines%20passed,1%2C%20Sec.> diakses 7 Februari 2021.

Faculty of Law Universitas Gadjah Mada
Jl. Sosio Yustisia No. 1, Bulaksumur,
Sleman, D.I. Yogyakarta 55281, Republic of Indonesia
Tel +62-811-1396-565
Mail contact@alsaindonesia.org
Web www.alsaindonesia.org

untuk membahas dan berdiskusi mengenai perlindungan data pribadi di Filipina.[73]

Mengenai sanksi yang ada di dalam Data Protection Act 2012 masih dimuat sanksi pidana, salah satunya dikenakan terkait pemrosesan data pribadi dan informasi sensitif yang tidak diizinkan dapat dikenakan pidana penjara hingga 3 (tiga) tahun serta denda minimal Php500.000,00 dan maksimal Php2.000.000,00.[74] Dalam hukum privat Filipina sendiri juga masih banyak menggunakan sanksi pidana yang prosedurnya pun lebih sulit dari tindak pidana biasa. Menurut Ms. Maria Francesca Montez, alangkah baiknya nantinya sanksi yang digunakan bukanlah sanksi pidana, melainkan sanksi denda untuk membayar kerugian sesuai nilai kerugian yang diakibatkan dari suatu permasalahan tersebut.[75]

2.2.7. Malaysia

Malaysia merupakan salah satu dari 5 (lima) negara di ASEAN yang telah memiliki regulasi perlindungan data pribadi atau yang dikenal dengan Personal Data Protection Act 2010 ("PDPA 2010"). Proses perancangan PDPA 2010 telah dimulai sejak tahun 1999 dan baru berlaku secara efektif pada tanggal 15 November 2013.[76] Pembahasan PDPA 2010 oleh pihak legislatif Malaysia dinilai cukup banyak menuai perdebatan yang menyebabkan lamanya pengesahan terhadap peraturan tersebut.[77] PDPA 2010 dibuat dengan berkiblat pada beberapa peraturan perlindungan data pribadi di kawasan Eropa, seperti Data Protection Directive 95/46/EC of the European Union dan The ISO/IEC 270001 Information Security Management System (ISMS) yang merupakan sebuah standar internasional mengenai risiko sistem

[73] Hasil wawancara dengan Ms. Maria Francesca Montez, Vice President - Head, Artificial Intelligence & Data Policy, Data Protection Officer of Union Bank Philippines, pada tanggal 29 Desember 2020.
[74] Data Protection Act Philippines Section 25.
[75] Loc. cit
[76] DLA Piper, 'Data Protection Laws of the World: Malaysia' (2021) DLA Piper <https://www.dlapiperdataprotection.com/system/modules/za.co.heliosdesign.dla.lotw.data_protection/functions/handbook.pdf?country-1=MY> diakses pada 21 Februari 2021.
[77] *Ibid*.

Faculty of Law Universitas Gadjah Mada
Jl. Sosio Yustisia No. 1, Bulaksumur,
Sleman, D.I. Yogyakarta 55281, Republic of Indonesia
Tel +62-811-1396-565
Mail contact@alsaindonesia.org
Web www.alsaindonesia.org

teknologi informasi seperti pembajakan, virus, *malware*, dan pencurian data.[78] Namun, pada pengimplementasiannya terdapat beberapa perbedaan mendasar antara beberapa peraturan tersebut dengan norma PDPA 2010.

Prinsip yang terkandung dalam PDPA terdiri dari *general principle*, *notice and choice*, *disclosure*, *security*, *data integrity*, *retention*, dan *right of access*.[79] Ketujuh prinsip tersebut merupakan prinsip dasar yang juga diterapkan pada regulasi perlindungan data pribadi di berbagai negara. Namun, perbedaan mencolok pada PDPA 2010 adalah pemerintah termasuk dalam subjek yang dikecualikan oleh undang-undang tersebut.[80] Pengecualian tersebut memang tidak dapat dilepaskan dari semangat pembentukan PDPA 2010 yang lebih berfokus pada upaya perlindungan data pribadi di sektor komersial/bisnis. Namun, hal tersebut pula yang membuat PDPA 2010 menjadi kurang komprehensif, apalagi jika mengingat bahwa pemerintah merupakan aktor paling dominan yang memproses data pribadi warga negaranya. [81]

Di samping itu, mengenai otoritas pelaksana PDPA 2010, Malaysia memiliki sebuah komisioner yang bernama Personal Data Protection Commissioner ("Commissioner").[82] Commissioner tersebut ditunjuk oleh Menteri *casu quo* Kementerian Komunikasi dan Multimedia Malaysia.[83] Konsekuensi dari penunjukkan tersebut adalah Commissioner terkait menjadi tidak independen. Hal ini berbeda dengan konsep otoritas berdasarkan GDPR yang harus bersifat independen.[84] Namun, melalui pengecualian PDPA 2010 untuk Pemerintah, maka Commissioner yang tidak bersifat independen menjadi tidak berpengaruh secara signifikan.[85] Mengenai sanksi, PDPA 2010 hanya menerapkan sanksi pidana, berupa pidana penjara maupun denda.

[78] Data Protection Directive kini sudah diganti dengan General Data Protection Regulation ("GDPR"). PDPA 2010 disahkan sebelum berlakunya GDPR.
[79] *Vide* Part 2 Division 1 PDPA 2010.
[80] *Vide* Part 1 Section 3 PDPA 2010.
[81] Hasil wawancara dengan Sonny Zulhuda, LL.B. (Honours), MCL., Ph.D., associate professor Cyber Law & Data Protection Law di International Islamic University Malaysia, pada tanggal 19 Desember 2020.
[82] *Vide* Section 47 verse (1) PDPA 2010.
[83] Ibid.
[84] *Vide* Pasal 52 PDPA 2010.
[85] Hasil wawancara dengan Sonny Zulhuda, LL.B. (Honours), MCL., Ph.D., associate professor Cyber Law & Data Protection Law di International Islamic University Malaysia, pada tanggal 19 Desember 2020.

Faculty of Law Universitas Gadjah Mada
Jl. Sosio Yustisia No. 1, Bulaksumur,
Sleman, D.I. Yogyakarta 55281, Republic of Indonesia
Tel +62-811-1396-565
Mail contact@alsaindonesia.org
Web www.alsaindonesia.org

Sanksi perdata berupa mekanisme ganti rugi belum diakomodasi dalam PDPA 2010, sehingga tuntutan ganti rugi oleh korban harus ditempuh melalui mekanisme hukum perdata (tidak melalui PDPA 2010).[86]

Salah satu keunikan yang menjadi ciri khas rezim PDPA 2010 adalah adanya pendekatan *self-regulatory approach* melalui eksistensi *Data User Forum* ("DUF"). DUF dapat dibentuk oleh berbagai asosiasi industri, seperti industri perbankan, industri lembaga pembiayaan, industri teknologi dan informasi, dan sebagainya. DUF juga diberikan hak untuk membuat *codes of practice*. Pembuatan *codes of practice* akan menjadi landasan dan berakibat hukum bagi setiap anggota DUF dalam melakukan pemroresan data apabila sudah terdaftar di kementerian terkait.[87] Pembuatan *codes of practice* oleh DUF setidaknya akan memuat tujuan pemrosesan data, pandangan/pendapat pemilik data, dan pandangan/pendapat dari otoritas regulator berwenang.[88]

2.2.8. Myanmar

Myanmar merupakan salah satu negara di ASEAN yang belum memiliki regulasi perlindungan data pribadi dan hingga saat ini belum terdapat progress pembuatan rancangan undang-undang perlindungan data pribadi.[89] Namun, apabila diteliti terdapat beberapa norma dalam beberapa undang-undang yang beririsan dengan norma perlindungan data. Beberapa di antaranya adalah pada Financial Institution Law 2016 ("FIL 2016"). Pasal 81 FIL 2016 pada intinya mewajibkan setiap lembaga perbankan di Myanmar untuk menjaga informasi rahasia yang berkaitan dengan akun, catatan, dan transaksi dari pihak nasabah.[90] Norma perlindungan data pribadi juga dapat ditemukan pada Undang-Undang Private Healthcare Services 2007 ("PHS 2007"). Pada Pasal 25 UU *a quo*, penyedia layanan kesehatan swasta diwajibkan untuk menjaga informasi kesehatan pasien.

[86] Hasil wawancara dengan Sonny Zulhuda, LL.B. (Honours), MCL., Ph.D., associate professor Cyber Law & Data Protection Law di International Islamic University Malaysia, pada tanggal 19 Desember 2020.
[87] *Vide* section 23 *verse* (2) PDPA 2010.
[88] Hasil wawancara dengan Sonny Zulhuda, LL.B. (Honours), MCL., Ph.D., associate professor Cyber Law & Data Protection Law di International Islamic University Malaysia, pada tanggal 19 Desember 2020.
[89] William Greenlee, 'Data Privacy in Myanmar' (In-House Community, 2020) <https://www.inhousecommunity.com/article/data-privacy-myanmar/> diakses pada 14 Februari 2021.
[90] *Vide* Pasal 81 FIL 2016.

Faculty of Law Universitas Gadjah Mada
Jl. Sosio Yustisia No. 1, Bulaksumur,
Sleman, D.I. Yogyakarta 55281, Republic of Indonesia
Tel +62-811-1396-565
Mail contact@alsaindonesia.org
Web www.alsaindonesia.org

Sebagai akibat dari pengaturan yang bersifat sektoral, otoritas yang berwenang dalam proses pengawasan dan penegakan hukum terhadap pelanggaran ketentuan tersebut di atas bukan menjadi wewenang satu otoritas saja sebagaimana fungsi dari Komisioner Perlindungan Data Pribadi.[91] Pada sektor perbankan, sesuai dengan ketentuan dalam FIL 2013, otoritas yang berwenang adalah Central Bank of Myanmar.[92] Sementara itu, otoritas berwenang pada sektor kesehatan adalah Kementerian Kesehatan dan Olahraga.[93]

2.2.9. Kamboja

Sampai saat ini, Kamboja belum memiliki undang-undang khusus mengenai perlindungan data pribadi. Namun, Kamboja sudah memiliki UU *E-commerce* yang pengaturannya mencakup perlindungan data pribadi. UU *E-commerce* tersebut ditetapkan pada tanggal 2 November 2019 dan mulai berlaku efektif pada tanggal 2 Mei 2020.[94] Data pribadi yang diatur dalam UU tersebut terbatas pada data yang diproses secara elektronik.[95] Dari pihak pengguna data, perusahaan *e-commerce* wajib menyediakan nama perusahaan, alamat perusahaan, nomor yang dapat dihubungi, deskripsi lengkap terhadap komoditas yang diperjualbelikan, hingga syarat dan ketentuan standar terkait pelaksanaan perdagangan.[96] Selain itu, UU tersebut juga mengatur kewajiban pernyataan persetujuan pihak pemilik data pribadi agar dapat digunakan oleh pengguna data melalui persetujuan terhadap syarat dan ketentuan, maupun melalui sisipan tanda tangan elektronik (*e-signature*).[97]

Di samping itu, dalam UU *E-commerce* juga dikenal adanya hak retensi oleh pengguna data. Namun, yang agak membedakan adalah UU

[91] Ross Taylor, 'Myanmar - Data Protection Overview' (DataGuidance, 2020) <https://www.dataguidance.com/notes/myanmar-data-protection-overview> diakses pada 14 Februari 2021.
[92] *Ibid*.
[93] *Ibid*.
[94] Jay Cohen, 'Cambodia Enacts a new E-commerce Law and a Consumer Protection Law' (intellectual property & technology journal, 2019) <https://www.iptjournal.com/cambodia-enacts-a-new-e-commerce-law-and-a-consumer-protection-law/> diakses pada 15 Februari 2021.
[95] Jay Cohen, 'Cambodia - Data Protection Overview' (DataGuidance, 2020) <https://www.dataguidance.com/notes/cambodia-data-protection-overview> diakses pada 15 Februari 2021.
[96] *Ibid*.
[97] *Vide Article 7* of E-Commerce Law.

Faculty of Law Universitas Gadjah Mada
Jl. Sosio Yustisia No. 1, Bulaksumur,
Sleman, D.I. Yogyakarta 55281, Republic of Indonesia
Tel +62-811-1396-565
Mail contact@alsaindonesia.org
Web www.alsaindonesia.org

tersebut tidak menetapkan batas minimal maupun maksimal pelaksanaan retensi data.[98] Namun, masih terdapat acuan dari beberapa peraturan lainnya mengenai waktu retensi yang wajar. Sebagai contoh, tagihan pajak dan catatan ekspor-impor harus diretensi setidaknya selama 10 (sepuluh) tahun.[99]

Penyedia layanan pasar elektronik wajib mengupayakan perlindungan terhadap informasi pribadi konsumen untuk menghindari kebocoran data, pencurian data, modifikasi data, dan pengungkapan data secara tidak resmi. Namun, UU *E-commerce* memperboleh pengungkapan data dalam 2 (dua) kondisi, yakni disetujui oleh otoritas yang berwenang dan/atau disetujui oleh subjek pemilik data.[100] UU *a quo* juga membuat pengamanan berlapis untuk menghindari terjadinya kejahatan siber tertentu melalui pemrosesan data dengan itikad buruk atau secara tidak sah. Pelanggaran terhadap berbagai ketentuan yang diatur dalam UU tersebut dapat dikenakan berbagai sanksi, seperti pencabutan dan penangguhan lisensi, pidana penjara dari 1 bulan hingga 3 tahun, hingga sanksi denda.[101]

Pengaturan lainnya mengenai perlindungan data pribadi di Kamboja tersebar di beberapa peraturan perundang-undangan, seperti *Cambodia Civil Code*, *Penal Code*, KUHAP, dan berbagai peraturan di sektor-sektor spesifik seperti lembaga pembiayaan dan perbankan, hingga sektor kesehatan.[102]

2.2.10. Indonesia

Secara peraturan Indonesia memang belum memiliki peraturan yang mengatur tentang perlindungan data pribadi. Saat ini, peraturan perlindungan data pribadi di Indonesia pada *e-commerce*, dapat dilihat dari beberapa peraturan terkait, di antaranya:

a. Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE);
b. Undang-Undang Republik Indonesia Nomor 7 Tahun 2014 tentang Perdagangan;

[98] Jay Cohen, (n 93).
[99] *Ibid*.
[100] *Vide* Pasal 32 *E-commerce Law*.
[101] *Vide* Chapter 11 *E-commerce Law*.
[102] Jay Cohen, (n 93).

Faculty of Law Universitas Gadjah Mada
Jl. Sosio Yustisia No. 1, Bulaksumur,
Sleman, D.I. Yogyakarta 55281, Republic of Indonesia
Tel +62-811-1396-565
Mail contact@alsaindonesia.org
Web www.alsaindonesia.org

c. Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem Elektronik (PP 71/2019):
d. Peraturan Pemerintah Republik Indonesia Nomor 80 Tahun 2019 tentang Perdagangan Melalui Sistem Elektronik; dan
e. Permenkominfo Nomor 20 Tahun 2016 Tentang Perlindungan Data Pribadi Dalam Sistem Elektronik.

Terkait hal-hal yang diatur dalam peraturan-peraturan di atas antara lain, dalam PP 71/2019 disebutkan pada Pasal 11 bahwa penyelenggara sistem elektronik harus menjamin tersedianya perjanjian tingkat layanan, perjanjian keamanan informasi terhadap jasa layanan teknologi yang digunakan, dan keamanan informasi dan sarana komunikasi internal yang diselenggarakan, serta harus menjamin setiap komponen dan keterpaduan seluruh sistem elektronik beroperasi sebagaimana mestinya,[103] juga disebutkan apabila terdapat kerugian yang disebabkan oleh kegagalan sistem maka pemilik data mempunyai hak untuk mengajukan gugatan, lalu terkait prinsip juga disebutkan dalam UU ITE bahwa setiap sistem harus benar-benar aman.[104] Namun belum ada peraturan yang terkhusus membahas perihal perlindungan data pribadi dan dapat dijadikan payung hukum.

Selain itu, Indonesia juga tengah berusaha merumuskan Undang-Undang Perlindungan Data Pribadinya. Rancangan Undang-Undang Perlindungan Data Pribadi (RUU PDP) sudah dibahas di awal tahun 2014, namun baru masuk menjadi bagian dari program legislasi nasional pada tahun 2020.[105]

RUU PDP ini sudah mengatur mengenai beberapa hal, yaitu prinsip-prinsip penyelenggaraan data pribadi,[106] dibedakannya penyelenggaraan data pribadi dan data pribadi sensitif yang diatur pada Pasal 6 dan 7, hak dari pemilik data pribadi pada Pasal 8-13, kewajiban penyelenggara data pribadi, transfer data pribadi baik yang bersifat regional maupun nasional, serta sanksi terhadap pelanggarannya. Meski demikian, RUU PDP masih belum mengatur

[103] *Vide* Pasal 11 Peraturan Pemerintah Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem Elektronik.
[104] Hasil wawancara dengan Tim Subdit Tata Kelola Perlindungan Data Pribadi Direktorat Jenderal Aplikasi Informatika Kementerian Komunikasi dan Informatika RI pada tanggal 17 Desember 2020.
[105] Ibid.
[106] Pasal 5 Rancangan Undang-Undang Tentang Perlindungan Data Pribadi

Faculty of Law Universitas Gadjah Mada
Jl. Sosio Yustisia No. 1, Bulaksumur,
Sleman, D.I. Yogyakarta 55281, Republic of Indonesia
Tel +62-811-1396-565
Mail contact@alsaindonesia.org
Web www.alsaindonesia.org

kewajiban perusahaan untuk memiliki Data Protection Officer (DPO), serta lembaga yang bertanggung jawab dan menaungi segala permasalahan terkait perlindungan data pribadi. Terkait sanksi, RUU ini merumuskan 2 jenis sanksi, yaitu sanksi administratif dan sanksi pidana.[107]

2.3 Penguatan Kerangka Perlindungan Data Pribadi di Negara Anggota ASEAN

Secara global, perlindungan data pribadi awalnya dipengaruhi oleh *Organization for Economic Cooperation and Development* (OECD) *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (2012) ("OECD Guidelines 2012").[108] Panduan ini telah menjadi dasar beberapa perlindungan data pribadi negara-negara dunia. Perkembangan selanjutnya ditandai dengan disahkannya General Data Protection Regulation ("GDPR") pada tahun 2016, dan diberlakukan pada tahun 2018 di kawasan Uni Eropa.[109] GDPR mendorong negara-negara untuk turut menciptakan standar regulasi perlindungan data pribadi yang komprehensif.[110]

Dewasa ini, tiga konsep yakni konvergensi (*convergence*), harmonisasi (*harmonization*), dan unifikasi (*unification*) menjadi konsep-konsep yang terus berkembang, khususnya dalam studi perbandingan hukum dalam menemukan kerangka terbaik dalam perlindungan hukum modern, terlebihnya yang berkaitan dengan hukum siber.[111] Hal ini tidak terkecuali dalam hal perlindungan data pribadi.

Komparasi regulasi perlindungan data pribadi sangat penting untuk dilakukan karena sifat dari perlindungan data pribadi yang sangat tidak terbatas. Hal ini menyebabkan banyak kemiripan antarnegara dalam melihat isu perlindungan data pribadi.[112] Hal tersebut pula yang membuat isu perlindungan data pribadi bersifat universal dan menjadi *unified*, sehingga norma-norma yang berlaku di negara-negara

[107] Hasil wawancara dengan Tim Subdit Tata Kelola Perlindungan Data Pribadi Direktorat Jenderal Aplikasi Informatika Kementerian Komunikasi dan Informatika RI pada tanggal 17 Desember 2020.
[108] Michael Kirby, 'The history, achievement and future of the 1980 OECD guidelines on privacy' (2011) International Data Privacy Law.[6].
[109] *Vide* GDPR.
[110] Pranaya Dayalu dan M. Punnagai, 'GDPR: A Privacy Regime' (2019) International Journal of Trend in Scientific Research and Development (IJTSRD).[713].
[111] Danrivanto Budhijanto, Cyber Law dan Revolusi Industri 4.0, Bandung: Logoz Publishing, 2019, hlm. 165.
[112] 'Asia Pacific Data Protection and Cyber Security Guide 2018' (*Hogan Lovells*, 2018) <https://www.hoganlovells.com/~/media/hogan-lovells/pdf/2018/ab-data-protection-and-cybersecurity.pdf> accessed 25 July 2020, 4.

Faculty of Law Universitas Gadjah Mada
Jl. Sosio Yustisia No. 1, Bulaksumur,
Sleman, D.I. Yogyakarta 55281, Republic of Indonesia
Tel +62-811-1396-565
Mail contact@alsaindonesia.org
Web www.alsaindonesia.org

yang berbeda dapat ditarik kerangka terbaik dalam upaya menetapkan standar regulasi perlindungan data pribadi yang baik.

Tentunya, setiap negara yang telah memiliki maupun sedang berupaya merumuskan regulasi perlindungan data pribadi memiliki kelebihan dan kekurangan masing-masing. Dari perbandingan yang telah dilakukan, maka dapat ditarik beberapa poin utama yang semestinya diatur dalam suatu regulasi perlindungan data pribadi, yaitu sebagai berikut:

2.3.1. Prinsip Utama dalam Perlindungan Data Pribadi

Prinsip merupakan unsur penting dalam suatu bangunan hukum. Prinsip merupakan gagasan dasar yang bersifat abstrak dari norma-norma hukum yang lebih spesifik dan konkrit. Dengan kata lain, prinsip merupakan sumber dari norma-norma tertulis yang pada umumnya termanifestasi dalam peraturan perundang-undangan.[113] Dalam beberapa kondisi, prinsip juga dapat berperan sebagai aturan yang berlaku apabila terdapat kekosongan hukum, kekeliruan hukum, maupun kekurangan hukum.[114] Oleh karena itu, prinsip yang komprehensif dan jelas akan sejalan dengan hukum yang komprehensif dan jelas pula.

Saat ini, banyak negara yang menjadikan GDPR sebagai acuan dalam perumusan regulasi perlindungan data pribadi. GDPR dinilai sebagai regulasi perlindungan data pribadi paling komprehensif dan progresif sehingga menjadi kiblat bagi rezim regulasi perlindungan data pribadi di dunia.[115] Namun, sebelum berlakunya GDPR, rezim regulasi perlindungan dari pribadi sudah terlebih dahulu dikenal melalui OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (2012) yang pada masanya dinilai sebagai regulasi yang cukup komprehensif dalam

[113] Guido Alpa, 'General Principles of Law' (1998) Annual Survey of International and Comparative Law.[35].
[114] *Ibid*.
[115] United Nation Conference on Trade and Development, 'Data Protection Regulations and International Data Flows: Implications for Trade and Development' (2019) UNCTAD <https://unctad.org/system/files/official-document/dtlstict2016d1_en.pdf> diakses pada 21 Februari 2021.

Faculty of Law Universitas Gadjah Mada
Jl. Sosio Yustisia No. 1, Bulaksumur,
Sleman, D.I. Yogyakarta 55281, Republic of Indonesia
Tel +62-811-1396-565
Mail contact@alsaindonesia.org
Web www.alsaindonesia.org

mengejawantahkan norma-norma perlindungan data pribadi.[116] Oleh karena itu, prinsip yang terkandung dalam kedua regulasi *a quo* setidaknya dapat menjadi pedoman yang layak untuk digunakan bagi setiap negara dalam merumuskan regulasi perlindungan data pribadi.

OECD *Guidelines* berdiri di atas beberapa prinsip, yaitu *collection limitation*, *data quality*, *purpose specification*, *use limitation*, *security safeguards*, *openness principle*, *individual participation*, dan *accountability principle*.[117] Kesemua prinsip tersebut pada dasarnya memiliki makna yang sama dengan prinsip yang saat ini terkandung dalam GDPR. Walaupun memang terdapat perbedaan dalam pengklasifikasian prinsip-prinsip yang ada. Kesamaan tersebut dapat dilihat pada 6 (enam) prinsip umum yang terdapat dalam GDPR, sebagai berikut:

1. *Lawfulness, Fairness, Transparency*

   Prinsip *lawfulness* menekankan pemrosesan data pribadi harus dilakukan menurut hukum, secara adil, dan melalui metode yang transparan.[118] Pengimplementasian terhadap prinsip ini didasarkan pada 6 (enam) indikator, yaitu: (1) pemrosesan dilakukan berdasarkan persetujuan pemilik data pribadi; (2) dilakukan atas keperluan pelaksanaan kontrak dengan pemilik data pribadi; (3) patuh pada kewajiban hukum yang telah diatur dalam undang-undang; (4) adanya kesadaran bahwa penyelenggaraan data pribadi tidak terlepas dari kepentingan vital pemilik data pribadi; (5) dilakukan untuk kepentingan publik, sebagaimana telah diatur dalam undang-undang; dan (6) pengendali data pribadi dapat menunjukkan

[116] World Wide Web Foundation, 'Personal Data: An Overview of Low and Middle-income Countries' (2017) <http://webfoundation.org/docs/2017/07/PersonalData_Report_WF.pdf> diakses pada 21 Februari 2021.[8].
[117] *Vide* Part Two of OECD Guidelines 2012.
[118] Peter H. Chase, 'Perspective on the General Data Protection Regulation of the European Union' (2019) German Marshall Fund of the United States.[5].

Faculty of Law Universitas Gadjah Mada
Jl. Sosio Yustisia No. 1, Bulaksumur,
Sleman, D.I. Yogyakarta 55281, Republic of Indonesia
Tel +62-811-1396-565
Mail contact@alsaindonesia.org
Web www.alsaindonesia.org

bahwa pemrosesan data pribadi dilakukan berdasarkan '*legitimate interests*' dari pengontrol maupun pihak ketiga.[119]

2. *Purpose Limitation*

Pemrosesan data pribadi hanya dapat dilakukan dengan tujuan yang spesifik, jelas, dan sah.[120] Prinsip ini bertujuan untuk memastikan bahwa pihak yang akan memproses data pribadi terbuka terhadap alasan pemerolehan data pribadi dan bahwa apa yang dilakukan oleh pihak yang memproses data pribadi sejalan dengan ekspektasi pemilik data pribadi.[121] Implementasi terhadap prinsip ini dilakukan melalui adanya alasan dan intensi pengumpulan data yang jelas sejak awal, kepatuhan terhadap kewajiban dokumentasi untuk melakukan spesifikasi tujuan, kepatuhan terhadap kewajiban transparansi perihal tujuan pemrosesan data kepada pemilik data pribadi, serta memastikan bahwa apabila data pribadi digunakan untuk tujuan tambahan atau tujuan yang berbeda dari tujuan semula, pemrosesan tersebut harus dilakukan secara adil, sesuai dengan hukum yang berlaku, dan transparan.[122]

3. *Data Minimisation*

Data minimisation berarti pemrosesan data harus dilaksanakan dengan 3 (tiga) indikator utama, yaitu:[123]

a. Memadai: data yang diperoleh cukup untuk memenuhi tujuan yang ada;
b. Relevan: data yang diperoleh memiliki kaitan/relevansi dengan tujuan; dan

[119] *Ibid*.
[120] *Ibid*.
[121] 'Guide to the General Data Protection Regulation GDPR', (Information Commissioner's Office (ICO), 2018) <https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf> diakses pada 20 Februari 2020.
[122] *Ibid*.
[123] *Ibid*.

Faculty of Law Universitas Gadjah Mada
Jl. Sosio Yustisia No. 1, Bulaksumur,
Sleman, D.I. Yogyakarta 55281, Republic of Indonesia
Tel +62-811-1396-565
Mail contact@alsaindonesia.org
Web www.alsaindonesia.org

c. Terbatas pada kebutuhan: pengendali data pribadi tidak boleh memproses data lebih dari tujuan yang sudah dinyatakan.

4. *Data Accuracy*

Prinsip *data accuracy* menekankan pada ketepatan data pribadi yang diproses. Ketepatan data tersebut diupayakan melalui langkah-langkah logis untuk memperoleh data yang akurat, memastikan sumber dan status data pribadi jelas, secara jeli mempertimbangkan tingkat akurasi data pribadi, dan mempertimbangkan apakah data pribadi yang diperoleh memerlukan pembaharuan secara berkala atau tidak.[124] Prinsip *data accuracy* berkaitan erat dengan eksistensi "hak rektifikasi" yang dimiliki oleh pemilik data pribadi.[125] Melalui hak tersebut, pemilik data pribadi berhak untuk melakukan pembetulan/koreksi terhadap kekeliruan data pribadinya sendiri. Hak tersebut semakin memperkuat kedudukan pemilik data pribadi dalam memastikan keakuratan data pribadinya.

5. *Storage Limitation*

Konsep prinsip *storage limitation* pada dasarnya sama dengan prinsip *retention* yang terdapat pada Data Protection Act 1998, yaitu penyimpanan data tidak boleh dilakukan lebih lama dari waktu yang dibutuhkan.[126] Prinsip *storage limitation* berkaitan erat dengan prinsip *data minimisation* dan *data accuracy* yang menekankan pada penggunaan data seminimal mungkin sesuai dengan kebutuhan dan mengupayakan data pribadi yang akurat dan relevan. Lebih lanjut, prinsip *storage limitation* sangat penting untuk mengurangi risiko penggunaan

[124] Ibid.
[125] Berdasarkan KBBI, Rektifikasi berarti pembetulan kesalahan atau perbaikan.
[126] 'Guide to General Data Protection Regulation (GDPR)' op.cit 40.

Faculty of Law Universitas Gadjah Mada
Jl. Sosio Yustisia No. 1, Bulaksumur,
Sleman, D.I. Yogyakarta 55281, Republic of Indonesia
Tel +62-811-1396-565
Mail contact@alsaindonesia.org
Web www.alsaindonesia.org

data yang salah, yang tentunya dapat merugikan semua pihak terkait.[127]

6. *Integrity and Confidentiality*

Prinsip ini juga dikenal dengan sebutan *security principle*. Pengejawantahan terhadap prinsip ini dilakukan dengan berbagai cara seperti melaksanakan analisis risiko, kebijakan organisatorial, serta pengukuran terhadap hal-hal teknis.[128] Selain itu, prinsip tersebut juga mendorong penerapan berbagai bentuk keamanan data seperti pseudominisasi dan enkripsi data.[129]

2.3.2. Ruang Lingkup Regulasi Perlindungan Data Pribadi

Ruang lingkup regulasi perlindungan data pribadi berbeda-beda di setiap negara. Secara garis besar, perbedaan ruang lingkup tersebut terbagi menjadi 2 (dua), yaitu:

a. meliputi baik sektor publik maupun swasta; atau
b. hanya meliputi sektor swasta.

Sebagai contoh, PDPA 2010 Malaysia hanya berlaku untuk sektor swasta, khususnya pada transaksi komersial.[130] Sementara itu, negara di kawasan Eropa yang tunduk pada GDPR memiliki regulasi perlindungan data pribadi yang berlaku secara umum, baik di sektor swasta maupun publik dengan beberapa *exemption clause*.[131]

Sebagai payung hukum perlindungan data pribadi, UU Perlindungan Data Pribadi sebaiknya dibuat untuk seluruh sektor. Hal ini bertujuan meningkatkan efektifitas upaya perlindungan data pribadi secara luas, baik di sektor publik maupun swasta. Pengecualian berbagai sektor seperti sektor publik, terutama pemerintah (seperti Malaysia), dapat mengerdilkan efektivitas regulasi perlindungan data pribadi. Terlebih lagi, pemerintah sebagai pemegang posisi paling

[127] *Ibid*.
[128] *Ibid*.
[129] *Ibid*
[130] *Vide* Article 2 ayat (1) PDPA 2010.
[131] *Vide* Article 2 GDPR.

Faculty of Law Universitas Gadjah Mada
Jl. Sosio Yustisia No. 1, Bulaksumur,
Sleman, D.I. Yogyakarta 55281, Republic of Indonesia
Tel +62-811-1396-565
Mail contact@alsaindonesia.org
Web www.alsaindonesia.org

dominan dalam memproses data pribadi sudah semestinya termasuk pada subjek pengelola data yang diawasi demi perlindungan data pribadi yang bersifat holistik.[132]

2.3.3. Adanya Lembaga Penegak Perlindungan Data Pribadi Independen

Keberadaan otoritas pengawasan perlindungan atau biasa disebut dengan *Data Protection Authority* ("DPA") sangat penting untuk memastikan bahwa perlindungan data pribadi berjalan sebagaimana mestinya. Otoritas pengawasan yang dimaksud merupakan lembaga publik yang berfungsi memastikan kepatuhan pengendali dan prosesor data pribadi, baik individu maupun badan privat/publik terhadap regulasi perlindungan data pribadi.[133] Selain sebagai pelaksana kebijakan perlindungan data pribadi, otoritas terkait juga mengupayakan peningkatan kesadaran masyarakat, memberikan layanan konsultasi, dan pengembangan jaringan kemitraan.[134]

Dari sisi independensi, otoritas atau yang sering disebut pula dengan Komisioner dapat dibedakan menjadi komisioner yang bersifat independen dan yang tidak independen. Dalam konteks perlindungan data pribadi, komisioner independen dinilai menjadi bentuk komisi yang lebih ideal. Berkaca pada GDPR, independensi dapat diukur melalui beberapa unsur, yaitu independensi kelembagaan, independensi komisioner, independensi organisasi, independensi sumber daya manusia, serta mencegah pengaruh sektor keuangan yang dapat menurunkan independensi.[135]

Melalui statusnya yang independen, komisioner dapat lebih leluasa dalam melakukan pengawasan, baik terhadap pihak swasta maupun pihak pemerintah. Kemudian, berkaitan dengan ruang lingkup yang telah dibahas di atas, posisi pemerintah yang sangat dominan akan sangat sulit dikendalikan apabila kedudukan struktural

[132] Hasil wawancara dengan Sonny Zulhuda, LL.B. (Honours), MCL., Ph.D., associate professor Cyber Law & Data Protection Law di International Islamic University Malaysia, pada tanggal 19 Desember 2020.
[133] Wahyudi Djafar, M. Jodi Santoso, "Perlindungan Data Pribadi: Pentingnya Otoritas Pengawasan Independen", (Lembaga Studi dan Advokasi Masyarakat, 2019).[1].
[134] *Ibid*.
[135] *Vide* Article 52 GDPR.

Faculty of Law Universitas Gadjah Mada
Jl. Sosio Yustisia No. 1, Bulaksumur,
Sleman, D.I. Yogyakarta 55281, Republic of Indonesia
Tel +62-811-1396-565
Mail contact@alsaindonesia.org
Web www.alsaindonesia.org

komisioner berada langsung di bawah pemerintah. Tegasnya, Komisi yang independen akan lebih menciptakan pelaksanaan dan penegakan yang bersifat imparsial dan objektif.

2.3.4. Adanya Perumusan Sanksi yang Efektif

Jenis sanksi yang diterapkan terhadap pelanggaran norma dalam regulasi perlindungan data pribadi sangat penting diperhatikan untuk menciptakan efektivitas penegakan hukum. Sebaiknya di dalam regulasi perlindungan data pribadi mencakup beberapa jenis sanksi, yakni sanksi administratif, perdata, dan pidana.

Pemberlakuan sanksi administratif, sebaiknya menjadi sanksi utama dalam perlindungan data pribadi, mengingat sifat pemanfaatan data yang juga bersifat administratif. Sanksi ini dapat diberikan seperti melalui penangguhan maupun pencabutan lisensi, juga dapat semakin mempertegas keseriusan pemerintah dalam pelaksanaan perlindungan data pribadi.[136] Hal tersebut akan berpengaruh pada kebiasaan para pengguna data untuk lebih sungguh-sungguh dalam mewujudkan perlindungan data pribadi.

Di samping itu, sanksi perdata berupa ganti rugi juga sangat penting untuk diatur sebagai upaya pemulihan hak korban yang dilakukan dalam satu mekanisme dengan pengenaan sanksi berdasarkan regulasi perlindungan data pribadi.[137] Apabila tidak diakomodasi, korban yang dirugikan harus menempuh gugatan ganti rugi secara perdata sendiri sebagaimana yang terjadi di Malaysia.[138] PDPA 2010 Malaysia tidak memuat adanya mekanisme ganti rugi bagi korban. Dengan mengakomodasi mekanisme ganti rugi, maka regulasi perlindungan data pribadi akan menjadi lebih kokoh dalam melindungi subjek perlindungan data pribadi.

Lebih lanjut, sanksi pidana berguna untuk menimbulkan efek jera bagi pelaku pelanggaran. Sanksi pidana yang dapat diterapkan

[136] *Ibid*.
[137] Hasil wawancara dengan Sonny Zulhuda, LL.B. (Honours), MCL., Ph.D., associate professor Cyber Law & Data Protection Law di International Islamic University Malaysia, pada tanggal 19 Desember 2020.
[138] *Ibid*.

Faculty of Law Universitas Gadjah Mada
Jl. Sosio Yustisia No. 1, Bulaksumur,
Sleman, D.I. Yogyakarta 55281, Republic of Indonesia
Tel +62-811-1396-565
Mail contact@alsaindonesia.org
Web www.alsaindonesia.org

antara lain yaitu pidana penjara maupun pidana denda. Sanksi ini terutama diberikan kepada individu yang dengan sengaja melakukan pelanggaran data pribadi.

2.3.5. Peningkatan Praktik Perlindungan Data Pribadi Melalui Inisiasi Sektoral

Praktik perlindungan data pribadi secara sektoral di beberapa negara sudah menunjukkan adanya kesadaran akan pentingnya inisiasi sektoral dalam upaya perlindungan data pribadi. Contohnya, di Malaysia, PDPA 2010 memberikan ruang bagi pelaku bisnis untuk membentuk *Data User Forum* ("DUF").[139] DUF kemudian berhak membentuk *codes of practice* yang berlaku bagi asosiasi industri yang menjadi anggota dari DUF.[140] Eksistensi DUF dan *codes of practice* tersebut merupakan bentuk dari *self-regulatory approach*, di mana pihak pelaku bisnis dapat memperjelas peraturan yang sudah ada sesuai dengan *nature* tiap sektor.[141] Hal ini dapat menjadi contoh bagi negara lain untuk menciptakan peraturan yang lebih fleksibel, dinamis, relevan, dan tetap komprehensif.

Praktik lain yang dapat menjadi contoh adalah adanya forum diskusi antara *privacy officer* di *council sector*. Keberadaan forum diskusi tersebut bertujuan menjadi wadah pembahasan permasalahan yang timbul untuk kemudian menemukan solusi atas permasalahan yang timbul. Di Filipina, misalnya, kegiatan ini memungkinkan para pelaku usaha untuk berdiskusi secara langsung dengan pembuat kebijakan dari *Security Exchange Commision* yang diadakan dalam bentuk berkala maupun insidentil dalam rangka memperkuat kerangka perlindungan itu sendiri.[142]

[139] *Vide* Pasal 21 ayat (1) PDPA 2010.
[140] *Vide* Pasal 23 ayat (1) PDPA 2010.
[141] Hasil wawancara dengan Sonny Zulhuda, LL.B. (Honours), MCL., Ph.D., associate professor Cyber Law & Data Protection Law di International Islamic University Malaysia, pada tanggal 19 Desember 2020.
[142] Hasil wawancara dengan Maria Francesca Montes, J.D., Head of Artificial Intelligence and Data Policy & Data Protection Officer at Union Bank of The Philippines, pada tanggal 24 Desember 2020.

Faculty of Law Universitas Gadjah Mada
Jl. Sosio Yustisia No. 1, Bulaksumur,
Sleman, D.I. Yogyakarta 55281, Republic of Indonesia
Tel +62-811-1396-565
Mail contact@alsaindonesia.org
Web www.alsaindonesia.org

BAB III
PENUTUP

3.1. Kesimpulan

ASEAN merupakan organisasi regional kerja sama antara negara-negara Asia Tenggara yang berkecimpung dalam kerjasama ekonomi, budaya, dan teknologi. Meningkatnya kemajuan teknologi turut memajukan ekonomi kawasan ini. Salah satunya adalah akibat perkembangan *e-commerce*, yang telah memberikan inovasi dan perkembangan ekonomi. Seiring perkembangan ini, maka ASEAN juga sedang dihadapi dengan tantangan baru, yakni mengenai perlindungan data pribadi di kawasannya. Privasi dan data pribadi merupakan bagian dari hak asasi manusia, yang perlindungannya merupakan hal yang sangat penting di era ini. Tidak hanya berurusan dengan kehidupan pribadi seseorang, pemanfaatan data pribadi juga dapat mengakibatkan kerugian secara finansial.

Pentingnya perlindungan data pribadi di negara-negara anggota ASEAN terutama dikarenakan dimungkinkannya transfer data lintas batas, yang memaksa negara-negara untuk mempersiapkan kerangka perlindungan yang kokoh untuk memastikan kepercayaan antar satu negara dengan negara yang lain dan mencegah adanya pelanggaran terhadap hak tersebut. Selain itu, biaya yang harus dikeluarkan oleh adanya kegagalan dalam melindungi data menurut survey sangatlah mahal. Kegagalan juga akan menurunkan kepercayaan konsumen apabila penyelenggara layanan ditemukan lalai dalam melaksanakan tanggung jawab melindungi data pribadi tersebut. Apabila tidak ditangani, tentunya hal ini akan menghambat kemajuan *e-commerce* di kawasan ASEAN.

Oleh sebab itu, penting untuk melihat bagaimana kerangka perlindungan data pribadi di masing-masing negara, mengingat sifat ASEAN yang menjunjung tinggi prinsip *non-intervention*. Meski tidak memiliki lembaga pengimplementasian di organisasinya, dapat dilihat bahwa terdapat prinsip-prinsip umum dan praktik-praktik yang mirip yang sudah diterapkan di sepuluh negara anggotanya. Beberapa negara telah memiliki kerangka yang komprehensif, beberapa negara lagi sedang mengusahakan perumusan aturan tersebut.

Kedepannya, diharapkan semua negara-negara tersebut untuk dapat memiliki kerangka perlindungan data pribadi yang kokoh, demi memaksimalkan potensi

Faculty of Law Universitas Gadjah Mada
Jl. Sosio Yustisia No. 1, Bulaksumur,
Sleman, D.I. Yogyakarta 55281, Republic of Indonesia
Tel +62-811-1396-565
Mail contact@alsaindonesia.org
Web www.alsaindonesia.org

perkembangan teknologi dan internet, khususnya di bidang *e-commerce*. Ada pun poin yang dapat diberikan dalam rangka menguatkan kerangka perlindungan data pribadi antara lain adalah dengan penyeragaman prinsip-prinsip umum dalam peraturan perlindungan data pribadi, mengatur ruang lingkup peraturan perlindungan data pribadi yang mencakup sektor publik dan privat, adanya lembaga penegak perlindungan data pribadi independen, perumusan sanksi yang efektif yang mengedepankan sanksi administratif, dan peningkatan praktik perlindungan data pribadi melalui inisiasi sektoral.

3.2. Rekomendasi ALSA Indonesia

Penelitian ini dilakukan dengan tujuan untuk memberikan gambaran umum (*overview*) mengenai keterkaitan perlindungan data pribadi dan penggunaan *e-commerce* di ASEAN. Maka dari itu, saran yang diberikan mengenai penguatan standar perlindungan data pribadi di ASEAN, sebagaimana dimaksud dalam poin 3 pembahasan penelitian, ditujukan secara umum kepada seluruh *stakeholder* terkait dalam upaya peningkatan perlindungan data pribadi dalam penggunaan *e-commerce* di kawasan ASEAN.

Namun melalui penelitian ini, ALSA Indonesia secara khusus juga memberikan saran dalam bentuk rekomendasi kepada seluruh *stakeholder* terkait yang sedang berupaya melakukan peningkatan perlindungan data pribadi di Indonesia, mengingat saat ini pemerintah bersama Dewan Perwakilan Rakyat Republik Indonesia (DPR-RI) secara bersama-sama sedang menyusun RUU PDP. Maka dari itu, berdasarkan data yang diperoleh dan hasil analisis yang dilakukan oleh ALSA Indonesia Specialized Research Team, ALSA Indonesia memiliki beberapa rekomendasi kepada pemerintah Indonesia maupun *stakeholder* terkait, sebagai berikut:

1. **Mengapresiasi dan mendukung upaya dari pemerintah** yang telah **memberikan atensi dan tengah berupaya** melakukan peningkatan dalam hal perlindungan data pribadi di Indonesia;
2. **Mengapresiasi inisiatif dari pemerintah**, serta **mendukung kinerja yang sinergis antara pemerintah dan DPR-RI** yang kini tengah **merancang draf Rancangan Undang-Undang Perlindungan Data Pribadi**;

Faculty of Law Universitas Gadjah Mada
Jl. Sosio Yustisia No. 1, Bulaksumur,
Sleman, D.I. Yogyakarta 55281, Republic of Indonesia
Tel +62-811-1396-565
Mail contact@alsaindonesia.org
Web www.alsaindonesia.org

3. **Mendorong pemerintah dan DPR-RI untuk dapat melakukan penguatan kerangka perlindungan data pribadi** dalam Rancangan Undang-Undang Perlindungan Data Pribadi, dengan rincian sebagai berikut:
    a. **Mengadopsi 6 (enam) prinsip umum dalam GDPR** sebagai acuan dalam perumusan Rancangan Undang-Undang Perlindungan Data Pribadi;
    b. **Meningkatkan efektifitas upaya perlindungan data pribadi secara luas**, dengan menyusun Rancangan Undang-Undang Perlindungan Data Pribadi yang **dapat diaplikasikan lintas sektor**, baik sektor publik maupun swasta, sebagai langkah optimalisasi perlindungan data pribadi yang bersifat holistik;
    c. **Membentuk lembaga penegak perlindungan data pribadi yang independen** sebagai **otoritas pengawasan** perlindungan data pribadi yang bersifat **imparsial dan objektif**, yang memiliki tugas pokok untuk **memastikan kepatuhan** pengendali dan prosesor data pribadi, baik individu maupun badan privat/publik terhadap regulasi perlindungan data pribadi;
    d. **Merumuskan sanksi yang efektif** dalam Rancangan Undang-Undang Perlindungan Data Pribadi, yang mencakup **sanksi administratif, perdata, dan pidana**, dengan **memberlakukan sanksi administratif sebagai sanksi utama dalam perlindungan data pribadi**, mengingat sifat pemanfaatan data yang juga bersifat administratif; dan
    e. **Mengadopsi metode *self-regulatory approach*** dalam Rancangan Undang-Undang Perlindungan Data Pribadi, sebagai bentuk **peningkatan praktik perlindungan data pribadi melalui inisiasi sektoral**, agar nantinya setelah disahkan, pengaturan dalam UU Perlindungan Data Pribadi dapat disesuaikan dengan karakteristik setiap sektor, baik dalam ruang lingkup publik maupun swasta.
4. **Mendorong diselenggarakannya *Privacy/Data Protection Officer Forum* secara berkala** sebagai **wadah diskusi pembahasan dan pencarian solusi bagi para *stakeholder* mengenai permasalahan perlindungan data pribadi** yang terus timbul secara dinamis. Diharapkan forum tersebut dapat menjadi wadah yang optimal untuk melakukan **peningkatan praktik perlindungan data pribadi melalui inisiasi sektoral berbasis *self-regulatory approach***.

Faculty of Law Universitas Gadjah Mada
Jl. Sosio Yustisia No. 1, Bulaksumur,
Sleman, D.I. Yogyakarta 55281, Republic of Indonesia
Tel +62-811-1396-565
Mail contact@alsaindonesia.org
Web www.alsaindonesia.org

5. **Mendorong pemerintah untuk meninjau substansi dalam Rancangan Undang-Undang Perlindungan Data Pribadi** dengan pengaturan yang telah ada di beberapa negara, seperti **Malaysia, Singapura, Filipina, Laos, dan Thailand** yang telah memiliki peraturan perlindungan data pribadi dalam lingkup nasional dan memiliki iklim ekonomi yang tidak jauh berbeda dengan Indonesia di kawasan ASEAN. Hal tersebut dirasa perlu dilakukan sebagai **pembelajaran konstruktif** bagi Indonesia untuk bisa **menerapkan konsep tersebut dalam Rancangan Undang-Undang Perlindungan Data Pribadi**.

Faculty of Law Universitas Gadjah Mada
Jl. Sosio Yustisia No. 1, Bulaksumur,
Sleman, D.I. Yogyakarta 55281, Republic of Indonesia
Tel +62-811-1396-565
Mail contact@alsaindonesia.org
Web www.alsaindonesia.org

DAFTAR PUSTAKA

Peraturan Perundang-undangan

ASEAN, ASEAN Human Rights Declaration (adopted 18 November 2012) (**AHRD**).

a. Brunei Darussalam
   - Data Protection Policy 2014
   - The Electronic Transaction Act

b. Filipina
   - The Republic Act No. 10173
   - The Implementing Rules and Regulations of the PDPA

c. Indonesia
   - Undang-Undang Republik Indonesia Nomor 7 Tahun 2014 tentang Perdagangan (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 45, Tambahan Lembaran Negara Republik Indonesia Nomor 5512).
   - Undang-Undang Nomor 19 Tahun 2016 tanggal 25 November 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).
   - Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem Elektronik (Lembaran Negara Republik Indonesia Tahun 2019 Nomor 185, Tambahan Lembaran Negara Republik Indonesia Nomor 6400).
   - Peraturan Pemerintah Nomor 80 Tahun 2019 tentang Perdagangan Melalui Sistem Elektronik (Lembaran Negara Republik Indonesia Tahun 2019 Nomor 222, Tambahan Lembaran Negara Republik Indonesia Nomor 6420).
   - Peraturan Menteri Komunikasi dan Informasi Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik (Berita Negara Republik Indonesia Tahun 2016 Nomor 1829).

d. Kamboja
   - Cambodia Civil Code
   - Cambodia Criminal Procedure Law
   - Cambodia Penal Code
   - *E-commerce* Law 2019.

Faculty of Law Universitas Gadjah Mada
Jl. Sosio Yustisia No. 1, Bulaksumur,
Sleman, D.I. Yogyakarta 55281, Republic of Indonesia

Tel +62-811-1396-565
Mail contact@alsaindonesia.org
Web www.alsaindonesia.org

e. Laos
   - Guidelines on the Implementation of the Law on Electronic Data Protection (No. 2126/MoPTC).
   - Law on Prevention and Combating Cyber Crime 2015.

f. Malaysia
   - Personal Data Protection Act 2010.

g. Myanmar
   - Law on Electronic Data Protection No. 25/NA (2017)
   - Financial Institutional Law 2016.
   - Private Healthcare Services 2007.

h. Singapura
   - Personal Data Protection Act 2012 (No. 26 of 2012)

i. Thailand
   - Personal Data Protection Act, B.E. 2562 (2019)

j. Vietnam
   - Civil Code 2013
   - Law on Information Technology (Law 67/2006/QH11)
   - Law on Consumer Protection (LoCP) 2010
   - Law on Digital Transaction (LoDT) 2005
   - Law on Network Information Safety (LoNIS)
   - Law on Cybersecurity (Law 24/2018/QH14) (CSL) 2018
   - Peraturan terkait, yakni Decree 52/2013/ND-CP dan Decree 72/2013/ND-CP

Buku

Budhijanto, Danrivanto, *Cyber Law dan Revolusi Industri 4.0*, Bandung: Logoz Publishing, 2019.

Davidson, Alan, *The Law of Electronic Commerce*, USA: Cambridge University Press, 2009.

Greenleaf, Graham, *Asian Data Privacy Laws: Trade & Human Rights Perspectives, 1st edn*, UK: Oxford University Press, 2014.

Ibrahim, Johnny, *Teori dan Metodologi Penelitian Hukum Normatif*, Malang: Bayumedia Publishing, 2006.

Munir, A Bakar dan Mohd SH Yasin, *Information and Communication Technology Law: State, Internet and Information, Legal and Regulatory Challenges*, Sweet and Maxwell Asia, 2018.

PDPC, *Advisory Guidelines On Key Concepts In The PDPA (revised 27 July 2017)*, PDPC, 2017.

Sandhusen, Richard L. *Marketing*, New York: Barron's Educational Series, 2008.

United Nation Conference on Trade and Development, *Data Protection Regulations and International Data Flows: Implications for Trade and Development*, New York and Geneva: UNCTAD, 2016.

Jurnal

Acharya, Amitav, 'Culture, Security, Multilateralism: "The ASEAN way" and Regional Order' (2007) 19 Contemporary Security Policy 55.

Azmi, Ida Madieha, '*E-commerce* and Privacy Issues: An Analysis of the Personal Data Protection Bill' (2002) 16 International Review of Law, Computers & Technology 317.

Cheng, Long (et.al), 'Enterprise data breach: causes, challenges, prevention, and future directions' (2017) 7 Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery Publisher: Wiley.

Chitranukroh, Athistha (Nop), 'Thailand Personal Data Protection Act', (Tilleke & Gibbins Thailand, 2021) [10-22].

Culnan, Mary J. '"How Did They Get My Name?": An Exploratory Investigation of Consumer Attitudes toward Secondary Information Use' (1993) 17 MIS Quarterly.

Guarda, Paolo, "Data Protection, Information Privacy, and Security Measures: An Essay on the European and the Italian Legal Frameworks" (2009) Ciberspazio e diritto.

Guido Alpa, 'General Principles of Law' (1998) Annual Survey of International and Comparative Law.

Head, Milena dan Yufei Yuan, "Privacy Protection in Electronic Commerce - A Theoretical Framework" (2001) 20 Human Systems Management.

Litan, Robert E. 'Law and policy in the age of the Internet' (2001) 50 Duke Law Journal.

Michael Kirby, 'The history, achievement and future of the 1980 OECD guidelines on privacy' (2011) International Data Privacy Law.

Miyazaki, Anthony D., "Online Privacy and the Disclosure of Cookie Use: Effects on Consumer Trust and Anticipated Patronage", (2008) 27 Online Privacy and the Disclosure of Cookie Use.

Peter H. Chase, 'Perspective on the General Data Protection Regulation of the European Union' (2019) German Marshall Fund of the United States.

Pranaya Dayalu dan M. Punnagai, 'GDPR: A Privacy Regime' (2019) International Journal of Trend in Scientific Research and Development (IJTSRD).

Romansky, Radi P. dan Irina S. Noninska, "Challenges of the digital age for privacy and personal data protection' (2020) 17 Mathematical Biosciences and Engineering.

Sengpunya, Phet, 'ASEAN *E-commerce* Legal Framework and Alignment of Lao PDR: A Review' (2019) 6 Lentera Hukum 269.

Treiblmaier, Horst, 'The Influence of Privacy Concerns on Perceptions of Web Personalisation' (2011) 1 In. J. Web Science 3.

Wignjosoebroto, Soetandyo, Hukum Paradigma, Metode dan Dinamika Masalahnya, Jakarta: ELSAM dan HUMA, 2002.

Laman

ASEAN, 'ASEAN Member States' (Association of Southeast Asian Nations) <https://asean.org/asean/asean - member-states/> diakses 24 November 2020.

'Amendments to the Personal Data Protection Act and Spam Control Act Passed' (Personal Data Protection Commission Singapore, 2020), <https://www.pdpc.gov.sg/news-and-events/announcements/2020/11/amendments-to-the-personal-data-protection-act-and-spam-control-act-passed>, diakses 24 Februari 2021.

'Asia Pacific Data Protection and Cyber Security Guide 2018' (*Hogan Lovells*, 2018) <https://www.hoganlovells.com/~/media/hogan-lovells/pdf/2018/ab-data-protection-and-cybersecurity.pdf> accessed 25 July 2020.

Bernard, Allen, 'Data privacy and data security are not the same', (Zdnet Austus 2020) <https://www.zdnet.com/article/data-privacy-and-data-security-are-not-the-same/> diakses 20 Februari 2021.

Chaffey, Dave, 'The reasons why consumers shop online instead of in stores', (Smart Insight, 2017) <https://www.smartinsights.com/ecommerce/ecommerce-strategy/the-reasons-why-consumers-shop-online-instead-of-in-stores/>, diakses 20 Januari 2021.

Choudhury, Saheli Roy, 'TECH Alibaba-owned Lazada suffers data breach for its grocery delivery business in Singapore' (CNBC, 1 November 2020) <https://www.cnbc.com/2020/11/02/alibaba-owned-lazada-suffers-databreach-on-redmart.html#:~:text=Southeast%20Asian%20e-commerce%20firm,service%20in%20the%20city-state.> diakses 24 November 2020.

Djafar, Wahyudi dan M. Jodi Santoso, "Perlindungan Data Pribadi: Pentingnya Otoritas Pengawasan Independen", (Lembaga Studi dan Advokasi Masyarakat, 2019). <https://elsam.or.id/wp-content/uploads/2020/07/Policy-Paper-3_Otoritas-Independen-PDP.pdf> diakses pada 8 Februari 2021.

DLA Piper, 'Data Protection Laws of the World: Malaysia' (2021) DLA Piper <https://www.dlapiperdataprotection.com/system/modules/za.co.heliosdesign.dla.lotw.data_protection/functions/handbook.pdf?country-1=MY> diakses pada 21 Februari 2021.

Eloksari, Eisya A., 'Tokopedia Data Breach Exposes Vulnerability of Personal Data" (The Jakarta Post, 5 May 2020) <https://www.thejakartapost.com/news/2020/05/04/tokopedia-data-breach-exposes-vulnerability-of-personaldata.html> diakses 24 November 2020.

Facebook and Bain & Company, 'Riding the Digital Wave' (Bain & Company, 14 January 2020), <https://www.bain.com/insights/riding-the-digital-wave/>, diakses 24 November 2020.

Goacher, Jonathan, 'Amendments to Singapore's Personal Data Protection Act' (Hill Dickinson LLP, Desember 2020) <https://www.lexology.com/library/detail.aspx?g=33fcd6d1-e505-4870-991b-f0a46d3bd742>, diakses 24 Februari 2021.

Google, Temasek and Bain & Company, ' e-Conomony Sea 2020, At full Velocity: Resilient and Racing Ahead' (e-Conomony Sea, 2020) <https://www.bain.com/globalassets/noindex/2020/e-conomy_sea_2020_report.pdf> diakses 24 November 2020.

Healey, Robert, " Thailand's New Data Protection Bill PDPA and It's Affect on Your Business?" (Relentless Data Privacy, 2020) <https://relentlessdataprivacy.com/thailands-new-data-protection-bill-pdpa-and-its-affect-on-your-business/> diakses 18 November 2020.

IBM, "Cost of a Data Breach Report 2019", (IBM Security, 2019) <https://www.ibm.com/downloads/cas/ZBZLY7KL?_ga=2.214883607.1034594978.1579101338-1286175879.1579101338>, diakses 20 Februari 2021.

____, "Cost of a Data Breach Report 2020", (IBM Security, 2020) https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/pdf/>, diakses 20 Februari 2021.

Jay Cohen, 'Cambodia - Data Protection Overview' (DataGuidance, 2020) <https://www.dataguidance.com/notes/cambodia-data-protection-overview> diakses pada 15 Februari 2021.

_____, 'Cambodia Enacts a new E-commerce Law and a Consumer Protection Law' (intellectual property & technology journal, 2019) <https://www.iptjournal.com/cambodia-enacts-a-new-e-commerce-law-and-a-consumer-protection-law/> diakses pada 15 Februari 2021.

Kemp, Simon & Sarah Moey, 'Digital 2019 Spotlight: *E-commerce* in Southeast Asia ' (Da ta Reportal, 2019) <https://datareportal.com/reports/digital-2019-spotlight-ecommerce-in-southeast-asia >, diakses 24 November 2020.

Kunal, 'Ministry of Posts and Telecommunications Guidelines Shed Light and Clarity on the Lao PDR's Data Protection Regime', (DFPL) <https://www.ela.law/Templates/media/files/Newsletter_Articles_Clients/AP/October/Ministry_of_Posts_and_Telecommunications_Guidelines_Shed_Light_and_Clarity_on_the_Lao_PDR's_Data_Protection_Regime.pdf>, diakses 21 Februari 2021.

Lago, Cristina, 'The biggest data breaches in Southeast Asia' (CSO, 2020) <https://www.csoonline.com/article/3532816/the-biggest-data-breaches-in-southeast-asia.html>, diakses 20 Februari 2021.

Ross Taylor, 'Myanmar - Data Protection Overview' (DataGuidance, 2020) <https://www.dataguidance.com/notes/myanmar-data-protection-overview> diakses pada 14 Februari 2021.

Rotella, P, "Is data the new oil?" (Forbes, 2012) <http://www.forbes.com /sites/perryrotella/2012/04/02/is-data-thenew-oil/.> diakses 20 Januari 2021.

Statista, Gross merchandise volume (GMV) of the *e-commerce* market in the ASEAN region in 2015 and 2019 with a forecast for 2025, by country', (Statista, 2019)

<https://www.statista.com/statistics/1177826/asean-e-commerce-gross-merchandise-volume-by-country/>, diakses 20 Januari 2021.

_____, 'Internet penetration rate Asia 2009-2020', (Statista 2020) <https://www.statista.com/statistics/265156/internet-penetration-rate-in-asia/>, diakses 20 Januari 2021.

Sargunaraj, Nadarashnaraj, 'Personal Data Protection in ASEAN' (ZICO, April 2019) < https://zico.group/publication/personal-data-protection-in-asean/> accesed 24 November 2020.

_____, 'Personal Data protection in ASEAN' (ASEAN Insider, 2019), <https://zico.group/publication/personal-data-protection-in-asean/> diakses 24 Februari 2021

Swinhoe, Dan, "What is the cost of a data breach?" (CSO, 2020) <https://www.csoonline.com/article/3434601/what-is-the-cost-of-a-data-breach.html#:~:text=The%20average%20cost%20of%20a,over%20the%20last%20five%20years> diakses 20 Februari 2021.

UNCTAD, 'Review of *e-commerce* legislation harmonization in ASEAN' (UNCTAD Org, 2013) <https://unctad.org/system/files/official-document/dtlstict2013d1_en.pdf> diakses 24 November 2020.

Wahyudi Djafar, M. Jodi Santoso, "Perlindungan Data Pribadi: Pentingnya Otoritas Pengawasan Independen", (Lembaga Studi dan Advokasi Masyarakat, 2019) <https://elsam.or.id/wp-content/uploads/2020/07/Policy-Paper-3_Otoritas-Independen-PDP.pdf> diakses pada 21 Februari 2021.

Wall, Alex 'Summary : Philippines Data Privacy Act and Implementing Regulations', (IAPP, 2017) <https://iapp.org/news/a/summary-philippines-data-protection-act-and-implementing-regulations/#:~:text=In%202012%20the%20Philippines%20passed,1%2C%20Sec.> diakses 7 Februari 2021.

William Greenlee, 'Data Privacy in Myanmar' (In-House Community, 2020) <https://www.inhousecommunity.com/article/data-privacy-myanmar/> diakses pada 14 Februari 2021.

Withers, Rachel, "Before Facebook, There Was GeoCities" (Slate, 2018) <https://slate.com/technology/2018/04/the-ftcs-1998-case-against-geocities-laid-the-groundwork-for-facebook-debates-today.html>, diakses 20 Februari 2021.

Worldometers, 'South-Eastern Asia Population' (Worldometer) <https://www.worldometers.info/world-population/south-eastern-asia-population/>, diakses pada 20 Januari 2021.

Wawancara

Wawancara dengan Ardhanti Nurwidya, *Senior Manager of Public Policy and Government Relation* & *Group Data Protection Officer* Gojek dan *Founder of* Asosiasi Praktisi Perlindungan Data Indonesia (APPDI).

Wawancara dengan Jansen Aw, *Partner* di Donaldson & Burkinshaw LLP. dan *Former Assistant* Chief Counsel Personal Data Protection Commission (PDPC) Singapore (Singapura).

Wawancara dengan Ms. Jasmine Wong, *Senior Manager of Legal Department* di Authority for Info Communications technology Industry (AITI) of Brunei Darussalam dan dan Pengiran Alias (AITI's Brunei Darussalam Network Information Centre (BNNIC), *Cyber Security & Data Protection Office Manager* pada tanggal 22 Desember 2021.

Wawancara dengan Ms. Maria Francesca Montez, *Vice President - Head, Artificial Intelligence & Data Policy, Data Protection Officer* of Union Bank Philippines

Wawancara dengan Mr. Nguyen Dung Mai, *Lecturer of Law* at University of Economics Ho Chi Minh City

Wawancara dengan Sonny Zulhuda, LL.B. (Honours), MCL., Ph.D., *Associate Professor Cyber Law & Data Protection Law* di International Islamic University Malaysia.

Wawancara dengan Tim Subdit Tata Kelola Perlindungan Data Pribadi Direktorat Jenderal Aplikasi Informatika Kementrian Komunikasi dan Informatika RI.

Wawancara dengan Wahyudi Djafar, Direktur Eksekutif ELSAM Periode 2021-2025.

Lain-Lain

ASEAN, 'The 16th ASEAN Telecommunications and Information Technology Ministers Meeting and Related Meetings: Joint Media Statement' (2016).

Guide to the General Data Protection Regulation GDPR, Information Commissioner's Office (ICO), 2018.

Kelvin Chia Partnership Yangon, December 15th, 2020, *Data Protection Law in Myanmar*, Working Paper.

Faculty of Law Universitas Gadjah Mada
Jl. Sosio Yustisia No. 1, Bulaksumur,
Sleman, D.I. Yogyakarta 55281, Republic of Indonesia

Tel +62-811-1396-565
Mail contact@alsaindonesia.org
Web www.alsaindonesia.org

Mekovec, R. dan Ž. Hutinski, *The role of perceived privacy and perceived security in online market* (2012) Proceedings of the 35th International Convention MIPRO 2012/ISS.

Muzatko, Steven dan Gaurav Bansal, *Timing of Data Breach Announcement and E-commerce Trust* (2018). MWAIS 2018 Proceedings.

Rancangan Undang-Undang Perlindungan Data Pribadi.

Tu Thien Huynh, January 30th, 2021, *Implementation of the ASEAN Framework on Personal Data Protection as a Personal Data Protection Regulation in ASEAN Countries,* Working Paper.

World Wide Web Foundation, Personal Data: An Overview of Low and Middle-income Countries, (2017) Policy White Papers.

Faculty of Law Universitas Gadjah Mada
Jl. Sosio Yustisia No. 1, Bulaksumur,
Sleman, D.I. Yogyakarta 55281, Republic of Indonesia

Tel +62-811-1396-565
Mail contact@alsaindonesia.org
Web www.alsaindonesia.org

ALSA,
Always be One!