CoMBInES
CONFERENCE ON MANAGEMENT, BUSINESS, INNOVATION, EDUCATION AND SOCIAL SCIENCES

Volume 1 No 1 (2021)

Received : February 01, 2021
Accepted : February 05, 2021
Published : February 24, 2021

Conference on Management, Business, Innovation, Education and Social Science
https://journal.uib.ac.id/index.php/combines

Perlindungan Hukum Atas Data Pribadi (Studi Perbandingan Hukum Indonesia dan Norwegia)

F. Yuhdi Priyo Amboro[1], Viona Puspita[2]
Email correspondence: Florianus.yudhi@uib.edu, 1751024.viona@uib.edu

[1-2]Fakultas Hukum, Universitas Internasional Batam, Batam, Indonesia

Abstrak

Perlindungan hukum merupakan salah satu kewajiban atau tanggung jawab negara termasuk perlindungan hukum atas data pribadi. Perlindungan hukum atas data pribadi dimaksudkan untuk menjamin hak-hak seorang individu agar hak atas privasinya tidak dilanggar. Tetapi dalam prakteknya sangat banyak terjadi pelanggaran hak atas privasi. Berbeda dengan Indonesia, Norwegia memiliki peraturan khusus yang mengatur mengenai perlindungan hukum atas data pribadi. Maka penelitian ini akan memaparkan persamaan dan perbedaan perlindungan hukum atas data pribadi di Negara Indonesia dan Norwegia. Metodologi penelitian yang digunakan oleh penulis dalam penelitian ini adalah yuridis normatif dengan menggunakan metode perbandingan hukum. Sehingga jenis data yang digunakan adalah data sekunder yang terdiri atas bahan hukum primer, sekunder dan tersier kemudian data-data yang diperoleh diuraikan dengan metode kualitatif-deskriptif. Persamaan dan perbedaan dalam perlindungan hukum atas data pribadi di Indonesia dan Norwegia, antara lain mengenai prinsip perlindungan data pribadi, Hak-hak pemilik data, sanksi, pihak yang bertanggung jawab, data pribadi spesifik, keamanan, pemberitahuan penerobosan, *profiling,* pengawas dan transfer data. Aturan hukum perlindungan data pribadi di Norwegia yang dapat diadaptasi oleh Indonesia berupa prinsip dalam perlindungan data pribadi, peraturan transfer data pribadi lintas negara, ketentuan sanksi, ganti rugi dan pertanggungjawaban, otoritas pengawas yang independen.

Kata Kunci:

Perbandingan Hukum, Perlindungan Hukum, Data Pribadi, Indonesia, Norwegia.

Pendahuluan

Sekarang perkembangan teknologi informasi sangat pesat, perkembangan teknologi informasi bisa kita lihat dengan munculnya berbagai jenis kegiatan yang berbasis pada teknologi, seperti e-government, e-health, e-payment, e-commerce, e-education, e-medicine, e-laboratory dan sebagainya (Wardiana, 2002). Pekembangan teknologi ini menimbulkan

berbagai kejadian seperti mengubah sifat masyarakat dalam melakukan interaksi (Setyawan, & Wijaya, 2018), orang-orang cenderung melakukan interaksi hanya menggunakan teknologi tanpa perlu melakukan tatap muka dan tidak hanya itu seiring dengan berkembangnya internet dapat menyebabkan terjadinya suatu penyalahgunaan terhadap informasi pribadi pengguna jasa internet tanpa adanya pengetahuan dan izin dari orang yang bersangkutan (Nugraha, 2018).

Data Pribadi dari seseorang merupakan sesuatu yang harus dijaga kerahasiaannya karena hal tersebut termasuk kedalam privasi orang yang bersangkutan. Jika privasi seseorang tidak dijaga maka orang tersebut akan mengalami kerugian yang berbeda dengan kerugian fisik karena orang lain akan dengan seenaknya mencampuri privasi orang lain dan menyalahgunakannya (Winarso, Disemadi & Prananingtyas, 2020). Perlindungan data privasi memiliki batasan, dalam hal tertentu terdapat beberapa data yang disepakati sebagai data pribadi yang tidak dilindungi bahkan atas nama hukum boleh disimpangi, contohnya seperti nama ibu (Amanda, 2008). Dalam perkembangan teknologi informasi, Informasi yang terdiri atas nama, e-mail dan nomor telepon merupakan data yang sangat berharga karena merupakan nilai ekonomis yang bisa diperolrh dalam dunia bisnis. Hal tersebut disebut dengan digital dossier atau berkas digital yang merupakan kumpulan dari informasi data pribadi yang dimiliki oleh sebagian besar atau bahkan hampir semua orang dengan menggunakan teknologi internet yang dikembangkan oleh pihak swasta yang sangat beresiko terhadap terjadinya pelanggaran hak privasi atas data pribadi seseorang (Priscyllia, 2019).

Meningkatnya aktivitas jumlah pengguna internet menyebabkan isu mengenai perlindungan data pribadi menjadi hal yang sangat serius karena penyebarannya dapat dilakukan dengan sangat cepat dan mudah melalui teknologi sehingga menimbulkan resiko bocornya data pribadi seseorang (Priscyllia, 2019). Kebocoran data yang terjadi sangat rentan untuk disalahgunakan oleh berbagai pihak sehingga munculnya kasus tindakan kriminal seperti pencurian identitas ataupun penipuan apalagi dengan meningkatnya perkembangan ekonomi modern saat ini kearah digital economy yang berbasis economy creative. Berdasarkan data Norton report, tahun 2013 mencatat bahwa tingkat potensi dan resiko terhadap tindakan kriminal dalam dunia maya di Indonesia memasuki status yang darurat dan terus menunjukkan peningkatan (dilansir dari Laman Indonesia Security Incident Team on Internet Infrastucture/Coordination Center (Id-SIRTII/CC)) (Rosalinda Elsina Latumahina, 2014).

Konsep dalam perlindungan data pribadi menekankan bahwa setiap orang memiliki hak untuk menentukan nasibnya sendiri contohnya dalam melakukan sharing data, mereka berhak menentukan apakah mereka akan melakukannya atau tidak dan jika memutuskan untuk sharing data mereka juga berhak untuk menentukan syarat yang ingin dipenuhi dalam suatu komunitas. Data pribadi pengguna yang diminta oleh pihak aplikasi seperti nama lengkap, email bahkan nomor rekening dalam berbagai layanan aplikasi memiliki berbagai tujuan, seperti untuk memastikan bahwa data pengguna merupakan data yang benar tetapi tidak terdapat jaminan bahwa data pribadi yang diminta oleh pihak aplikasi terhindar dari penyalahgunaan.

Perlindungan terhadap data pribadi sudah sangat banyak diterapkan oleh beberapa negara, salah satunya adalah Norwegia. Di Norwegia perlindungan data pribadi diatur pada Personal Data Act, Personal Data Act mengadopsi General Data Protection Regulation atau yang disebut dengan GDPR dan ditetapkan menjadi peraturan perlindungan data pribadi yang terbaru di Norwegia sejak 20 Juli 2018. GDPR mengatur sangat jelas mengenai perlindungan data pribadi sedangkan Indonesia tidak memiliki aturan khusus perlindungan data pribadi, melainkan diatur pada beberapa peraturan perundang-undangan yang pengaturannya tidak

secara komperhensif menekankan pada prinsip dari perlindungan data pribadi. Oleh karena itu, pemerintah Indonesia masih membutuhkan referensi mengenai perlindungan data pribadi di Indonesia dari negara lain seperti Norwegia yang telah memiliki peraturan yang spesifik. Terdapat berbagai masalah yang dapat dirumuskan yang berhubungan dengan Perlindungan hukum atas Data Pribadi (Studi Perbandingan Hukum Indonesia dan Norwegia): a) Bagaimana persamaan dan perbedaan yang terdapat pada hukum Negara Indonesia dengan hukum Negara Norwegia terkait perlindungan hukum atas data pribadi? b) Pengaturan hukum seperti apa yang dapat diadaptasi oleh Indonesia dari studi perbandingan hukum perlindungan hukum atas data pribadi dengan Norwegia?

Tinjauan Pustaka

Undang-Undang Dasar Negara Republik Indonesia 1945 merupakan acuan yang menunjukkan bahwa adanya perlindungan hukum atas data pribadi dari Negara Indonesia kepada pemilik data. Hal ini diamanatkan dalam pasal 28 G yang berbunyi: "Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaanya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi."

Pada Kitab Undang-Undang Hukum Pidana tidak mengatur tentang kejahatan pada bidang siber dan masih belum ada undang-undang khusus yang mengatur tentang data prviasi, tetapi Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik Juncto Undang-undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik (Selanjutnya disebut dengan "UU ITE") mengatur bahwa dalam pemanfaatan teknologi informasi, perlidungan data pribadi merupakan bagian dari hak pribadi. Undang-undang ini secara komperhensif telah mengatur tentang perlindungan data pribadi dan melarang seseorang mengakses data orang lain dengan melawan hukum yaitu dengan menerobos sistem keamanan.

Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan Juncto Undang-Undang Nomor 24 Tahun 2013 tentang Perubahan Atas Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan (Selanjutnya disebut dengan "UU Amniduk"), Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (Selanjutnya disebut dengan "PP No.71/2019"), Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik (Selanjutnya disebut dengan "Perkominfo No.20/2016") dan Peraturan Menteri Komunikasi dan Informatika Nomor 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi (Selanjutnya disebut dengan "Perkominfo No.4/2016") merupakan bukti perwujudan perlindungan hukum atas data pribadi dari Negara Indonesia kepada pemilik data.

Disepakati Parlemen Uni Eropa 27 April 2016, GDPR adalah undang-undang yang mengatur perlindungan data pribadi penduduk atau warga Uni Eropa yang berada di dalam maupun di luar Uni Eropa, serta yang dikelola pihak mana pun di dalam maupun di luar teritori Uni Eropa. Berlandaskan pada Piagam Hak Asasi Uni Eropa yang menetapkan "warga Uni Eropa memiliki hak untuk melindungi data pribadi masing-masing", GDPR menjadi instrumen utama harmonisasi hukum perlindungan data di seluruh negara anggota Uni Eropa. Hal yang mesti digaris bawahi, regulasi ini juga mengikat semua pihak di mana saja yang mengumpulkan, memproses dan memanfaatkan data pribadi penduduk atau warga Uni Eropa. Melalui pengaturan yang ketat dan ketentuan denda yang besar, GDPR dengan tegas menyatakan

setiap orang berdaulat atas perlindungan data pribadi masing-masing di hadapan pihak mana pun. Setiap orang di sini mencakup setiap orang yang bertempat tinggal di Uni Eropa, baik yang berstatus warga negara atau bukan. Obyek pengaturan GDPR mencakup orang, perusahaan, organisasi dan lembaga pemerintah Eropa di seluruh dunia yang memproses dan memanfaatkan data pribadi semua orang yang bertempat tinggal di Uni Eropa. Berfungsi menggantikan Undang-Undang Perlindungan Data Uni Eropa (EU *Data Protection Directive*) Tahun 1995, GDPR mulai berlaku 25 Mei 2018 dan pada 20 Juli 2018 Norwegia mengadopsi GDPR dan ditetapkan menjadi peraturan baru yang mengatur tentang data pribadi.

Metodologi Penelitian

Dalam penelitian ini penulis menggunakan jenis penelitian normatif. Keterkaitan dengan penelitian normatif, pendekatan yang penulis gunakan dalam penulisan hukum menurut Peter Mahmud Marzuki adalah: Pendekatan Kasus (*case approach),* Pendekatan perundang-undangan (*statute approach),* Pendekatan historis (*historical approach*), Pendekatan perbandingan (*comparative approach)*, Pendekatan konseptual *(conceptual approach. (Marzuki, 2017.)* Pada penelitian hukum normatif, bahan pustaka merupakan data dasar yang dalam penelitian digolongkan sebagai data sekunder. (Mamudji, 2004) Data sekunder meliputi surat-surat, buku-buku hingga pada dokumen resmi yang dikeluarkan oleh pemerintah. Sumber data sekunder dalam penelitian ini dibagi menjadi bahan hukum primer, bahan hukum sekunder dan bahan hukum tersier.

Data yang digunakan oleh penulis merupakan data sekunder sehingga teknik pengumpulan data yang digunakan oleh penulis adalah dengan cara studi kepustakaan, sehingga memperoleh bahan-bahan hukum, yakni: Peraturan perundang-undangan, pendapat ahli, jurnal ilmiah dan peraturan perundang-undangan Eropa. Metode analisis data yang digunakan oleh penulis adalah metode Kualitatif. Penelitian kualitatif adalah penelitian ilmiah yang bertujuan untuk memahami suatu fenomena tentang apa yang dialami oleh subjek penelitian misalya perilaku, persepsi, motivasi dan tindakan lain secara holistic dengan cara deskripsi dalam bentuk kata-kata dan Bahasa, pada suatu konteks khusus alamiah dan dengan memafaatkan berbagai metode alamiah. (Moleong, 2011)

Hasil dan Pembahasan

a) Persamaan dan Perbedaan Perlindungan Data Pribadi di Indonesia dan Norwegia

Berbicara mengenai perlindungan data pribadi, kewajiban atau tanggung jawab negara dalam konteks pelaksanaan hak asasi manusia di Indonesia dituangkan dalam pasal 28I ayat (4) dan (5) UUD 1945 sebagai rangkaian dari pasal-pasal yang mengatur tentang hak asasi manusia. Konsep tanggung jawab yang dilaksanakan oleh negara dalam hal ini adalah pemerintah terhadap hak asasi manusia dalam UUD 1945 merupakan tindakan seperti perlindungan, penegakan, pemajuan dan pemenuhan-pemenuhan dalam hak asasi manusia.

Pada tahun 2014, Norwegia memasukkan hak asasi manusia kedalam konstitusinya karena terinspirasi dari *European Convention on Human Rights.* Pasal 92 *The Constitution of the Kingdom of Norway* berbunyi, "*The authorities of the State shall respect and ensure human rights as they are expressed in this Constitution and in the treaties concerning human rights that are binding for Norway*." Perlindungan data pribadi di Norwegia dianggap sebagai bagian

dari hak asasi manusia yaitu hak atas privasi, hak atas privasi termaktub dalam pasal 102 *The Constitution of the Kingdom of Norway* yang berbunyi, "*Everyone has the right to the respect of their privacy and family life, their home and their communication. Search of private homes shall not be made except in criminal cases. The authorities of the state shall ensure the protection of personal integrity*."

Prinsip perlindungan data pribadi pada setiap negara memiliki perbedaan karena menyesuaikan situasi dan kondisi dalam negara tersebut agar dapat mengoptimalkan segala sumber daya untuk pemenuhan hak asasi manusia dalam hal perlindungan data pribadi (Rianarizkiwati, 2020). Berikut telampir tabel perbandingan peraturan perlindungan data pribadi di negara lain:

Tabel 4.1 Perbandingan Peraturan Perlindungan Data Pribadi di Negara Lain
(**Sumber : Kebebasan Informasi versus Hak Atas Privasi Tanggung Jawab Negara Dalam Perlindungan Data Pribad [hlm.65])**

No.	Negara	Pengertian data pribadi		Prinsip	Para pihak			Pengakuan hak
		Umum	sensitif		pengendali	pengolah	Badan	
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)
Klaster negara dengan IPM sangat tinggi								
1	Amerika Serikat*)	✓					✓	
2	Norwegia	✓	✓	✓	✓	✓	✓	✓
3	Jepang	✓		✓				
4.	Australia	✓		✓			✓	
Klaster negara dengan IPM tinggi								
5	Barbados	✓	✓	✓	✓	✓	✓	✓
6	Serbia	✓		✓	✓	✓	✓	✓
7	Mauritius	✓	✓	✓	✓	✓	✓	✓

8	Kazakthan	✓		✓	✓	✓	✓	✓

Klaster negara dengan IPM menengah dan rendah

9	Moldova	✓	✓	✓	✓	✓	✓	✓
10	Nigeria*)	✓					✓	
11	India*)	✓					✓	

Perbandingan negara ASEAN

12	Singapura	✓		✓			✓	✓
13	Malaysia	✓	✓	✓	✓	✓	✓	✓
14	Filipina	✓	✓	✓	✓	✓	✓	✓

*) Merupakan undang-undang tentang privasi atau rancangan undang-undang tentang perlindungan data pribadi.

Indonesia dan Norwegia mengatur mengenai prinsip dalam perlindungan data pribadi, berikut merupakan prinsip perlindungan data pribadi di Indonesia: Berdasarkan pasal 39 ayat (3) PP No.71/2019, terdapat enam (6) prinsip dalam pengendalian, pengamanan data pengguna, yaitu: Kerahasiaan; integritas; ketersediaan; keautentikan; otorisasi dan kenirsangkalan. Sedangkan di Norwegia, terdapat tujuh (7) prinsip dalam pemrosesan data, yaitu: *lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality; Accountability.* Hak-hak pemilik data pada undang-undang Indonesia terdapat pada pasal 2 Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan Juncto Undang-Undang Nomor 24 Tahun 2013 tentang Perubahan Atas Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan yaitu Setiap Penduduk mempunyai hak untuk memperoleh: a. Dokumen Kependudukan; w b. pelayanan yang sama dalam Pendaftaran Penduduk dan Pencatatan Sipil; c. perlindungan atas Data Pribadi; d. kepastian hukum atas kepemilikan dokumen; e. informasi mengenai data hasil Pendaftaran Penduduk dan Pencatatan Sipil atas dirinya dan/atau keluarganya; dan f. ganti rugi dan pemulihan nama baik sebagai akibat kesalahan dalam Pendaftaran Penduduk dan Pencatatan Sipil serta penyalahgunaan Data Pribadi oleh Instansi Pelaksana sedangkan hak pemilik data di Norwgia yaitu : *Right of acces by the data subject, Right to rectification, Right to erasure/ Right to be forgotten, Right of restriction of proxessing, Right to data portability.* Undang-Undang Indonesia mengatur mengenai sanksi administratif dan sanksi pidana, pasal 36 Peraturan menteri komunikasi dan informatika Nomor 20 Tahun 2016 mengatur mengenai sanksi administratif sedangkan pasal 51 Undang-Undang Informasi dan Transaksi Elektronik mengatur mengenai sanksi pidana. Pasal 83 GDPR mengatur mengenai denda yaitu hingga 20.000.000 Euro atau 4% pendapatan global tahunan perusahaan jika terbukti melanggar ketentuan-ketentuan tertentu. Ketentuan denda tergantung pada jenis pelanggaran pembobolan yang dilakukan dan kerugian yang ditimbulkan, denda tersebut

digolongkan denda hingga 2% atau 10.000.000 Euro dan denda hingga 4% 20.000.000 Euro. donesia menggunakan istilah penyelenggara sistem elektronik sebagai pihak yang bertanggung jawab berdasarkan PP No.71/2019. Berdasarkan pasal 1 ayat (4) PP No.71/2019, Penyelenggara Sistem Elektronik adalah setiap Orang, penyelenggara negara, Badan Usaha, dan masyarakat yang menyediakan, mengelola, dan/atau mengoperasikan Sistem Elektronik secara sendiri-sendiri maupun bersama-sama kepada Pengguna Sistem Elektronik untuk keperluair dirinya dan/ atau keperluan pihak lain. Berbeda dengan Indonesia, Norwegia menggunakan istilah *controllers (*pengendali) dan *processor (*pengelolah) sebagai pihak yang bertanggung jawab dalam penjaminan perlindungan data pribadi. Pengendali atau *controllers* merupakan pihak yang menentukan maksud dan tujuan dari pengolahan data pribadi sedangkan pengelolah atau *processor* memberikan instruksi mengenai bagaimana dan mengapa data pribadi digunakan untuk keperluan suatu organisasi. Tanggung jawab Pengendali atau *controlles* termaktub dalam pasal 24 GDPR sedangkan tanggung jawab pengelolah atau *processor* termaktub dalam pasal 28 GDPR. Indonesia dan Norwegia mengatur mengenai jenis data pribadi yang harus dilindungi atau data pribadi spesifik. Data pribadi yang harus dilindungi termaktub dalam pasal 84 UU Amniduk , yaitu: (1) Data Pribadi Penduduk yang harus dilindungi memuat: a) keterangan tentang cacat fisik dan/atau mental; b) sidik jari; c) iris mata; d) tanda tangan; dan e) elemen data lainnya yang merupakan aib seseorang. GDPR menggunakan istilah "*special categories of personal data"* Data pribadi spesifik termaktub dalam pasal 9 GDPR yang berbunyi: *Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited*. Dalam menjamin keamanan data atau informasi, Indonesia menggunakan istilah sistem manajemen keamanan informasi. Pengertian sistem manajemen keamanan informasi termaktub dalam pasal 1 ayat (5) Perkominfo No.4/2016 yang berbunyi: Sistem Manajemen Pengamanan Informasi adalah pengaturan kewajiban bagi Penyelenggara Sistem Elekronik dalam penerapan manajemen pengamanan informasi berdasarkan asas risiko. Pasal 7 Perkominfo No.4/2016 mengatur mengenai standar sistem manajemen pengamanan informasi, yang berbunyi: (1) Penyelenggara Sistem Elektronik yang menyelenggarakan Sistem Elektronik strategis harus menerapkan standar SNI ISO/IEC 27001 dan ketentuan pengamanan yang ditetapkan oleh Instansi Pengawas dan Pengatur Sektornya. (2) Penyelenggara Sistem Elektronik yang menyelenggarakan Sistem Elektronik tinggi harus menerapkan standar SNI ISO/IEC 27001. (3) Penyelenggara Sistem Elektronik yang menyelenggarakan Sistem Elektronik rendah harus menerapkan pedoman Indeks Keamanan Informasi. (4) Ketentuan mengenai pedoman Indeks Keamanan Informasi sebagaimana dimaksud pada ayat (3) diatur dalam Peraturan Menteri. Berbeda dengan Indonesia, Norwegia tidak menentukan standar atau ukuran teknis yang spesifik, tetapi Norwegia mengadopsi pendekatan pengamanan yang proposional dan keadaan spesifik. Pasal 32 GDPR mengatakan bahwa pengendali dan pengelolah wajib menerapkan tindakan teknis yang cocok untuk memastikan tingkat keamanan sesuai dengan resiko pemrosesan data. Indonesia dan Norwegia mengatur mengenai pemberitahuan penerobosan atau terjadinya kegagalan atas perlindungan data pribadi, Pemberitahuan mengenai terjadinya kegagalan atas perlindungan data pribadi di Indonesia termaktub dalam pasal 28 huruf C Perkominfo 20/2016, pemberitahuan dilakukan secara tertulis kepada pemilik data paling lambat 14 hari sejak diketahui terjadinya kegagalan terhadap perlindungan data, Norwegia juga mengatur

mengenai persyaratan umum dimana jika terjadi penerobosan terhadap data pribadi wajib diberitahukan kepada *supervisory authority* (*The Norwegian Data Protection Authority)* dan pemilik data. Pemberitahuan penerobosan di Norwegia diberitahukan kepada pemilik data paling lambat 72 jam setelah diketahui terjadinya penerobosan data. Undang-Undang Indonesia belum mengatur mengenai *profiling* sedangkan Norwegia dalam GDPR menjelaskan bahwa *profiling* merupakan bentuk pengolahan data pribadi secara otomatis untuk tujuan tertentu. Indonesia tidak memiliki badan pengawas khusus terkait dengan perlindungan data pribadi sedangkan Norwegia memiliki badan khusus untuk mengawasi pelaksanaan perlindungan data pribadi. Merujuk pada GDPR terdapat supervisory authority dan European data protection board. supervisory authority merupakan otoritas pengawas pada tingkat negara anggota Uni Eropa dan dan European data protection board merupakan otoritas pengawas pada tingkat regional Uni Eropa. Indonesia belum mengatur mengenai transfer data pribadi antarnegara sedangkan Norwegia memiliki aturan mengenai transfer data pribadi diluar Uni Eropa, transfer data pribadi di Norwegia termaktub dalam pasal 44 GDPR.

b) Pengaturan hukum yang dapat Diadaptasi oleh Indonesia dari Studi Perbandingan Hukum Perlindungan Hukum atas Data Pribadi dengan Norwegia

Pada masa pandemi ini kebutuhan terhadap undang-undang perlindungan data pribadi semakin mendesak karena seringnya penggunaan internet tetapi Indonesia masih belum memiliki instrumen hukum yang responsif terhadap kebutuhan masyarakat untuk mendapatkan perlindungan yang lebih kuat. Kebutuhan terhadap undang-undang khusus yang mengatur tentang perlindungan data pribadi adalah untuk melengkapi perlindungan data pribadi yang pengaturannya telah diatur dalam beberapa pasal dalam peraturan perundang-undangan dan peraturan menteri. Perlindungan terhadap data pribadi juga dibutuhkan agar dapat melindungi hak-hak dari seorang individu didalam masyarakat karena maraknya perbuatan melawan hukum yang berkaitan dengan data pribadi seperti pengelolaan, pengumpulan, pemrosesan dan penyebarluasan data pribadi tanpa seiizin pemilik data. Perlindungan data pribadi juga dibutuhkan dalam memberikan kepercayaan kepada masyarakat untuk memberikan informasi dan data yang berkaitan dengan dirinya agar tidak khawatir bahwa data pribadinya akan di salahgunakan dan melanggar hak atas privasinya. Hingga saat ini undang-undang tentang perlindungan data pribadi di Indonesia masih dalam tahap perancangan dalam bentuk Rancangan Undang-Undang (RUU). Suatu instrument hukum perlindungan data pribadi setidaknya harus memenuhi 3 kriteria yaitu: pertama, memiliki karakter internasional; kedua, mencakup perlindungan hak personal; ketiga, merupakan elemen perekat individu dan masyarakat ekonomi. (Niffari, 2020) Pengadaptasian hukum perlindungan data pribadi Norwegia ke hukum Indonesia dapat dilakukan oleh pemerintah dengan membuat peraturan khusus mengenai perlindungan data pribadi, mengingat bahwa saat ini pengaturan mengenai perlindungan data pribadi masih diatur secara terpisah di berbagai undang-undang dan peraturan menteri ketika sudah banyak negara lain yang telah menerapkan perlindungan data pribadi secara khusus. Pengaturan mengenai perlindungan data pribadi di Norwegia dipelajari dan dilakukan penyesuaian terhadap undang-undang dan keadaan masyarakat Indonesia.

Pengaturan mengenai perlindungan data pribadi yang dapat diadaptasi oleh Indonesia dengan menggunakan metode perbandingan yang diuraikan dalam bab sebelumnya adalah mengenai prinsip dalam perlindungan data pribadi, Norwegia memberikan 7 (tujuh) prinsip yang harus dipenuhi agar dapat melindungi data pribadi secara komperhensif, 7 Prinsip

tersebut adalah keabsahan, keadilan dan transparansi; pembatasan tujuan; minimalisasi data; akurasi; batasan penyimpanan; integritas dan kerahasiaan; serta akuntabilitas. Prinsip-prinsip tersebut merupakan prinsip dasar agar dapat diterapkan di Indonesia dengan berbagai modifikasi dan perubahan dengan menyesuaikan kebutuhan dan keadaan masyarakat Indonesia. Prinsip perlindungan setidaknya harus memuat kejelasan tujuan dari pengumpulan data, keadilan, transparan, akurasi serta kerahasiaan. Perlindungan terhadap data pribadi harus ditegaskan dalam suatu peraturan payung sebagai pedoman bagi setiap individu dalam berinteraksi dengan individu lainnya. Adanya standar mengenai apa saja yang merupakan data pribadi dan bagaimana cara data pribadi tersebut dilindungi dalam semua kegiatan yang berkaitan dengan pengolahan serta penyebarluasan data pribadi. Prinsip perlindungan data pribadi dibutuhkan karena merupakan sebuah jaminan bagi hak pemilik data pribadi serta sebuah pedoman dalam melakukan proses pengolahan data pribadi. Prinsip-prinsip tersebut kemudian diaplikasikan dalam berbagai kegiatan pengumpulan data, pengolahan data dan penyebarluasan data. Pada prinsipnya pengaturan mengenai perlindungan data pribadi "*seek to give rights to individuals in how data identifying them or pertaining to them are processed and to subject such processing to a defined set of safeguards"* (Kuner, 2009) yaitu untuk menjamin hak setiap orang untuk mengetahui bagaimana data pribadi seseorang diproses sesuai dengan prosedur. Munculnya *startup digital* juga memicu pengumpulan data-data pribadi dari konsumen secara besar-besaran serta perilaku aktivitas maupun belanja dari konsumen. Mengacu pada beberapa *e-commerce* di Indonesia, *e-commerce* terserbut mengumpulkan data-data pribadi dari konsumen, bahkan jika dilihat hampir semua aplikasi jika ingin dijalankan oleh calon penggunanya maka para pengguna harus memberikan akses ke data-data lainnya seperti identitas diri, lokasi, media, file, daftar kontak dan lain-lain. Sehingga jika pengguna ingin menjalankan aplikasi tersebut maka ia tidak akan memiliki pilihan kecuali menyetujui akses terhadap data-data tersebut, tidak adanya standardisasi prinsip perlindungan data dapat menyebabkan minimnya pengakuan terhadap *right of data subject.*.

Mengenai peraturan transfer data pribadi lintas negara, dalam Norwegia yaitu data pribadi dapat di transfer ke negara lain dengan syarat tunduk kepada peraturan khusus mengenai perlindungan data pribadi selain GDPR dan tingkat perlindungan data pribadi pada peraturan tersebut memadai, peraturan mengenai transfer data pribadi sangat dibutuhkan dalam pengimplementasian perlindungan data pribadi karena agar setiap pemilik data atau individu merasa aman dalam memberikan data pribadinya kepada pihak pengendali serta dengan adanya peraturan mengenai transfer data pribadi Indonesia juga bisa bersaing dalam level internasional dalam kegiatan ekonomi dan bisnis dengan adanya aturan yang akomodatif berkaitan dengan data pribadi negara-negara lain juga akan mengizinkan transfer data antarnegara.

Mengenai ketentuan sanksi, ganti rugi dan pertanggungjawaban, GDPR menegaskan bahwa siapa saja yang melanggar ketentuan-ketentuan dalam perlindungan data pribadi seperti data pribadi seseorang disalahgunakan atau diproses tidak berdasarkan tujuan akan dikenakan denda administratif pengaturan mengenai sanksi, ganti rugi serta pertanggungjawaban sangat penting karena dapat memberikan efek jera bagi orang yang melakukan penyalahgunaan atas data pribadi dan dengan adanya ketentuan sanksi, ganti rugi serta pertanggungjawaban akan memenuhi atau menjamin hak perlindungan data pribadi di Indonesia. Contoh-contoh kasus yang terjadi pada Indonesia pada tahun 2020 terkait dengan pembocoran data yaitu kasus zoom, tokopedia dan spotify. Tokopedia dibobol oleh seorang

hacker yang mengakibatkan 91.000.000 (Sembilan puluh satu juta) data dari pengguna bocor, *hacker* ini pun kemudian menjual data-data dari pengguna tokopedia kepada pihak *darkweb* seharga Rp. 70.000.000,- (ujuh puluh juta) karena *hacker* mengetahui bahwa data pribadi tersebut dapat digunakan untuk berbagai tujuan contohnya seperti penipuan *online.* Berdasarkan *international bussines machines corporation¸* kerugian pertahun yang diakibatkan dari terbobolnya data pribadi adalah 44.000.000.000.000 (empat puluh empat triliun). Dengan itulah Indonesia sangat membutuhkan pengaturan terkait dengan perlindungan data pribadi serta sanksi yang sesuai dengan apa yang telah dilakukan oleh pelanggar dengan adanya pengaturan mengenai sanksi setidaknya memberikan tembok yang jelas untuk keamanan data pribadi (Brook, 2020).

Mengenai otoritas pengawas yang independen berupa lembaga atau komisi, dalam GDPR lembaga tersebut memiliki berbagai macam tugas dan melibatkan berbagai pihak mulai dari parlemen, pemerintah, institusi masyarakat hingga badan legislatif dan administratif. Berdasarkan pasal 57 GDPR, pengawas memiliki tugas untuk mengamati dan memastikan pelaksanaan regulasi, memberikan nasehat kepada parlemen, pemerintah, institusi serta badan legislatif dan administratif untuk mengukur perlindungan dari hak dan kebebasan seseorang pada saat dilakukannya pengolahan data, menyediakan informasi kepada pemilik data mengenai hak pemilik data pribadi serta bekerjasama dengan pengawas dari negara anggota lainnya. Pengawas juga melakuan pengedukasian kepada masyarakat agar sadar dan memahami resiko, pengaturan, pengamanan dan hak-hak merka saat dilakukannya pengolahan data serta melakukan pengedukasian kepada pengendali dan pengelolah yang berkaitan dengan kewajiban masing-masing dalam melaksanakan regulasi. Pengawas juga menerima keberatan atau gugatan yang diajukan oleh pemilik data, badan termasuk melakukan penyelidikan tentang pelaksanaan regulasi apabila terapat laporan dari otoritas pengawas ataupun pemerintah. Fungsi pengawas harus ditekankan tidak hanya untuk mengawasi implementasi peraturan, tetapi juga untuk memastikan bahwa para pihak yang terkait dalam perlindungan data pribadi memperoleh keamanan serta kenyamanan dalam melakukan interaksi. Edukasi kepada para pemilik data merupakan hal yang penting agar para pemilik data mengerti tentang hak dan kewajibannya jika berhadapan dengan pengendali dan pengelolah mulai dari pengumpulan data hingga penyebarluasan data. Seperti adanya komisi khusus yang menangani permasalahan korupsi di Indonesia, Indonesia juga dapat mengadaptasi pengaturan mengenai komisi independen sebagai bentuk pengawasan dan pemastian terhadap para pihak dalam perlindungan data pribadi dikarenakan penyalahgunaan terhadap data pribadi dapat dilakukan oleh pihak manapun, dengan adanya lembaga pengawas yang independen perlindungan terhadap data pribadi akan menjadi lebih maksimal. Komisi pengawas juga memiliki peran untuk membatasi fungsi pengamatan (*surveillance)* dan mendukung akuntabilitas kinerja birokrasi. Masalah mengenai akuntabilitas merupakan hal yang penting karena pemerintah mencari data-data dari suatu individu untuk merancang dan mengevaluasi program kerja, memungkinkan pemerintah menggunakan teknologi perangkat lunak serta perangkat keras.

Mengenai hak-hak pemilik data, undang-undang Indonesia perlu menjelaskan secara merinci terkait dengan hak-hak yang dimiliki oleh pemilik data contohnya pemilik data berhak untuk mengakses informasi terhadap data pribadinya dengan adanya hak akses, pemilik data dapat mengetahui jika terjadi pencatatan yang salah terkait data pribadinya sehingga kesalahan pencatatan tersebut dapat diperbaiki; pemilik data berhak untuk memperoleh informasi dalam hal pemrosesan data pribadi, hak ini memberikan kepastian kepada pemilik

data mengenai proses dan hasil dari pengolahan data pribadinya sehingga pemilik data dapat mengawasi apakah data pribadi yang dikumpulkan tersebut digunakan sesuai dengan tujuan pengumpulan atau tidak; pemilik data berhak untuk menghapus dan mengoreksi data pribadinya, hak untuk mengoreksi merupakan hak yang harus dipenuhi karena pemilik datalah yang mengetahui data-datanya sendiri, jika terdapat kesalahan pada datanya tersebut pemilik data berhak untuk mengoreksi data terebut karena untuk menghindari kesalahan-kesalahan lainnya yang dapat merugikan pemilik data penggunaan hak ini juga memberikan kesempatan bagi kedua belah pihak baik pemilik data maupun pengolah data untuk melakukan pengecekan ulang terhadap data pribadi yang dikumpulkan kemudian hak untuk menghapus data pribadi harus dipenuhi karena apabila data pribadi sudah tidak relevan untuk dikumpulkan sebagaimana tujuan awal dari pengumpulan data tersebut contohnya data pribadi dikumpulkan ketika pemilik data masih anak-anak dan kemudian pemilik data telah beranjak dewasa, maka pemilik data berhak untuk menghapus data terkait dirinya ketika masih anak-anak, pemilik data juga berhak untuk menghapus data pribadinya jika proses pengolahan data pribadi tidak sesuai dengan prosedur atau mekanisme yang telah ditetapkan oleh undang-undang; pemilik data berhak untuk membatasi pemrosesan terhadap data pribadinya, penggunaan hak ini memberikan hak kepada pemilik data jika pengolahan terhadap data pribadi tidak dibutuhkan lagi sebagai tujuan dari pengolahan melainkan digunakan untuk keperluan-keperluan lainnya .

Kesimpulan

Berdasarkan hasil penelitian dan pembahasan yang dikaji penulis berdasarkan teori perbandingan hukum terkait dengan perlindungan data pribadi antara Indonesia dan Norwegia, maka dapat ditarik kesimpulan atas rumusan masalah yang dibahas dalam penelitian ini, yaitu: Terdapat persamaan dan perbedaan dalam perlindungan hukum atas data pribadi di Indonesia dan Norwegia, antara lain mengenai prinsip perlindungan data pribadi, Hak-hak pemilik data, sanksi, pihak yang bertanggung jawab, data pribadi spesifik, keamanan, pemberitahuan penerobosan, profiling, pengawas dan transfer data. Prinsip perlindungan data pribadi di Indonesia adalah Kerahasiaan, integritas, ketersediaan, keautentikan, otorisasi dan kenirsangkalan sedangkan Norwegia adalah keabsahan, keadilan dan transparansi, pembatasan tujuan, minimalisasi data, akurasi, batasan penyimpanan, integritas dan kerahasiaan serta akuntabilitas. Sanksi dalam pelanggaran terhadap data pribadi di Indonesia terdapat sanksi administratif dan sanksi pidana, pada Norwegia terdapat denda administratif. Indonesia menyebut pihak yang bertanggungjawab sebagai penyelenggara sistem elektronik, Norwegia menyebut pihak tersebut sebagai Controller (pengendali) dan processor (pengelolah). Untuk menjaga keamanan dalam perlindungan data pribadi, Indonesia menetapkan beberapa standar yang disesuaikan dengan tingkat penyelenggara sistem elektronik tinggi dan rendah, sedangkan Norwegia tidak menentukan standar keamanan yang harus dilaksanakan. Jika terjadi penerobosan data di Indonesia akan diberitahukan secara tertulis kepada pemilik data dan jika penerobosan terjadi di Norwegia akan diberitahukan kepada supervisory authority dan pemilik data. Indonesia tidak mengatur mengenai profiling sedangkan pada Norwegia, profiling boleh dilakukan atas persetujuan negara dan tidak boleh dilakukan kepada anak-anak. Indonesia masih belum memiliki lembaga pengawas yang independen sedangkan Norwegia memiliki lembaga pengawas yang indepen yaitu supervisory authority (The Norwegian Data Protection Authority (NDPA)) dan European data protection board kedua lembaga tersebut memiliki tugas masing-masing dan aturan hukum perlindungan

data pribadi di Norwegia yang dapat diadaptasi oleh Indonesia berupa prinsip dalam perlindungan data pribadi, peraturan transfer data pribadi lintas negara, ketentuan sanksi, ganti rugi dan pertanggungjawaban serta otoritas pengawas yang independen berupa lembaga atau komisi serta mengenai hak-hak pemilik data.

Daftar Pustaka

Amanda, A. P. B. A. (2008). Tinjauan Yuridis Perlindungan Data Pribadi Dari Penyalahgunaan Data Pribadi Pada Media Sosial. *Jurnal Hukum*. Retrieved from https://media.neliti.com/media/publications/34738-ID-tinjauan-yuridis-perlindungan-data-pribadi-dari-penyalahgunaan-data-pribadi-pada.pdf

Brook, C. (2020). What Does a Data Breach Cost in 2020? Retrieved from ?", https://digitalguardian.com/blog/what-does-data-breach-cost-2020

Kuner, C. (2009). An international legal framework for data protection: Issues and prospects. *Computer Law & Security Review*, *25*(No.1), Hlm. 308.

Mamudji, S. S. dan S. (2004). *Penelitian Hukum Normatif* (Cetakan ke). Jakarta: Raja Grafindo Persada.

Marzuki, P. M. (n.d.). *Penelitian Hukum* (Edisi revi). Jakarta: Kencana Prenada Media Group.

Moleong, L. J. (2011). *Metodologi Penelitian Kualitatif Edisi Revisi*. Bandung: PT Remaja Rosdakarya.

Niffari, H. (2020). PERLINDUNGAN DATA PRIBADI SEBAGAI BAGIAN DARI HAK ASASI MANUSIA ATAS PERLINDUNGAN DIRI PRIBADI Suatu Tinjauan Komparatif Dengan Peraturan Perundang-Undangan Di Negara Lain. *SELISIK -*, *6*(1), hlm. 8.

Nugraha, R. A. (2018). Perlindungan Data Pribadi dan Privasi Penumpang Maskapai Penerbangan pada Era Big Data. *Mimbar Hukum - Fakultas Hukum Universitas Gadjah Mada*, *30*(2), 262. https://doi.org/10.22146/jmh.30855

Priscyllia, F. (2019). *PERLINDUNGAN PRIVASI DATA PRIBADI PERSPEKTIF PERBANDINGAN HUKUM*. *34*(3), 1–5.

Rianarizkiwati, N. (2020). *Kebebasan Informasi versus Hak atas Privasi Tanggung Jawab Negara dalam Perlindungan Data Pribadi*. Depok: Infermia Publishing.

Rosalinda Elsina Latumahina. (2014). Aspek Hukum Perlindungan Data Pribadi di Dunia Maya. *Jurnal GEMA AKTUALITA*, *3*(2), 14–25.

Setyawan, A., & Wijaya, B. (2018). Perlindungan Konsumen dalam Transaksi E-Commerce Ditinjau dari Undang-Undang Perlindungan Konsumen. *Journal of Judicial Review*, *19*(2), 46-70.

Wardiana. (2002). *Aspek-Aspek Pemanfaatan ITE*. Yogyakarta: Raja Grafindo Persada.

Winarso, T., Disemadi, H. S., & Prananingtyas, P. (2020). Protectıon Of Prıvate Data Consumers P2p Lendıng As Part Of E-Commerce Busıness In Indonesıa. *Tadulako Law Review*, *5*(2), 206-221.

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik Juncto Undang-undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik

Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik

Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan

Data Pribadi Dalam Sistem Elektronik
Peraturan Menteri Komunikasi dan Informatika Nomor 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi
General Data Protection Regulation
The Constitution of the Kingdom of Norway