



ANALISIS HUKUM PERLINDUNGAN DATA PRIBADI TERHADAP KEWAJIBAN NOTIFIKASI PELANGGARAN DATA PRIBADI OLEH PENGENDALI DATA PRIBADI: STUDI PERBANDINGAN ANTARA INDONESIA DAN INGGRIS

Arfista Rifqi Putra* dan Umar Mubdi

Fakultas Hukum, Universitas Gadjah Mada,
Jl. Sosio Justicia No. 1, Bulaksumur, Kab. Sleman, D.I. Yogyakarta, 55281

Abstract

This research was made to review the obligation of controller to notify the data subjects in their legal relationship in terms of the concept of civil law as well as to compare arrangements regarding the obligation of notification in Indonesia and the UK and explore lessons that can be drawn from the results of this comparison. This research was made using the juridical-normative research method, namely by examining various legal materials based on the applicable laws and regulations. Based on this research, the Author concludes that the obligation of controller to notify the data subjects in their legal relationship with the data controllers can be studied in various civil law concepts and difference in the context could affect on the assessment of their legal relationship. Then, the Author also finds that there are significant differences in the arrangement of these obligations in the two countries, even though both of them refer to the GDPR. From these differences, some of the best lessons can be found that can be used as media for reflection to improve personal data protection regulations and policies in Indonesia which cover several aspects, namely legal certainty; bargaining position of the Subject; convenience/facilities for the data controller in carrying out their obligations; as well as regarding the competent authority.

Keywords: *Data Protection, Notification Mandatory, Data Controller.*

Abstrak

Penelitian ini dibuat dengan tujuan untuk mengulas mengenai kewajiban notifikasi pelanggaran data pribadi dalam hubungan hukum antara pengendali data pribadi dan subjek data pribadi ditinjau dari konsep hukum perdata serta membandingkan pengaturan mengenai kewajiban notifikasi tersebut di Indonesia dan Inggris dan menggali pelajaran-pelajaran yang dapat dipetik dari hasil perbandingan tersebut. Penelitian ini dibuat dengan metode penelitian yuridis-normatif, yakni dengan menelaah berbagai bahan hukum dengan didasarkan kepada peraturan perundang-undangan yang berlaku. Berdasarkan penelitian ini, Penulis menyimpulkan bahwa kewajiban notifikasi pelanggaran data pribadi dalam hubungan hukum antara pengendali dan subjek data pribadi tersebut dapat dikaji dalam berbagai konsep hukum perdata serta perbedaan konteks dapat mempengaruhi bagaimana hubungan tersebut dapat dikaji. Kemudian, Penulis juga menemukan adanya perbedaan yang cukup signifikan dalam pengaturan kewajiban tersebut di kedua belah negara, terlepas dari fakta bahwa keduanya sama-sama mengacu kepada GDPR. Dari perbedaan tersebut, dapat ditarik beberapa pelajaran terpetik yang dapat digunakan sebagai media refleksi dalam rangka membenahi peraturan dan kebijakan perlindungan data pribadi di Indonesia yang meliputi beberapa aspek, yaitu kepastian

* Alamat korespondensi: arfistarifqi@mail.ugm.ac.id

hukum; posisi tawar Subjek; kemudahan/fasilitas bagi pengendali data pribadi dalam melakukan kewajibannya; serta mengenai lembaga otoritas yang bewenang.

Kata Kunci: Pelindungan Data Pribadi, Kewajiban Notifikasi, Pengendali Data.

A. PENDAHULUAN

Aktivitas sehari-hari manusia modern tidaklah terlepas dari pemanfaatan teknologi informasi. Hal ini tercermin dari beberapa kegiatan seperti pemanfaatan layanan berbasis digital seperti *e-commerce* untuk melakukan kegiatan jual beli; penggunaan *e-money*, *e-wallet*, dan *internet banking* untuk bertransaksi; serta penggunaan media sosial untuk bersosialisasi yang kini telah mengalami perkembangan yang relatif pesat.¹ Perkembangan teknologi ini ditandai dengan miniaturisasi perangkat keras (*hardware*) dan peningkatan kekuatan komputasi.² Miniaturisasi *hardware* dan peningkatan kekuatan komputasi tersebut semakin memudahkan pengumpulan data dalam volume yang besar.³ Data-data pribadi tersebut dikumpulkan untuk kemudian diproses dalam rangka meningkatkan performa layanan berbasis digital yang disediakan.⁴ Fenomena yang sebagaimana digambarkan di atas menjadi suatu pertanda bahwa kini umat manusia telah memasuki era dunia pintar (*smart world*) atau dunia yang terkumpul (*collected world*), yakni dunia yang di dalamnya terjadi pengumpulan data secara masif dari banyak perangkat bersensor dengan jenis yang beragam.⁵

Pemanfaatan layanan berbasis digital di Indonesia terpantau cukup masif. Pada tahun 2021, Indonesia menjadi negara dengan jumlah penggunaan *e-commerce* terbanyak di dunia, yakni sejumlah 88,1% pengguna internet menggunakan *e-commerce*.⁶ Selain itu, pengguna aktif media sosial di Indonesia juga mengalami peningkatan sebesar 12,35% dibandingkan dengan tahun sebelumnya sehingga kini total pengguna media sosial aktif di Indonesia berjumlah 191 juta orang.⁷ Transformasi digital di sektor-sektor tertentu juga kian kerap dilakukan, seperti munculnya bank dan lembaga keuangan non-bank digital pada sektor

¹ Wawan Setiawan, "Era Digital dan Tantangannya", Makalah, Seminar Nasional Pendidikan 2017, 1 Januari 2017, hlm. 1.

² Aurelia Tamò-Larrieux, 2018, *Designing for Privacy and its Legal Framework: Data Protection by Design and Default for the Internet of Things*, Springer International Publishing, Cham, hlm. 2.

³ *Ibid.*

⁴ Mark Burdon, 2020, *Digital data collection and information privacy law*, Cambridge University Press, New York, hlm. 15.

⁵ *Ibid.*

⁶ Andrea Lidwina, "Penggunaan E-Commerce Indonesia Tertinggi di Dunia," <https://databoks.katadata.co.id/datapublish/2021/06/04/penggunaan-e-commerce-indonesia-tertinggi-di-dunia>, diakses pada 13 September 2022.

⁷ M. Ivan Mahdi, "Pengguna Media Sosial di Indonesia Capai 191 Juta pada 2022," <https://dataindonesia.id/internet/detail/pengguna-media-sosial-di-indonesia-capai-191-juta-pada-2022>, diakses pada 13 September 2022.

perbankan.⁸ Selain itu, terdapat pula layanan pembayaran non-tunai di sektor minyak dan gas (seperti *MyPertamina*⁹) dan sektor ketenagalistrikan (seperti *PLN Mobile*¹⁰). Kemudian, skema perizinan usaha di Indonesia kini juga sudah menggunakan skema perizinan daring satu pintu berupa Online Single Submission Risk-Based Approach (OSS-RBA) sejak tahun 2021 lalu.¹¹

Namun, perkembangan penggunaan dan penyediaan layanan digital pada realitanya diikuti pula oleh munculnya potensi pelanggaran data yang mengancam privasi data pribadi. Hal ini tercermin dalam kasus kebocoran data pribadi pengguna *Facebook* pada 2019 silam yang berdampak bagi 533 juta pengguna dari berbagai negara, termasuk Indonesia.¹² Kemudian, telah terjadi pula kebocoran data pengguna *Tokopedia* dan *Bukalapak* pada tahun 2020.¹³ Lalu, pada tahun 2021 telah terjadi kebocoran 279 juta data penduduk Indonesia.¹⁴ Terakhir, pada Agustus 2022 telah muncul pula dugaan terjadinya kebocoran data pengguna layanan *IndiHome*.¹⁵

Berdasarkan penjelasan di atas, kepastian akan pelaksanaan tanggung jawab oleh pengendali data pribadi (selanjutnya disebut “Pengendali”)¹⁶ kepada subjek data pribadi (selanjutnya disebut “Subjek”)¹⁷ atas pelanggaran data yang terjadi menjadi penting untuk dilakukan. Salah satu tanggung jawab yang sangat urgen untuk dilakukan oleh Pengendali

⁸ Hilal Ahmad, “Digitalisasi Lembaga Keuangan pada 2022, Ini Tantangannya!”, *Bisnisbanten.com*, 14 Desember 2021, <https://bisnisbanten.com/digitalisasi-lembaga-keuangan-pada-2022-ini-tantangannya>

⁹ Pertamina, “Tingkatkan Komitmen Layanan, Pertamina Luncurkan My Pertamina Loyalty Program dan Bright Package”, <https://pertamina.com/id/news-room/news-release/tingkatkan-komitmen-layanan-pertamina-luncurkan-my-pertamina-loyalty-program-dan-bright-package>, diakses pada 12 Januari 2022.

¹⁰ Perusahaan Listrik Negara (PLN), “Lebih Dekat Dengan Pelanggan, PLN Luncurkan Aplikasi New PLN Mobile”, <https://web.pln.co.id/media/siaran-pers/2020/12/lebih-dekat-dengan-pelanggan-pln-luncurkan-aplikasi-new-pln-mobile>, diakses pada 12 Januari 2022.

¹¹ OSS Kementerian Investasi/BKPM “Presiden Jokowi Resmikan Peluncuran OSS Berbasis Risiko”, <https://oss.go.id/baca/artikel/presiden-jokowi-resmikan-peluncuran-oss-berbasis-risiko>, diakses pada 12 Januari 2022.

¹² Galuh Putri Wiyanto, “Data 533 Juta Pengguna Facebook Bocor, Termasuk Indonesia”, *Kompas.com*, 4 April 2021, <https://tekno.kompas.com/read/2021/04/04/09330067/data-533-juta-pengguna-facebook-bocor-termasuk-indonesia?page=all>

¹³ Wahyunanda Kesuma Pertiwi, “Data Tokopedia, Gojek, dan Bukalapak Bocor di Tengah Absennya RUU PDP,” *KOMPAS.com*, 4 Mei 2020, <https://tekno.kompas.com/read/2020/05/04/20170027/data-tokopedia-gojek-dan-bukalapak-bocor-di-tengah-absennya-ruu-pdp>

¹⁴ Arief Rahman Hakim, “279 Juta Data Penduduk Indonesia Bocor, Tim Periksa Data Akan Gugat Tiga Lembaga,” *Liputan6*, 17 Juni 2021, <https://www.liputan6.com/tekno/read/4584634/279-juta-data-penduduk-indonesia-bocor-tim-periksa-data-akan-gugat-tiga-lembaga>

¹⁵ Zulfikar Hardiansyah, “Fakta Kebocoran Data Pelanggan Indihome, sedang Diinvestigasi hingga Kominfo Panggil Manajemen Telkom,” *KOMPAS.com*, 22 Agustus 2022, <https://tekno.kompas.com/read/2022/08/22/12150017/fakta-kebocoran-data-pelanggan-indihome-sedang-diinvestigasi-hingga-kominfo?page=all>

¹⁶ Menurut Pasal 1 Angka 4 UU PDP, Pengendali merupakan setiap orang, badan publik, dan organisasi internasional yang menentukan tujuan dan mengendalikan pemrosesan data pribadi.

¹⁷ Pasal 1 angka 6 UU PDP tidak memberikan batasan terkait dalam status apa seseorang dapat dikatakan sebagai Subjek. Selama dia adalah orang perseorangan dan pada dirinya melekat data pribadi, maka dia dapat digolongkan sebagai Subjek.

adalah melakukan notifikasi pelanggaran data (*data breach notification*) kepada Subjek dan otoritas yang berwenang perihal pelanggaran data yang dialami. Notifikasi ini penting untuk dilakukan karena kewajiban tersebut sangat erat kaitannya dengan hak bagi Subjek untuk mengetahui bahwa data pribadinya telah dicuri atau disusupi yang sebagaimana dijamin dalam Pasal 16 ayat (2) Undang-undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (selanjutnya disebut “UU PDP”) serta dalam rangka menyelenggarakan perlindungan data pribadi bagi suatu bangsa.

Dalam era dunia *smart world* atau *collected world* yang sebagaimana telah digambarkan di atas, Subjek tentunya akan seringkali akan berhubungan dengan Pengendali dan juga prosesor data pribadi (selanjutnya disebut “Prosesor”) dalam kehidupan sehari-harinya selaku pihak yang akan berperan dalam kegiatan pemrosesan data pribadi. Menurut Pasal 16 ayat (1) UU PDP, kegiatan pemrosesan data pribadi meliputi pemerolehan dan pengumpulan; pengolahan dan penganalisisan; penyimpanan; perbaikan dan pembaruan; penampilan, pengumuman, transfer, penyebarluasan, dan pengungkapan; dan/atau penghapusan atau pemusnahan. Dalam kegiatan pemrosesan data pribadi suatu aplikasi misalnya, umumnya penyedia aplikasi (selaku Pengendali) akan menggunakan kontrak baku berbentuk elektronik untuk mengikat Subjek dalam rangka melakukan pengumpulan data pribadi.¹⁸ Hal ini dapat dilihat dalam Pemberitahuan Privasi (*Privacy Notice*) atau Kebijakan Privasi (*Privacy Policy*) yang harus disetujui oleh calon pengguna sebelum menggunakan layanan yang ditawarkan oleh penyedia. Sebagai contoh, dalam kebijakan privasi milik aplikasi Gojek, pengguna aplikasi Gojek akan memberikan persetujuan kepada PT GoTo Gojek Tokopedia Tbk dan/atau afiliasinya untuk mengumpulkan, menggunakan, mentransfer, hingga mengolah data pribadi pengguna disertai dengan rincian data pribadi apa saja yang dikumpulkan dan jaminan perlindungan data pribadi.¹⁹ Hal yang sama juga dapat ditemukan dalam Kebijakan Privasi Bukalapak. Di dalam Kebijakan Privasi Bukalapak, pengguna aplikasi Bukalapak memberikan persetujuan kepada PT Bukalapak Tbk. untuk mengumpulkan, mengolah, menganalisis, menyimpan, dan lain-lain terhadap data pribadi milik pengguna yang berupa nama, nomor telepon, alamat, profil pribadi, foto KTP dan data pribadi lainnya.²⁰ Lalu, apabila menghendaki, Pengendali dapat menunjuk dan memerintah Pemroses untuk melakukan kegiatan pemrosesan

¹⁸ M.Z. Wilona, E. Latifah, dan H. Purwadi, “Privacy Policy on Smart Contracts in E-Commecre Transactions”, *Law Reform*, Vol. 17, No. 1, 2021, hlm. 48.

¹⁹ Gojek, “Pemberitahuan Privasi”, <https://www.gojek.com/id-id/privacy-policies/>, diakses pada 3 Februari 2023.

²⁰ Bukalapak, “Kebijakan Privasi”, <https://www.bukalapak.com/privacy>, diakses pada 4 Februari 2023.

data pribadi yang lainnya.²¹ Dengan demikian, peralihan data dari Subjek kepada Pengendali umumnya adalah suatu hubungan kontraktual antara Subjek dan Pengendali dengan objek berupa data pribadi yang pengaturannya didasarkan kepada Kitab Undang-undang Hukum Perdata (selanjutnya disebut “KUHPerdata”).

Sebelum UU PDP diberlakukan, notifikasi pelanggaran data pribadi di Indonesia diatur dalam beberapa peraturan, di antaranya adalah Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem Elektronik (selanjutnya disebut “PP 71/2019”) dan Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik (selanjutnya disebut “Permenkominfo 20/2016”). PP 71/2019 mengatur tentang kewajiban Penyelenggara Sistem Elektronik untuk memberitahukan pemilik data pribadi, aparat penegak hukum, dan kementerian terkait dalam hal terjadi kegagalan data pribadi, sedangkan Permenkominfo 20/2016 mengatur secara lebih mendetil bagaimana pemberitahuan tersebut harus dilakukan. Kini, kedua peraturan tersebut masih berlaku sepanjang tidak bertentangan dengan UU PDP.²²

Pembentukan UU PDP, yang mana baru diundangkan pada tahun 2022 lalu, dilakukan dengan mengacu kepada The General Data Protection Regulation Uni Eropa (selanjutnya disebut “GDPR”).²³ Dengan demikian, terdapat beberapa kemiripan antara UU PDP dengan GDPR, seperti pada penggunaan istilah “Subjek Data Pribadi”, “Pengendali Data Pribadi”, dan “Prosesor Data Pribadi” serta adanya pengaturan terkait suatu lembaga otoritas khusus untuk menyelenggarakan perlindungan data pribadi. Selain Indonesia, beberapa negara lain juga telah mengambil inspirasi dari GDPR dalam pembentukan hukum nasionalnya dan kini GDPR juga telah digunakan sebagai model dalam reformasi hukum di seluruh dunia.²⁴ Dengan demikian, terlihat bahwa GDPR memiliki pengaruh yang cukup kuat di dalam dunia internasional.

Selain menjadi model dan inspirasi bagi pembentukan hukum di negara lain, pengaruh yang kuat tersebut juga tercermin dalam adanya prinsip ekstrateritorial yang dianut oleh GDPR.²⁵ Prinsip ini dapat ditemukan dalam Pasal 3 GDPR yang mengatur bahwa GDPR berlaku untuk Pengendali/Prosesor yang pendiriannya (*establishment*) dilakukan di Uni Eropa; Pengendali/Prosesor yang tidak didirikan di Uni Eropa, tetapi melakukan penawaran barang

²¹ Pasal 51 ayat (1) UU PDP.

²² Pasal 75 UU PDP.

²³ Direktorat Jenderal Aplikasi Informatika Kementerian Komunikasi dan Informatika, “UU PDP akan Permudah Pertukaran Data dengan Negara Lain”, <https://aptika.kominfo.go.id/>, diakses pada 21 Februari 2023.

²⁴ Hendrik Mildebrath, 2023, *Understanding EU Data Protection Policy*, European Parliamentary Research Service.

²⁵ Angela Daly, “The introduction of data breach notification legislation in Australia: A comparative view,” *Computer Law & Security Review*, Vol. 34, No. 3, Juni, 2018, hlm. 486.

dan/atau jasa atau memonitor kebiasaan/perilaku Subjek di Uni Eropa; dan Pengendali yang tidak didirikan di Uni Eropa, namun didirikan di tempat yang memberlakukan hukum dari negara anggota berdasarkan hukum internasional. Dengan demikian, GDPR mengandung perluasan dalam hal tanggung jawab Pengendali/Prosesor atas data pribadi yang diprosesnya. Kemudian, menurut Tambou, GDPR merupakan suatu regulasi khusus (*special regulation*) yang berbeda dengan regulasi oleh Uni Eropa lainnya karena GDPR mewajibkan negara-negara anggota Uni Eropa untuk mengadaptasikan hukum nasionalnya dengan ketentuan GDPR tersebut.²⁶ Selain itu, GDPR juga memberikan ruang bagi negara anggota untuk membuat dan menerapkan aturan khusus pada sektor-sektor tertentu (dengan secara selaras dengan GDPR), seperti dalam sektor publik, ketenagakerjaan, kesehatan, keamanan sosial, serta untuk mencapai tujuan dalam hal kepentingan umum, penelitian, statistika, jurnalistik, dan lain sebagainya.²⁷

Inggris, sebagai salah satu negara yang semula merupakan anggota Uni Eropa, juga turut mengadopsi GDPR dalam hukum nasionalnya. Inggris mengadopsi GDPR dengan mengalihkannya menjadi hukum nasional melalui Regulation (EU) 2016/679 of The European Parliament and of the Council (yang pada umumnya disebut sebagai “UK GDPR”). Inggris juga telah mengundangkan Data Protection Act 2018 (selanjutnya disebut “DPA 2018”) yang merupakan hukum perlindungan data pribadi generasi ketiga setelah Data Protection Act 1984 dan Data Protection Act 1998. DPA 2018 merupakan pelengkap dari UK GDPR sehingga keduanya harus dibaca secara bersamaan.²⁸ Pada tahun 2019, pemerintah Inggris juga telah menetapkan Data Protection, Privacy and Electronic Communications Regulations 2019 untuk mengamandemen UK GDPR dan DPA 2018. Kemudian dalam perkembangannya setelah keluar dari Uni Eropa, pemerintah Inggris juga tengah mengupayakan untuk membuat suatu peraturan perlindungan data pribadi baru dalam rangka mereformasi rezim hukum perlindungan data pribadi, yakni dengan membuat rancangan undang-undang yang berjudul “Data Protection and Digital Information (No. 2) Bill” pada bulan Maret 2023 lalu.²⁹ Rancangan tersebut dibuat dalam rangka memperbarui dan menyederhanakan kerangka hukum

²⁶ Olivia Tambou, “Opening Remarks”, dalam Karen Mc.Kullagh, Olivia Tambou, dan Sam Bourton, 2019, *National Adaptations of the GDPR*, Blogdroiteuropeen, Luxembourg, hlm. 25.

²⁷ *Ibid*, hlm. 26.

²⁸ UK Information Commissioner’s Office (ICO), “The UK GDPR”, <https://ico.org.uk/for-organisations/data-protection-and-the-eu/data-protection-and-the-eu-in-detail/the-uk-gdpr>, diakses pada 15 Maret 2023.

²⁹ UK Parliament, “Data Protection and Digital Information (No. 2) Bill”, <https://bills.parliament.uk/bills/3430>, diakses pada 15 Maret 2023.

perlindungan data pribadi Inggris untuk mengurangi beban bagi organisasi dalam mematuinya, di samping tetap mempertahankan standar perlindungan data yang mumpuni.³⁰

Berdasarkan penjelasan diatas, Inggris menjadi salah satu negara yang menarik untuk diteliti karena Indonesia dan Inggris sama-sama mengacu kepada GDPR; adanya pengaturan-pengaturan khusus di luar UK GDPR; dan adanya komitmen pemerintah Inggris untuk membenahi hukum perlindungan data pribadi di negara mereka. Adapun rumusan masalah yang diajukan dalam penelitian ini adalah:

- 1) Bagaimana kewajiban notifikasi pelanggaran data pribadi dalam hubungan antara Subjek dan Pengendali ditinjau dari konsep dan teori hukum keperdataan?
- 2) Bagaimana persamaan dan perbedaan ketentuan pengaturan notifikasi pelanggaran data pribadi di Indonesia dan Inggris serta pelajaran terpetik (*lesson learned*) yang dapat diambil darinya?

B. PEMBAHASAN

1. Kewajiban Notifikasi Pelanggaran Data Pribadi dalam Hubungan Hukum antara Subjek dan Pengendali Ditinjau dari Konsep Hukum Keperdataan

Hubungan hukum antara Pengendali dengan Subjek pada umumnya akan didasari kepada suatu persetujuan. Hal ini sesuai dengan ketentuan Pasal 20 Ayat (1) dan (2) UU PDP yang mewajibkan Pengendali untuk memiliki dasar pemrosesan data pribadi sebelum memproses data pribadi. Berdasarkan pasal tersebut, beberapa bentuk dasar pemrosesan data pribadi diantaranya adalah sebagai berikut.

1. Persetujuan yang sah dan eksplisit dari Subjek kepada Pengendali untuk 1 (satu) atau beberapa tujuan tertentu yang telah disampaikan sebelumnya;
2. Pemenuhan kewajiban perjanjian dalam hal Subjek menjadi salah satu pihak atau memenuhi permintaan Subjek pada saat perjanjian akan dilakukan;
3. Pemenuhan kewajiban hukum dari Pengendali sesuai dengan ketentuan dalam peraturan perundang-undangan.³¹

Dengan demikian, oleh karena kesepakatan antara Pengendali dengan Subjek merupakan salah satu unsur yang penting dalam hubungan hukum antara Pengendali dengan Subjek, maka Penulis hendak mengkaji terlebih kewajiban notifikasi pelanggaran

³⁰ Departement for Science, Innovation and Technology, 2023, *Data Protection and Digital Information (No. 2) Bill Explanatory Notes*, The House of Commons, hlm. 10.

³¹ Pasal 20 Ayat (1) dan (2) UU PDP.

data pribadi berdasarkan tiga konsep, yakni konsep hukum perikatan yang menitikberatkan kepada hubungan hukum yang terjadi antara Subjek dengan Pengendali; kemudian konsep hukum perjanjian yang menitikberatkan kepada persetujuan/kesepakatan yang menjadi dasar hubungan hukum antara Pengendali dengan Subjek; serta konsep hukum perlindungan konsumen yang menitikberatkan kepada status Pengendali sebagai pelaku usaha, Subjek sebagai konsumen, serta kontrak baku di antara keduanya. Pembahasan ini penting untuk dilakukan untuk memberikan pemahaman yang mendalam mengenai kewajiban notifikasi pelanggaran data pribadi dalam hubungan hukum antara Subjek dan Pengendali dalam kegiatan pemrosesan data pribadi.

a. Kewajiban Notifikasi Data Pribadi Ditinjau dari Konsep Hukum Perikatan

Sekalipun disinggung di dalamnya, KUHPerdata tidak memberikan suatu definisi yang jelas terkait dengan apa yang disebut sebagai “perikatan” itu.³² Namun, istilah “perikatan” dapat didefinisikan secara keilmuan. Menurut Muhammad, perikatan secara sederhana dapat dipahami sebagai hal yang mengikat antara orang yang satu dengan orang yang lainnya.³³ Hal yang mengikat tersebut merupakan suatu peristiwa hukum berupa perbuatan (seperti jual-beli dan utang-piutang); kejadian (seperti kelahiran dan kematian); dan keadaan (seperti rumah susun dan pekarangan yang berdampingan).³⁴ Peristiwa hukum tersebut-lah yang akan menciptakan hubungan hukum antara satu pihak dengan pihak yang lainnya serta setiap pihak memiliki hak dan kewajiban yang saling bertimbang balik.³⁵ Sedangkan Subekti mendefinisikan perikatan sebagai hubungan hukum antara dua orang/pihak yang di dalamnya pihak yang satu berhak untuk menuntut sesuatu dari pihak yang lain dan pihak yang lain tersebut wajib memenuhi tuntutan tersebut.³⁶ Selaras dengan definisi tersebut, Badrulzaman merumuskan definisi perikatan sebagai suatu hubungan hukum antara dua orang atau lebih yang terdapat dalam lapangan harta kekayaan yang di dalamnya terdapat satu pihak yang wajib berprestasi terhadap pihak lainnya dan pihak yang lain tersebut wajib memenuhi prestasi tersebut.³⁷

³² Meskipun tidak terdapat definisi yang jelas, Pasal 1233 KUHPer menentukan bahwa suatu perikatan itu timbul atau lahir dari dua hal: karena persetujuan dan karena undang-undang. Kemudian, dalam Pasal 1234 KUHPer diatur bahwa suatu perikatan itu bertujuan untuk “memberikan sesuatu, berbuat sesuatu, atau untuk tidak berbuat sesuatu.”

³³ Abdulkadir Muhammad, *Hukum Perdata Indonesia*, PT Citra Aditya Bakti, Bandung hlm. 229.

³⁴ *Ibid.*

³⁵ *Ibid.*

³⁶ Subekti, 1995, *Pokok-pokok Hukum Perdata*, Intermasa, Jakarta, hlm. 122-123.

³⁷ Miriam D. Badrulzaman, *Hukum Perikatan dalam KUH Perdata Buku Ketiga, Yurisprudensi, Doktrin, serta Penjelasan*, PT Citra Aditya Bakti, Bandung, hlm. 9.

Menurut Drion, perikatan karena undang-undang dapat dibagi menjadi dua kategori, yakni perikatan dari undang-undang semata-mata dan perikatan dari undang-undang karena perbuatan manusia.³⁸ Perikatan dari undang-undang semata-mata adalah perikatan yang lahir dari suatu perbuatan hukum yang sah yang terhadapnya undang-undang melekatkan hak dan kewajiban di antara kedua belah pihak, sekalipun para pihak tidak memperjanjikannya.³⁹ Sedangkan perikatan dari undang-undang karena perbuatan manusia adalah perikatan yang dilekatkan oleh undang-undang terhadap suatu perbuatan tertentu, baik berupa perbuatan yang sah maupun perbuatan yang melawan hukum.⁴⁰

Setelah definisi, unsur, asal-usul, dan jenis dari perikatan telah dipaparkan, apabila kita meninjau kepada definisi dan unsur tersebut, maka dapat ditarik suatu kesimpulan bahwa notifikasi pelanggaran data pribadi merupakan suatu perikatan yang didasarkan kepada undang-undang antara Pengendali dan Subjek. Hal ini dibuktikan dengan fakta bahwa Pengendali terikat dengan Subjek akibat adanya suatu peristiwa hukum, yakni pemrosesan data pribadi oleh Pengendali⁴¹ serta terjadinya pelanggaran data pribadi⁴², baik yang disebabkan oleh kesalahan dari Pengendali sendiri ataupun dari pihak ketiga. Kemudian, terkait dengan unsur kedua (perikatan terletak di lapangan hukum harta kekayaan), perlu ditekankan bahwa pengkategorian perikatan sebagai hubungan hukum yang dapat dinilai dengan uang kini sudah tidak relevan karena pada saat ini terdapat pula hubungan hukum yang tidak dapat dinilai dengan uang.⁴³ Data pribadi, khususnya apabila data pribadi tersebut diproses, di satu sisi memiliki memang nilai ekonomis bagi Pengendali.

Kutipan tersebut menggambarkan kondisi, yakni dengan kemajuan teknologi yang telah ada kini, data atau informasi pribadi yang dihimpun oleh Pengendali dapat menjadi aset yang penting dan berharga bagi perusahaan Pengendali. Hal ini didukung pula oleh pendapat Lieshout, yang menyatakan bahwa kumpulan data dalam jumlah yang besar memiliki suatu nilai ekonomis bagi pemasar/*marketer*.⁴⁴ Bahkan, dalam dinamika bisnis terkini, data (dalam jumlah yang besar) dapat dijadikan sebagai jaminan untuk

³⁸ *Ibid.*, hlm. 18.

³⁹ *Ibid.*, hlm. 11.

⁴⁰ *Ibid.*

⁴¹ Pasal 1 Angka 4 jo. Pasal 20 UU PDP.

⁴² Pasal 46 Ayat (1) UU PDP, Pasal 14 Ayat (5) PP 71/2019, dan Pasal 28 Huruf c Permenkominfo 20/2016.

⁴³ M.D. Badruzaman, "Kerangka Hukum Perjanjian (Kontrak)", dalam P.M. Marzuki *et.al.* (ed.), 1998, *Seri Dasar Hukum Ekonomi 5: Hukum Kontrak di Indonesia*, ELIPS.

⁴⁴ Marc van Lieshout, "The Value of Personal Data", Makalah, dalam *IFIP Advances in Information and Communication Technology: IFIP International Summer School on Privacy and Identity Management*, Patras, 2014, hlm. 29

memperoleh pinjaman.⁴⁵ Namun, di sisi lain, mengenai apakah data pribadi memiliki nilai ekonomis *per se* atau tidak hingga kini masih sesuatu yang diperdebatkan.⁴⁶ Terakhir, di dalam hubungan hukum tersebut, Pasal 46 Ayat (1) UU PDP, Pasal 14 Ayat (5) PP 71/2019, dan Pasal 28 Huruf c Permenkominfo 20/2016 juga mewajibkan Pengendali untuk memberikan notifikasi tertulis apabila pelanggaran data pribadi telah terjadi dan Subjek berhak untuk menerima notifikasi tersebut. Dalam kata lain, peraturan perundang-undangan memberikan kewajiban bagi Pengendali untuk memberikan notifikasi dalam hal terjadinya pelanggaran data pribadi, di sisi lain Subjek berhak untuk menerima notifikasi tersebut dari Pengendali. Alhasil, unsur-unsur perikatan sudah terpenuhi. Kemudian, karena hak dan kewajiban yang terkandung di dalam perikatan notifikasi pelanggaran data pribadi pada dasarnya bersumber dari peraturan, maka dapat dikatakan bahwa perikatan tersebut merupakan perikatan yang bersumber dari peraturan perundang-undangan, khususnya UU PDP, PP 71/2019, dan Permenkominfo 20/2016. Dengan demikian, pada dasarnya kewajiban notifikasi tersebut akan tetap berlaku sebagai perikatan bagi Pengendali sekalipun tidak ada perjanjian apapun di antara keduanya.

b. Kewajiban Notifikasi Data Pribadi Ditinjau dari Konsep Hukum Perjanjian

UU PDP mewajibkan Pengendali memiliki dasar pemrosesan data pribadi yang salah satunya adalah persetujuan yang sah dan eksplisit dari Subjek yang bersangkutan. Melalui kesepakatan tersebut, Subjek dapat memberikan kewenangan kepada Pengendali untuk memperoleh data dari Subjek dan menggunakannya sesuai dengan ketentuan-ketentuan yang diperjanjikan. Selain itu, Pengendali dan Subjek dapat pula menyepakati hal-hal terkait dengan kewajiban Pengendali untuk memberikan notifikasi dalam hal terjadinya pelanggaran data pribadi serta hak-hak yang terkait dengannya di dalam perjanjian yang mereka buat.⁴⁷ Karena hubungan hukum dan perikatan mereka didasarkan pada suatu perjanjian, maka akan berlaku ketentuan dalam Pasal 1313–1351 KUHPerdara yang mengatur perikatan yang timbul dari perjanjian. Berdasarkan Pasal 1338 ayat (1) KUHPerdara, perjanjian tersebut akan berlaku sebagai undang-undang bagi para pembuatnya (*pacta sunt servanda*).

⁴⁵ Douglas B. Laney, “Leveraging Data As Collateral Starts With Knowing Its True Value”, Forbes, 20 Desember 2022, www.forbes.com/

⁴⁶ G. Versaci, “Personal Data and Contract Law: Challenges and Concerns about the Economic Exploitation of the Right to Data Protection”, *European Review of Contract Law*, Vol. 14, No. 4, 2018, hlm. 376.

⁴⁷ Hal ini dapat dilihat dalam templat kontrak standar/baku pemrosesan data pribadi antara Pengendali dan Subjek yang dapat disediakan dalam lampiran (*annex*) Commission Implementing Decision (EU) 2021//915 oleh Uni Eropa.

Agar perjanjian dapat mengikat serta dapat dilaksanakan oleh para pihak yang membuatnya, maka suatu perjanjian harus memenuhi kumulasi syarat-syarat perjanjian yang sebagaimana tercantum dalam Pasal 1320 KUHPerdara, yaitu kesepakatan dari mereka yang mengikatkan dirinya; kecakapan untuk membuat suatu perikatan; suatu pokok persoalan tertentu; suatu sebab yang tidak terlarang. Syarat pertama dan kedua merupakan syarat subjektif, yakni persyaratan terkait dengan subjek yang membuat perjanjian.⁴⁸ Sedangkan syarat ketiga dan keempat adalah syarat objektif, yakni persyaratan yang terkait dengan objek perjanjian.⁴⁹ Apabila dalam syarat subjektif suatu perjanjian tidak terpenuhi, maka perjanjian akan dapat dibatalkan demi hukum. Sedangkan apabila syarat objektif tidak terpenuhi, maka perjanjian akan batal demi hukum.

Dapat disimpulkan dari penjelasan di atas bahwa isi dari suatu perjanjian harus dibuat dengan tidak melanggar rambu-rambu peraturan perundang-undangan yang berlaku, kesusilaan yang hidup dan berlaku di masyarakat, serta ketertiban umum. Pembatasan tersebut menjadi pertanda bahwa kebebasan yang dimiliki para pihak tersebut tidaklah berlaku mutlak. Dengan demikian, Pengendali tetap harus mematuhi hukum yang berlaku dalam mengikatkan dirinya melalui perjanjian dengan Subjek, khususnya terkait dengan kewajiban-kewajiban yang harus dipenuhinya dalam kegiatan pemrosesan data pribadi. Pengendali tidak bisa membuat klausul-klausul perjanjian yang menyimpangi pasal-pasal yang terkait dengan kewajibannya untuk memberikan notifikasi apabila terjadi pelanggaran data pribadi.

Akan tetapi, perlu ditekankan bahwa terkhusus terkait dengan hubungan antara perjanjian dengan peraturan perundang-undangan, berdasarkan pendapat yang diutarakan oleh M. Yahya Harahap, wajib dipatuhinya atau tidaknya suatu peraturan hukum itu tergantung kepada sifat dari peraturan hukum itu sendiri. Apabila suatu peraturan hukum bersifat memaksa (seperti Pasal 46 ayat (1) UU PDP yang mengandung perintah/kewajiban untuk melakukan notifikasi) maka aturan tersebut harus dipatuhi dan tidak dapat disimpangi, sedangkan terhadap peraturan yang bersifat mengatur (seperti Pasal 1460 KUHPerdara yang tidak mengandung kewajiban/perintah) masih memberikan ruang untuk disimpangi dengan suatu persetujuan oleh para pihak dalam perjanjian.⁵⁰

⁴⁸ Subekti, *Op.cit.*, hlm. 17.

⁴⁹ *Ibid.*

⁵⁰ M. Yahya Harahap, *Segi-Segi Hukum Perjanjian*, Alumni, Bandung, hlm. 184.

c. Kewajiban Notifikasi Data Pribadi Ditinjau dari Konsep Hukum Perlindungan Konsumen

Secara normatif, perlindungan konsumen didefinisikan sebagai: “segala upaya yang menjamin adanya kepastian hukum untuk memberi perlindungan kepada konsumen”.⁵¹ Menurut Syawali dan Imaniyati, perlindungan tersebut pada dasarnya ditujukan kepada hak-hak konsumen secara umum/universal, yakni hak atas keamanan dan keselamatan; hak atas informasi, hak untuk memilih; hak untuk didengar; dan hak atas lingkungan hidup.⁵²

Berdasarkan definisi di atas, maka dapat disimpulkan bahwa konsumen dalam hukum di Indonesia didefinisikan sebagai pengguna akhir atau *end-user* atau pengguna yang menggunakan atau mengonsumsi suatu barang atau jasa.⁵³ Dengan demikian, orang atau badan hukum yang menggunakan barang atau jasa untuk didistribusikan atau diperjualbelikan kembali tidak dapat dikatakan sebagai konsumen.

Lalu, mengapa konsumen penting untuk dilindungi? Urgensi perlindungan terhadap konsumen timbul sebagai respon terhadap perkembangan perekonomian dunia yang pesat dengan didukung oleh kemajuan teknologi, sehingga pelaku usaha dapat menghasilkan barang dan/atau jasa secara masif dan variatif yang diperdagangkan secara lintas batas wilayah dari suatu negara.⁵⁴ Oleh karena itu, pelaku usaha dituntut untuk melakukan pendistribusian barang dan/atau jasa yang dihasilkannya secara efektif dan seefisien mungkin dalam rangka memenuhi permintaan pasar.⁵⁵ Kondisi tersebut menimbulkan dua konsekuensi bagi konsumen, yakni di satu sisi kebutuhan mereka atas barang dan/atau jasa menjadi terpenuhi dan terbukanya pilihan atas barang dan/atau jasa untuk mereka beli serta di sisi lain kedudukan konsumen menjadi lemah dibandingkan dengan kedudukan pelaku usaha karena konsumen hanya menjadi objek bisnis bagi pelaku usaha untuk memperoleh keuntungan sebesar-besarnya.⁵⁶

Lemahnya kedudukan konsumen, khususnya dalam kegiatan pemrosesan data pribadi, tercermin dalam adanya fenomena komodifikasi data serta adanya perjanjian antara pelaku usaha dengan konsumen yang pada umumnya tertuang dalam suatu kontrak

⁵¹ Pasal 1 Angka 1 UUPK.

⁵² Husni Syawali dan Neni Sri Imaniyati dalam Abdul Halim Barkatullah, 2008, *Hukum Perlindungan Konsumen: Kajian Teoretis dan Perkembangan Pemikiran*, Penerbit Nusa Media, Bandung, hlm. 3.

⁵³ Black's Law Dictionary, s.v. “end user”, diakses pada 1 Mei 2023, <https://thelawdictionary.org/end-user/>

⁵⁴ Abdul Halim Barkatullah, *op.cit.*, hlm 10- 11. Lihat juga Yusuf Shofie, 2003, *Perlindungan Konsumen dan Instrumen-Instrumen Hukumnya*, PT Citra Aditya Bakti, Bandung, hlm. 8-9

⁵⁵ *Ibid.*, hlm. 11.

⁵⁶ *Ibid.*, hlm. 12.

baku. Menurut Skilton, komodifikasi data merupakan “*a discrete package of personal information that can be exchanged for something else*”.⁵⁷ Hal senada juga dapat diutarakan Sevignani. Menurutnya, komodifikasi data dapat dipahami sebagai suatu proses yang menjadikan data pribadi dapat dipertukarkan di pasar, baik secara aktual maupun secara diskursif.⁵⁸ Komodifikasi data tersebut memungkinkan terjadinya eksploitasi data pribadi yang mengakibatkan terjadinya pengumpulan data pribadi secara massal oleh satu Pengendali serta timbulnya ketimpangan daya tawar antara Subjek dengan Pengendali. Ketimpangan tersebut dicerminkan dalam adanya kontrak baku antara Pengendali dan Subjek dalam suatu kegiatan pemrosesan data pribadi seperti yang sebagaimana telah dicontohkan dalam bagian Pendahuluan. Menurut Treitel, kontrak baku adalah kontrak yang memiliki bentuk terstandar yang dipergunakan untuk semua perjanjian yang berjenis sama.⁵⁹ Karena sifatnya yang terstandarisasi, kontrak baku ini tidak dinegosiasikan di dalam pembuatannya sehingga ia dipandang menimbulkan suatu hubungan yang asimetris/tidak seimbang di antara para pihak yang membuatnya.⁶⁰ Karena minimnya ruang negosiasi bagi pihak yang dibuatkan kontrak, dalam hal ini adalah konsumen, mereka umumnya hanya dihadapkan kepada dua pilihan, yakni untuk menyepakati klausul-klausul perjanjian yang telah dibuat (dengan menandatangani kontrak yang bersangkutan atau memberikan persetujuan dalam wujud lain) atau tidak menyepakatinya.

Di dalam hukum Inggris, perlindungan konsumen secara umum diatur dalam Consumer Rights Act 2015 (selanjutnya disebut “CRA 2015”). Undang-undang ini mengatur perlindungan konsumen secara lebih spesifik karena pengaturan terkait dengan kontrak barang, jasa, dan konten digital (*digital content*) atau kontrak campuran serta ketentuan yang tidak adil (*unfair terms*) diatur secara terpisah dalam bab dan bagian tersendiri. Selain itu, undang-undang ini tidak hanya mengatur mengenai kontrak baku, namun juga meliputi pemberitahuan (*notices*), baik yang tertulis maupun tidak tertulis, yang terkait dengan hak dan kewajiban antara pelaku usaha dan konsumen.⁶¹ Perbedaan antara kontrak dengan pemberitahuan ini sangat relevan dengan kondisi terkini, yakni dalam kegiatan pemrosesan data pribadi, Pengendali seringkali mencantumkan klausul-

⁵⁷ Mark Skilton, 2015, *The Digital Enterprise: A Guide to Constructing Monetization Models using Digital Technologies*, Palgrave Macmillan, Hampshire, hlm. 207.

⁵⁸ S. Sevignani, “The Commodification of Privacy on the Internet”, *Science and Public Policy*, Vol. 40, No. 6, 2013, hlm. 733.

⁵⁹ G. H. Treitel, 2003, *The law of contract*, Sweet & Maxwell, London, hlm. 216.

⁶⁰ S. J. Choi dan G. M. Gulati, “Contract as Statute,” *Michigan Law Review*, Vol. 104, No. 5, 2006, hlm. 1130.

⁶¹ Section 61 CRA 2015.

klausul mengenai pemrosesan data pribadi dalam pemberitahuan/kebijakan privasi (*privacy notices/policy*) yang dibuat olehnya seperti yang sebagaimana telah dicontohkan dalam bagian Pendahuluan.

Berdasarkan pemaparan di atas, nyata bahwa ketentuan terkait dengan perlindungan konsumen dan perlindungan data pribadi, baik di Indonesia maupun di Inggris, memiliki hubungan yang cukup erat. Namun, perlu ditegaskan bahwa sekalipun hubungan di antara keduanya erat, pelanggaran terhadap kewajiban notifikasi dalam UU PDP atau UK GDPR dan DPA 2018 tidak serta merta akan menimbulkan pelanggaran terhadap UUPK atau CRA 2015 di atas. Dalam konteks hukum Indonesia, pelanggaran terhadap UU PDP dan UUPK dapat terjadi secara bersamaan apabila dalam suatu kasus:

- 1) Terdapat pelaku usaha yang menghasilkan suatu barang/jasa, serta terdapat konsumen yang mengonsumsi barang/jasa tersebut;⁶²
- 2) Terdapat pemrosesan data pribadi yang sebagaimana dimaksud dalam UU PDP oleh pelaku usaha terhadap data pribadi konsumen;
- 3) Pemrosesan data pribadi bukan merupakan pemrosesan data pribadi yang dikecualikan dalam UU PDP.⁶³

2. Persamaan dan Perbedaan serta Pelajaran Terpetik (Lesson Learned) dalam Pengaturan Kewajiban Notifikasi Pelanggaran Data Pribadi di Indonesia dan Inggris

a. Persamaan dan Perbedaan Pengaturan Kewajiban Notifikasi Pelanggaran Data Pribadi di Indonesia dan Inggris

UU PDP membawa beberapa perubahan dan penyempurnaan dalam pengaturan terkait dengan kewajiban notifikasi pelanggaran data pribadi. Semula di dalam PP 71/2019 dan Permenkominfo 20/2016 tidak dikenal mengenai pembedaan antara data

⁶² Pasal 1 Angka 1 dan 2 UUPK.

⁶³ Apabila terjadi sengketa konsumen antara Pengendali dan Subjek, maka terdapat dua jalur penyelesaian sengketa yang dapat ditempuh, yakni jalur litigasi (melalui pengadilan) dan non-litigasi. Di dalam KUHPerdara, dapat ditemukan dua dasar pengajuan gugatan di pengadilan, yakni wanprestasi (Pasal 1243 KUHPerdara) dan perbuatan melawan hukum/PMH (Pasal 1365 KUHPerdara). Berdasarkan Pasal 1243 KUHPerdara, gugatan wanprestasi hanya dapat dilakukan apabila terdapat perjanjian di antara kedua belah pihak; terdapat pihak yang melanggar perjanjian; dan pihak yang melanggar tersebut telah dinyatakan lalai dan ia tetap tidak melaksanakan perikatannya. Sedangkan berdasarkan Pasal 1365 KUHPerdara, gugatan PMH dapat dilakukan apabila Pengendali melakukan perbuatan yang berlawanan dengan hukum yang menimbulkan kerugian bagi Subjek yang mana hal tersebut terjadi akibat terdapatnya kesalahan. Kemudian untuk jalur non-litigasi, salah satu lembaga yang dapat dipertimbangkan oleh kedua pihak adalah Badan Penyelesaian Sengketa Konsumen (BPSK) sesuai dengan Pasal 23 UUPK. Berdasarkan pasal tersebut, penyelesaian sengketa melalui BPSK hanya dapat dilakukan apabila Pengendali/pelaku usaha menolak dan/atau tidak memberi tanggapan dan/atau tidak memenuhi tuntutan ganti rugi konsumen yang sebagaimana diatur dalam Pasal 19 UUPK.

pribadi umum dan data pribadi khusus. Sedangkan kini dalam UU PDP, sebagaimana dengan yang telah dipaparkan di atas, perbedaan antara keduanya dapat ditemukan. Lalu, Pasal 28 huruf c nomor 1 Permenkominfo 20/2016 mengatur bahwa:

“(Setiap Penyelenggara Sistem Elektronik wajib) memberitahukan secara tertulis kepada Pemilik Data Pribadi jika terjadi kegagalan perlindungan rahasia Data Pribadi dalam Sistem Elektronik yang dikelolanya, dengan ketentuan pemberitahuan sebagai berikut: 1. harus disertai alasan atau penyebab terjadinya kegagalan perlindungan data pribadi.”

Berdasarkan pasal tersebut, apabila terjadi pelanggaran data pribadi, Pengendali hanya diwajibkan untuk memberitahukan adanya peristiwa pelanggaran data pribadi tersebut disertai dengan alasan/penyebab terjadinya pelanggaran data pribadi tersebut. Namun, dengan diundangkannya UU PDP, kini Pengendali juga harus memberitahukan kepada Subjek perihal kapan dan bagaimana data pribadi mereka terungkap/dilanggar serta mengenai bagaimana upaya penanganan dan pemulihan atas insiden tersebut. Selain itu, sebagaimana yang telah diuraikan di atas, di dalam UU PDP telah ditetapkan pula mengenai beberapa pengecualian atas kewajiban notifikasi pelanggaran data pribadi. Namun, Penulis tidak menemukan penjelasan yang jelas mengenai maksud dari beberapa kepentingan yang menjadi pengecualian tersebut.

Kemudian, UU PDP juga mengamanatkan suatu lembaga pelaksana penyelenggaraan perlindungan data pribadi di Indonesia yang bertanggung jawab secara langsung kepada Presiden. Semula pada tahun 2018, sebelum UU PDP diundangkan, Kementerian Komunikasi dan Informatika RI (“selanjutnya disebut Kemkominfo”) pernah berencana untuk membentuk suatu komisi yang secara terkhusus menangani perlindungan data pribadi di Indonesia.⁶⁴ Namun, hingga awal tahun 2022, pembentukan komisi ini masih belum dapat direalisasikan akibat adanya pertentangan pendapat antara Komisi I DPR RI dengan Kemkominfo terkait dengan lembaga negara yang akan membawahi lembaga perlindungan data pribadi tersebut. DPR RI menghendaki agar lembaga perlindungan data pribadi tersebut merupakan lembaga independen di bawah presiden, sedangkan Kemkominfo menghendaki agar lembaga tersebut berada di bawah kementerian.⁶⁵ Namun, hingga kini lembaga tersebut belum dibentuk sehingga ketentuan

⁶⁴ Kementerian Komunikasi dan Informatika RI, “Wewenang 9 Anggota Komisi Perlindungan Data Pribadi”, <https://www.kominfo.go.id/>, diakses pada 27 Mei 2023.

⁶⁵ Fahmi Ahmad Burhan, “Pembahasan Komisi Perlindungan Data Alot, Bagaimana di Negara Lain?”, *Katadata.co.id*, diunggah pada 12 April 2022, <https://katadata.co.id/>

mengenai kewajiban notifikasi kepada lembaga yang bersangkutan belum dapat dilaksanakan.

Terakhir, berbeda dengan PP 71/2019 dan Permenkominfo 20/2016, kini di dalam UU PDP telah ditetapkan secara tegas mengenai batasan maksimal besaran sanksi pelanggaran kewajiban notifikasi pelanggaran data pribadi (maksimal 2% pendapatan/penerimaan tahunan). Namun, Penulis juga tidak menemukan penjelasan mengenai apa yang dimaksud sebagai pendapatan/penerimaan tahunan ini, apakah berupa *global annual turnover* atau *local annual turnover*.

Selanjutnya, Penulis akan paparkan temuan-temuan mengenai pengaturan kewajiban notifikasi pelanggaran data pribadi di Negara Inggris. Pada bahasan ini, UK GDPR dan DPA 2018 akan menjadi fokus dari observasi Penulis karena keduanya mengatur perlindungan data pribadi di Inggris secara umum.

Inggris memberlakukan DPA 2018 dan UK GDPR sebagai dua produk hukum yang saling melengkapi satu dengan lainnya. Selain itu, terlihat pula ada beberapa peraturan terkhusus lainnya yang turut melengkapi kedua peraturan tersebut. Akan tetapi, perlu ditekankan kembali bahwa observasi di atas hanya terbatas kepada peraturan-peraturan yang mengandung ketentuan mengenai kewajiban notifikasi pelanggaran data pribadi. Apabila ditinjau dalam cakupan yang lebih luas, yakni hukum perlindungan data pribadi, Inggris juga memberlakukan peraturan-peraturan lain seperti Freedom of Information Act 2000, The Environmental Information Regulations 2004, dan The INSPIRE Regulations 2009 yang kesemuanya masih termasuk ke dalam cakupan wewenang ICO.⁶⁶

Selain itu, terlihat pula bahwa Inggris masih menerapkan beberapa peraturan yang bersumber dari Uni Eropa sekalipun Inggris kini sudah keluar dari keanggotaan Uni Eropa. Salah satu aturan tersebut yang memiliki peran sentral dalam perlindungan data pribadi di Inggris adalah EU GDPR yang kemudian diadopsi dan kini dikenal sebagai UK GDPR. Pengadopsian tersebut, yang dilakukan dengan tanpa perubahan EU GDPR secara substantif, memungkinkan Inggris untuk mendapatkan Keputusan Kecukupan (*Adequacy Decision*) dari Uni Eropa.⁶⁷ Dengan diperolehnya Keputusan Kecukupan tersebut, maka Inggris (di samping 13 negara di luar Uni Eropa lainnya, yang di

⁶⁶ UK Information Commissioner's Office (ICO), "Legislation we cover", <https://ico.org.uk/about-the-ico/what-we-do/legislation-we-cover/>, diakses pada 14 Juni 2023.

⁶⁷ European Commission, "Data protection: Commission adopts adequacy decisions for the UK", diakses pada 15 Juni 2023, https://ec.europa.eu/commission/presscorner/detail/en/ip_21_3183

antaranya adalah Jepang, Korea Selatan, Swiss, Argentina, Andorra, New Zealand, dan Uruguay⁶⁸) telah memenuhi kriteria-kriteria tertentu yang menjamin bahwa Inggris memiliki tingkat perlindungan data pribadi yang pada dasarnya sama atau “*essentially equivalent*” dengan Uni Eropa.⁶⁹ Selain itu, hal ini juga akan menyederhanakan proses transfer data antara entitas pada negara anggota EU dengan Inggris, baik dalam kegiatan bisnis atau kegiatan lainnya.⁷⁰

Baik di Indonesia maupun Inggris, persoalan mengenai ketentuan pelanggaran data pribadi oleh Pengendali sama-sama menjadi suatu isu yang krusial untuk diatur. Pengaturan notifikasi pelanggaran data pribadi menjadi suatu langkah yang penting dalam menjamin hak-hak Subjek selaku entitas dari mana data pribadi tersebut berasal. Terlepas dari nilai penting tersebut, berdasarkan pemaparan di atas, terlihat bahwa terdapat suatu pola persamaan dan perbedaan terkait pengaturan kewajiban notifikasi pelanggaran data pribadi di antara kedua belah negara yang dapat menarik untuk lebih lanjut. Persamaan-persamaan pengaturan notifikasi tersebut tercermin pada hal-hal sebagai berikut:

1. Terdapat beberapa peraturan dan ketentuan terkhusus yang berlaku di dalam sektor-sektor tertentu;
2. Kedua belah negara sama-sama menggunakan konsep mengenai data pribadi sebagai informasi orang perorangan/individu yang teridentifikasi atau dapat diidentifikasi; Subjek sebagai entitas tempat data pribadi berasal/melekat; Pengendali sebagai entitas yang membuat keputusan dalam pemrosesan data pribadi; dan Pemroses sebagai entitas yang memproses data pribadi dengan atas nama dari Pengendali;
3. Terdapat data pribadi khusus yang dibedakan dari data pribadi secara umum;
4. Subjek hanya berupa orang perseorangan yang masih hidup dan bukan badan hukum;
5. Kewajiban notifikasi kepada Subjek dalam hal terjadinya pelanggaran data pribadi sama-sama diemban oleh Pengendali;

⁶⁸ European Commission, “Adequacy decisions”, diakses pada 15 Juni 2023, https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

⁶⁹ *Recital* 104 Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

⁷⁰ O.J. Gestrein dan A.J. Zwitter, “Extraterritorial application of the GDPR: promoting European values over power?”, *Internet Policy Review*, Vol. 10, No. 3, 2021, hlm. 11.

6. Terdapat kewajiban Prosesor untuk memberitahu Pengendali mengenai pelanggaran data pribadi yang terjadi padanya;
7. Jangka waktu untuk memberikan notifikasi sama-sama dibatasi dalam jangka waktu 72 jam atau 3 hari;
8. Sama-sama terdapat lembaga khusus yang wewenang dan tugasnya melingkupi penyelenggaraan perlindungan data pribadi, termasuk wewenang untuk menerima dan memproses notifikasi dari Pengendali apabila terjadi pelanggaran data pribadi;
9. Notifikasi sama-sama dikecualikan dalam kegiatan pemrosesan data pribadi untuk keperluan pribadi atau rumah tangga serta dalam rangka penegakkan hukum, keamanan nasional, dan keamanan umum;
10. Pelanggaran dikenakan sanksi administratif dengan batas besaran maksimal tertentu serta terdapat hak bagi Subjek untuk menggugat Pengendali atas kerugian yang ditimbulkannya.

Sedangkan perbedaan-perbedaan dalam hukum kedua negara terdapat dalam beberapa aspek sebagai berikut:

1. Terkait data khusus/spesifik: Walaupun di antara kedua belah negara terdapat kesamaan yaitu adanya pengkhususan terhadap jenis-jenis data tertentu, namun pengkhususan tersebut tidaklah sama. Misalnya, mengenai data keuangan pribadi, UU PDP menegaskan bahwa data tersebut merupakan data pribadi spesifik. Dengan demikian, data keuangan pribadi dianggap sebagai salah satu data yang dapat mengakibatkan dampak yang lebih besar bagi Subjek dalam kegiatan pemrosesannya.⁷¹ Sedangkan di dalam UK GDPR dan DPA 2018, data keuangan pribadi tidak digolongkan sebagai data pribadi khusus yang sebagaimana ditentukan dalam *Recital 51* UK GDPR dan *Article 9 Paragraph 1* UK GDPR. Sekalipun data keuangan pribadi merupakan data sensitif, data tersebut tidak digolongkan sebagai data pribadi khusus karena data tersebut dianggap tidak cukup berisiko bagi hak-hak dasar/fundamental seseorang.⁷²
2. Terkait ketentuan mengenai pemberian notifikasi pelanggaran pribadi kepada Subjek:

⁷¹ Penjelasan Pasal 4 Ayat (1) UU PDP.

⁷² UK Information Commissioner's Office (ICO), "What is special category data?", <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/special-category-data/what-is-special-category-data/>, diakses pada 20 Juni 2023.

- a. Di dalam UU PDP; PP 71/2019; dan Permenkominfo 20/2016, ditentukan secara tegas bahwa pemberian notifikasi kepada otoritas yang berwenang atau Subjek wajib diberikan secara tertulis. Sedangkan di dalam UK GDPR dan DPA 2018 tidak demikian sehingga Pengendali dapat memberikan notifikasi secara lisan melalui telepon atau dengan cara serta media lainnya.
- b. Tidak seperti di Indonesia, pemberian notifikasi berdasarkan UK GDPR dan DPA 2018 dilakukan dilakukan secara bertahap/berjenjang karena kewajiban notifikasi ditentukan berdasarkan ada atau tidaknya serta tinggi atau tidaknya resiko yang telah atau akan ditimbulkan. Dengan demikian, asesmen risiko menjadi hal yang penting untuk dilakukan terlebih dahulu oleh Pengendali sebelum memberikan notifikasi kepada ICO dan Subjek. Kewajiban notifikasi kepada ICO berlaku dalam hal pelanggaran telah/berpotensi menimbulkan risiko, sedangkan kewajiban notifikasi kepada Subjek hanya berlaku apabila risiko tersebut tinggi. Sedangkan di dalam UU PDP; PP 71/2019; dan Permenkominfo 20/2016, Pengendali diwajibkan memberikan notifikasi apabila terjadi insiden kegagalan perlindungan data pribadi/pelanggaran data pribadi, terlepas dari dampak/risiko terhadap Subjek yang bersangkutan. Kemudian, tidak ditemukan pula kewajiban bagi Pengendali untuk melakukan asesmen risiko terhadap insiden pelanggaran data pribadi yang dialaminya di dalam UU PDP.
- c. Berbeda dengan UU PDP yang mewajibkan Pengendali untuk memberikan notifikasi kepada masyarakat luas dalam hal terjadinya pelanggaran data pribadi yang mengganggu pelayanan publik atau berdampak luas bagi masyarakat, di dalam UK GDPR dan DPA 2018 tidak ditemukan kewajiban yang serupa.
- d. Mengenai materi informasi yang harus dimuat dalam notifikasi, perbedaan di antara kedua negara terletak pada:
 - i. Berbeda dengan UK GDPR dan DPA 2018, di dalam UU PDP; PP 71/2019; dan Permenkominfo 20/2016 tidak ditemukan kewajiban bagi Pengendali untuk mencantumkan informasi mengenai kontak petugas data pribadi yang dapat dihubungi dari Pengendali yang bersangkutan.
 - ii. UU PDP mewajibkan pengendali untuk mencantumkan informasi mengenai data pribadi yang terungkap. Namun, tidak dapat ditemukan kejelasan mengenai apa saja rincian informasi yang harus dimuat

- terkait data pribadi yang terungkap tersebut. Sedangkan rincian informasi terkait dengan ketentuan dalam UK GDPR dan DPA 2018 dapat ditemukan dalam panduan daring yang disediakan oleh ICO;
- iii. Berbeda dengan UK GDPR dan DPA 2018, di dalam UU PDP; PP 71/2019; dan Permenkominfo 20/2016 tidak ditemukan ketentuan khusus yang mewajibkan Pengendali untuk merekam/mendokumentasikan semua pelanggaran data yang terjadi terhadapnya yang ditujukan untuk memastikan kepatuhan Pengendali dalam memenuhi kewajibannya terkait dengan notifikasi pelanggaran data pribadi;
 - iv. Kemudian, di dalam UU PDP tidak dapat ditemukan ketentuan yang mewajibkan Pengendali untuk memberikan deskripsi mengenai konsekuensi pelanggaran data pribadi tersebut atau tidak. Di dalam UU PDP hanya disebutkan bahwa Pengendali wajib untuk memuat “data pribadi yang terungkap”, namun tidak ditemukan penjelasan mengenai maksud dari frasa tersebut. Hal ini berbeda dengan UK GDPR dan DPA 2018 yang secara tegas membedakan kewajiban untuk memberikan deskripsi konsekuensi tersebut dengan kewajiban untuk memberitahukan sifat dasar (*nature*) dari pelanggaran data pribadi. Selain itu, UK GDPR dan DPA 2018 juga secara tegas mewajibkan Pengendali untuk menginformasikan hal tersebut;
 - v. UK GDPR dan DPA 2018 secara tegas mewajibkan Pengendali untuk menginformasikan materi notifikasi kepada Subjek secara jelas (*clear*) dan lugas (*plain*). Kewajiban yang demikian tidak dapat ditemukan dalam UU PDP; PP 71/2019; dan Permenkominfo 20/2016
 - vi. Selain itu, tidak dapat ditemukan pedoman-pedoman terkait dengan ketentuan notifikasi pelanggaran data pribadi yang sebagaimana diatur dalam UU PDP; PP 71/2019; dan Permenkominfo 20/2016 yang dapat menjadi acuan praktik terbaik (*best practice*) bagi Pengendali di Indonesia. Hal ini berbeda dengan Inggris yang, melalui lembaga ICO, telah menghasilkan beberapa pedoman mendetail mengenai UK GDPR, DPA 2018, dan beberapa peraturan perlindungan data pribadi lainnya. Pedoman-pedoman tersebut meliputi pedoman mengenai

pemberian notifikasi pelanggaran data pribadi berdasarkan peraturan-peraturan tersebut.

- e. UK GDPR dan DPA 2018 memberikan pengecualian terhadap kewajiban notifikasi pelanggaran data pribadi yang lebih luas dibandingkan dengan UU PDP; PP 71/2019 dan Permenkominfo 20/2016.
 - f. Tidak seperti UK GDPR dan DPA 2018, UU PDP; PP 71/2019; dan Permenkominfo 20/2016 tidak menjadikan kepentingan untuk melindungi hak dan kebebasan individu menjadi pengecualian dalam pemberian notifikasi pelanggaran data pribadi.
3. Terkait lembaga otoritas perlindungan data pribadi: Hingga saat ini, lembaga otoritas perlindungan data pribadi di Indonesia belum dibentuk. Berbeda dengan Inggris yang sudah mempunyai lembaga khusus, yakni ICO.
 4. Terkait sanksi:
 - a. Batas maksimal denda administratif yang dikenakan terhadap pelanggaran kewajiban notifikasi oleh Pengendali dalam UU PDP dan UK GDPR adalah berbeda. Dalam UU PDP, besaran maksimal dari denda tersebut adalah sebesar 2% pendapatan/penerimaan tahunan terhadap variabel pelanggaran. Namun, Penulis tidak menemukan kejelasan mengenai denda tersebut, apakah berupa *local turnover* atau *global turnover*. Selain itu, di dalam UU PDP tidak dapat ditemukan penjelasan mengenai maksud dari frasa “terhadap variabel pelanggaran”. Sedangkan dalam UK GDPR ditentukan bahwa maksimal denda yang dapat dikenakan adalah sebesar £17,500,000 atau 2% dari *global turnover* tahunan pada tahun finansial sebelumnya.
 - b. Terkait dengan besaran denda yang dapat dikenakan, UK GDPR memberikan dua opsi, yakni denda sebesar £17,500,000 atau sebesar 2% dari *global turnover* tahunan pada tahun finansial sebelumnya. Di antara kedua pilihan tersebut, dipilih denda dengan nominal tertinggi. Hal ini berbeda dengan UU PDP yang tidak ditemukan opsi seperti yang demikian. UU PDP hanya memberikan batas besaran maksimal denda, yakni sebesar 2% pendapatan/penerimaan tahunan terhadap variabel pelanggaran.

b. Pelajaran Terpetik (Lesson Learned) yang Dapat Diambil dalam Perbandingan Pengaturan Kewajiban Notifikasi Pelanggaran Data Pribadi di Indonesia dan Inggris

Perbandingan di atas menunjukkan suatu perbedaan yang cukup signifikan dalam ketentuan mengenai notifikasi pelanggaran data pribadi oleh Pengendali di Indonesia dan Inggris. Namun, perlu ditekankan bahwa sekalipun di antara kedua belah negara tersebut terdapat perbedaan yang signifikan, bukan berarti bahwa penelitian ini ditujukan untuk menonjolkan bahwa hukum salah satu negara lebih baik daripada hukum negara yang lain dan masih diperlukan penelitian yang lebih lanjut untuk membahas mengenai persoalan tersebut. Perbandingan tersebut ditujukan untuk menekankan bahwa keberagaman hukum di tengah bangsa-bangsa yang berbeda dapat menjadi suatu modal bagi suatu bangsa untuk membenahi dan mengembangkan kebijakan yang lebih efektif di masa yang akan datang. Dengan demikian, pengambilan pelajaran yang dapat dipetik (*lesson learned*) dari perbandingan ketentuan hukum di kedua belah negara tersebut menjadi penting dan relevan untuk dilakukan.

Berdasarkan pemaparan dan perbandingan ketentuan notifikasi di kedua belah negara, terdapat beberapa pelajaran terpetik yang dapat berguna dalam membenahi dan mengembangkan peraturan dan kebijakan perlindungan data pribadi di Indonesia, yakni sebagai berikut:

1. Soal kepastian hukum: Dalam ketentuan perlindungan data pribadi di Indonesia, khususnya yang terkait dengan kewajiban notifikasi pelanggaran data pribadi, masih terdapat ketentuan-ketentuan yang belum diatur secara jelas. Misalnya, terkait maksud dari istilah “data pribadi yang terungkap” serta istilah “2% pendapatan/penerimaan tahunan”. Selain itu, terdapat pula hal-hal yang sudah sepatutnya diatur, namun di dalam UU PDP belum diatur. Misalnya, seperti ketentuan mengenai data yang dianonimisasi. Inggris melalui UK GDPR dan DPA 2018 serta Uni Eropa melalui GDPR, telah mengatur pengecualian data yang telah dianonimisasi serta telah mengatur pula ketentuan mengenai re-identifikasi⁷³ dari data-data yang telah dianonimisasi tersebut. Sedangkan hal-hal tersebut belum dapat ditemukan di dalam UU PDP beserta PP dan Permenkominfo yang terkait. Sesuai dengan yang sebagaimana telah dibahas sebelumnya, tercapainya tujuan-tujuan hukum yang dalam hal ini terkhusus kepada hukum perlindungan data pribadi (yang di dalamnya melingkupi keamanan privasi data dan keamanan data pribadi itu sendiri) dapat dicapai dengan turut memperhatikan kepastian hukum.

⁷³ Section 171 DPA 2018.

2. Soal posisi tawar Subjek: Pada kenyataannya, masih terdapat hal-hal lain yang sebenarnya penting untuk diatur dalam rangka memberikan jaminan yang lebih besar terhadap perlindungan hak Subjek serta memperkuat posisi tawar Subjek, namun hal tersebut belum diatur di dalam UU PDP beserta PP dan Permenkominfo terkait. Hal ini tercermin dalam fakta terkait dengan tiadanya ketentuan bagi Pengendali untuk menyampaikan materi notifikasi secara jelas dan lugas kepada Subjek; ketentuan mengenai kewajiban bagi Pengendali untuk mendokumentasikan segala pelanggaran data pribadi yang terjadi terhadapnya; serta tidak adanya pengecualian notifikasi dalam hal adanya kepentingan yang menyangkut perlindungan hak dan kebebasan individu seperti yang sebagaimana dapat ditemukan dalam UK GDPR dan DPA 2018. Padahal, sudah seharusnya hukum turut memberikan kesetimbangan posisi antara Subjek dan Pengendali dalam rangka menjamin kontrol Subjek atas privasinya sendiri serta hak dan kebebasan yang dimilikinya.
3. Soal kemudahan/fasilitas bagi Pengendali dalam melaksanakan kewajibannya: Hingga kini, Penulis tidak menemukan panduan serta arahan yang dapat dijadikan sebagai acuan bagi Pengendali dalam melaksanakan kewajiban notifikasi dalam hal terjadi pelanggaran data pribadi di Indonesia. Panduan tersebut sudah seharusnya dapat ditemukan dalam petunjuk teknis dan/atau petunjuk pelaksanaan yang diterbitkan/dikeluarkan oleh kementerian atau badan terkait. Kondisi tersebut berbeda dengan Inggris yang kini sudah memiliki beberapa panduan perlindungan data pribadi lintas sektor yang di dalamnya terdapat pedoman serta anjuran-anjuran yang dapat dijadikan acuan praktik terbaik (*best practice*) oleh Pengendali dalam melaksanakan kewajibannya tersebut, seperti adanya anjuran bagi Pengendali untuk memberikan saran dan arahan mengenai hal-hal apa saja yang harus dilakukan dalam hal terjadinya pelanggaran data pribadi. Sesuai dengan prinsip "*sunlight as disinfectant*", kemudahan/fasilitas bagi Pengendali tentunya akan menjadi insentif tambahan bagi Pengendali untuk menjalankan kewajibannya.
4. Soal lembaga otoritas yang berwenang: Ketiadaan otoritas independen yang berwenang dalam menyelenggarakan perlindungan data pribadi di Indonesia menjadikan ketentuan UU PDP, termasuk ketentuan terkait dengan notifikasi pelanggaran data pribadi, menjadi tidak sepenuhnya efektif. Pembentukan otoritas tersebut diharapkan dapat mengisi kekosongan hukum yang terjadi. Selain itu, pembentukan otoritas ini diharapkan dapat memberikan kemudahan bagi

Pengendali untuk melaksanakan kewajibannya sesuai dengan UU PDP dan aturan lain yang terkait. Misalnya, dengan dibentuknya aturan/pedoman khusus yang membahas mengenai aspek teknis serta aspek lainnya mengenai penyampaian notifikasi kepada otoritas yang bersangkutan, kepada Subjek, dan kepada masyarakat secara mendetail.

Namun, sebagaimana yang telah dijelaskan pada bagian Tinjauan Pustaka, hukum sangat erat kaitannya dengan kekuasaan. Selain itu, hukum juga harus memiliki kekuatan yuridis, sosiologis, dan normatif agar dapat berlaku dengan efektif di masyarakat. Sekalipun terdapat pelajaran penting yang dapat dipetik dari perbandingan tersebut, tetap akan percuma apabila hal-hal di atas nyatanya tidak selaras dengan konfigurasi politik hukum di Indonesia pada saat ini atau tidak memiliki ketiga kekuatan keberlakuan tersebut. Mengenai persoalan terkait apakah pelajaran-pelajaran terpetik di atas sudah selaras dengan politik hukum Indonesia atau apakah memiliki ketiga kekuatan tersebut, perlu dilakukan penelitian lebih lanjut. Akan tetapi, salah satu masalah yang sangat penting untuk disampaikan dalam penelitian ini adalah mengenai kenyataan bahwa pemahaman masyarakat atas keamanan dan kerahasiaan data pribadinya masih belum optimal. Berdasarkan Survey Status Literasi Digital di Indonesia 2022, 61,3% responden pernah membagikan nomor *handphone* pribadi miliknya dan 58,1% responden pernah membagikan tanggal lahirnya di ranah publik.⁷⁴ Selain itu, 61,1% responden tidak menggunakan kata sandi yang berbeda di akun-akun sosial media miliknya.⁷⁵ Hasil survey di atas merupakan cerminan dari kenyataan mengenai kesadaran masyarakat akan pentingnya keamanan dan kerahasiaan data pribadinya yang tentunya sangat berkaitan dengan kondisi sosiologis masyarakat di Indonesia. Tanpa adanya kesadaran yang tinggi di masyarakat terkait dengan keamanan dan kerahasiaan data pribadi tersebut, tentunya perlindungan data pribadi di Indonesia tidak dapat berjalan dengan efektif sepenuhnya.

C. PENUTUP

Hukum perlindungan data pribadi, yang menjadi sumber dari perikatan antara Subjek dan Pengendali, juga memiliki kompleksitasnya tersendiri dalam hal bagaimana ketentuan-ketentuan di dalamnya diformulasikan di berbagai negara. Terkhusus mengenai salah satu

⁷⁴ Kementerian Komunikasi dan Informatika Republik Indonesia dan Katadata Insight Center, 2023, *Status Literasi Digital di Indonesia 2022*, hlm. 55.

⁷⁵ *Ibid.*

aspek dalam hukum perlindungan data pribadi yang mengenai kewajiban notifikasi pelanggaran data pribadi, Penulis menemukan variasi dalam bagaimana ketentuan tersebut diformulasikan di Negara Indonesia dan Inggris. Variasi tersebut terletak dalam adanya perbedaan dalam berbagai aspek mengenai kewajiban tersebut, seperti dalam hal bagaimana notifikasi tersebut harus diberikan serta mengenai besaran sanksi denda apabila kewajiban tersebut tidak dilakukan. Dari adanya variasi pengaturan tersebut, Penulis menemukan beberapa pelajaran terpetik yang melingkupi beberapa persoalan, yakni mengenai kepastian hukum; posisi tawar Subjek; kemudahan/fasilitas bagi Pengendali dalam melakukan kewajibannya; serta mengenai lembaga otoritas yang bewenang.

D. DAFTAR PUSTAKA

- Amboro, F. Yudhi Priyo dan Viona Puspita, “Perlindungan Hukum Atas Data Pribadi (Studi Perbandingan Hukum Indonesia dan Norwegia)”, *Conference on Management, Business, Innovation, Education and Social Science*, Vol. 1, No. 1, 2021.
- Amiruddin dan Zainal Asikin, 2004, *Pengantar Metode Penelitian Hukum*, PT Raja Grafindo Persada, Jakarta.
- Badruzaman, Miriam D., 2015, *Hukum Perikatan dalam KUH Perdata Buku Ketiga, Yurisprudensi, Doktrin, serta Penjelasan*, PT Citra Aditya Bakti, Bandung.
- Barkatulah, Abdul Halim, 2008, *Hukum Perlindungan Konsumen: Kajian Teoretis dan Perkembangan Pemikiran*, Penerbit Nusa Media, Bandung.
- Bertino, Elisa, “Data security”, *Data & Knowledge Engineering*, Vol. 25, No. 1-2, 1998.
- Black’s Law Dictionary, s.v. “end user”, <https://thelawdictionary.org/end-user/>
- Bukalapak, “Kebijakan Privasi”, <https://www.bukalapak.com/privacy>
- Burdon, Mark, 2020, *Digital data collection and information privacy law*. Cambridge University Press, New York.
- Choi, S. J. dan G. M. Gulati, “Contract as Statute,” *Michigan Law Review*, Vol. 104, No. 5, 2006
- Choi, Stephen J. dan G. Mitu Gulati, “Contract as Statute,” *Michigan Law Review*, Vol. 104, No. 5, 2006.
- Congressional Research Service (CRS), 2022, *Data Protection and Privacy Law: An Introduction*, CRS, Washington, D.C.
- Daly, Angela, “The introduction of data breach notification legislation in Australia: A comparative view,” *Computer Law & Security Review*, Vol. 34, No. 3, Juni, 2018.

- Departement for Science, *Innovation and Technology*, 2023, Data Protection and Digital Information (No. 2) Bill Explanatory Notes, The House of Commons.
- Dhawan, Sandeep, “Information and Data Security Concepts, Integrations, Limitations and Future”, *International Journal of Advanced Information Science and Technology (IJAIST)*, Vol. 1, No. 1, Oktober 2014.
- Direktorat Jenderal Aplikasi Informatika Kementerian Komunikasi dan Informatika, “UU PDP akan Permudah Pertukaran Data dengan Negara Lain”, <https://aptika.kominfo.go.id/>.
- European Commission, “Adequacy decisions”, https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en
- European Commission, “Data protection: Commission adopts adequacy decisions for the UK”, https://ec.europa.eu/commission/presscorner/detail/en/ip_21_3183
- Foresmith, Donald, “Specifying Reusable Security Requirements”, *Journal of Object Technology*, Vol. 3, No. 1, 2004
- Gestrein, O.J. dan A.J. Zwitter, “Extraterritorial application of the GDPR: promoting European values over power?”, *Internet Policy Review*, Vol. 10, No. 3, 2021
- Gojek, “Pemberitahuan Privasi”, <https://www.gojek.com/id-id/privacy-policies/>
- Hakim, Arief Rahman. “279 Juta Data Penduduk Indonesia Bocor, Tim Periksa Data Akan Gugat Tiga Lembaga.” *Liputan6*, <https://www.liputan6.com/tekno/read/4584634/279-juta-data-penduduk-indonesia-bocor-tim-periksa-data-akan-gugat-tiga-lembaga>.
- Harahap, M. Yahya, *Segi-Segi Hukum Perjanjian*, Alumni, Bandung.
- Hardiansyah, Zulfikar. “Fakta Kebocoran Data Pelanggan Indihome, sedang Diinvestigasi hingga Kominfo Panggil Manajemen Telkom.” *Kompas.com*, 22 Agustus, 2022, <https://tekno.kompas.com/read/2022/08/22/12150017/fakta-kebocoran-data-pelanggan-indihome-sedang-diinvestigasi-hingga-kominfo?page=all>.
- Hartkamp, Arthur S., 2015, *Contract Law in the Netherlands*, Edisi Kedua, Kluwer Law International BV.
- Hernoko, Agus Yudha, *Hukum Perjanjian: Asas Proporsionalitas dalam Hukum Perjanjian*, Kencana, Jakarta, hlm. 160.
- Inness, Julie C., *Privacy, Intimacy, and Isolation*, Oxford University Press, New York, 1992.
- Kementerian Komunikasi dan Informatika Republik Indonesia dan Katadata Insight Center, 2023, *Status Literasi Digital di Indonesia 2022*.
- Khairandy, Ridwan, 2004, *Itikad Baik dalam Kebebasan Berkontrak*, Fakultas Hukum Universitas Indonesia, Jakarta.

- Laney, Douglas B., “Leveraging Data As Collateral Starts With Knowing Its True Value”, *Forbes*, 20 Desember 2022, <https://www.forbes.com/sites/douglaslaney/2022/12/20/leveraging-data-as-collateral-starts-with-knowing-its-true-value/>
- Legislation.gov.uk, “Understanding Legislation”, <https://www.legislation.gov.uk/understanding-legislation>.
- Lidwina, Andrea, *Penggunaan E-Commerce Indonesia Tertinggi di Dunia*. <https://databoks.katadata.co.id/datapublish/2021/06/04/penggunaan-e-commerce-indonesia-tertinggi-di-dunia>.
- Lorenzen, Ernest G., “Causa and Consideration in the Law of Contracts”, *The Yale Law Journal*, Vol. 28, No. 7, Mei, 1919.
- Lundgren, B., “A Dilemma for Privacy as Control”, *The Journal of Ethics*, Vol. 24, No. 1, 2020.
- Mahdi, M. Ivan, *Pengguna Media Sosial di Indonesia Capai 191 Juta pada 2022*, <https://dataindonesia.id/digital/detail/pengguna-media-sosial-di-indonesia-capai-191-juta-pada-2022>.
- Marzuki, Peter Mahmud, 2005, *Penelitian Hukum*, Kencana, Jakarta.
- Mas, Marwan, 2018, *Pengantar Ilmu Hukum*, Ghalia Indonesia, Bogor.
- Mertokusumo, Sudikno, 2007, *Mengenal Hukum: Suatu Pengantar*, Liberty, Yogyakarta
- Muhaimin, 2020, *Metode Penelitian Hukum*, Mataram University Press, Mataram.
- Muhammad, Abdulkadir, *Hukum Perdata Indonesia*, PT Citra Aditya Bakti, Bandung.
- Nasution, Az., 2011, *Hukum Perlindungan Konsumen: Suatu Pengantar*, Diadit Media, Jakarta
- Nurhardianto, Fajar, “Sistem Hukum dan Posisi Hukum Indonesia”, *Jurnal TAPIS*, Vol. 11, No. 1, 2015.
- OSS Kementerian Investasi/BKPM “Presiden Jokowi Resmikan Peluncuran OSS Berbasis Risiko”, <https://oss.go.id/baca/artikel/presiden-jokowi-resmikan-peluncuran-oss-berbasis-risiko>.
- Parent, W.A., “Privacy, Morality, and the Law”, *Philosophy and Public Affairs*, Vol 12, No. 4, 1983.
- Pertiwi, Wahyunanda Kesuma. “Data Tokopedia, Gojek, dan Bukalapak Bocor di Tengah Absennya RUU PDP.” *Kompas.com*. 4 Mei, 2020, <https://tekno.kompas.com/read/2020/05/04/20170027/data-tokopedia-gojek-dan-bukalapak-bocor-di-tengah-absennya-ruu-pdp>.
- Petrina, Stephen, 2022, *Methods of Analysis*, The University of British Columbia, Vancouver.

- Post, Robert C, “Three Concepts of Privacy,” *The Georgetown Law Journal*, Vol. 89, 2001.
- Ramadhani, Syafira Agata, “Komparasi Pengaturan Perlindungan Data Pribadi di Indonesia dan Uni Eropa”, *Rawang Rencang: Jurnal Hukum Lex Generalis*, Vol. 3, No. 1, Januari, 2021.
- Sevignani, S., “The Commodification of Privacy on the Internet”, *Science and Public Policy*, Vol. 40, No. 6, 2013.
- Shofie, Yusuf, 2003, *Perlindungan Konsumen dan Instrumen-Instrumen Hukumnya*, PT Citra Aditya Bakti, Bandung.
- Skilton, Mark, 2015, *The Digital Enterprise: A Guide to Constructing Monetization Models using Digital Technologies*, Palgrave Macmillan, Hampshire.
- Soekanto, Soerjono dan Sri Mamudji, 2001, *Penelitian Hukum Normatif: Suatu Tinjauan Singkat*, Rajawali Pers, Jakarta.
- Subekti, 1995, *Pokok-Pokok Hukum Perdata*, PT Intermedia, Jakarta.
- Sunggono, Bambang, 2007, *Metode Penelitian Hukum*, PT Raja Grafindo Persada, Jakarta.
- Tamò-Larrieux, Aurelia. 2018. *Designing for Privacy and its Legal Framework: Data Protection by Design and Default for the Internet of Things*, Springer International Publishing, Cham.
- Treitel, G. H., 2003, *The Law of Contract*, Sweet & Maxwell, London.
- Tsamara, Nadia, “Perbandingan Aturan Perlindungan Privasi Atas Data Pribadi Antara Indonesia Dengan Beberapa Negara”, *Jurnal Suara Hukum*, Vol. 3, No. 1, Maret, 2021.
- UK Information Commissioner’s Office (ICO), “Legislation we cover”, <https://ico.org.uk/about-the-ico/what-we-do/legislation-we-cover/>
- UK Information Commissioner’s Office (ICO), “Personal data breaches: a guide”, <https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/personal-data-breaches-a-guide/>
- UK Information Commissioner’s Office (ICO), “The UK GDPR”, <https://ico.org.uk/for-organisations/data-protection-and-the-eu/data-protection-and-the-eu-in-detail/the-uk-gdpr>.
- UK Information Commissioner’s Office (ICO), “UK GDPR data breach reporting (DPA 2018)”, <https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/>
- UK Information Commissioner’s Office (ICO), “What is special category data?”, <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/special-category-data/what-is-special-category-data/>,

UK Information Commissioner's Office (ICO), 2018, *Guide to the Privacy and Electronic Communications Regulations*, ICO.

UK Information Commissioner's Office (ICO), 2021, *The Guide to NIS*, ICO.

UK Information Commissioner's Office (ICO), 2022, *Guide to eIDAS*, ICO.

UK Information Commissioner's Office (ICO), 2022, *Guide to the General Data Protection Regulation*, ICO.

Van Apeldoorn, L.J., *Pengantar Ilmu Hukum*, Balai Pustaka, Jakarta.

Versaci, G., "Personal Data and Contract Law: Challenges and Concerns about the Economic Exploitation of the Right to Data Protection", *European Review of Contract Law*, Vol. 14, No. 4, 2018.

Wilona, M.Z., E. Latifah, dan H. Purwadi, "Privacy Policy on Smart Contracts in E-Commerce Transactions", *Law Reform*, Vol. 17, No. 1, 2021.