



**PERTANGGUNGJAWABAN HUKUM BAGI LINKEDIN ATAS  
KEBOCORAN DATA PRIBADI *END-USER* MELALUI  
*APPLICATION PROGRAMMING INTERFACE***

**SKRIPSI**

Diajukan Untuk Memenuhi Sebagian Syarat-Syarat  
Memperoleh Gelar Sarjana Hukum

Oleh:

**AURORA IZZA SABILA**

**18501010011134**



**KEMENTERIAN PENDIDIKAN, KEBUDAYAAN, RISET, DAN  
TEKNOLOGI**

**UNIVERSITAS BRAWIJAYA**

**FAKULTAS HUKUM**

**MALANG**

**2022**



**HALAMAN PERSETUJUAN**

**Judul Skripsi**

**: PERTANGGUNGJAWABAN HUKUM BAGI LINKEDIN ATAS PENYALAHGUNAAN DATA PRIBADI END-USER MELALUI APPLICATION PROGRAMMING INTERFACE**

**Identitas Penulis**

**:**

**a. Nama**

**: Aurora Izza Sabila**

**b. NIM**

**: 185010100111134**

**Konsentrasi**

**: Hukum Ekonomi dan Bisnis**

**Jangka waktu penelitian**

**: 9 bulan**

**Disetujui pada tanggal**

**: 20 Juli 2022**

**Pembimbing Utama**



**Moch. Zairul Alam, S.H., M.H.  
NIP. 197409092006041002**

**Pembimbing Pendamping**



**Ranitya Ganindha S.H., M.H.  
NIP. 198806302014042001**

**Mengetahui,  
Ketua Jurusan Ilmu Hukum**



**Dr. Sukarmi, S.H., M.Hum.  
NIP. 196705031991032002**







**HALAMAN PENGESAHAN**

**PERTANGGUNGJAWABAN HUKUM BAGI LINKEDIN ATAS  
PENYALAHGUNAAN DATA PRIBADI *END-USER* MELALUI *APPLICATION  
PROGRAMMING INTERFACE***

Oleh:

**AURORA IZZA SABILA  
NIM 18501010011134**

Disetujui pada tanggal : 20 Juli 2022

Pembimbing Utama



Moch. Zairul Alam, S.H., M.H.  
NIP. 197409092006041002

Pembimbing Pendamping



Ranitya Ganindha S.H., M.H.  
NIP. 198806302014042001

Mengetahui,  
Ketua Jurusan Ilmu Hukum



Dr. Sukarmi, S.H., M.Hum.  
NIP. 196705031991032002





## KATA PENGANTAR

Syukur Alhamdulillah penulis haturkan kepada Allah SWT., Sang Pencipta seluruh alam yang tak ada sekutu bagi-Nya, tiada daya upaya melainkan atas Izin-Nya penulis berhasil menyelesaikan penulisan skripsi ini dengan lancar. Doa tak berujung juga tak lupa penulis haturkan kepada Nabiullah Muhammad SAW., panutan kaum muslimin, yang telah membawa umat muslim menuju zaman yang lebih terang-benderang.

Di saat menulis skripsi ini, penulis memperoleh tuntunan dan bantuan yang penuh kasih dan cinta dari berbagai pihak. Oleh karena itu, terima kasih penulis antarkan teruntuk:

1. Bapak Dr. M. Ali Safa'at, S.H., M.H., selaku Dekan Fakultas Hukum Universitas Brawijaya;
2. Bapak Moch. Zairul Alam, S.H., M.H., selaku Ketua Kompartemen Hukum Ekonomi dan Bisnis sekaligus Dosen Pembimbing I. Saya mengucapkan banyak terima kasih kepada Bapak untuk segenap pengertian dan perhatiannya, serta kalimat-kalimat mutiara, pembangkit semangat, dan petunjuk yang telah bapak bagikan kepada kami. Hal-hal tersebut sangat berarti bagi Penulis sehingga dapat menuntaskan skripsi ini;
3. Ibu Ranitya Ganindha, S.H., M.H., selaku Dosen Pembimbing II. Terima kasih atas segala masukan yang telah ibu beri guna menyempurnakan skripsi ini;
4. Yang tercinta dan yang saya hormati, Aunur El Rifqie, S.E. dan Noor Fidiana, S.E. selaku orang tua penulis. Terima kasih atas harapan tulus serta dukungan yang tak berujung dicurahkan demi putri pertamanya ini;
5. Laili Fatqulia Rahma dan Razita Audie Jannah selaku saudara kandung penulis atas doa, semangat, dan dukungan lainnya;
6. Sahabat-sahabat penulis yaitu Laa Tansa Amalia, Maulidiyah Fitriana Sari, Silvana Natasya Baby Pratika, Sri Hartanti, dan Nurul Faridah. Terima kasih selalu ada untuk penulis dan segala kekurangannya;
7. Teman penulis, Thufail Rozaan. Terima kasih untuk selalu menanyakan progress skripsi penulis di segala kesempatan guna mengingatkan penulis; serta





8. Pihak lain yang ikut serta mengulurkan bantuan guna terselesainya skripsi ini yang tak mampu penulis sebutkan satu demi satu.

Penulis mengetahui sepenuhnya bahwa skripsi ini masih memiliki banyak kekurangan dan tidak paripurna, oleh karena itu nasihat dan tanggapan yang membangun dari semua pihak selalu penulis nantikan bagi pembetulan dan penyempurnaan skripsi ini agar dapat memberikan faedah yang lebih luas.

Penulis memohon maaf yang sebanyak-banyaknya apabila di dalam penyusunan skripsi ini masih terdapat kekurangan baik yang disengaja maupun tidak disengaja.

Malang, 6 April 2022

Penulis



**DAFTAR ISI**

<b>HALAMAN PERSETUJUAN .....</b>	<b>ii</b>
<b>HALAMAN PENGESAHAN.....</b>	<b>iii</b>
<b>KATA PENGANTAR.....</b>	<b>iv</b>
<b>DAFTAR ISI .....</b>	<b>vi</b>
<b>DAFTAR TABEL .....</b>	<b>viii</b>
<b>DAFTAR GAMBAR .....</b>	<b>ix</b>
<b>RINGKASAN.....</b>	<b>x</b>
<b>SUMMARY.....</b>	<b>xi</b>
<b>BAB I PENDAHULUAN .....</b>	<b>1</b>
A. LATAR BELAKANG.....	1
B. ORISINALITAS PENELITIAN.....	6
C. RUMUSAN MASALAH.....	10
D. TUJUAN PENELITIAN.....	10
E. MANFAAT PENELITIAN.....	11
F. METODE PENELITIAN.....	12
<b>BAB II TINJAUAN PUSTAKA .....</b>	<b>17</b>
A. TINJAUAN UMUM TENTANG PERTANGGUNGJAWABAN HUKUM.....	17
B. TINJAUAN UMUM TENTANG DATA PRIBADI.....	25
1. Pengertian Data Pribadi.....	25
2. Dasar Hukum Perlindungan Data Pribadi di Indonesia .....	29
C. TINJAUAN UMUM TENTANG APPLICATION PROGRAMMING INTERFACE (API).....	31
1. Definisi <i>Application Programming Interface</i> (API).....	31
2. Skema Kerja <i>Application Programming Interface</i> (API).....	32
3. Kategori <i>Application Programming Interface</i> (API) .....	32
4. LinkedIn API .....	33
<b>BAB III PEMBAHASAN .....</b>	<b>35</b>
A. Analisis <i>Privacy Policy</i> LinkedIn Mengenai Perlindungan Data Pribadi dikaitkan Pasal 26 Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.....	35





1. Analisis <i>Privacy Policy</i> (Kebijakan Privasi) LinkedIn Terkait Data Pribadi Pengguna.....	35
2. Analisis <i>Privacy Policy</i> LinkedIn dikaitkan dengan Pasal 26 Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik serta peraturan turunan yang relevan.....	51
B. Pertanggungjawaban Hukum bagi LinkedIn Jika Terjadi Penyalahgunaan Data Pribadi Pengguna Akhir ( <i>End-User</i> ) Melalui <i>Application Programming Interface</i> (API) Platform.....	70
<b>BAB IV KESIMPULAN .....</b>	<b>78</b>
A. Kesimpulan.....	78
B. Saran.....	79

**DAFTAR PUSTAKA**





**DAFTAR TABEL**

**Tabel 1.1** Tabel Orisinalitas Penelitian.....7

**Tabel 3.1** Tabel Substansi *Privacy Policy* LinkedIn yang Terkait dengan Data Pribadi Pengguna.....49

**Tabel 3.2** Tabel Kewajiban PSE terkait Perlindungan Data Pribadi yang Diatur di Peraturan Perundang-Undangan.....65



**DAFTAR GAMBAR**

**Gambar 1.1** Media Sosial yang paling banyak digunakan di Indonesia pada 2020..... 3

**Gambar 1.2** Sampel Data Pengguna LinkedIn Asal Indonesia yang Dijual di Salah Satu Forum Hacker.....4

**Gambar 2.1** Skema Konektivitas API..... 32

**Gambar 3.1** Laman Pendaftaran Akun pada LinkedIn..... 41



## RINGKASAN

Aurora Izza Sabila, Hukum Ekonomi dan Bisnis, Fakultas Hukum Universitas Brawijaya, April 2022, PERTANGGUNGJAWABAN HUKUM BAGI LINKEDIN ATAS PENYALAHGUNAAN DATA PRIBADI END-USER MELALUI *APPLICATION PROGRAMMING INTERFACE*, Moch. Zairul Alam, S.H., M.H., Ranitya Ganindha, S.H., M.H.

Pemilihan topik ini dilatar belakangi oleh adanya data pribadi pengguna LinkedIn yang bocor dan dijual belikan di forum peretas / *hacker* dan didapatkan melalui API platform, bukan melalui server LinkedIn secara langsung. Pada *Privacy Policy* LinkedIn terdapat klausula yang menyatakan bahwa LinkedIn akan membagikan data pribadi penggunanya di berbagai layanan mereka dan entitas yang berafiliasi dengan LinkedIn. Namun tidak ada pernyataan mengenai sejauh apa tanggung jawab LinkedIn atas perlindungan data pribadi penggunanya yang telah dibagikan tersebut. Peraturan perundang-undangan di Indonesia belum mengatur secara spesifik mengenai bagaimana pertanggungjawaban hukum bagi PSE atas data pribadi *end-user* ketika data pribadi tersebut dibagikan kepada pihak ketiga yang juga melakukan pengelolaan terhadapnya, baik dalam rangka untuk menjalankan tugas dari platform ataupun untuk kepentingannya.

Penulisan skripsi ini bertujuan untuk: (1) Untuk menganalisis *Privacy Policy LinkedIn* mengenai perlindungan data pribadi yang dikaitkan dengan Pasal 26 Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi Dan Transaksi Elektronik; dan (2) Untuk menganalisis mengenai bagaimana pertanggungjawaban hukum bagi LinkedIn jika terjadi penyalahgunaan data pribadi pengguna akhir (*end-user*) melalui *Application Programming Interface* (API) platform.

Penulisan skripsi ini menggunakan metode yuridis normatif dengan jenis pendekatan perundang-undangan dan konseptual. Bahan hukum primer, sekunder, dan tersier yang diperoleh penulis akan dianalisis dengan teknik deskriptif dan menggunakan metode interpretasi sistematis dan gramatikal.

Dari hasil penelitian dengan metode diatas, penulis memperoleh jawaban bahwa di dalam *Privacy Policy*-nya, LinkedIn telah memuat beberapa klausula dalam rangka pemenuhan prinsip-prinsip perlindungan data pribadi serta kewajibannya. Namun LinkedIn belum memenuhi kewajiban untuk "memberitahukan kepada pemilik data pribadi yang bersangkutan apabila terjadi kegagalan dalam perlindungan terhadap data pribadi yang dikelolanya". Selain itu, walaupun pada *Privacy Policy* LinkedIn sudah mencantumkan bahwa mereka akan membagikan data pribadi pengguna di berbagai layanan dan entitas yang berafiliasi dengan LinkedIn, namun belum diatur mengenai apakah LinkedIn tetap memiliki tanggung jawab atas data pribadi pengguna yang telah dibagikan kepada pihak ketiga tersebut. Kemudian berdasarkan prinsip *vicarious liability*, LinkedIn tetap dapat dimintai pertanggungjawaban atas adanya kebocoran data pribadi penggunanya walaupun kebocoran tersebut terjadi melalui API dan LinkedIn dapat digugat dengan PMH disebabkan adanya kesalahan atau kelalaian yang menimbulkan kerugian serta karena LinkedIn tidak memenuhi kewajiban-kewajibannya sebagai Penyelenggara Sistem Elektronik yang telah dibebankan kepadanya menurut peraturan perundang-undangan.



## SUMMARY

Aurora Izza Sabila, Economics and Business Law, Faculty of Law, University of Brawijaya, 2022, LINKEDIN'S LEGAL RESPONSIBILITY FOR MISUSE OF END-USER PERSONAL DATA THROUGH APPLICATION PROGRAMMING INTERFACE, Moch. Zairul Alam, S.H., M.H., Ranitya Ganindha, S.H., M.H.

The choice of this topic was motivated by the accident of LinkedIn users' personal data that was leaked and traded on hacker forums/hackers and obtained through the platform API, not through LinkedIn's servers directly. In LinkedIn's Privacy Policy, there is a clause that states that LinkedIn will share its users' personal data across their various services and entities affiliated with LinkedIn. However, there is no statement regarding the extent of LinkedIn's responsibility for the protection of users' personal data that has been shared.

Indonesia's law has not specifically stipulated how the PSE is legally responsible for end-user personal data when the personal data is shared with third parties who also manage it, either in order to carry out the duties of the platform or for its interests.

Therefore, this thesis aims to: (1) To analyze LinkedIn's Privacy Policy regarding the protection of personal data associated with Article 26 of the Law 19 of 2016 concerning Amendments to Law 11 of 2008 on Information and Electronic Transactions; and (2) To analyze LinkedIn's legal liability in the event of misuse of end-user personal data via the Platform's Application Programming Interface (API).

This thesis uses a normative juridical method with the statute approach and the conceptual approach. The primary, secondary, and tertiary legal materials obtained by the author will be analyzed using descriptive techniques and using systematic and grammatical interpretation methods.

The author obtained the answer that in its Privacy Policy, LinkedIn has contained several clauses in order to fulfill the principles of personal data protection and its obligations. However, LinkedIn has not fulfilled its obligation to "notify the owner of the personal data concerned in the event of a failure to protect the personal data it manages". In addition, although LinkedIn's Privacy Policy has stated that they will share users' personal data in various services and entities affiliated with LinkedIn, it has not been regulated whether LinkedIn still has responsibility for user's personal data that has been shared with these third parties. Then, based on the principle of vicarious liability, LinkedIn can still be held responsible for the leakage of its users' personal data even though the leak occurs through the API and LinkedIn can be sued on the basis of tort due to errors or omissions that cause losses and because LinkedIn does not fulfill its obligations as an Electronic System Operator that have been charged to him according to the laws and regulations.





## BAB I

### PENDAHULUAN

#### A. LATAR BELAKANG

Alenia ke-4 Pembukaan UUD NRI 1945 menerangkan bahwa menjadi kewajiban Pemerintah Indonesia secara konstitusional untuk melindungi segenap bangsa Indonesia dan seluruh tumpah darah Indonesia dan untuk memajukan kesejahteraan umum, mencerdaskan kehidupan bangsa, dan ikut melaksanakan ketertiban dunia yang berdasarkan kemerdekaan, perdamaian abadi dan keadilan sosial.<sup>1</sup> Dalam konteks perkembangan Teknologi informasi dan komunikasi (TIK), kewajiban-kewajiban tersebut dimanifestasikan ke dalam perlindungan data pribadi bagi setiap penduduk Indonesia.<sup>2</sup>

TIK dan elektronik saat ini tumbuh dengan cepat. Kehadiran komputer hingga telepon pintar serta internet menandakan terjadinya perkembangan TIK dan elektronik di tengah peradaban manusia. Internet sendiri merupakan jaringan komunikasi elektronik yang dapat mengkoneksikan jaringan dan fasilitas komputer yang terorganisasi di berbagai belahan dunia.<sup>3</sup> Jaringan Internet secara fisik dikembangkan pertama kali di tahun 1969 oleh Departemen Pertahanan Amerika Serikat melalui proyek pengembangan jaringan *Advanced Research Project Agency Network* atau ARPANET dan tetap bertumbuh hingga kini.

Dikutip dari laporan yang diterbitkan oleh agensi pemasaran media sosial *We Are Social* dan layanan manajemen konten *HootSuite* yang berjudul "Digital 2021", pemakai internet di seluruh dunia hingga Januari 2021 mencapai 4,66 Miliar orang, dengan pengguna aktif media sosial sebanyak 4,2 Miliar orang. Sedangkan di Indonesia sendiri, hingga Januari tercatat sebanyak 202,6 juta pengguna internet dan sebanyak 170 juta

<sup>1</sup> **Pembukaan Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.**

<sup>2</sup> Direktorat Jenderal IKP, Kementerian Komunikasi dan Informatika, dan *Cyberlaw Centre* Fakultas Hukum Universitas Padjadjaran, 2016, **Naskah Akademik RUU Perlindungan Data Pribadi (Penyelarasan)**, Badan Pembinaan Hukum Nasional, hlm. 1.

<sup>3</sup> Merriam-Webster, **Internet**, diterjemahkan dari <http://www.merriam-webster.com/dictionary/Internet> (24 Agustus 2021)



pengguna media sosial.<sup>4</sup> Oleh karena itu, dengan melihat betapa besarnya pemanfaatan internet dan media sosial di tengah masyarakat Indonesia, maka perlindungan data pribadi menjadi unsur yang esensial pada saat berkegiatan di dunia maya dan media sosial guna memberikan kenyamanan dan keamanan bagi masyarakat Indonesia.

Berbagai media sosial banyak yang mulai menggunakan sistem *Application Programming Interface* (API) dalam platform mereka. API adalah sebuah sistem antarmuka yang mengkoneksikan suatu program dengan program lain guna mengakses sebagian sistem operasi maupun data yang terdapat pada suatu aplikasi. Dimungkinkan seorang developer membuat suatu *software* baru tanpa harus benar-benar menyusun sistem *software* dari awal, karena developer bisa memanfaatkan API dari *software* sejenis untuk mendapatkan sebagian sistem operasi ataupun data yang dapat ia gunakan untuk menyusun *software* miliknya.

Selain itu, *software* ataupun aplikasi yang menggunakan API dapat mempertahankan kode mereka sambil mendapatkan lebih banyak publisitas untuk produk mereka.<sup>5</sup> Mereka dapat terhubung dengan *software* ataupun aplikasi lain dan bertukar sebagian informasi, data, ataupun susunan sistem dengan memanfaatkan API. Maka API merupakan standar komunikasi yang dibuat oleh perusahaan perangkat lunak agar dapat dimanfaatkan oleh pengembang pihak ketiga untuk mendesain aplikasi yang menggunakan sistem atau data mereka dengan mudah tanpa harus mengorbankan seluruh sistem dan data yang dimilikinya.

Jika diibaratkan, maka API merupakan jembatan penghubung antara dua daratan yang terpisah dan dibentuk dengan kumpulan kode yang menyediakan pelbagai *access point* sehingga informasi, data, ataupun kode pemrograman dari aplikasi A dapat terkirim ke aplikasi B dengan baik.<sup>6</sup>

<sup>4</sup> We are Social, 2021, *Digital 2021* (Online), <https://wearesocial.com/digital-2021> (24 Agustus 2021)

<sup>5</sup> Nur Aini Rakhmawati dkk, 2019, *Indonesia's Public Application Programming Interface (API)*, Jurnal Penelitian Pos dan Informatika, Volume 9, Nomor 2, Kementerian Komunikasi dan Informatika, Jakarta, 2019, Hlm. 86.

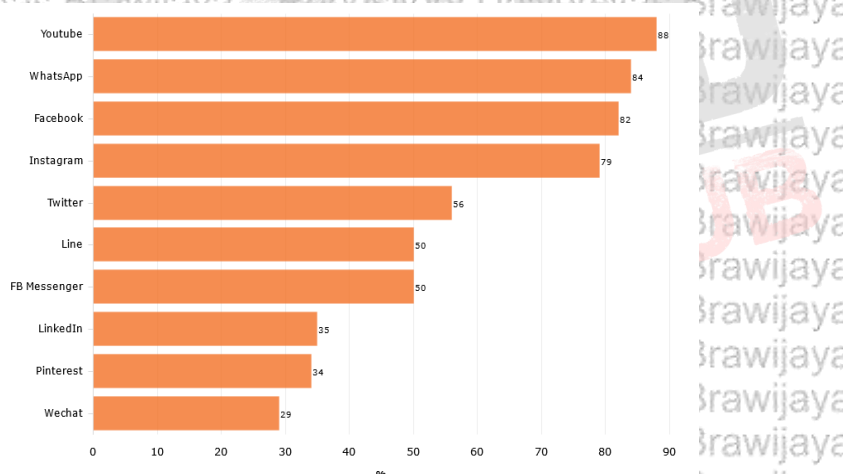
<sup>6</sup> BRI API, 2021, *Apa Itu API: Pengertian, Cara Kerja, hingga Manfaat API* (online), <https://developers.bri.co.id/id/news/apa-itu-api-pengertian-cara-kerja-hingga-manfaat-api> (01 Maret 2022)





Salah satu media sosial yang memanfaatkan API adalah LinkedIn. LinkedIn ialah salah satu media sosial yang tergolong jenis *Social Networking* yang berorientasi pada bisnis, dapat digunakan untuk mendapatkan pekerjaan atau magang yang sesuai, menyambungkan dan memperkuat hubungan profesional, dan mendalami keterampilan yang dapat menunjang karir (kepentingan bisnis dan karir profesional). LinkedIn didirikan pada Desember 2002 dan diresmikan pada 5 Mei 2003 di California, Amerika Serikat dan didirikan Reid Hoffman bersama anggota dari PayPal dan Socialnet.com.<sup>7</sup> LinkedIn menduduki posisi kedelapan dari 10 media sosial dengan pengguna terbesar di Indonesia di tahun 2020 dengan jumlah persentase sebesar 35% dari jumlah penduduk Indonesia seperti yang terlihat pada Gambar 1.1.

**Gambar 1.1 Media Sosial yang paling banyak digunakan di Indonesia pada 2020**



Sumber: *We Are Social, Hootsuite, 2020*

Kehadiran fitur API pada LinkedIn sejatinya menguntungkan terutama dari segi bisnis dan pengembangan teknologi dan fitur dari LinkedIn karena pengguna dapat masuk ke aplikasi lain menggunakan akun LinkedIn mereka, sehingga tidak perlu memasukkan data diri lagi. Selain itu, developer dapat mengembangkan aplikasi yang dimilikinya dengan data yang terdapat pada LinkedIn. Namun di samping itu, pemanfaatan API pada

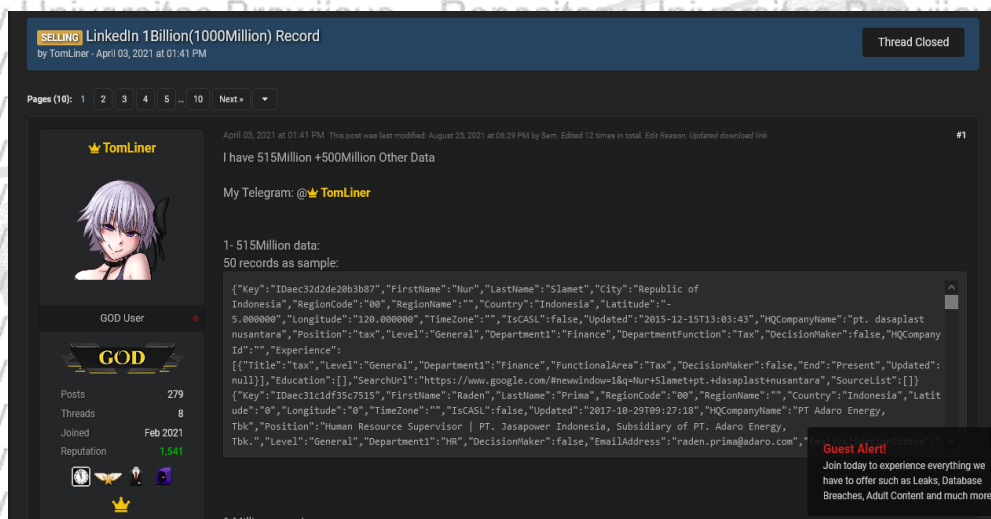
<sup>7</sup> Fransisca Stefanie Chandra, 2017, **Kepuasan Pengguna Jejaring Sosial LinkedIn sebagai Jejaring Sosial yang Berorientasi pada Dunia Bisnis dan Profesional di Indonesia** (*online*), Jurnal E-Komunikasi, Volume 5, Nomor 2, <http://publication.petra.ac.id/index.php/ilmu-komunikasi/article/view/7079>, (24 Agustus 2021)



LinkedIn juga tidak lepas dari permasalahan hukum, seperti mengenai kebocoran data pribadi.

Pada tahun Juni 2021, 700 juta data pengguna LinkedIn bocor dan dijual bebas di forum *hacker*. Sebelumnya LinkedIn juga mengalami kejadian serupa pada April 2021 dengan jumlah 500 juta pengguna. Adapun data dan informasi yang bocor termasuk nama email, nama lengkap, nomor telepon, alamat fisik, riwayat lokasi geolokasi, username linkedin, URL *profile*, latar belakang/pengalaman personal dan profesional, gender, serta *username* akun sosial media lain dari pengguna. Adapun contoh data pribadi pengguna LinkedIn asal Indonesia yang dijual dapat diamati pada Gambar 1.2. berikut.

**Gambar 1.2. Sampel Data Pengguna LinkedIn Asal Indonesia yang Dijual di Salah Satu Forum Peretas**



Sumber: *RaidForum*, 2021

Data-data yang dijual oleh peretas didapatkan dengan mengeksploitasi LinkedIn API untuk mendapatkan informasi yang di upload di situs.<sup>8</sup> Pernyataan resmi dari LinkedIn menyatakan bahwa tidak semua data bisa diperoleh melalui LinkedIn API. Dan kejadian tersebut bukanlah kebocoran data/*data breach* dan tidak ada data privat/pribadi dari pengguna yang terekspos.<sup>9</sup>

<sup>8</sup> Taylor, Sven, 2021, ***New LinkedIn Data Leak Leaves 700 Million Users Exposed*** (online), <https://restoreprivacy.com/linkedin-data-leak-700-million-users/>, (24 Agustus 2021)

<sup>9</sup> LinkedIn, 2021, ***An update on report of scraped data*** (online), <https://news.linkedin.com/2021/june/an-update-from-linkedin> (24 Agustus 2021)



Jika kita merujuk kepada peraturan perundang-undangan di Indonesia, Pasal 26 UU ITE menyatakan bahwa pemanfaatan tiap-tiap informasi via alat-alat elektronik yang melibatkan data pribadi seseorang harus dilaksanakan berdasarkan persetujuan orang tersebut atau yang terkait, dan jika hak itu tidak dipenuhi, maka orang itu dapat melayangkan gugatan mengenai adanya kerugian yang muncul.<sup>10</sup> Kewajiban platform atas perlindungan data pribadi pengguna lebih lanjut juga diatur pada peraturan turunannya, seperti pada beberapa Peraturan Pemerintah dan Peraturan Menteri Komunikasi dan Informatika (Permenkominfo) terkait.

Pada *Privacy Policy* (Kebijakan Privacy) LinkedIn terdapat klausula yang menyatakan bahwa LinkedIn akan membagikan data pribadi pengguna di berbagai layanan mereka dan entitas yang berafiliasi dengan LinkedIn. Namun tidak ada pernyataan lebih lanjut mengenai sejauh apa tanggung jawab LinkedIn terhadap perlindungan data pribadi pengguna yang telah dibagikan tersebut. Perundang-undangan Indonesia tidak mengatur dengan khusus bagaimana platform (atau yang dalam peraturan perundang-undangan Indonesia disebut Penyelenggara Sistem Elektronik (PSE)) akan bertanggung jawab secara hukum atas data pribadi pengguna akhir (*end-user*) ketika data pribadi tersebut dibagikan kepada pihak ketiga yang juga melakukan pengelolaan terhadapnya, baik dalam rangka untuk menjalankan tugas dari platform ataupun untuk kepentingannya. Ketiadaan pengaturan mengenai hal tersebut menimbulkan permasalahan hukum, yakni apakah LinkedIn tetap dapat dimintai pertanggungjawaban atas adanya kebocoran data pribadi pengguna meskipun kebocoran data pribadi tersebut terjadi melalui API yang disediakan oleh penyedia API, bukan melalui *server* milik LinkedIn.

Dari permasalahan yang telah dijelaskan sebelumnya dan melihat cukup banyaknya persentase dari penduduk Indonesia yang menggunakan aplikasi LinkedIn, maka penulis ingin mengkajinya lebih lanjut dengan ke dalam skripsi berjudul **"PERTANGGUNGJAWABAN HUKUM BAGI LINKEDIN ATAS PENYALAHGUNAAN DATA PRIBADI *END-USER*"**

<sup>10</sup> Pasal 26 ayat (1) dan (2) Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.



**MELALUI APPLICATION PROGRAMMING INTERFACE**. Nantinya, penulis akan membedah sejauh apa perlindungan data pribadi yang telah diatur *Privacy Policy* LinkedIn secara lebih lengkap dan menyeluruh. Guna mengetahui apakah *Privacy Policy* LinkedIn telah selaras dengan pengaturan terkait perlindungan data pribadi yang telah diwajibkan oleh UU ITE dan peraturan turunannya, maka selanjutnya analisis tersebut akan penulis kaitkan dengan peraturan-peraturan yang mengatur berkenaan dengan perlindungan data pribadi, yaitu Pasal 26 Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik (UU 19/2016) serta ketentuan turunannya. Setelah itu, hasil analisis yang telah dilakukan sebelumnya akan digunakan untuk menemukan jawaban mengenai bagaimana pertanggungjawaban hukum bagi LinkedIn atas terjadinya penyalahgunaan data pribadi pengguna akhir (*end-user*) melalui *Application Programming Interface* (API) LinkedIn.

## **B. ORISINALITAS PENELITIAN**

Untuk menunjukkan kebaruan serta arah penelitian yang lain dengan hasil penelitian sebelumnya, maka penulis memaparkan perbedaannya dengan Tabel 1.1 berikut:



Tabel 1.1

## Tabel Orisinalitas Penelitian

No	Nama Peneliti dan Asal Instansi	Judul dan Tahun Penelitian	Rumusan Masalah
1	Achmad Paku Braja Arga Amanda, Fakultas Hukum Universitas Brawijaya	Tinjauan Yuridis Perlindungan Data Pribadi dari Penyalahgunaan Data Pribadi pada Media Sosial (Ditinjau dari <i>Privacy Policy Facebook</i> dan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik), 2013	<ol style="list-style-type: none"> <li>1. Bagaimana tanggung jawab hukum media sosial <i>Facebook</i> dalam melindungi pengguna dari penyalahgunaan data pribadi.?</li> <li>2. Bagaimana UU No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik beserta Peraturan Pelaksanaannya melindungi data pribadi pengguna media sosial <i>Facebook</i> dari penyalahgunaan data pribadi?</li> </ol>
2	Virginia Rosalina Dewi, Fakultas Hukum Universitas Brawijaya	Perlindungan Data Pribadi Konsumen Pengguna Jasa Transportasi Berbasis Aplikasi (Studi Analisis pasal 26 Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik dan Pasal 15 Peraturan Pemerintah Nomor 82 Tahun 2012 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik)	<ol style="list-style-type: none"> <li>1. Bagaimana perlindungan hukum data pribadi konsumen pengguna jasa transportasi berbasis aplikasi menurut pasal 26 Undang-Undang Informasi dan Transaksi Elektronik dan Pasal 15 Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik ?</li> <li>2. Apa solusi yang dilakukan oleh</li> </ol>



		Elektronik), 2016	konsumen jika terjadi pelanggaran atas data pribadi konsumen pengguna jasa transportasi berbasis aplikasi?
Mody Malinda, Fakultas Hukum Universitas Brawijaya		Tinjauan Yuridis <i>Privacy Policy</i> Pada <i>Online Store</i> Terkait Perlindungan Data Pribadi Berdasarkan Ketentuan Di Negara Malaysia Dan Indonesia, 2017	<ol style="list-style-type: none"> <li>1. Bagaimana perbedaan ruang lingkup ketentuan tentang perlindungan data pribadi pengguna <i>Online Store</i> dalam Malaysia <i>Personal Data Protection Act</i> 2010 dan Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi Dan Transaksi Elektronik?</li> <li>2. Bagaimana analisa perlindungan data pribadi pengguna <i>Online Store</i> dalam <i>privacy policy</i> pada website shopee, lazada dan qoo10 apabila dikaitkan dengan Malaysia <i>Personal Data Protection Act</i> 2010 dan Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi Dan Transaksi Elektronik?</li> </ol>

Sumber: *Data diolah, 2021*





Penjelasan lebih lanjut mengenai perbedaan penelitian pada skripsi ini dengan penelitian sebelumnya:

1. Pada penelitian berjudul "Tinjauan Yuridis Perlindungan Data Pribadi Dari Penyalahgunaan Data Pribadi Pada Media Sosial (Ditinjau dari *Privacy Policy* Facebook dan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik)" penulis sebelumnya memberatkan kepada bagaimana perlindungan data pribadi ketika terjadi penyalahgunaan data pribadi pada media sosial Facebook. Kemudian, Saudara Achmad masih menggunakan UU ITE beserta peraturan turunan sebelum perubahan di dalam kajiannya. Sedangkan penelitian ini telah menggunakan UU ITE serta peraturan turunan berkenaan perlindungan data pribadi yang terbaru sertaditautkan dengan media sosial LinkedIn.
2. Di tahun 2016, Saudari Virginia melangsungkan penelitian berkenaan dengan "Perlindungan Data Pribadi Konsumen Pengguna Jasa Transportasi Berbasis Aplikasi (Studi Analisis Pasal 26 Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik dan Pasal 15 Peraturan Pemerintah Nomor 82 Tahun 2012 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik)". Penelitian berpusat kepada perlindungan data pribadi untuk pengguna jasa transportasi berbasis aplikasi serta penyelesaian yang dapat dilakukan jika terjadi pelanggaran data pribadi. Selain itu penulis sebelumnya juga masih menggunakan UU ITE dan PP PSTE yang belum mengalami perubahan sebagai dasar analisisnya. Adapun penelitian ini menekankan pada aplikasi LinkedIn dan telah memakai UU ITE dan PP PSTE terbaru sebagai bahan kajian, yakni UU 19/2016 tentang Perubahan Atas UU 11/2008 tentang ITE dan PP 71/2019 tentang PSTE.
3. Penulis sebelumnya (Mody Malinda) pada penelitian yang dilakukan pada tahun 2017 berjudul "Tinjauan Yuridis *Privacy Policy* Pada *Online Store* Terkait Perlindungan Data Pribadi Berdasarkan Ketentuan Di Negara Malaysia Dan Indonesia" berfokus pada perbandingan ruang lingkup ketentuan tentang perlindungan data pribadi yang diatur pada Malaysia *Personal Data Protection Act* 2010 dengan UU 19/2016 tentang Perubahan Atas UU 11/2008 tentang ITE. Kemudian penulis sebelumnya



juga menganalisis perlindungan data pribadi pengguna yang diatur *privacy policy* beberapa *Online Store* seperti *shopee, lazada dan qoo10* dan dikaitkan dengan perbandingan yang telah dianalisis sebelumnya. Sedangkan pada penelitian ini, penulis hanya akan menganalisis perlindungan data pribadi dari *Privacy Policy* milik satu platform saja, yakni LinkedIn. Selain itu, pada penelitian ini analisis *Privacy Policy* tersebut hanya akan dikaitkan dengan ketentuan perlindungan data pribadi di Indonesia saja.

Selain itu, pada penelitian ini juga akan dianalisis lebih lanjut mengenai apakah LinkedIn tetap dapat dimintai pertanggungjawaban atas adanya penyalahgunaan data pribadi penggunaannya meskipun data pribadi tersebut didapatkan melalui *Application Programming Interface (API)*, bukan dengan cara membobol server dari LinkedIn secara langsung. Analisis lanjutan inilah yang juga membedakan penelitian ini dengan penelitian sebelumnya.

### C. RUMUSAN MASALAH

Beralaskan paparan latar belakang yang sudah diuraikan sebelumnya, maka pada skripsi ini, penulis telah merumuskan beberapa masalah yang akan dianalisis lebih jauh. Rumusan masalah penelitian ini adalah:

1. Bagaimana analisis *Privacy Policy* LinkedIn mengenai perlindungan data pribadi dan dikaitkan dengan Pasal 26 Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi Dan Transaksi Elektronik?
2. Bagaimana pertanggungjawaban hukum bagi LinkedIn jika terjadi penyalahgunaan data pribadi pengguna akhir (*end-user*) melalui *Application Programming Interface (API)* platform?

### D. TUJUAN PENELITIAN

Berdasarkan latar belakang dan rumusan masalah tersebut, tujuan penelitian ini antara lain:

1. Untuk menganalisis *Privacy Policy* LinkedIn mengenai perlindungan data pribadi yang dikaitkan dengan Pasal 26 Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-



Undang Nomor 11 Tahun 2008 tentang Informasi Dan Transaksi Elektronik.

2. Untuk menganalisis mengenai bagaimana pertanggungjawaban hukum bagi LinkedIn jika terjadi penyalahgunaan data pribadi pengguna akhir (*end-user*) melalui *Application Programming Interface* (API) platform.

## **E. MANFAAT PENELITIAN**

### **a. Manfaat Teoritis**

Diharapkan penelitian ini mampu memberikan sumbangan perenungan untuk pertumbuhan ilmu hukum telematika utamanya mengenai perlindungan data pribadi bagi pengguna akhir/*end-user* dalam pemanfaatan teknologi API pada media sosial seperti LinkedIn.

### **b. Manfaat Praktis**

#### **1. Bagi Pemerintah**

Diharapkan penelitian ini dapat menjadi *insight* untuk pemerintah tentang sejauh apa perlindungan data pribadi yang telah diatur *Privacy Policy* LinkedIn. Sehingga Pemerintah dapat lebih memperhatikan mengenai bagaimana media sosial yang banyak digunakan oleh masyarakat, termasuk LinkedIn, mengatur terkait perlindungan data pribadi penggunanya.

#### **2. Bagi LinkedIn**

Diharapkan penelitian ini dapat menjadi bahan evaluasi bagi LinkedIn guna menyempurnakan *Privacy Policy* platformnya agar lebih mengakomodir mengenai perlindungan data pribadi bagi penggunanya.

#### **3. Bagi pengguna akhir (*end-user*) LinkedIn**

Diharapkan penelitian ini dapat menambah wawasan bagi pengguna LinkedIn mengenai substansi dari *Privacy Policy* LinkedIn utamanya terkait dengan perlindungan data pribadi bagi penggunanya.



## F. METODE PENELITIAN

### 1. Jenis Penelitian : Yuridis Normatif

Jenis penelitian yang dipakai penelitian ini adalah yuridis normatif. Penelitian yuridis normatif merupakan penelitian hukum yang hanya mengkaji bahan pustaka atau data sekunder.<sup>11</sup> Yuridis normatif digunakan untuk memperoleh bahan kajian seperti asas-asas hukum, teori-teori, konsep-konsep, serta peraturan hukum yang relevan dengan topik skripsi. Adapun ruang lingkup penelitian hukum normatif berdasarkan pandangan Soerjono Soekanto melingkupi:

- a. Penelitian terhadap asas-asas hukum,
- b. Penelitian terhadap sistematika hukum,
- c. Penelitian terhadap taraf sinkronisasi hukum secara vertikal dan horizontal,
- d. Perbandingan hukum,
- e. Sejarah hukum.<sup>12</sup>

### 2. Pendekatan Penelitian

Dalam penelitian ini, penulis memakai (dua) jenis pendekatan, yaitu:

#### a. Pendekatan Perundang-undangan (*Statute Approach*)

Pendekatan perundang-undangan dilakukan dengan menelaah semua peraturan perundang-undangan dan regulasi terkait dengan permasalahan hukum yang dipersoalkan,<sup>13</sup> karena berbagai aturan hukum yang relevan dengan fokus penelitian tersebut akan digunakan dalam penelitian ini. Dengan dipakainya pendekatan perundang-undangan, maka pengkajian hukum yang dihasilkan nantinya akan lebih tepat.

Penulis akan mempelajari dan mengkaji peraturan-peraturan yang nantinya akan digunakan untuk menjawab rumusan masalah pada penelitian ini, yaitu bagaimana analisis *Privacy Policy* LinkedIn

<sup>11</sup> Soerjono Soekanto dan Sri Mamudji, **Penelitian Hukum Normatif, Suatu Tinjauan Singkat**, cetakan ke-10, PT Raja Grafindo Persada, Jakarta, 2007, hlm. 13-14.

<sup>12</sup> Ibid, hlm. 14.

<sup>13</sup> Peter Mahmud Marzuki, **Penelitian Hukum (edisi revisi)**, Kencana Prenada Media Group, Jakarta, 2013, hlm. 133.



mengenai perlindungan data pribadi jika dikaitkan dengan Pasal 26 UU 19/2016 serta bagaimana pertanggungjawaban hukum bagi LinkedIn apabila ada kebocoran data pribadi pengguna akhir (*end-user*) oleh pihak lain melalui *Application Programming Interface* (API) platform.

b. Pendekatan Konseptual (*Conceptual Approach*)

Pendekatan konseptual yakni pendekatan yang berangkat dari pendapat dan doktrin yang tumbuh di dalam ilmu hukum, untuk mendapatkan gagasan yang memmanifestasikan definisi, konsep, dan asas hukum yang relevan, sebagai tumpuan dalam menyusun argumentasi hukum ketika menyelesaikan isu hukum yang ditemui.<sup>14</sup> Dengan menggunakan pendekatan ini, penulis akan membangun argumentasi hukum untuk menjawab rumusan masalah yang telah ditentukan dalam penelitian ini, yaitu mengenai yaitu mengenai bagaimana analisis *Privacy Policy* LinkedIn mengenai perlindungan data pribadi jika dikaitkan dengan Pasal 26 UU 19/2016 serta bagaimana pertanggungjawaban hukum bagi LinkedIn apabila ada kebocoran data pribadi pengguna akhir (*end-user*) oleh pihak lain melalui *Application Programming Interface* (API) platform.

### 3. Jenis dan Sumber Bahan Hukum

Selain memerlukan metode pendekatan dalam melakukan penelitian, tentu suatu penelitian hukum yuridis normatif juga membutuhkan bahan hukum yang terkait. Oleh karena itu, penulis menghimpun beberapa jenis dan sumber bahan hukum di dalam penelitian ini, yang diklasifikasikan menjadi 3 (tiga) bagian, yakni:

a. Bahan Hukum Primer

Merupakan bahan hukum utama yang dapat meliputi peraturan perundang-undangan serta dokumen formal yang memuat ketentuan hukum. Adapun bahan hukum primer penelitian ini adalah:

1. Kitab Undang-Undang Hukum Perdata (KUH Perdata);

<sup>14</sup> Ibid, hlm. 135-136.



2. Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi Dan Transaksi Elektronik (UU ITE 19/2016);

3. Peraturan Pemerintah Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE 71/2019);

4. Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik (Permenkominfo 20/2016);

5. Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 5 Tahun 2020 tentang Penyelenggara Sistem Elektronik Lingkup Privat (Permenkominfo 5/2020 tentang PSTE Lingkup Privat);

6. *Privacy Policy* dari LinkedIn.

b. Bahan Hukum Sekunder

Bahan hukum sekunder ialah dokumen atau bahan hukum yang dipergunakan untuk menjelaskan bahan hukum primer; bersumber dari buku, jurnal, artikel, kamus hukum/*legal dictionary*, dan doktrin para ahli hukum.

c. Bahan Hukum Tersier

Bahan hukum tersier adalah bahan hukum yang memberi penjelasan terhadap bahan hukum primer dan bahan hukum sekunder. Yang menjadi bahan hukum tersier pada penelitian ini bersumber dari Kamus Besar Bahasa Indonesia (KBBI), ensiklopedia, serta penjelasan dari laman resmi terkait permasalahan yang dibahas.

#### 4. Teknik Penelusuran Bahan Hukum

Penulis mengumpulkan bahan hukum menggunakan metode studi kepustakaan, yakni inventarisasi bahan-bahan hukum yang relevan pada pokok permasalahan, baik bahan hukum primer, bahan hukum sekunder, ataupun bahan hukum tersier, yang kemudian akan diklasifikasi dan disusun secara terstruktur guna memudahkan penggunaan bahan hukum yang didapat. Untuk penelusuran bahan





hukum sendiri, penulis akan mencari bahan hukum dari Pusat Dokumentasi dan Informasi Hukum Fakultas Hukum Universitas Brawijaya (PDIH FH UB), Perpustakaan Pusat Universitas Brawijaya, dan perpustakaan lain yang sekiranya menyediakan bahan hukum yang sesuai dengan topik yang dikaji oleh penulis. Studi kepustakaan penting sekali untuk dilakukan karena tidak mungkin ada suatu penelitian yang dibuat tanpa membaca terlebih dulu.<sup>15</sup> Penulis juga melakukan penelusuran bahan hukum dari internet untuk mendapatkan *e-book*, *e-journal* nasional maupun internasional, dan artikel yang dapat dipertanggungjawabkan kebenarannya serta memiliki relevansi dengan permasalahan yang diteliti oleh penulis.

## 5. Teknik Analisis Bahan Hukum

Pada penelitian ini, penulis melakukan analisis interpretasi dan analisis gramatikal. Interpretasi yang digunakan adalah interpretasi gramatikal dan interpretasi sistematis. Interpretasi sistematis adalah bahan hukum yang diolah untuk mewujudkan sistematika mengenai bahan hukum tertulis, sedangkan interpretasi gramatikal adalah memberikan penafsiran menurut arti kalimat secara bahasa terhadap ketentuan atau kaidah-kaidah hukum.<sup>16</sup> Penulis akan mengaitkan peraturan perundang-undangan, asas-asas hukum, teori-teori hukum, doktrin, serta penerapan hukum dengan permasalahan yang sedang diteliti. Penulis akan menganalisisnya guna mendapatkan argumentasi akhir berupa jawaban atas permasalahan penelitian.<sup>17</sup>

Pengelolaan dilaksanakan dengan sistem penyortiran bahan hukum, selanjutnya digolongkan berdasarkan kategorisasi bahan hukum dan hasil kategorisasi tersebut disusun secara sistematis dan logis. Hal ini menunjukkan bahwa terdapat keterkaitan antara suatu bahan hukum

<sup>15</sup> Nursapia Harahap, 2014, **Penelitian Kepustakaan** (*online*), Jurnal *Iqra'*, Volume 08, Nomor 01, <http://jurnal.uinsu.ac.id/index.php/iqra/article/download/65/245> (31 Maret 2022)

<sup>16</sup> H. Enju Juanda, 2016, **Konstruksi Hukum dan Metode Interpretasi Hukum** (*online*), <https://jurnal.unigal.ac.id/index.php/galuhjustisi/article/download/322/312> (20 Februari 2022)

<sup>17</sup> I Made Pasek Diantha, **Metodologi Penelitian Hukum Normatif dalam Justifikasi Teori Hukum**. Kencana, Jakarta, 2017, Hlm. 152.





dengan bahan hukum lain demi memperoleh gambaran umum dari hasil penelitian.<sup>18</sup>

Dengan demikian, dalam penelitian ini, bahan hukum diuraikan dan dikaji menggunakan interpretasi sistematis dan interpretasi gramatikal sehingga dapat menjawab permasalahan mengenai bagaimana pertanggungjawaban hukum bagi LinkedIn atas terjadinya penyalahgunaan data pribadi pengguna akhir (*end-user*) melalui API LinkedIn.

## 6. Definisi Konseptual

### 1. LinkedIn

LinkedIn merupakan media sosial yang tergolong jenis *Social Networking* yang dapat digunakan untuk mendapatkan pekerjaan atau magang, menyambungkan dan meningkatkan hubungan profesional, serta memperdalam keahlian yang mampu membantu karir (kepentingan bisnis dan karier professional).

### 2. Pengguna Akhir/*end-user*

Pengguna akhir merupakan suatu pihak yang dirancang untuk memakai *software* (perangkat lunak), produk, atau *hardware* (perangkat keras) setelah sepenuhnya dikembangkan, dipasarkan, dan dipasang.

### 3. Platform

Platform adalah program yang digunakan untuk mengeksekusi suatu rencana kerja. Dalam dunia komputasi dan teknologi, arti dari platform adalah suatu media dimana *software* dapat dijalankan/dioperasikan, aplikasi termasuk di dalamnya.

### 4. *Privacy Policy*

*Privacy Policy* adalah pernyataan ataupun dokumen hukum yang menerangkan sepenggal atau seluruhnya terkait tata cara pihak pembuat kebijakan menghimpun, memakai, menyajikan dan mengolah data pengguna, *client* atau *User*.<sup>19</sup>

<sup>18</sup> Mukti Fajar dan Yulianto Achmad, **Dualisme Penelitian Hukum Normatif dan Empiris**, Pustaka Pelajar, Yogyakarta, 2010, hlm 181.

<sup>19</sup> McCormick, Michelle, 2003, **New Privacy Legislation** (online), <http://www.ica.bc.ca> (24 Agustus 2021)





## BAB II

### TINJAUAN PUSTAKA

#### A. TINJAUAN UMUM TENTANG PERTANGGUNGJAWABAN HUKUM

Menurut KBBI, tanggung jawab yaitu kondisi wajib menanggung segala sesuatunya. Sedangkan pada konteks hukum, KBBI mendefinisikan tanggung jawab sebagai kewajiban menerima pembebanan, sebagai akibat sikap pihak sendiri atau pihak lain.<sup>20</sup> Sugeng Istanto mendefinisikan pertanggungjawaban sebagai keharusan untuk memberikan jawaban yang merupakan perhitungan atas segala hal yang terjadi dan kewajiban untuk memberikan pemulihan atas kerugian yang sepertinya ditimbulkan.<sup>21</sup>

Hans Kelsen berpendapat bahwa konsep tanggung jawab hukum (*liability*) ialah suatu konsep yang berkaitan dengan konsep kewajiban hukum. Secara hukum, seseorang dikatakan bertanggung jawab berkenaan suatu perbuatan apabila ia dapat dikenai suatu sanksi dalam kasus perbuatan yang berlawanan dengan hukum.<sup>22</sup> *Black Law Dictionary* menyatakan bahwa definisi *legal liability* ialah "*a liability which courts recognize and enforce as between parties*".<sup>23</sup>

Terdapat pendapat yang membagi prinsip tanggung jawab hukum menjadi tiga (tiga), yakni *accountability*, *responsibility*, dan *liability*. *Accountability* adalah tanggung jawab hukum terkait keuangan, sebagai contoh seorang akuntan yang memiliki tanggung jawab atas hasil pembukuan. Sedangkan Tanggung jawab *responsibility* ialah tanggung jawab untuk menanggung beban. Tanggung jawab dalam arti *liability* adalah kewajiban menanggung atas kerugian yang diderita.<sup>24</sup>

<sup>20</sup> KBBI, 2016, **Tanggung Jawab** (*online*), <https://kbbi.kemdikbud.go.id/entri/tanggung%20jawab> (30 Agustus 2021)

<sup>21</sup> Sugeng Istanto, **Hukum Internasional**, Cetakan ke-2, Universitas Atma Jaya Yogyakarta, Yogyakarta, 2016, hlm. 77.

<sup>22</sup> Jimly Asshiddiqie dan Ali Safa'at, **Teori Hans Kelsen Tentang Hukum**, Cetakan ke-1, Sekretariat Jenderal & Kepaniteraan Mahkamah Konstitusi RI, Jakarta, 2006, hlm. 61

<sup>23</sup> Soekidjo Notoatmojo, **Etika dan Hukum Kesehatan**, Rineka Cipta, Jakarta, 2010, hlm. 55.

<sup>24</sup> Zainal Asikin dkk, **Pengantar Hukum Perusahaan**, Prenada Media Group, Jakarta, 2016, hlm. 252.



Secara perdata, pertanggungjawaban hukum dapat berdasarkan hubungan kontraktual atau perjanjian (*privacy of contract*) sebagaimana yang diatur pada Pasal 1317 dan Pasal 1338 KUH Perdata yang apabila diingkari akan terjadi wanprestasi, maupun tanggung jawab yang timbul berdasarkan undang-undang. Sedangkan tanggung jawab karena undang-undang terbagi lagi, yaitu murni timbul karena Undang-Undang maupun Perbuatan Melawan Hukum/PMH (*onrechtmatige daad*). Tanggung jawab kontraktual dan tanggung jawab atas PMH ialah terkait ada tidaknya kesepakatan dalam hubungan hukum yang terjadi. Jika hubungan hukum terjadi didasarkan pada kesepakatan, maka tanggung jawab yang mencul adalah tanggung jawab kontrak. Sedangkan jika tidak ada kesepakatan namun ada pihak yang merugikan pihak lainnya, maka tanggung jawab yang timbul adalah perbuatan melawan hukum.<sup>25</sup>

Prof. R. Subekti berpandangan bahwa wanprestasi merupakan keadaan dimana suati pihak mempunyai kewajiban untuk melaksanakan prestasi tetapi:

- a. Tidak berprestasi;
- b. Berprestasi, namun tidak tepat seperti yang disepakati;
- c. Terlambat berprestasi;
- d. Melakukan suatu hal yang dilarang oleh perjanjian.<sup>26</sup>

Pengaturan Perbuatan Melawan Hukum (*onrechtmatige daad*) terdapat pada Pasal 1365 sampai dengan Pasal 1380 KUH Perdata. Adanya hubungan hukum, kewajiban, dan hak para pihak menjadi salah satu syarat timbulnya tanggung jawab hukum secara perdata yang didasarkan PMH. Pasal 1365 KUH Perdata: "*Tiap perbuatan yang melanggar hukum dan membawa kerugian kepada orang lain, mewajibkan orang yang menimbulkan kerugian itu karena kesalahannya untuk menggantikan kerugian tersebut*".<sup>27</sup> Jika mengacu ke pasal tersebut, suatu perbuatan dapat

<sup>25</sup> Ari Purwadi dkk, ***From Liability Based on Fault Principle towards Presumption of Liability Principle in Medical Disputes***, Journal of Advanced Research in Law and Economics (JARLE), Volume X, Issue 5(43), Fall 2019, hlm. 1518.

<sup>26</sup> R. Subekti, **Hukum Perjanjian**, Alumni, Bandung, 1979, hlm. 50

<sup>27</sup> **Pasal 1365 Kitab Undang-Undang Hukum Perdata**





dikatakan merupakan perbuatan melawan hukum serta dapat dimintakan pertanggungjawaban jika sudah memenuhi unsur-unsur:<sup>28</sup>

a. Perbuatan dilakukan dengan kesalahan

Unsur perbuatan dapat dibedakan menjadi 2 (dua), yakni perbuatan yang dilakukan dengan kesengajaan dan perbuatan yang merupakan kelalaian. Dalam hukum perdata, seseorang dapat disebut bersalah atau tidak apabila ia telah melakukan atau tidak melakukan suatu perbuatan yang seharusnya dihindari. Perbuatan yang seharusnya dilakukan atau tidak dilakukan tersebut tidak terlepas dari apakah suatu perbuatan tersebut dapat dikira-kira. Dapat dikira-kira itu harus diukur secara objektif, artinya manusia normal dapat mengira-ngirakan dalam keadaan tertentu apakah perbuatan tersebut seharusnya dilakukan atau tidak dilakukan.<sup>29</sup>

b. Melawan Hukum

Setelah putusan *Lindenbaum vs. Cohen* dan mulai berlakunya *arrest Hoge Raad* pada tahun 1919, Belanda telah memperluas pemahaman terkait perbuatan melawan hukum. Sehingga PMH tidak hanya diartikan sebagai tindakan yang berbenturan dengan peraturan-peraturan tertulis, namun juga tindakan yang bertolak belakang dengan kaidah tidak tertulis, yakni kaidah yang mengatur mengenai kesusilaan, kepatutan, dan kehati-hatian yang sepatutnya dipunyai seseorang di dalam bermasyarakat atau terhadap harta benda warga masyarakat.

c. Adanya Kerugian

Memang Pasal 1365 KUH Perdata tidak mengatur lebih lanjut mengenai ganti kerugian yang menjadi kewajiban bagi pihak yang melakukan PMH. Pasal 1371 ayat (2) KUH Perdata menyebutkan "...*Juga penggantian kerugian ini dinilai menurut kedudukan dan kemampuan kedua belah pihak, dan menurut keadaan*".<sup>30</sup>

<sup>28</sup> Kiki Ristanto, **Tinjauan Yuridis Pertanggungjawaban Marketplace Online Terhadap Pelanggaran Hak Cipta Berdasarkan Undang-Undang Nomor 28 Tahun 2014 tentang Hak Cipta**, Skripsi tidak diterbitkan, Batam, Fakultas Hukum Universitas Internasional Batam, 2017, hlm. 16

<sup>29</sup> Abdulkadir Muhammad, **Hukum Perikatan**, Alumni, Bandung, 2002, hlm. 147.

<sup>30</sup> **Pasal 1371 ayat (2) Kitab Undang-Undang Hukum Perdata**





d. Adanya hubungan kausalitas antara kesalahan dan kerugian

Harus dapat dibuktikan bahwa kesalahan dan kerugian ialah suatu kepaduan yang tidak dapat dipisahkan, yakni kesalahan dari seseorang yang digugat membuat kerugian bagi orang lain. Namun hukum alam menyatakan bahwa terjadinya alam ini ditimbulkan oleh terjadinya beberapa faktor yang terhubung satu sama lain. Jika diperhatikan dari penjabaran tersebut, maka hubungan kausalitas antara kesalahan dan kerugian juga terdiri dari beberapa alasan yang menjadi kejadian, maka dari itu kerugian tidak hanya dikarenakan adanya perbuatan, namun terdiri dari beberapa syarat dari perbuatan. Hal ini selaras dengan pandangan yang diutarakan oleh Von Buri, yaitu :

"Harus dianggap sebagai sebab dari pada suatu perubahan adalah semua syarat-syarat yang harus ada untuk timbulnya akibat. Karena dengan hilangnya salah satu syarat tersebut, akibatnya tidak akan terjadi dan oleh sebab tiap-tiap syarat-syarat tersebut *conditio sine qua non* untuk timbulnya akibat, maka setiap syarat dengan sendirinya dapat dinamakan sebab."<sup>31</sup>

Abdulkadir Muhammad mengkategorikan tanggung jawab dalam PMH ke dalam teori, yaitu:

- a. Tanggung jawab disebabkan perbuatan melanggar hukum dengan kesengajaan;
- b. Tanggung jawab disebabkan perbuatan melanggar hukum yang dilakukan karena kelalaian, didasarkan atas konsep kesalahan (*concept of fault*) yang berhubungan dengan hukum dan moral yang sudah bercampur baur;
- c. Tanggung jawab mutlak disebabkan perbuatan melanggar hukum tanpa memperdebatkan apakah perbuatan tersebut dilakkan dengan sengaja ataupun tidak sengaja (*strict liability*).<sup>32</sup>

Menurut teori tradisional, pertanggungjawaban hukum hanya dibedakan menjadi dua, yakni pertanggungjawaban yang didasarkan adanya kesalahan (*based on fault*) dan pertanggungjawaban mutlak (*absolut*

<sup>31</sup> R. Setiawan, **Pokok-Pokok Hukum Perdata**, Bina Cipta, 2007, hlm. 87

<sup>32</sup> Abdulkadir Muhammad, **Hukum Perusahaan Indonesia**, Citra Aditya Bakti, Bandung, 2010, hlm. 336.



*responsibility/strict liability*).<sup>33</sup> Namun pada perkembangannya, prinsip tanggung jawab hukum dibagi:

1. Prinsip tanggung jawab yang didasarkan adanya unsur kesalahan (*Liability based on fault*)

Prinsip ini di dalam hukum perdata nampak pada Pasal 1365 KUH Perdata, "*Tiap perbuatan yang melanggar hukum dan membawa kerugian kepada orang lain, mewajibkan orang yang menimbulkan kerugian itu karena kesalahannya untuk menggantikan kerugian tersebut.*" Maka dari itu, perwujudan dari prinsip ini harus memperhatikan unsur-unsur yang dapat diketahui pada Pasal 1365 KUH Perdata, yaitu adanya suatu perbuatan, unsur kesalahan, adanya kerugian yang timbul, dan adanya hubungan kausalitas antara unsur kesalahan dan unsur kerugian tersebut (penjabaran mengenai unsur-unsur tersebut telah penulis jabarkan di halaman sebelumnya).

Pada dasarnya, prinsip ini memiliki makna bahwa tiada pertanggungjawaban jika tiada kesalahan yang dilakukan dalam suatu perbuatan. Seseorang baru dianggap bertanggung jawab secara hukum jika telah jelas bahwa kerugian yang timbul disebabkan atas unsur kesalahan yang dilakukannya. Oleh karena itu pemenuhan terhadap unsur pembuktian kesalahan menjadi hal yang krusial di dalam prinsip *liability based on fault*. Kesalahan yang dimaksud merupakan hal yang berbenturan dengan hukum; bukan hanya dengan undang-undang, namun juga kesesuaian dan kepatutan menurut masyarakat.

Pada prinsipnya, beban pembuktian diberikan kepada pihak yang dirugikan/penggugat. Penggugat/pihak yang dirugikan lah yang wajib membuktikan bahwa kerugian yang dialaminya disebabkan oleh kesalahan pihak tergugat. Hal ini sesuai dengan Pasal 1365 KUH Perdata yang menyatakan, "*Setiap orang yang mengaku mempunyai suatu hak, atau menunjuk suatu peristiwa untuk meneguhkan haknya itu atau untuk membantah suatu hak orang lain, wajib membuktikan adanya hak itu atau kejadian yang dikemukakan itu.*"<sup>34</sup>

<sup>33</sup> Jimly Asshiddiqie dan Ali Safa'at, *loc.cit.*

<sup>34</sup> Pasal 1365 **Kitab Undang-Undang Hukum Perdata**





Unsur *negligence* dapat menjadi dasar dari gugatan, apabila memenuhi syarat:

- a. Tindakan tersebut menimbulkan kerugian, tidak mencerminkan sikap kehati-hatian yang normal;
- b. Harus dapat dibuktikan bahwa tergugat lalai dalam kewajiban berhati-hati terhadap penggugat;
- c. Perilaku tersebut merupakan penyebab nyata dari kerugian yang timbul.<sup>35</sup>

## 2. Prinsip praduga untuk selalu bertanggung jawab (*Presumption of liability*)

Prinsip praduga untuk selalu bertanggung jawab (*Presumption of liability*) memandang bahwa jikalau tergugat tiada melakukan kesalahan, maka penggugat tidak mendapat kerugian. Secara *acontrario*, apabila penggugat mengalami kerugian, maka tergugat telah melakukan kesalahan.

*Presumption of liability* merupakan modifikasi dari prinsip tanggung jawab berdasarkan unsur kesalahan dengan beban pembuktian terbalik (*Reversal Burden of Proof* atau *Omkering van het Bewijslast*).<sup>36</sup> Jika pada prinsip *Liability based on fault* beban pembuktian diberikan kepada penggugat (pihak yang dirugikan) yang berkewajiban untuk menunjukkan bahwa kerugian yang dideritanya diakibatkan unsur kesalahan dari tergugat, dan apabila unsur kesalahan tersebut tidak dapat ditunjukkan, maka pihak tergugat tidak dapat dipersalahkan; maka pada prinsip ini menyatakan sebaliknya. *Presumption of liability* dibebankan kepada tergugat. Tergugat selalu dianggap bersalah atas kerugian yang dialami penggugat, sampai tergugat dapat membuktikan jika kerugian tersebut bukan disebabkan oleh tindakannya.

## 3. Prinsip pertanggungjawaban pengganti (*Vicarious liability*)

Pada dasarnya, seseorang bertanggung jawab atas kesalahan yang dilakukannya sendiri dan tidak bertanggung jawab atas kesalahan

<sup>35</sup> Ahmadi Miru, **Hukum Perlindungan Konsumen**, Jakarta: RajaGrafindo Persada, 2004, hlm. 148.

<sup>36</sup> Soemardjono B. Soedjono, **Hukum Perlindungan Konsumen dalam Transaksi Konsumen di Dunia Maya Tentang Tanggungjawab Produk**, Ragam Penelitian Mesin, Volume 3, Nomor 2, Universitas Surakarta, Surakarta, 2014, hlm. 7.





yang dibuat oleh orang lain. Namun dalam beberapa kasus, berlaku prinsip pertanggungjawaban pengganti (*Vicarious liability*). *Vicarious liability* adalah sistem tanggung di mana suatu entitas dibuat bertanggung jawab secara mutlak atas kesalahan yang dilakukan entitas lain, meskipun sebenarnya dirinya sendiri tidak bersalah.<sup>37</sup> Sedangkan menurut Barda Nawawi Arief merupakan suatu prinsip dimana seseorang dibebankan pertanggungjawaban atas kesalahan yang telah dibuat oleh orang lain, sebagai contoh ketika kesalahan tersebut dilakukan ketika masih berada di dalam area pekerjaannya.<sup>38</sup> Prinsip ini dapat dilihat pada Pasal 1367 ayat (1) KUH Perdata yang menyatakan:

“Seseorang tidak hanya bertanggung jawab, atas kerugian yang disebabkan perbuatannya sendiri, melainkan juga atas kerugian yang disebabkan perbuatan-perbuatan orang-orang yang menjadi tanggungannya atau disebabkan barang-barang yang berada di bawah pengawasannya.”

Kemudian pada ayat-ayat selanjutnya di pasal yang sama menyatakan bahwa *vicarious liability* dapat muncul dari hubungan:

- a) Orangtua dan/atau wali yang bertanggung jawab atas kerugian yang ditimbulkan oleh anak-anak yang belum dewasa;
- b) Majikan yang bertanggung jawab atas kerugian yang disebabkan oleh bawahan dalam melaksanakan pekerjaan yang ditugaskan;
- c) Guru sekolah yang bertanggung jawab atas kerugian yang ditimbulkan oleh muridnya selama berada di bawah pengawasannya;
- d) Kepala tukang yang bertanggung jawab atas kerugian yang ditimbulkan oleh tukang-tukangnya selama berada di bawah pengawasannya.<sup>39</sup>

Pengaturan mengenai prinsip *vicarious liability* yang diatur pada ketentuan di dalam Pasal 1367 KUH Perdata dapat dikategorikan:

- a) Teori tanggung jawab atasan;

<sup>37</sup> Morgan, Philip, *Recasting Vicarious Liability*, The Cambridge Law Journal, Volume 71, Nomor 3, Faculty of Law, University of Cambridge, November 2012, hlm. 617.

<sup>38</sup> Galuh Dwi Purnama Putra, **Bentuk Pertanggungjawaban Hukum Orangtua Terhadap Pelaku Anak Dalam Kasus Kecelakaan Lalu Lintas**, Tesis tidak dipublikasikan, Surabaya, Fakultas Hukum Universitas Airlangga, 2015, hlm. 16.

<sup>39</sup> **Pasal 1367 ayat (2) dan (3) Kitab Undang-Undang Hukum Perdata**





- b) Teori tanggung jawab pengganti yang bukan dari atasan atas orang-orang dalam tanggungannya; dan
- c) Teori tanggung jawab pengganti yang disebabkan barang-barang yang berada di bawah tanggungannya.<sup>40</sup>

*Vicarious liability* tidak hanya berlaku pada hubungan majikan dan pelayannya, tetapi juga berlaku dalam konteks *principal* dan *agent*, juga antara mitra (*partners*). Dan seiring berjalannya waktu, kategori dari *vicarious liability* juga terus meningkat.<sup>41</sup> Akan tetapi, walaupun pihakB(majikan, mitra, atau *principal*) juga bertanggung jawab atas kesalahan pihakA(pihak yang melakukan kesalahan), namun pihakA tetap wajib bertanggung jawab atas kesalahan yang dilakukan. *Vicarious liability* yang biasanya diterapkan pada kasus-kasus hukum berkaitan dengan pembagian kerugian dan tanggung jawab perusahaan/*enterprise liability*.<sup>42</sup>

#### 4. Prinsip Praduga untuk Tidak Selalu Bertanggung Jawab (*presumption non liability*)

Prinsip ini hanya dapat diterapkan dalam *scope* yang amat tertentu, misalnya saja di dalam hukum pengangkutan. Contoh sederhananya adalah pihak pengangkut tidak bertanggung jawab atas kerusakan ataupun ketiadaan pada barang penumpang yang diletakkan di bagasi kabin yang mana barang tersebut pada umumnya dibawa dan diawasi oleh penumpang sendiri. Namun prinsip ini juga tidak dapat diterapkan secara mutlak, karena ketika kesalahan pihak pengangkut dapat dibuktikan atas rusak/hilangnya barang tersebut, maka pihak pengangkut harus memberikan uang ganti rugi.

#### 5. Prinsip *Strict Liability* (tanggung jawab mutlak)

*Strict liability* adalah salah satu jenis pertanggungjawaban hukum yang tidak mensyaratkan unsur kesalahan sebagai dasar untuk membebankan tanggung jawab kepada seseorang (*liability without fault*) atas tindakannya yang menyebabkan kerugian untuk penggugat.

<sup>40</sup> Krisnadi Nasution, **Penerapan Prinsip Tanggung Jawab Pengangkut Terhadap Penumpang Bus Umum**, *Mimbar Hukum*, Volume 26, Nomor 1, Fakultas Hukum Universitas Gadjah Mada, Yogyakarta, 2014, hlm. 59.

<sup>41</sup> Morgan, Philip, loc. cit.

<sup>42</sup> Ibid, hlm. 618.



Sehingga menurut prinsip ini, penggugat tidak perlu membuktikan bahwa kerugian yang dialaminya didasarkan atas unsur kesalahan dari pihak tergugat.

Menurut Black's Law Dictionary, tanggung jawab mutlak memiliki makna:

*"Liability that does not depend on actual negligence or intent to harm, but that is based on the breach of an absolute duty to make something safe. Strict liability most often applies either to ultrahazardous activities or in product-liability cases.-Also termed absolute liability; liability without fault."*

Dari pengertian diatas, kita dapatkan penegasan bahwa tanggung jawab mutlak tidak disandarkan pada *actual negligence or intent to harm*, namun lebih didasarkan pada tidak terpenuhinya *absolute duty to make something safe* atau kewajiban mutlak untuk membuat sesuatu menjadi aman.

Di Indonesia prinsip ini pertama kali diakomodir pada hukum lingkungan. Namun akhir-akhir ini, prinsip tanggung jawab mutlak juga mulai dikaitkan pada hukum perlindungan konsumen dan bidang hukum lainnya.

## B. TINJAUAN UMUM TENTANG DATA PRIBADI

Era digital menyebabkan pertumbuhan data pribadi menjadi begitu pesat, yang dibuat, disimpan dan ditransmisikan pada komputer, perangkat *mobile*, *broadband* dan situs internet hingga media.<sup>43</sup>

### 1. Pengertian Data Pribadi

KBBI mendefinisikan "data" ialah keterangan yang benar dan nyata yang dapat dijadikan dasar kajian.<sup>44</sup> Sedangkan "pribadi" bermakna manusia sebagai perseorangan (diri sendiri).<sup>45</sup> Apabila pengertian-pengertian tersebut dirangkai, maka data pribadi merupakan

<sup>43</sup> Shilling, Cameron G., **Privacy and Data Security : New Challenges of the Digital Age**, New Hampshire Bar Journal, Concord, 2011, hlm. 1

<sup>44</sup> KBBI, 2016, **Data** (online), <https://kbbi.kemdikbud.go.id/entri/data> (30 Agustus 2021)

<sup>45</sup> KBBI, 2016, **Pribadi** (online), <https://kbbi.kemdikbud.go.id/entri/pribadi> (30 Agustus 2021)



keterangan yang nyata dan benar dan dipunyai oleh manusia sebagai diri sendiri.

Pasal 1 ayat 1 *Data Protection Act* 1998 menyatakan:

"data" means information which –

- (a) "is being processed by means of equipment operating automatically in response to instructions given for that purpose,"
- (b) "is recorded with the intention that it should be processed by means of such equipment,
- (c) "is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system, or"
- (d) "does not fall within paragraph (a), (b) or (c) but forms part of an accessible record as defined by section 68;"<sup>46</sup>

Pasal 68 ayat (1):

(1) "In this Act "accessible record" means—"

- (a) "a health record as defined by subsection (2),
- (b) "an educational record as defined by Schedule 11, or"
- (c) "an accessible public record as defined by Schedule 12."<sup>47</sup>

Maka, menurut *Data Protection Act 1998*, data merupakan informasi yang diproses dengan peralatan yang beroperasi otomatis meladeni instruksi yang ditugaskan dengan maksud agar dapat diproses serta dengan maksud untuk menjadi bagian dari sistem pengarsipan yang relevan. Data juga termasuk informasi yang merupakan bagian dari catatan yang dapat diakses seperti catatan kesehatan, pendidikan, dan catatan publik lain yang disimpan untuk menjadi bagian dari sistem pengarsipan yang relevan.

Sedangkan definisi data pribadi berdasarkan *Data Protection Act 1998* yakni:

" "Personal data" means data which relate to a living individual who can be identified—"

- (a) "from those data, or"
- (b) "from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, "

"and includes any expression of opinion about the individual and any indication of the intention of the data controller or any other person in respect of the individual;"<sup>48</sup>

<sup>46</sup> Pasal 1 ayat (1) ***Data Protection Act 1998***

<sup>47</sup> Pasal 68 ayat (1) ***Data Protection Act 1998***



Menurut *Data Protection Act 1998*, data pribadi merupakan data yang berkenaan dengan suatu individu yang dapat diidentifikasi dari data tersebut atau dari data dan informasi lain yang dimiliki atau yang akan dimiliki oleh *data controller*.

Namun definisi 'data' tidak dimunculkan di GDPR ataupun *Data Protection Act 2018*, yang memberi arti bahwa informasi dalam bentuk apapun berpotensi menjadi data pribadi. Meski begitu, Pasal 2 ayat (1) telah membatasi cakupan materi GDPR. Pasal tersebut menyebutkan bahwa GDPR berlaku untuk pemrosesan data pribadi, yang dilakukan dengan cara otomatis baik secara keseluruhan atau sebagian. Selain itu GDPR juga berlaku untuk pemrosesan data pribadi selain dengan cara otomatis yang merupakan bagian dari sistem pengarsipan atau dimaksudkan untuk menjadi bagian dari sistem pengarsipan.<sup>49</sup>

Definisi data pribadi juga mengalami perubahan yang di atur pada GDPR (General Data Protection Regulation 2016/679). Makna data pribadi menurut GDPR adalah informasi apapun yang berkaitan dengan subjek data (*natural person*) yang teridentifikasi ataupun yang dapat diidentifikasi. Sedangkan subjek data (*natural person*) dapat diidentifikasi secara langsung atau tidak langsung, dengan mengacu kepada *identifier* seperti nama, nomor identifikasi, data lokasi, *online identifier*, ataupun satu atau lebih faktor-faktor khusus yang dapat mengidentifikasi seseorang, seperti fisik, fisiologis, identitas genetik, mental, ekonomi, sosial, atau budayanya.

Masuk kepada regulasi di Indonesia mengenai data pribadi, UU ITE tidak memberikan definisi hukum dari data pribadi secara eksplisit. Namun jika kita melihat pada Penjelasan Pasal 26 ayat (1), maka data pribadi meliputi urusan kehidupan pribadi termasuk (riwayat) komunikasi seseorang dan data tentang seseorang.<sup>50</sup>

<sup>48</sup> Pasal 1 ayat (1) *Data Protection Act 1998*

<sup>49</sup> Wong, Benjamin, *Delimiting the concept of personal data after the GDPR*, Legal Studies, Volume 39, Issue 3, Cambridge University Press, September 2019, Hlm. 519.

<sup>50</sup> Daniar Supriyadi, 2017, **Data Pribadi dan Dua Dasar Legalitas Pemanfaatannya** (*online*), <https://www.hukumonline.com/berita/a/data-pribadi-dan-dua-dasar-legalitas-pemanfaatannya-lt59cb4b3feba88/> (27 Januari 2022)





Definisi data pribadi baru muncul di PP PSTE yakni pada Pasal 1 angka 29 yang menyatakan:

"Data Pribadi adalah setiap data tentang seseorang baik yang teridentifikasi dan/atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui Sistem Elektronik dan/atau nonelektronik."<sup>51</sup>

RUU PDP (Rancangan Undang-Undang Perlindungan Data Pribadi) mengklasifikasikan data pribadi menjadi 2 (dua) jenis, yakni data pribadi yang bersifat umum serta spesifik. Yang termasuk data pribadi umum adalah: nama lengkap, jenis kelamin, kewarganegaraan, agama, dan/atau data pribadi yang diintegrasikan untuk mengidentifikasi seseorang.

Sedangkan data pribadi spesifik meliputi:<sup>52</sup>

- 1) informasi dan data kesehatan;
- 2) data biometrik;
- 3) data genetika;
- 4) kehidupan/orientasi seksual;
- 5) pandangan politik;
- 6) catatan kejahatan;
- 7) data anak;
- 8) data keuangan pribadi; dan/atau
- 9) data lainnya sesuai dengan ketentuan perundang-undangan.<sup>53</sup>

Secara garis besar, data pribadi berisi fakta-fakta yang terkait dengan individu/seseorang di mana fakta tersebut akan membedakan karakteristik dirinya dengan individu yang lain, yang menyebabkan orang yang bersangkutan tersebut ingin menyimpan guna mengamankannya untuk dirinya sendiri dan/atau membatasi orang lain untuk membagikan kepada pihak lain ataupun menyalahgunakannya.<sup>54</sup>

<sup>51</sup> Pasal 1 angka 29 **Peraturan Pemerintah Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik**

<sup>52</sup> Pasal 3 ayat (1-3) Rancangan Undang-Undang Perlindungan Data Pribadi

<sup>53</sup> Pasal 3 ayat (1) sampai ayat (3) **Rancangan Undang-Undang Perlindungan Data Pribadi**

<sup>54</sup> Jerry, Kang, *Information Privacy in Cyberspace Transaction*, Stanford Law Review, Volume 50, Issue 4, Stanford Law School, Stanford, hlm. 5



## 2. Dasar Hukum Perlindungan Data Pribadi di Indonesia

Perlindungan hukum dapat dibagi menjadi 2 (dua) bentuk, yakni perlindungan hukum preventif serta represif. Perlindungan hukum preventif merupakan perlindungan hukum yang bersifat pencegahan sebelum terjadinya suatu kegiatan yang negatif atau kejahatan, sehingga tindakan nyata tersebut dapat dihindari. Sedang perlindungan hukum represif ialah bentuk perlindungan hukum yang dibuat dengan tujuan untuk menyelesaikan suatu sengketa atau perkara hukum. Perlindungan hukum ini dimanifestasikan dengan memberikan beban kewajiban bagi para pihak terkait dan diikuti dengan sanksi.<sup>55</sup>

Perlindungan data pribadi merupakan perlindungan yang secara khusus berkaitan dengan bagaimana undang-undang melindungi data pribadi yang akan dihimpun, didaftarkan, disimpan dan dicadangkan, didayagunakan, dan didistribusikan.<sup>56</sup> Pasal 28G UUD NRI telah menyatakan:

“Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang dibawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi.”<sup>57</sup>

Walaupun UUD NRI 1945 tidak mencantumkan mengenai perlindungan data pribadi secara eksplisit, namun semangat dan intisari dari pasal tersebut telah digunakan oleh para pembuat regulasi sebagai fondasi di dalam penyusunan peraturan turunan mengenai perlindungan data pribadi yang lebih khusus.

Perlindungan hukum dalam konteks data pribadi sejatinya dapat ditemukan pada UU 11/2008 tentang ITE yang kemudian disempurnakan dengan perubahannya, yakni UU 19/2016.

<sup>55</sup> Made Metu Dahana, **Perlindungan Hukum dan Keamanan Terhadap Wisatawan**, Paramita, Surabaya, 2021, hlm. 58

<sup>56</sup> Shinta Dewi, **CyberLaw : Aspek Data Privasi Menurut Hukum Internasional, Regional dan Nasional**, Refika Aditama, Bandung, 2015, hlm.1

<sup>57</sup> Pasal 28 G **Undang-Undang Dasar Negara Republik Indonesia 1945**



Pasal 26 ayat (1) UU ITE:

"Kecuali ditentukan lain oleh peraturan perundang-undangan, penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan orang yang bersangkutan."<sup>58</sup>

Bapak Johnny G. Plate selaku Menteri Komunikasi dan Informatika (Menkominfo) mengutarakan bahwa saat ini pengaturan mengenai data pribadi tersebar pada 32 undang-undang yang sektoral. Misalnya data-data pribadi nasabah atau seseorang yang berkaitan dengan keuangan ada di UU Perbankan dan UU OJK. Sedangkan terkait data-data pribadi pasien atau yang berkaitan dengan kesehatan diatur di dalam UU Kesehatan.<sup>59</sup> Di Indonesia, belum ada undang-undang yang secara tersendiri mengatur mengenai data pribadi. RUU PDP juga masih dalam proses penyusunan dan belum juga disahkan hingga saat ini.

Namun terdapat pasal-pasal di ketentuan-ketentuan turunan UU ITE yang mengatur mengenai data pribadi secara umum, seperti Peraturan Pemerintah Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik (selanjutnya di dalam skripsi ini akan disebut PP 71/2019 tentang PSTE), Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik (selanjutnya pada skripsi ini akan disebut Permenkominfo 20/2016 tentang Perlindungan Data Pribadi dalam SE), dan Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 5 Tahun 2020 tentang Penyelenggara Sistem Elektronik Lingkup Privat (selanjutnya pada skripsi ini akan disebut Permenkominfo 5/2020 tentang PSE Privat).

<sup>58</sup> Pasal 26 ayat (1) **Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi Dan Transaksi Elektronik**

<sup>59</sup> Kominfo, 2020, **Lindungi Data Pribadi, Ada Empat Unsur Penting Pengaturan RUU PDP**, (*online*), <https://www.kominfo.go.id/content/detail/27503/lindungi-data-pribadi-ada-empat-unsur-penting-pengaturan-ruu-pdp/0/artikel>, (03 April 2022)





## C. TINJAUAN UMUM TENTANG APPLICATION PROGRAMMING INTERFACE (API)

### 1. Definisi *Application Programming Interface* (API)

*Application Programming Interface* (API) adalah himpunan berbagai, fungsi, perintah, dan protokol agar suatu program dapat terkonsolidasi dengan bagian dari program lain secara bersamaan. Selain itu, API juga dipakai oleh programmer untuk membentuk suatu sistem operasi untuk perangkat lunak tertentu. API diperlukan untuk mengakses sumber daya/*resource* dari program tersebut. API akan membentuk suatu sistem antar muka/*interface* yang akan dipakai oleh aplikasi untuk berbagi informasi dan data dengan aplikasi lain. API dapat dimanfaatkan oleh dua perangkat lunak dengan berbagai bahasa *programming* yang berbeda.

Dengan menggunakan API, maka layanan dari suatu program dapat diakses oleh beragam pihak, mulai dari pengembang, pelanggan, kolaborator, pihak yang berafiliasi dengan program tersebut, *mobile users*, serta *internal project*.<sup>60</sup> Disamping hal tersebut, pemanfaatan API dapat mempersingkat proses pengembangan program dengan menyediakan *function* secara terpisah, sehingga *developer* tidak perlu membuat fitur yang sejenis.

API banyak dimanfaatkan pada kegiatan bisnis karena memiliki keuntungan yaitu:

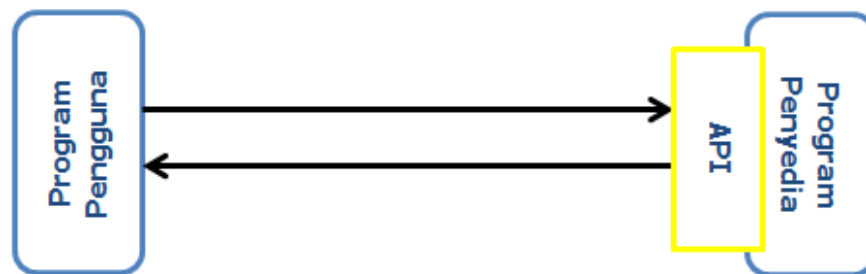
- a) Portabilitas. *Programmer* yang memanfaatkan API dapat membuat dan mengoperasikan programnya dalam sistem operasi apa saja asalkan sudah terinstall API tersebut.
- b) Lebih dapat dipahami. API menggunakan bahasa yang lebih sistematis dan lebih dapat dipahami dari bahasa *system call*. Hal ini cukup penting dalam pembuatan dan pengembangan program.

<sup>60</sup> 3 scale, *What is an API? Your guide to the Internet Business (R)evolution*, 3scale Networks S.L., Barcelona, 2011, hlm. 8



## 2. Skema Kerja *Application Programming Interface* (API)

Gambar 2.1. Skema Konektivitas API



Sumber: 3Scale, *What is an API? Your guide to the Internet Business* (R)evolution, 2011

Untuk mempermudah memahami bagaimana skema kerja API, maka penulis akan menjelaskannya menggunakan contoh. Misalnya saja, Program A (program pengguna) ingin mengakses sebagian infrastruktur pemrograman dari Program B (Program Penyedia). Apabila Program A mengakses ke dalam sistem operasi dari Program B secara langsung, tentu tidak akan menguntungkan bagi Program B karena seluruh sistem operasinya akan diketahui oleh Program A; padahal Program A hanya membutuhkan sebagian infrastruktur pemrograman dari Program B saja. Selain itu, ternyata bahasa pemrograman yang digunakan oleh Program A dan B berbeda.

Disinilah kehadiran API menjadi berguna. Program Penyedia akan menempatkan bahan sistem operasi yang diperlukan oleh Program Pengguna pada API. Nantinya API akan mengonversikan bahasa pemrograman bahan tersebut agar cocok dan dapat dimanfaatkan oleh program pengguna yang memakai bahasa pemrograman yang berbeda.

## 3. Kategori *Application Programming Interface* (API)

API dapat diklasifikasikan ke sejumlah kategori, yaitu:

### 1. *API Operating System*

Yakni API yang dipakai untuk membuat fungsi dasar yang dilangsungkan oleh komputer. Seperti proses I/O (*Input/Output*) dan eksekusi program. Contohnya adalah API untuk MS Windows.



## 2. *API Programming Languages*

Adalah API yang dimanfaatkan untuk meningkatkan kapabilitas dalam melakukan eksekusi terhadap suatu bahasa pemrograman. Sebagai contoh ialah Java API.

## 3. *API Application Services*

Merupakan API yang dipakai untuk mengakses layanan dan data yang disediakan oleh suatu aplikasi. Contohnya *Business API* (BAPI).

## 4. *Infrastructure Services*

Yakni API yang dimanfaatkan untuk mengakses infrastruktur seperti komputer beserta perangkat tambahannya seperti penyimpanan, aplikasi, dan lain-lain. Contohnya ialah Amazon EC2 (*Elastic Compute Cloud*) untuk *virtual computing* dan Amazon S3 (*Simple Storage Service*) untuk menyimpan data dalam jumlah besar.

## 5. *Web Services*

Merupakan API yang dipakai untuk mengakses konten dan layanan yang disediakan oleh suatu aplikasi yang berbentuk web. Contohnya Twitter API yang dimanfaatkan oleh program lain untuk mengakses informasi dari twitter yang dapat dibagikan seperti akun pengguna.

## 4. LinkedIn API

Jika kita mengakses web resmi dari LinkedIn *Developers*, maka kita dapat menemukan produk API yang ditawarkan, yakni *Consumer Solutions Platform APIs*. Pemanfaatan LinkedIn API ini memungkinkan aplikasi lain untuk mengembangkan pengalaman *Sign In* dan berbagi lewat akun LinkedIn, yang menjadi *professional network* terbesar di dunia.<sup>61</sup>

LinkedIn API memakai OAuth 2.0<sup>62</sup> untuk otorisasi pengguna dan autentikasi API. Aplikasi harus terlebih dahulu diotorisasi dan diautentikasi

<sup>61</sup> LinkedIn, 2021, *LinkedIn Consumer Solutions Platform* (online), <https://docs.microsoft.com/en-us/linkedin/consumer/> (02 September 2021)

<sup>62</sup> OAuth 2.0 adalah protokol standar industri untuk otorisasi. OAuth 2.0 berfokus pada kesederhanaan pengembang klien sambil memberikan alur otorisasi khusus untuk aplikasi web, aplikasi desktop, ponsel, dan *living room devices*. Spesifikasi ini dan ekstensinya dikembangkan oleh IETF OAuth *Working Group*.





sebelum dapat memanfaatkan data LinkedIn atau mendapatkan akses ke data pengguna LinkedIn. Ada 2 (dua) jenis izin yang dapat diperoleh Aplikasi pihak ketiga yang akan mengakses *resources* dari LinkedIn, yaitu:<sup>63</sup>

a. Otorisasi Pengguna atau *Authorization Code Flow*

Merupakan jenis izin yang paling umum digunakan di LinkedIn API. Jenis ini digunakan jika suatu aplikasi ingin meminta akses ke akun pengguna LinkedIn untuk menggunakan data mereka. Otorisasi ini memerlukan persetujuan pengguna agar aplikasi dapat mengaksesnya.

b. Otorisasi Aplikasi atau *Client Credential Flow*

Yakni jenis izin yang dipakai jika terdapat aplikasi yang ingin mengakses *resources* LinkedIn yang tidak berkaitan dengan akun anggota secara spesifik. Misalnya saja untuk mendapatkan data agregat untuk keperluan riset.

LinkedIn memakai REST API v2 yang berisi sejumlah konsep yang membantu menerapkan prinsip RESTful standar dalam skala besar, memodelkan data secara konsisten, dan pada akhirnya memberikan pengalaman pengembang menyeluruh yang terstruktur dengan baik.<sup>64</sup> REST API atau RESTful API adalah jenis API yang akan mentransfer informasi yang diminta dari status *resources* kepada pemohon atau *endpoint*. Informasi tersebut akan diberikan dalam salah satu dari beberapa format, yakni JSON (*Javascript Object Notation*), HTML, XLT, Python, PHP, atau teks biasa.<sup>65</sup> Dalam LinkedIn API, format yang digunakan adalah format JSON.

<sup>63</sup> LinkedIn, 2021, *Authenticating with OAuth 2.0 Overview* (online), <https://docs.microsoft.com/en-us/linkedin/shared/authentication/authentication?context=linkedin/consumer/context> (02 September 2021)

<sup>64</sup> LinkedIn, 2021, *API Concepts* (online), <https://docs.microsoft.com/en-us/linkedin/shared/api-guide/concepts?context=linkedin/consumer/context> (02 September 2021)

<sup>65</sup> Red Hat, Inc., 2020, *What is a REST API?*, <https://www.redhat.com/en/topics/api/what-is-a-rest-api> (02 September 2021)





### BAB III

## PEMBAHASAN

### A. Analisis *Privacy Policy* LinkedIn mengenai perlindungan data pribadi dikaitkan Pasal 26 Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi Dan Transaksi Elektronik

#### 1. Analisis *Privacy Policy* (Kebijakan Privasi) LinkedIn Terkait Data Pribadi Pengguna

Pada bagian *Introduction*, dinyatakan bahwa *Privacy Policy* ini berlaku untuk setiap Anggota maupun Pengunjung yang menggunakan layanan dari LinkedIn. Makna "Anggota" yang dimaksud dalam *policy* tersebut adalah pengguna layanan LinkedIn yang terdaftar. Sedangkan makna "Pengunjung" yang dimaksud dalam *policy* tersebut adalah pengguna layanan LinkedIn yang tidak terdaftar. LinkedIn juga menyatakan bahwa *Privacy Policy* LinkedIn ini tidak hanya berlaku untuk LinkedIn.com, tetapi juga untuk LinkedIn-branded apps, LinkedIn *Learning*, serta situs, aplikasi, komunikasi, dan layanan lain yang terkait LinkedIn.

Selanjutnya masih pada bagian *Introduction* pada *Privacy Policy* ini, juga dinyatakan bahwa untuk pengguna yang bertempat tinggal di *Designated Countries*/Negara Tertunjuk<sup>66</sup>, maka yang akan bertindak sebagai pengontrol data pribadinya/*controller*<sup>67</sup> adalah LinkedIn Ireland Unlimited Company ("LinkedIn Ireland"). Sedangkan untuk pengguna yang berdomisili di luar Negara Tertunjuk, maka LinkedIn Corporation

<sup>66</sup> LinkedIn telah memberikan definisi *Designated Countries* atau Negara Tertunjuk adalah istilah yang digunakan LinkedIn di dalam *Privacy Policy* untuk menyebut Negara-negara di Uni Eropa, *European Economic Area* (EEA), dan Swiss.

<sup>67</sup> *Article 4 GDPR* : *Controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law* (terjemahan bebas : Pengontrol adalah orang perseorangan atau badan hukum, otoritas publik, agensi atau badan lain yang secara sendiri atau bersama-sama dengan orang lain, menentukan tujuan dan sarana pemrosesan data pribadi; di mana tujuan dan cara pemrosesan tersebut ditentukan oleh undang-undang Union atau Negara Anggota, pengontrol atau kriteria khusus untuk pencalonannya dapat diatur oleh undang-undang Union atau Negara Anggota;



yang akan bertindak sebagai pengontrol/*controller* data pribadi pengguna tersebut. Karena Indonesia bukan termasuk Negara Tertunjuk, maka data pribadi pengguna yang berasal dari Indonesia dikendalikan oleh LinkedIn Corporation, seperti bagaimana data pribadi pengguna diberikan, dihimpun, atau diolah terkait dengan Layanan LinkedIn.

Kemudian masih pada bagian *Introduction* pada *Privacy Policy* ini, terdapat klausul mengenai perubahan, yang menyatakan:

*"LinkedIn can modify this Privacy Policy, and if we make material changes to it, we will provide notice through our Services, or by other means, to provide you the opportunity to review the changes before they become effective. If you object to any changes, you may close your account."*

*"You acknowledge that your continued use of our Services after we publish or send notice about our changes to this Privacy Policy means that the collection, use and sharing of your personal data is subject to the updated Privacy Policy, as of its effective date."<sup>68</sup>*

Pada klausul di atas, terdapat penegasan ulang bahwa pengumpulan, penggunaan, serta pembagian data pribadi pengguna LinkedIn didasarkan pada *Privacy Policy* yang berlaku dan dokumen lain yang dirujuk beserta segala pembaruannya. Sehingga, LinkedIn menyatakan bahwa pihaknya dapat mengubah *Privacy Policy* tersebut sewaktu-waktu. Apabila terdapat perubahan isi dari *Privacy Policy* tersebut, maka LinkedIn memberitahukannya kepada pengguna untuk memberikan *review* atas perubahan tersebut sebelum berlaku efektif, baik melalui akun LinkedIn pengguna maupun melalui cara lain. Jika pengguna menolak perubahan tersebut, maka pengguna dapat segera menutup akunnya. Jika pengguna melanjutkan penggunaan Layanan LinkedIn setelah pihak LinkedIn memublikasikan *Privacy Policy* dengan substansi yang telah berubah, maka *Privacy Policy* terbaru berlaku bagi pengaturan data pribadi pengguna LinkedIn dan pengguna dianggap menyetujui perubahan tersebut.

<sup>68</sup> LinkedIn, *Privacy Policy* (online), Effective August 11, 2020, <https://www.linkedin.com/legal/privacy-policy> (1 Februari 2022)





Pada bagian 1. *Data We Collect* angka 1.1 mengenai *Data You Provide To Us*, LinkedIn menyatakan bahwa nama, alamat email dan/atau nomor telepon serta kata sandi harus diberikan untuk mendaftar dan membuat akun. Untuk registrasi layanan premium, maka informasi pembayaran dan penagihan (*payment and billing information*) harus diberikan oleh pengguna kepada LinkedIn. Informasi pembayaran dan penagihan merupakan informasi yang dijaga atau dihimpun dengan baik, yang mana informasi tersebut dapat merekognisi konsumen serta kewajiban keuangan harus dibayarkannya; contohnya informasi yang berkaitan dengan kartu pembayaran konsumen, kartu tagihan, kartu kredit, kartu debit, tabungan, giro, atau rekening perbankan lainnya, dan informasi transfer dana elektronik.<sup>69</sup>

Selanjutnya pada bagian dan angka yang sama, terdapat klausul yang menyatakan:

*"You have choices about the information on your profile, such as your education, work experience, skills, photo, city or area and endorsements. Some Members may choose to complete a separate ProFinder profile. You don't have to provide additional information on your profile; however, profile information helps you to get more from our Services, including helping recruiters and business opportunities find you. It's your choice whether to include sensitive information on your profile and to make that sensitive information public. Please do not post or add personal data to your profile that you would not want to be publicly available."*<sup>70</sup>

Pengguna diberi keleluasaan untuk menyertakan informasi dan data diri apa saja yang ada di profil akun LinkedIn miliknya; seperti foto profil, kota, riwayat pendidikan, pengalaman kerja, keahlian, dan informasi yang cukup sensitif lainnya. Memang tidak ada kewajiban bagi pengguna untuk mencantumkan informasi-informasi tersebut, akan tetapi LinkedIn juga telah memberikan himbauan bahwa mencantumkan informasi profil yang lebih lengkap memungkinkan pengguna untuk memperoleh manfaat yang lebih banyak dari layanan, seperti lebih mudah ditemukan dan dilirik oleh perekrut kerja/*recruiter* dan peluang

<sup>69</sup> **Code of Federal Regulation, Telemarketing Sales Rule 16 CFR Part 310.2**

<sup>70</sup> LinkedIn, **Privacy Policy** (online), Effective August 11, 2020, <https://www.linkedin.com/legal/privacy-policy> (1 Februari 2022)





bisnis lainnya. Himbauan tersebut masuk akal. Pasti seorang *recruiter* akan lebih tertarik kepada akun dengan informasi pribadi yang lebih lengkap sehingga perekrut kerja dapat mencocokkannya dengan kebutuhan perusahaan.

Kemudian masih di bagian dan angka yang sama, LinkedIn menyatakan:

*"We collect personal data from you when you provide, post or upload it to our Services, such as when you fill out a form, (e.g., with demographic data or salary), respond to a survey, or submit a resume or fill out a job application on our Services. If you opt to import your address book, we receive your contacts (including contact information of your service provider(s) or app automatically added to your address book when you communicate with addresses or numbers not already in your list)."*

*"If you sync your contacts or calendars with our Services, we will collect your address book and calendar meeting information to keep growing your network by suggesting connections for you and others, and by providing information about events, e.g. times, places, attendees and contacts."*

*"You don't have to post or upload personal data; though if you don't, it may limit your ability to grow and engage with your network over our Services."<sup>71</sup>*

Klausula ini menjabarkan terkait bagaimana cara LinkedIn mengumpulkan data pribadi penggunanya, yaitu saat pengguna menyetorkan atau mengunggah data pribadi tersebut ke Layanan LinkedIn, misalnya saat pengguna mengisi formulir atau survei, mengirim resume, atau mengisi formulir lamaran pekerjaan di layanan LinkedIn. Lalu ketika pengguna memilih untuk mengkoneksikan akun LinkedIn dengan kalender atau kontak pada *smartphone*, maka LinkedIn akan menghimpun data-data tersebut untuk memperluas jejaring akun pengguna dan menyediakan informasi mengenai saran koneksi maupun acara.

Sama seperti sebelumnya, pengguna tidak diwajibkan untuk mengunggah hal-hal yang memuat data pribadi tersebut. Akan tetapi LinkedIn juga telah memberikan himbauan jikalau pengguna tidak

<sup>71</sup> Ibid.





menyertakannya, maka kesempatan pengguna untuk melebarkan koneksi dan korelasi jaringan pada Layanan LinkedIn menjadi sempit.

Pada bagian yang sama angka 1.2 mengenai *Data From Others* secara umum LinkedIn menyatakan bahwa LinkedIn bisa saja menerima beberapa data pribadi pengguna dari orang lain, seumpama saja ketika orang lain tersebut sedang melakukan sinkronisasi kontak, kalender, ataupun akun email mereka dengan Layanan LinkedIn. LinkedIn juga akan mendapatkan data pribadi pengguna, sebagai contoh jabatan pekerjaan dan alamat email kerja, ketika pengguna tersebut menggunakan layanan dari pelanggan/*customer* ataupun mitra/*partners* yang tergabung dalam LinkedIn, seperti penyedia kerja dan sistem pelacakan pelamar yang memberikan data lamaran kerja yang telah diisi pengguna.

Kemudian pada bagian yang sama angka 1.5 mengenai *Your Device and Location*, LinkedIn menyatakan:

*"... If you use our Services from a mobile device, that device will send us data about your location based on your phone settings. We will ask you to opt-in before we use GPS or other tools to identify your precise location".<sup>72</sup>*

Berdasarkan kalimat tersebut, maka LinkedIn akan menggunakan data lokasi *real-time* pengguna berdasarkan pengaturan di teleponnya. Namun LinkedIn tidak akan mengambil data pengguna tanpa izin, karena LinkedIn akan terlebih dahulu meminta persetujuan kepada pengguna sebelum menggunakan GPS atau perangkat lain untuk mengidentifikasi lokasi pengguna pada saat menggunakan LinkedIn.

Pada bagian yang sama angka 1.7 mengenai *Workplace and School Provided Information*, terdapat klausul yang menyatakan:

*"When your organization (e.g., employer or school) buys a premium Service for you to use, they give us data about you."*

*"Others buying our Services for your use, such as your employer or your school, provide us with personal data about you and your eligibility to use the Services that they purchase for use by their workers, students or alumni. For example, we will get contact information for "Company Page" administrators and for*

<sup>72</sup> Ibid.



*authorizing users of our premium Services, such as our recruiting, sales or learning products.*<sup>73</sup>

Klausula ini menyatakan bahwa apabila organisasi pengguna (penyedia kerja/employer atau kampus) membeli Layanan Premium untuk pengguna gunakan, maka pihak organisasi tersebut akan memberikan data pribadi pengguna tersebut, seperti mengenai informasi kontak administrator dengan tujuan untuk melakukan otorisasi pengguna Layanan premium, misalnya produk dari perekrutan (*recruiting*), penjualan (*sales*) atau pembelajaran (*learning*). Sebagai contoh, Abekerja sebagai HR (*Human Resource*) di suatu perusahaan, kemudian perusahaan tersebut membeli akun premium untuk digunakan dalam pekerjaannya. Maka perusahaan dapat mendaftarkan akun kerja bagi Adan meng-input data pribadi. Aduna pendaftaran akun tersebut.

Selanjutnya pada bagian 2. *How We Use Your Data*:

*"How we use your personal data will depend on which Services you use, how you use those Services and the choices you make in your settings. We use the data that we have about you to provide and personalize our Services, including with the help of automated systems and inferences we make, so that our Services (including ads) can be more relevant and useful to you and others."*<sup>74</sup>

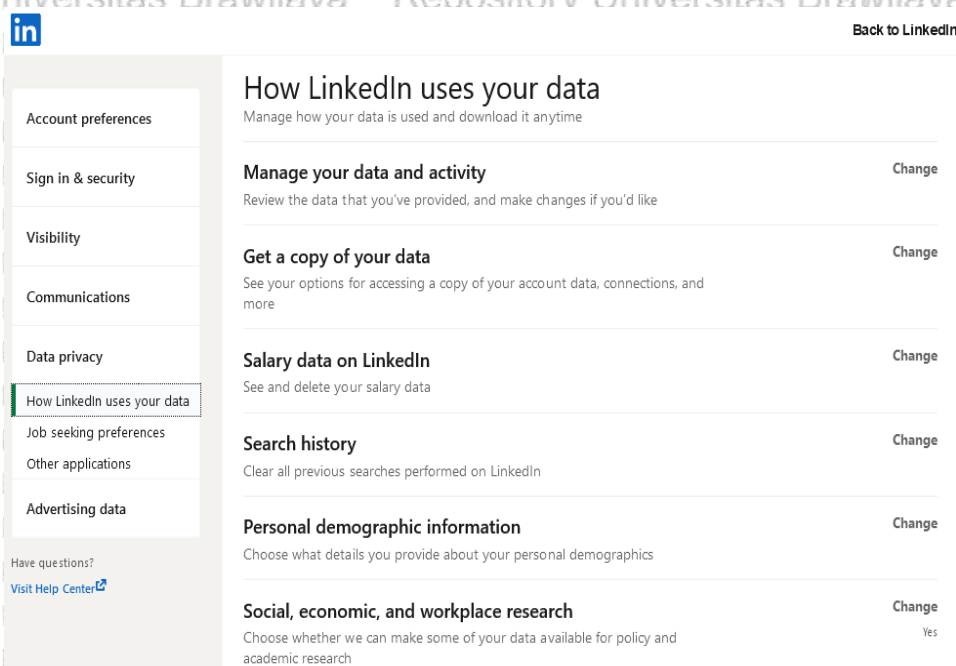
Pada klausula ini, LinkedIn menyatakan bahwa pihaknya akan menggunakan data pribadi pengguna untuk menyediakan, mempersonalisasi, dan mengembangkan layanan. Mengenai bagaimana cara LinkedIn menggunakan data pribadi pengguna tergantung pada jenis layanan yang digunakan dan bagaimana pengguna menggunakan layanan tersebut, serta "pilihan/choices" yang pengguna pilih pada pengaturan akun masing-masing.

<sup>73</sup> Ibid.

<sup>74</sup> Ibid.



### Gambar 3.1 Tampilan Pengaturan pada Akun LinkedIn terkait Bagaimana LinkedIn akan Menggunakan Data Pengguna



Sumber: Data Privacy Settings, LinkedIn.com, 2022

Sebagaimana yang terlihat pada gambar di atas, di opsi pengaturan akun pada bagian data pribadi, pengguna dapat mengelola data serta aktivitas akunnya. Pengguna dapat melihat riwayat aktivitas akun miliknya; misalnya ketika pengguna menambahkan alamat email atau nomor telepon, ketika pengguna membagikan data LinkedIn dengan aplikasi lain, atau ketika LinkedIn telah memperbarui ketentuan layanan mereka. Kemudian pada opsi ini pengguna juga dapat mengunduh serta mengarsipkan data akun LinkedIn miliknya, seperti koneksi, profil, rekomendasi, dan lain sebagainya. LinkedIn juga menyediakan opsi bagi pengguna apabila ingin menghapus semua riwayat pencarian yang pengguna lakukan selama menggunakan layanan.

Selain itu, pada opsi ini terdapat beberapa hal yang dapat pengguna pilih mengenai cara LinkedIn untuk menggunakan data pribadinya. Misalnya mengenai data gaji. Apabila pengguna sebelumnya telah memberikan data gaji kepada LinkedIn, maka pada opsi ini pengguna dapat meminta LinkedIn untuk menghapus data tersebut dari



layanan. Lalu pengguna dapat menambahkan informasi demografi pribadi, seperti jenis kelamin ataupun riwayat disabilitas, yang akan digunakan sebagai *insight* oleh LinkedIn. Pengguna juga dapat mengizinkan LinkedIn untuk membagikan data pengguna kepada pihak ketiga untuk digunakan sebagai riset, baik untuk kepentingan akademis dan kebijakan. Namun hal ini merupakan opsional, tidak ada kewajiban bagi pengguna untuk menambahkan informasi ataupun mengizinkan pihak ketiga untuk menggunakan datanya.

Kemudian pada bagian yang sama angka 2.6 tentang *Developing Services and Research*, terdapat klausul yang menyatakan:

*"We seek to create economic opportunity for Members of the global workforce and to help them be more productive and successful. We use the personal data available to us to research social, economic and workplace trends, such as jobs availability and skills needed for these jobs and policies that help bridge the gap in various industries and geographic areas. In some cases, we work with trusted third parties to perform this research, under controls that are designed to protect your privacy. We publish or allow others to publish economic insights, presented as aggregated data rather than personal data."<sup>75</sup>*

Klausula tersebut menyatakan bahwa LinkedIn akan menggunakan data pribadi pengguna yang ada untuk melakukan riset mengenai tren sosial, ekonomi, dan tempat kerja (*workplace*); seperti misalnya mengenai ketersediaan dan keahlian yang sekiranya dibutuhkan untuk suatu pekerjaan. LinkedIn juga akan bekerja sama dengan pihak ketiga yang terpercaya guna pelaksanaan riset, yang didasarkan pada pengaturan yang dirancang untuk melindungi privasi pengguna.

Pada bagian 3. *How We Share Information* angka 3.4 tentang *Related Services*, LinkedIn menyatakan:

*"We will share your personal data with our affiliates to provide and develop our Services. We may combine information internally across the different Services covered by this Privacy Policy to help our Services be more relevant and useful to you and others. For example, we may personalize your feed or job recommendations based on your learning history."<sup>76</sup>*

<sup>75</sup> Ibid.

<sup>76</sup> Ibid.





Klausula di atas menyatakan bahwa LinkedIn akan membagikan data pribadi pengguna di berbagai layanan mereka dan entitas yang berafiliasi dengan LinkedIn. Hal ini dilakukan guna mengembangkan layanan serta agar layanan lebih bermanfaat bagi pengguna. Dengan adanya klausula ini, maka dimungkinkan bagi LinkedIn untuk membagikan data pribadi penggunanya secara internal.

Selanjutnya pada bagian yang sama angka 3.5 tentang *Service Providers*, LinkedIn juga menyatakan:

*"We use others to help us provide our Services (e.g., maintenance, analysis, audit, payments, fraud detection, marketing and development). They will have access to your information as reasonably necessary to perform these tasks on our behalf and are obligated not to disclose or use it for other purposes."<sup>77</sup>*

Guna menyediakan layanan terbaik bagi para penggunanya, tentunya LinkedIn akan bekerja sama dan menggunakan bantuan dari pihak lain, misalnya dalam hal pemeliharaan, analisis, audit, pembayaran/*payment*, *fraud detection*, pemasaran, serta pengembangan. Oleh karena itu, berdasarkan klausula di atas maka pihak ketiga tersebut diizinkan oleh LinkedIn untuk mengakses informasi pengguna untuk menjalankan tugasnya. Pada klausula ini, LinkedIn telah menyatakan bahwa pihak ketiga tersebut berkewajiban untuk tidak menggunakan informasi tersebut untuk keperluan lain selain yang ditugaskan oleh LinkedIn kepadanya dan tidak mengungkapkannya tanpa izin.

Selanjutnya pada bagian yang sama angka 3.6 tentang *Legal Disclosures*, LinkedIn menyatakan bahwa dimungkinkan bagi LinkedIn untuk membagikan data pengguna apabila diwajibkan oleh hukum atau dalam rangka melindungi hak dan keselamatan pengguna, pihak LinkedIn, ataupun pihak lain yang sekiranya terkait. LinkedIn menyatakan bahwa terdapat kemungkinan LinkedIn harus mengungkapkan informasi pengguna ketika diwajibkan oleh hukum, atas surat perintah pengadilan, oleh proses hukum lain, atau apabila diyakini secara wajar dibutuhkan untuk:

<sup>77</sup> Ibid.



- 1) Membantu badan pelaksana pemerintahan untuk memeriksa, mengantisipasi, atau bertindak terkait adanya atau dugaan aktivitas ilegal;
- 2) Menegakkan perjanjian antara LinkedIn dan pengguna;
- 3) Menyelidiki klaim pihak ketiga;
- 4) Melindungi integritas dan keamanan layanan;
- 5) Melaksanakan dan melindungi kepentingan dan keamanan LinkedIn.

Pada dasarnya, LinkedIn akan memberitahu pemilik akun atas adanya permintaan hukum atas data pribadi mereka, kecuali apabila hukum/perintah pengadilan melarang atau apabila permintaan tersebut bersifat darurat. Akan tetapi LinkedIn berwenang menolak adanya permintaan tersebut apabila dianggap berlebihan, tidak jelas, atau permintaan tersebut tidak berasal dari otoritas yang tepat.

Kemudian pada bagian yang sama angka 3.7 tentang *Change in Control or Sale*, LinkedIn menyatakan bahwa pihaknya dapat membagikan data pribadi penggunanya apabila terjadi *merger*, perubahan kontrol atau penjualan bisnis oleh perusahaan kepada entitas lain. Entitas tersebut akan memiliki hak untuk menggunakan data pribadi pengguna, namun penggunaan harus sesuai dengan *Privacy Policy* yang telah dibuat oleh LinkedIn sebelumnya.

Pada bagian 4. *Your Choices & Obligations* angka 4.1 tentang *Data Retention*, LinkedIn menyatakan bahwa pihaknya akan menyimpan sebagian besar data pribadi pengguna selama akun aktif dan terbuka, kecuali pengguna memutuskan untuk menutup akun mereka. Selanjutnya pada angka 4.2 tentang *Rights to Access and Control Your Personal Data*, terdapat klausul yang menyatakan bahwa pengguna dapat secara sendiri atau meminta pihak LinkedIn untuk mengakses dan/atau mengambil, mengubah atau mengoreksi, serta menghapus data pribadinya. Pengguna juga dapat meminta LinkedIn untuk menghentikan atau membatasi penggunaan data pribadinya sesuai dengan hukum yang berlaku.





Akan tetapi terdapat pengecualian dari pernyataan pada klausula angka 4.1, yakni pada klausul angka 4.3 tentang *Account Closure* yang menyatakan:

*"If you choose to close your LinkedIn account, your personal data will generally stop being visible to others on our Services within 24 hours. We generally delete closed account information within 30 days of account closure, except as noted below.*

*We retain your personal data even after you have closed your account if reasonably necessary to comply with our legal obligations (including law enforcement requests), meet regulatory requirements, resolve disputes, maintain security, prevent fraud and abuse (e.g., if we have restricted your account for breach of our Professional Community Policies), enforce our User Agreement, or fulfill your request to "unsubscribe" from further messages from us. We will retain de-personalized information after your account has been closed.*"<sup>78</sup>

Pada klausula di atas dinyatakan bahwa pada umumnya data pribadi pengguna tidak dapat dilihat oleh orang lain setelah 24 jam, dan terhapus dari sistem LinkedIn dalam jangka waktu 30 sejak penutupan akun LinkedIn. Namun terdapat beberapa kondisi tertentu yang memungkinkan bagi LinkedIn untuk tetap menyimpan data pribadi pengguna pada *database* layanan meskipun pengguna telah menutup akun, yakni apabila diperlukan secara wajar untuk memenuhi kewajiban hukum LinkedIn, memenuhi persyaratan regulasi, menyelesaikan perselisihan/sengketa, menjaga keamanan, mencegah penipuan (*fraud*) dan penyalahgunaan (*abuse*) serta dalam rangka menegakkan *User Agreement* layanan LinkedIn.

Pada bagian 5. *Other Important Information* angka 5.1 tentang *Security*, dinyatakan bahwa LinkedIn telah menerapkan *security safeguards* guna melindungi data pribadi pengguna, termasuk adanya *two-factor authentication* atau autentikasi dua faktor. Autentikasi dua faktor atau *two-factor authentication* adalah verifikasi yang memerlukan lebih dari satu proses untuk mengakses suatu akun, misalnya saja verifikasi kata sandi akun dan perangkat seluler. Penggunaan metode ini dinilai dapat mencegah secara signifikan pencurian identitas dan *illegal*

<sup>78</sup> Ibid.





*access* pada akun, karena mayoritas kasus pembajakan akun menggunakan perangkat baru atau yang tidak dikenal.<sup>79</sup>

Selain telah menerapkan *security safeguards*, LinkedIn juga secara rutin memantau sistem guna menemukan ada atau tidaknya kemungkinan kerentanan (*vulnerabilities*) dan serangan. Namun pihak LinkedIn tidak dapat menjamin keamanan setiap informasi pengguna yang ada pada LinkedIn. Tidak ada jaminan bahwa tidak akan ada penerobosan perlindungan baik secara fisik, teknis, atau manajerial layanan yang menyebabkan data diakses, diubah, diungkapkan, atau dimusnahkan tanpa seizin pemilik data.

Pada bagian yang sama angka 5.3 tentang *Lawful Bases for Processing*, LinkedIn menyatakan bahwa pihaknya hanya akan mengumpulkan, menggunakan, memproses, dan membagikan data pribadi pengguna apabila LinkedIn memiliki dasar hukum yang mencakup persetujuan dari pengguna (*consent*), kontrak (*contract*), dan kepentingan yang sah (*legitimate interest*).

Kepentingan yang sah (*legitimate interest*) adalah salah satu dari enam dasar hukum dalam pemrosesan data pribadi yang mana membenarkan tindakan suatu entitas untuk menggunakan dan memproses data pribadi orang lain diluar ketentuan hukum (baik oleh peraturan perundang-undangan maupun kontrak), selama tindakan tersebut merupakan tindakan pemrosesan secara wajar dan diperlukan untuk dilakukan. Kepentingan yang sah (*legitimate interest*) dapat termasuk kepentingan entitas pemroses data pribadi atau kepentingan pihak ketiga, termasuk kepentingan komersial, kepentingan individu atau manfaat sosial yang lebih luas. Entitas pemroses data pribadi memiliki kewajiban untuk menyeimbangkan kepentingan tersebut dengan kepentingan pemilik data pribadi. Entitas pemroses data pribadi juga harus menyertakan secara detail *legitimate interest*-nya di dalam informasi/kebijakan privasinya.<sup>80</sup>

<sup>79</sup> LinkedIn, 2021, **Two-Step Verification Overview**, <https://www.linkedin.com/help/linkedin/answer/531?lang=en> (6 Februari 2022)

<sup>80</sup> Information Commissioner's Office Inggris, **Legitimate interests**, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/> (07 Februari 2022)





LinkedIn dalam pengumpulan dan pemrosesan data pribadi penggunaannya didasari oleh kepentingan yang sah dari LinkedIn atau kepentingan yang sah dari pihak ketiga (karyawan atau konsumen LinkedIn, dan lain sebagainya) termasuk kepentingan komersial, kepentingan pengguna lain, atau kebermanfaatannya yang lebih luas bagi masyarakat. LinkedIn mendasarkan pada kepentingan yang sah ketika memproses data pribadi pengguna demi:<sup>81</sup>

- a) Melindungi pengguna, LinkedIn ataupun pihak lain dari ancaman (seperti ancaman keamanan, *scraping*, atau penipuan) guna memenuhi kepentingan yang sah LinkedIn dan kepentingan pengguna serta konsumen untuk menjaga keamanan layanan dan melindungi data pribadi pengguna;
- b) Mematuhi hukum non-EU yang berlaku bagi LinkedIn guna memenuhi kepentingan yang sah LinkedIn untuk menghindari sanksi akibat ketidakpatuhan dan mengutamakan kepentingan yang sah dari komunitas kami yang lebih luas dalam memastikan bahwa LinkedIn mematuhi hukum tersebut;
- c) Mengelola urusan untuk hal-hal seperti *quality control* (QC), pembuatan laporan terpadu tentang bisnis LinkedIn, dan *customer service* (CS) guna memenuhi kepentingan yang sah LinkedIn untuk menjalankan bisnis secara efektif dan efisien, serta memenuhi ekspektasi pengguna dan konsumen LinkedIn mengenai kualitas layanan yang tinggi;
- d) Mengelola transaksi perusahaan, seperti *merger*, akuisisi, atau penjualan, guna mendukung kepentingan yang sah dari LinkedIn untuk mengembangkan, memperkuat, dan mengelola bisnis serta aset mereka;
- e) Memahami dan meningkatkan bisnis atau hubungan dengan konsumen secara umum guna memenuhi kepentingan yang sah LinkedIn untuk menyempurnakan dan mengembangkan bisnis, memenuhi kebutuhan konsumen, dan menjamin bahwa pengguna menerima layanan terbaik dari LinkedIn;

<sup>81</sup> LinkedIn, *LinkedIn's processing on the basis of legitimate interests*, <https://www.linkedin.com/help/linkedin/answer/89878?lang=en>, 2022 (07 Februari 2022)



f) Memungkinkan pengguna untuk saling terhubung, menemukan pekerjaan dan peluang ekonomi, mengemukakan pendapat, bertukar informasi, dan berbisnis guna mendukung kepentingan yang sah dalam memenuhi misi LinkedIn untuk menghubungkan para profesional di seluruh dunia agar mereka lebih produktif dan sukses.

Dari klausul-klausul pengaturan pada *Privacy Policy* yang terkait dengan data pribadi pengguna di atas, maka dapat penulis rangkum ke dalam tabel untuk mempermudah pembaca sebagai berikut:





**Tabel 3.1 Tabel Substansi *Privacy Policy* LinkedIn yang Terkait dengan Data Pribadi Pengguna**

	<i>Privacy Policy</i> ini berlaku untuk pengguna layanan, baik Anggota maupun Pengunjung. <i>Policy</i> ini berlaku untuk LinkedIn.com serta seluruh layanan yang terkait dengan LinkedIn.
<b>Introduction</b>	Entitas pengelola data pribadi pengguna untuk pengguna di <i>Designated Countries</i> dikontrol oleh LinkedIn Ireland, sedangkan untuk pengguna di <i>Non-Designated Countries</i> dikelola oleh LinkedIn Corporation.
	LinkedIn dapat memodifikasi <i>Privacy Policy</i> sewaktu-waktu, yang pemberitahuannya akan disampaikan kepada pengguna sebelum berlaku efektif.
<b>1. Data We Collect, 1.1 Data You Provide To Us</b>	Nama, alamat email dan/atau nomor telepon, dan kata sandi (serta informasi pembayaran dan penagihan untuk pendaftaran akun premium) wajib diberikan pada saat pendaftaran akun. Pemberian data pribadi lain bersifat opsional, namun kesempatan dan manfaat akan terbatas bagi pengguna apabila tidak menyertakannya.
<b>1. Data We Collect, 2.2 Data From Others</b>	Dimungkinkan bagi LinkedIn untuk menerima beberapa data pribadi pengguna dari orang lain, misalnya ketika orang tersebut melakukan sinkronisasi kontak atau ketika pengguna menggunakan layanan penyedia kerja.
<b>1. Data We Collect, 1.5 Your Device and Location</b>	LinkedIn dapat memiliki data lokasi pengguna pada saat menggunakan LinkedIn dengan terlebih dahulu meminta izin kepada pengguna.
<b>1. Data We Collect, 1.6 Messages</b>	LinkedIn dapat mengakses pesan pengguna di LinkedIn.
<b>1. Data We Collect, 1.7 Workplace and School Provided Information</b>	Apabila organisasi membeli layanan premium untuk digunakan oleh pengguna, maka pihak organisasi akan memberikan data pribadi pengguna tersebut.
<b>2. How We Use Your Data</b>	Data pengguna digunakan oleh LinkedIn untuk menjadikan layanan lebih baik lagi yang penggunaannya akan disesuaikan dengan pilihan pengguna pada pengaturan serta jenis layanan yang ambil pengguna
<b>2. How We Use Your Data, 2.6 Developing Services and Research</b>	LinkedIn akan memakai data pribadi pengguna dalam hal riset, serta memungkinkan adanya kerja sama dengan pihak ketiga yang berintegritas di dalam riset tersebut.
<b>3. How We Share Information,</b>	LinkedIn akan membagikan data pribadi pengguna pada pelbagai layanan serta entitas yang terafiliasi



<b>3.4 Related Services</b>	dengan LinkedIn.
<b>3. How We Share Information, 3.5 Service Providers</b>	LinkedIn memperbolehkan pihak ketiga untuk mengakses informasi pengguna dalam rangka melaksanakan perintah yang ditugaskan oleh LinkedIn.
<b>3. How We Share Information, 3.6 Legal Disclosure</b>	LinkedIn dapat membagikan data pengguna jikalau diharuskan oleh hukum, surat perintah pengadilan, atau dalam rangka menaungi dan melindungi hak serta keselamatan pengguna, pihak LinkedIn, maupun pihak terkait.
<b>3. How We Share Information, 3.7 Change in Control or Sale</b>	Dimungkinkan bagi LinkedIn untuk dapat membagikan data pribadi penggunanya jika terjadi <i>merger</i> , perubahan kontrol atau penjualan bisnis oleh perusahaan kepada entitas lain, namun pemanfaatan data pribadi tersebut wajib selaras dengan <i>Privacy Policy</i> .
<b>4. Your Choices &amp; Obligations, 4.1 Data Retention</b>	LinkedIn akan menyimpan data pribadi pengguna selama akun aktif.
<b>4. Your Choices &amp; Obligations, 4.2 Rights to Access and Control Your Personal Data</b>	Pengguna dapat mengakses dan/atau mengambil, mengubah atau mengoreksi, menghapus data pribadinya, menghentikan atau membatasi penggunaan data pribadinya.
<b>4. Your Choices &amp; Obligations, 4.3 Account Closure</b>	Beberapa kondisi yang memungkinkan LinkedIn untuk tetap menyimpan data pribadi pengguna pada <i>database</i> layanan meskipun pengguna telah menutup akun.
<b>5. Other Important Information, 5.1 Security</b>	LinkedIn telah menerapkan perlindungan keamanan guna melindungi data pribadi pengguna.
<b>5. Other Important Information, 5.3 Lawful Bases for Processing</b>	LinkedIn hanya akan mengumpulkan, menggunakan, memproses, dan membagikan data pribadi pengguna berdasarkan <i>consent</i> , <i>contract</i> , dan <i>legitimate interest</i> .

Sumber: *Bahan Hukum Primer Diolah, 2021*

Dapat kita lihat bahwa *Privacy Policy* LinkedIn sebenarnya lebih detail memuat beberapa hal terkait data pribadi pengguna. Dari *privacy policy* tersebut dapat kita ketahui siapa entitas pengelola data pribadi pengguna; bagaimana data pribadi tersebut dikumpulkan, digunakan, dibagikan, dan disimpan; serta bagaimana keamanan yang diterapkan guna melindungi data pribadi pengguna. Namun pada *privacy policy* LinkedIn tidak dimuat secara tersurat mengenai apa yang menjadi kewajiban dari pihak LinkedIn terhadap perlindungan data pribadi pengguna dan bagaimana tanggung jawab LinkedIn kepada pengguna



apabila terjadi kebocoran terhadap data pribadi yang berada dalam pengelolaannya. Hal inilah yang menjadi perhatian penulis dan akan penulis analisis lebih dalam pada bagian selanjutnya dari penelitian ini.

Oleh karena dalam *Privacy Policy* ini tidak disertakan apa yang menjadi kewajiban dari LinkedIn selaku platform terhadap perlindungan data pribadi pengguna dan bagaimana tanggung jawab LinkedIn kepada pengguna apabila terjadi kebocoran terhadap data pribadi yang berada dalam pengelolaannya, maka kewajiban-kewajiban materiil tersebut harus kita lihat pada peraturan perundang-undangan hukum di negara tujuan layanan serta hukum dimana pengguna berkedudukan. Di Indonesia sendiri, kita dapat mengetahui bagaimana kewajiban platform terkait perlindungan data pribadi pengguna mengacu kepada UU ITE serta peraturan turunannya yang mengatur secara lebih terperinci mengenai perlindungan data pribadi. Di Indonesia, Secara umum peraturan mengenai perlindungan data pribadi membebaskan beberapa kewajiban kepada platform (atau yang kemudian dalam peraturan disebut dengan Penyelenggara Sistem Elektronik/PSE) mengenai perlindungan dan pengamanan data pribadi pengguna. Oleh karena itu, sub bab sebelumnya akan memberikan penjelasan yang lebih rinci berkenaan dengan perlindungan data pribadi serta kewajiban platform terhadap data pribadi pengguna apa saja yang sudah diatur menurut ketentuan di Indonesia.

## **2. Analisis *Privacy Policy* LinkedIn dikaitkan dengan Pasal 26 Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi Dan Transaksi Elektronik serta peraturan turunan yang relevan**

Pada sub bab ini, penulis akan menganalisis beberapa peraturan di Indonesia yang sesuai dengan substansi pada penelitian ini untuk menyajikan gambaran berkenaan ketentuan perlindungan data pribadi di Indonesia.



## 2.1 Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi Dan Transaksi Elektronik

Undang-Undang 19/2016 tentang Perubahan atas UU 11/2008 tentang ITE menjadi pembuka adanya pengaturan di Indonesia berkenaan dengan pemanfaatan teknologi informasi dan transaksi elektronik. UU ITE telah memberikan pengertian gramatikal mengenai Informasi Elektronik, yakni:

"Informasi Elektronik adalah satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, *electronic data interchange* (EDI), surat elektronik (*electronic mail*), telegram, teleks, *teletcopy* atau sejenisnya, huruf, tanda, angka, Kode Akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya."<sup>82</sup>

Sedangkan Transaksi Elektronik berdasarkan UU ITE ialah perbuatan hukum yang dilaksanakan dengan menggunakan Komputer, jaringan Komputer, dan/atau media elektronik lainnya.<sup>83</sup>

Pada UU ITE, ketentuan terkait data pribadi dapat ditemukan pada Pasal 26. Pasal 26 ayat (1):

"Kecuali ditentukan lain oleh peraturan perundang-undangan, penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan Orang yang bersangkutan."<sup>84</sup>

Pasal tersebut mewajibkan adanya izin dari pemilik data pribadi atau yang bersangkutan jika suatu pihak akan memakai data pribadi orang tersebut, Alasannya, bahwa hal tersebut adalah sebagian dari hak pribadi (*privacy rights*) yang harus dilindungi implementasinya.

<sup>82</sup> Pasal 1 angka 1 Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi Dan Transaksi Elektronik

<sup>83</sup> Pasal 1 angka 2 Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi Dan Transaksi Elektronik

<sup>84</sup> Pasal 26 ayat (1) Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi Dan Transaksi Elektronik





Hak pribadi merupakan hak untuk menikmati kehidupan pribadi dan bebas dari berbagai gangguan, hak untuk dapat berkomunikasi dengan orang lain tanpa tindakan memata-matai, juga hak untuk mengawasi akses informasi mengenai kehidupan pribadi dan data seseorang.<sup>85</sup> Jika terdapat seseorang yang merasa data pribadinya dipakai oleh pihak lain namun tidak disertai dengan persetujuan dari orang tersebut, maka berdasarkan Pasal 26 ayat (2), orang tersebut dapat mengajukan gugatan atas kerugian yang dialaminya kepada pihak tersebut selaras dengan yang telah diatur pada UU ITE.

Pada ayat (3) hingga ayat (5) Pasal 26 UU ITE 19/2016, walaupun tidak secara tersurat menyebutkan data pribadi, namun pasal-pasal tersebut mengharuskan PSE untuk menghapuskan Dokumen dan/atau Informasi Elektronik yang sudah tidak sesuai didasarkan pada penetapan pengadilan atas permintaan Pemilik data pribadi/yang bersangkutan.<sup>86</sup> Selain itu, menjadi kewajiban dari tiap PSE untuk menyediakan mekanisme penghapusan Informasi dan/atau Dokumen Elektronik yang selaras dengan ketentuan perundang-undangan (PUU) yang absah berlaku.<sup>87</sup>

## **2.2 Peraturan Pemerintah Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik**

PP 71/2019 tentang PSTE merupakan salah satu ketentuan turunan dari UU ITE. PP PSTE ini merevisi PP PSTE yang terdahulu, yakni PP 82/2012 karena dirasa tidak selaras lagi dengan keperluan hukum di tengah masyarakat yang sudah mendayagunakan teknologi dengan perkembangan yang luar biasa lajunya. PP ini menekankan pengaturannya kepada PSE, baik

<sup>85</sup> Penjelasan Pasal 26 ayat (1) **Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi Dan Transaksi Elektronik**

<sup>86</sup> Pasal 26 ayat (3) **Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi Dan Transaksi Elektronik**

<sup>87</sup> Pasal 26 ayat (4) **Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi Dan Transaksi Elektronik**



Lingkup Publik maupun Lingkup Privat. PSE sendiri merupakan setiap Orang, Badan Usaha, penyelenggara negara, dan masyarakat yang memfasilitasi, mengoperasikan dan/atau mengelola SE (Sistem Elektronik) secara bersama-sama maupun masing-masing kepada PSE guna keperluan pihak lain maupun dirinya sendiri.<sup>88</sup>

Pada Pasal 14 PP 71/2019 tentang PSTE, PSE dibebani kewajiban untuk melaksanakan dan mengadopsi prinsip-prinsip perlindungan data pribadi dalam menerapkan pemrosesan data pribadi, yaitu:

- a. Pengumpulan Data Pribadi dilakukan secara terbatas dan spesifik, sah secara hukum, adil, dengan sepengetahuan dan persetujuan dari pemilik Data Pribadi;
- b. Pemrosesan Data Pribadi dilakukan sesuai dengan tujuannya;
- c. Pemrosesan Data Pribadi diterapkan dengan menjamin hak pemilik Data Pribadi;
- d. Pemrosesan Data Pribadi dilakukan secara akurat, lengkap, tidak menyesatkan, mutakhir, dapat dipertanggungjawabkan, dan memperhatikan tujuan pemrosesan Data Pribadi;
- e. Pemrosesan Data Pribadi diterapkan dengan melindungi keamanan Data Pribadi dari penyalahgunaan, kehilangan, pengungkapan yang tidak sah, serta kerusakan atau perubahan Data Pribadi;
- f. Pemrosesan Data Pribadi dilakukan dengan memberitahukan tujuan pengumpulan, aktivitas pemrosesan, dan kegagalan perlindungan Data Pribadi; dan

<sup>88</sup> Pasal 1 angka 4 Peraturan Pemerintah Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik



g. Pemrosesan Data Pribadi dimusnahkan dan/atau dihapus kecuali masih dalam masa retensi sesuai dengan kebutuhan berdasarkan ketentuan perundang-undangan.<sup>89</sup>

Prinsip-prinsip tersebut harus diterapkan oleh PSE pada saat pemrosesan data pribadi yang meliputi perolehan dan pengumpulan; pengolahan dan penganalisisan; penyimpanan; perbaikan dan pembaruan; penampilan, pengumuman, transfer, penyebarluasan, atau pengungkapan; dan/atau penghapusan atau pemusnahan.<sup>90</sup>

Sebagaimana pengaturan pada Pasal 14 ayat (3), Pemrosesan atas data pribadi harus didasarkan atas persetujuan yang sah dari pemiliknya, untuk apa data pribadi tersebut akan digunakan oleh pihak PSE, dan tujuan tertentu tersebut harus telah disampaikan kepada pemilik data pribadi. Selain atas adanya persetujuan, pemrosesan data pribadi dapat dilakukan untuk pemenuhan kewajiban perjanjian yang telah dibuat antara pihak PSE dengan pengguna, pemenuhan kewajiban hukum bagi pengendali data pribadi sebagaimana ketentuan perundang-undangan, pemenuhan perlindungan kepentingan yang sah/*vital interest*<sup>91</sup> pemilik data pribadi, pelaksanaan kewenangan dan pemenuhan kewajiban bagi pengendali data pribadi, dan pemenuhan vital interest lainnya bagi PSE atau pemilik data pribadi.<sup>92</sup> Apabila terjadi kegagalan dalam perlindungan terhadap data pribadi yang dikelolanya, maka PSE memiliki kewajiban untuk

<sup>89</sup> Pasal 14 ayat (1) **Peraturan Pemerintah Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik**

<sup>90</sup> Pasal 14 ayat (2) **Peraturan Pemerintah Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik**

<sup>91</sup> Menurut Penjelasan PP 71/2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik Pasal 14 ayat (4) huruf c, yang dimaksud dengan "kepentingan yang sah (*vital interest*)" adalah kebutuhan/keperluan untuk melindungi hal yang sangat penting tentang keberadaan seseorang.

<sup>92</sup> Pasal 14 ayat (4) **Peraturan Pemerintah Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik**





memberitahukan hal tersebut secara tertulis kepada pemilik data pribadi yang bersangkutan.<sup>93</sup>

Pada Pasal 15 PP PSTE 71/2019 mengharuskan tiap PSE yang menerima dan/atau mengolah Data Pribadi di dalam pengaturannya untuk menghapus Dokumen dan/atau Informasi Elektronik yang sudah tidak sesuai atas permintaan pemilik data pribadi atau yang bersangkutan.<sup>94</sup> Terdapat 2 jenis hak yang menyertai kewajiban penghapusan tersebut, yakni pengeluaran dari daftar mesin pencari (*right to delisting*) dan penghapusan (*right to erasure*) dan<sup>95</sup> *Right to delisting* serta *Right to erasure* merupakan suatu hak yang didasarkan pada sebuah gagasan bahwa seseorang memiliki hak hukum untuk menghapus informasi tentang dirinya sendiri yang dapat diakses secara online dan/atau yang berpotensi mengganggu kenyamanan kehidupan pribadi seseorang.<sup>96</sup>

Pasal 16 ayat (1) PP 71/2019 tentang PSTE telah mengkategorikan data pribadi yang dilakukan penghapusan, yakni data pribadi yang:

- a. Yang didapatkan dan diolah namun tidak disertai izin dari pemilik Data Pribadi;
- b. Izin penggunaannya telah diambil atau dibatalkan oleh pemilik Data Pribadi;
- c. Perolehan dan pemrosesannya bertentangan dengan hukum dengan cara melawan hukum;
- d. Pemrosesan yang dilakukan sudah bertentangan dengan tujuan perolehan menurut perjanjian yang sudah dibuat sebelumnya dan/atau ketentuan perundang-undangan;

<sup>93</sup> Pasal 14 ayat (5) **Peraturan Pemerintah Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik**

<sup>94</sup> Pasal 15 ayat (1) dan ayat (3) **Peraturan Pemerintah Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik**

<sup>95</sup> Pasal 15 ayat (2) **Peraturan Pemerintah Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik**

<sup>96</sup> Guadamuz, A., *Developing a Right to be Forgotten*. In: EU Internet Law: Regulation and Enforcement. Cham : Springer, hlm. 60.





- e. Pemanfaatannya sudah melewati batas waktu menurut perjanjian yang sudah dibuat sebelumnya dan/atau ketentuan perundang-undangan; dan/atau
- f. Ditampilkan oleh PSE yang memberikan kerugian untuk pemilik Data Pribadi.<sup>97</sup>

Namun ayat (2) dari pasal yang sama mencantumkan bahwa kewajiban-kewajiban yang telah diatur di ayat (1) pasal tersebut tidak berlaku jika Dokumen dan/atau Informasi Elektronik yang akan dihapus tersebut oleh ketentuan perundang-undangan dan pihak yang berwajib dilarang untuk dihapus dan harus disimpan oleh PSE.<sup>98</sup> Maka dari itu, tidak semua data pribadi yang dimintakan untuk dihapus dapat langsung dihapus oleh PSE.

Untuk *right to delisting*, Pasal 15 ayat (2) huruf b pada penjelasannya serta Pasal 17 memaparkan lebih lanjut bahwa keharusan untuk mengeluarkan dari daftar mesin pencari oleh PSE yang mengoperasikan mesin pencari, dan/atau meniadakan Akses Dokumen dan/atau Informasi Elektronik yang sudah tidak sesuai dilaksanakan dengan didasarkan pada penetapan pengadilan. Pemilik Data Pribadi dapat mengajukan permohonan sehubungan dengan penetapan tersebut kepada Pengadilan Negeri dengan menyertakan identitas pemohon, identitas PSE dan/atau alamat Sistem Elektronik, Data Pribadi dibawah kendali PSE tersebut yang akan dihapus, serta alasan permintaan penghapusan.<sup>99</sup> Penetapan tersebutlah yang menjadi dasar kewajiban PSE untuk menghapus Dokumen dan/atau Informasi Elektronik yang sudah tidak sesuai. Namun kewajiban tersebut belum melekat pada PSE apabila belum ada penetapan dari pengadilan terkait hal tersebut.

Disamping memiliki kewajiban untuk menghapus Dokumen dan/atau Informasi Elektronik yang sudah tidak sesuai atas

<sup>97</sup> Pasal 16 ayat (1) **Peraturan Pemerintah Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik**

<sup>98</sup> Pasal 16 ayat (2) **Peraturan Pemerintah Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik**

<sup>99</sup> Pasal 17 ayat (2) dan (3) **Peraturan Pemerintah Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik**





permintaan pemilik Data Pribadi, PSE juga memiliki kewajiban untuk membuat mekanisme penghapusan Dokumen dan/atau Informasi Elektronik yang sudah tidak sesuai, dimana mekanisme tersebut paling tidak berisi ketentuan terkait kontak yang dapat menghubungkan PSE dengan pemilik data pribadi, fitur yang memungkinkan pemilik Data pribadi melakukan penghapusan atas Data Pribadinya secara mandiri, serta pencatatan atas permintaan penghapusan Dokumen dan/atau Informasi Elektronik tersebut.<sup>100</sup>

### **2.3 Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik.**

Permenkominfo 20/2016 diundangkan pada tanggal 1 Desember 2016 dan merupakan peraturan pelaksana dari PP PSTE yang lama, yakni PP 82/2012. Permenkominfo ini merupakan wujud implementasi PP 82/2012 sehingga terdapat pengaturan selanjutnya berupa Permenkominfo mengenai pedoman perlindungan data pribadi dalam sistem elektronik. Walaupun PP 82/2012 telah dicabut dan digantikan oleh PP 71/2019 tentang PSTE, namun sebagaimana Ketentuan Penutup pada PP 71/2019, selama tidak bertentangan dan belum digantikan dengan peraturan yang baru, ketentuan pelaksana dari PP 82/2012 tetap dinyatakan berlaku.<sup>101</sup> Oleh karena itu, pengaturan pada Permenkominfo 20/2016 tetap berlaku karena hingga saat ini, belum ada perubahan atau pencabutan atas Permenkominfo tersebut.

Pada Permenkominfo ini, dinyatakan bahwa dalam melaksanakan perlindungan data pribadi harus didasarkan pada 10 asas perlindungan data pribadi yang baik, yakni:

- a. Penghormatan terhadap Data Pribadi sebagai privasi;

<sup>100</sup> Pasal 18 ayat (1) dan (2) **Peraturan Pemerintah Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik**

<sup>101</sup> Pasal 103 ayat (1) **Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik**



- b. Data Pribadi bersifat rahasia selaras dengan Persetujuan yang telah dibuat sebelumnya dan/atau ketentuan perundang-undangan;
- c. Berdasarkan izin atau persetujuan;
- d. Kesesuaian dengan tujuan perolehan, penghimpunan, pengolahan, penganalisisan, penyimpanan, penampilan, pengumuman, pemindahan, dan penyebarluasan;
- e. Kelaikan Sistem Elektronik yang dimanfaatkan;
- f. Itikad baik untuk lekas memberitahukan setiap kegagalan atas perlindungan Data Pribadi secara tertulis;
- g. Kesiapan aturan internal pengelolaan perlindungan Data Pribadi;
- h. Tanggung jawab atas Data Pribadi yang ada dalam penguasaannya;
- i. Kemudahan akses serta pembetulan Data Pribadi bagi Pemilik Data Pribadi; dan
- j. Kelengkapan, akurasi, dan validitas serta kemutakhiran Data Pribadi.<sup>102</sup>

Selain itu, perlindungan data pribadi dalam sistem elektronik juga harus diimplementasikan di dalam setiap proses perolehan, pengumpulan, pengolahan, penganalisisan, penyimpanan, penampilan, pengumuman, pengiriman, penyebarluasan dan/atau pembukaan akses, hingga pemusnahan Data Pribadi.<sup>103</sup>

Pasal Permekominfo 20/16 ini mengharuskan PSE untuk memiliki ketentuan internal sehubungan dengan perlindungan Data Pribadi di saat melakukan semua proses yang melibatkan data pribadi seseorang.<sup>104</sup> Pasal 6 Permenkominfo 20/2016 telah memberikan kewajiban kepada PSE untuk menyediakan formulir persetujuan dalam Bahasa Indonesia untuk meminta persetujuan

<sup>102</sup> Pasal 2 ayat (2) **Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik.**

<sup>103</sup> Pasal 3 **Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik.**

<sup>104</sup> Pasal 5 **Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik.**





dari pemilik data pribadi untuk memproses data pribadinya.<sup>105</sup>

Selain itu dalam memperoleh dan mengumpulkan data pribadi, PSE harus dibatasi pada informasi yang relevan dan digunakan sesuai dengan tujuan dan akurat serta harus menghormati data pribadi dari pemiliknya yang bersifat privasi.<sup>106</sup>

Pasal 11 memberikan syarat terkait SE yang dimanfaatkan guna mewadahi data pribadi yang didapatkan dan dihimpun, yakni wajib mempunyai kemampuan interoperabilitas dan keadaan penyesuaian diri (kompatibilitas) yang telah selaras dengan ketentuan perundang-undangan dan telah memakai *software* yang legal.<sup>107</sup> Kemudian Pasal 12 Permenkominfo 20/2016 menyatakan bahwa PSE hanya boleh mengolah dan menganalisis data pribadi yang ada di dalam sistemnya sesuai dengan kebutuhan PSE dan dengan berlandaskan pada persetujuan yang sebelumnya telah dinyatakan secara jelas pada saat mendapatkan dan menghimpun data pribadi tersebut.<sup>108</sup>

Terkait penyimpanan data pribadi, Pasal 15 Permenkominfo 20/2016 mensyaratkan bahwa data pribadi yang disimpan dalam sistem elektronik adalah data pribadi yang telah diverifikasi keakuratannya, harus dalam bentuk data terenkripsi, dan wajib disimpan paling singkat 5 (lima) tahun (atau jika telah ada yang secara khusus mengatur mengenai hal tersebut, maka disesuaikan dengan ketentuan perundang-undangan).<sup>109</sup> Penyimpanan juga harus dilakukan sesuai dengan ketentuan mengenai prosedur dan sarana pengamanan Sistem Elektronik.<sup>110</sup>

<sup>105</sup> Pasal 6 **Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik.**

<sup>106</sup> Pasal 7 ayat (1) dan Pasal 8 ayat (1) **Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik.**

<sup>107</sup> Pasal 11 **Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik.**

<sup>108</sup> Pasal 12 **Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik.**

<sup>109</sup> Pasal 15 **Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik.**

<sup>110</sup> Pasal 18 **Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik.**





Pasal 21 ayat (1) Permenkominfo 20/2016 menyatakan bahwa memublikasikan, menampilkan, membagikan, menyebarluaskan, dan/atau membuka akses Data Pribadi di dalam SE hanya dapat dilaksanakan atas Persetujuan kecuali jika ditentukan lain oleh ketentuan perundang-undangan dan setelah diverifikasi kecocokan dan kesesuaian dengan tujuan perolehan dan pengumpulan Data Pribadi tersebut.<sup>111</sup>

PSE juga memiliki kewajiban untuk memberikan Data Pribadi yang ada padanya dalam rangka untuk keperluan hukum atas permintaan yang sah dari aparat penegak hukum berdasarkan ketentuan peraturan perundang-undangan. Akan tetapi, Data Pribadi yang wajib diberikan hanyalah data pribadi yang relevan dan sesuai dengan kebutuhan penegakan hukum.<sup>112</sup>

Permenkominfo 20/2016 ini juga mengatur mengenai pemusnahan data pribadi. Menurut Permenkominfo ini, pemusnahan data pribadi hanya dapat dilakukan apabila telah melewati ketentuan jangka waktu penyimpanan Data Pribadi dalam Sistem Elektronik sebagaimana yang telah diatur pada peraturan ini ataupun peraturan perundang-undangan yang mengatur secara khusus. Selain itu, pemusnahan data pribadi dapat dilakukan atas permintaan dari pemilik data pribadi tersebut, kecuali apabila peraturan perundang-undangan menentukan lain.<sup>113</sup>

Pasal 26 Permenkominfo 20/2016 mengatur mengenai hak dari pemilik data pribadi, yaitu pemilik data pribadi berhak:

- a. Atas kerahasiaan Data Pribadinya;
- b. Mengajukan pengaduan dalam rangka penyelesaian sengketa Data Pribadi atas kegagalan perlindungan

<sup>111</sup> Pasal 21 ayat (1) **Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik.**

<sup>112</sup> Pasal 23 **Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik.**

<sup>113</sup> Pasal 25 **Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik.**





kerahasiaan Data Pribadinya oleh Penyelenggara Sistem Elektronik kepada Menteri;

- c. Mendapatkan akses atau kesempatan untuk mengubah atau memperbarui Data Pribadinya tanpa mengganggu sistem pengelolaan Data Pribadi, kecuali ditentukan lain oleh ketentuan peraturan perundang-undangan;
- d. Mendapatkan akses atau kesempatan untuk memperoleh historis Data Pribadinya yang pernah diserahkan kepada Penyelenggara Sistem Elektronik sepanjang masih sesuai dengan ketentuan peraturan perundang-undangan; dan
- e. Meminta pemusnahan Data Perseorangan Tertentu miliknya dalam Sistem Elektronik yang dikelola oleh Penyelenggara Sistem Elektronik, kecuali ditentukan lain oleh ketentuan peraturan perundang-undangan.<sup>114</sup>

Sedangkan Pasal 28 dari Permenkominfo ini mengatur mengenai kewajiban dari Penyelenggara Sistem Elektronik (PSE) yaitu wajib:

- a. Melakukan sertifikasi Sistem Elektronik yang dikelolanya sesuai dengan ketentuan peraturan perundang-undangan;
- b. Menjaga kebenaran, keabsahan, kerahasiaan, keakuratan dan relevansi serta kesesuaian dengan tujuan perolehan, pengumpulan, pengolahan, penganalisisan, penyimpanan, penampilan, pengumuman, pengiriman, penyebarluasan, dan pemusnahan Data Pribadi;
- c. Memberitahukan secara tertulis kepada Pemilik Data Pribadi jika terjadi kegagalan perlindungan rahasia Data Pribadi dalam Sistem Elektronik yang dikelolanya, dengan ketentuan pemberitahuan sebagai berikut:
  - 1) Harus disertai alasan atau penyebab terjadinya kegagalan perlindungan rahasia Data Pribadi;
  - 2) Dapat dilakukan secara elektronik jika Pemilik Data Pribadi telah memberikan Persetujuan untuk itu yang

<sup>114</sup> Pasal 26 Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik.



dinyatakan pada saat dilakukan perolehan dan pengumpulan Data Pribadinya;

3) Harus dipastikan telah diterima oleh Pemilik Data Pribadi jika kegagalan tersebut mengandung potensi kerugian bagi yang bersangkutan; dan

4) Pemberitahuan tertulis dikirimkan kepada Pemilik Data Pribadi paling lambat 14 (empat belas) hari sejak diketahui adanya kegagalan tersebut;

d. Memiliki aturan internal terkait perlindungan Data Pribadi yang sesuai dengan ketentuan peraturan perundang-undangan;

e. Menyediakan rekam jejak audit terhadap seluruh kegiatan penyelenggaraan Sistem Elektronik yang dikelolanya;

f. Memberikan opsi kepada Pemilik Data Pribadi mengenai Data Pribadi yang dikelolanya dapat/atau tidak dapat digunakan dan/atau ditampilkan oleh/pada pihak ketiga atas Persetujuan sepanjang masih terkait dengan tujuan perolehan dan pengumpulan Data Pribadi;

g. Memberikan akses atau kesempatan kepada Pemilik Data Pribadi untuk mengubah atau memperbaiki Data Pribadinya tanpa mengganggu sistem pengelolaan Data Pribadi, kecuali ditentukan lain oleh ketentuan peraturan perundang-undangan;

h. Memusnahkan Data Pribadi sesuai dengan ketentuan dalam Peraturan Menteri ini atau ketentuan peraturan perundang-undangan lainnya yang secara khusus mengatur di masing-masing Instansi Pengawas dan Pengatur Sektor untuk itu; dan

i. Menyediakan narahubung (*contact person*) yang mudah dihubungi oleh Pemilik Data Pribadi terkait pengelolaan Data Pribadinya.<sup>115</sup>

<sup>115</sup> Pasal 28 Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik.





Dapat kita lihat, bahwa ketiga peraturan yang penulis analisis tersebut telah memperlihatkan bagaimana perlindungan data pribadi di Indonesia diatur, termasuk mengenai bagaimana kewajiban-kewajiban yang dibebankan kepada Penyelenggara Sistem Elektronik terkait data pribadi, yang dapat dirangkum sebagaimana yang terdapat pada tabel di bawah ini.





**Tabel 3.2 Tabel Kewajiban PSE terkait Perlindungan Data Pribadi yang Diatur di Peraturan Perundang-Undangan**

Terkait persetujuan kepada pemilik data pribadi dalam hal pemrosesan data pribadinya.	Pasal 26 (1) UU ITE; Pasal 14 ayat (3) PP 71/2019; Pasal 6, Pasal 12, Pasal 21 ayat (1) Permenkominfo 20/2016.
Melaksanakan prinsip-prinsip perlindungan data pribadi pada pemrosesan data pribadi.	Pasal 14 ayat (1) & (2) PP 71/2019; Pasal 2 ayat (2) Permenkominfo 20/2016.
Menyelenggarakan sistem elektronik secara andal, aman, dan bertanggung jawab.	Pasal 15 ayat (1) UU ITE; Pasal 3 ayat (1) & (2) PP 71/2019; Pasal 9 ayat (1) Permenkominfo 5/2020
Memberitahukan kepada pemilik data pribadi apabila terjadi kegagalan dalam perlindungan data pribadi yang dikelola PSE.	Pasal 14 ayat (5) PP 71/2019; Pasal 2 ayat (2) huruf f & Pasal 28 huruf c Permenkominfo 20/2016.
Terkait penghapusan dan pemusnahan data pribadi beserta penyediaan mekanismenya.	Pasal 26 (3) dan (4) UU ITE, Pasal 15, Pasal 17, dan Pasal 18 PP 71/2019; Pasal 25 Permenkominfo 20/2016.
Menyampaikan informasi kepada pengguna mengenai Identitas PSE, Objek yang ditransaksikan, kelaikan atau keamanan SE, Tata cara penggunaan perangkat, syarat kontrak, prosedur mencapai kesepakatan, jaminan privasi dan/atau perlindungan data pribadi, & nomor telepon pusat pengaduan	Pasal 29 PP 71/2019
Memberikan data pribadi yg dikelolanya dalam rangka u/ keperluan hukum atas permintaan yg sah dari aparat penegak hukum berdasarkan ketentuan PUU.	Pasal 23 Permenkominfo 20/2016.
Mempunyai aturan internal terkait perlindungan data pribadi.	Pasal 5 Permenkominfo 20/2016
Sistem elektronik yang digunakan untuk menampung data pribadi harus telah sesuai ketentuan peraturan perundang-undangan	Pasal 11 Permenkominfo 20/2016
Kewajiban lainnya	Pasal 28 Permenkominfo 20/2016

Sumber: *Bahan Hukum Primer Diolah, 2021*

Setelah kita mempunyai gambaran mengenai bagaimana pengaturan perlindungan data pribadi di Indonesia, selanjutnya penulis akan menganalisis apakah *privacy policy* dari LinkedIn telah memenuhi kewajiban-



kewajiban yang telah diatur pada pengaturan perlindungan data pribadi di Indonesia. LinkedIn telah memiliki *privacy policy* atau kebijakan privasi yang secara khusus berisi mengenai bagaimana pihak LinkedIn akan memproses data pribadi penggunanya. Dengan adanya *privacy policy* tersebut, maka kewajiban Pasal 5 Permenkominfo 20/2016 telah terpenuhi. LinkedIn juga telah menyediakan *Privacy Policy* dalam Bahasa Indonesia. Hal tersebut sebagai bentuk pemenuhan kewajiban LinkedIn yang juga termasuk ke dalam Penyelenggara Sistem Elektronik/PSE yang telah diatur pada Pasal 6 Permenkominfo Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik.

Mengenai kewajiban adanya persetujuan dari pemilik data pribadi atas penggunaan data pribadinya sebagaimana yang diatur pada Pasal 26 ayat (1) UU Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik dan Pasal 14 ayat (3) PP Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, LinkedIn pada *privacy policy*-nya telah menyertakannya pada bagian 5.3 *Lawful Bases for Processing* yang pada intinya menyatakan bahwa LinkedIn hanya akan mengumpulkan, menggunakan, memproses, dan membagikan data pribadi pengguna berdasarkan *consent*/persetujuan, *contract*/kontrak, dan *legitimate interest*/kepentingan yang sah.

Kemudian *Privacy Policy* dari LinkedIn juga telah mengakomodir secara umum mengenai beberapa prinsip-prinsip perlindungan data pribadi sebagaimana yang terdapat pada Pasal 14 PP 71/2019 tentang PSTE. Hal ini dapat dilihat dari bagaimana LinkedIn dalam *Privacy Policy*-nya juga telah secara spesifik menjelaskan mengenai bagaimana mereka memperoleh data pribadi pengguna, bagaimana dan untuk apa saja data pribadi tersebut digunakan (termasuk juga pemenuhan kewajiban bagi LinkedIn selaku PSE sebagaimana yang diatur pada Pasal 12 Permenkominfo 20/2016), serta bagaimana LinkedIn membagikan data pribadi penggunanya (bahkan terdapat pernyataan bahwa LinkedIn akan membagikan data pribadi pengguna kepada afiliasi LinkedIn dan pihak ketiga dalam rangka menjalankan tugasnya). LinkedIn juga telah menjelaskan bahwa mereka telah menggunakan keamanan *two-factor authentication* sebagai penjaminan keamanan atas data pribadi penggunanya.



Selain itu telah dicantumkan pula pada *privacy policy* tersebut mengenai mekanisme penghapusan data pribadi dari sistem LinkedIn yang dapat dilakukan oleh pengguna, baik pengguna secara mandiri yang menghapusnya ataupun dihapus oleh LinkedIn. Maka kewajiban yang dibebankan oleh Pasal 26 ayat (3) dan (4) UU ITE, Pasal 15, Pasal 17, dan Pasal 18 PP 71/2019; Pasal 25 Permenkominfo 20/2016 telah terpenuhi.

Namun, setelah dilakukan analisis, ditemukan bahwa terdapat kewajiban yang belum dipenuhi oleh LinkedIn selaku PSE sebagaimana yang telah diatur di peraturan perundang-undangan di Indonesia, yaitu kewajiban untuk "memberitahukan kepada pemilik data pribadi yang bersangkutan apabila terjadi kegagalan dalam perlindungan terhadap data pribadi yang dikelolanya". Pada *privacy policy*-nya, LinkedIn sama sekali tidak menyertakan pernyataan mengenai adanya pemberitahuan dari LinkedIn apabila terjadi kegagalan dalam melindungi data pribadi penggunanya atau bagaimana mekanisme yang akan dilakukan mereka. Selama ini, LinkedIn hanya akan mengeluarkan *press release* untuk mengklarifikasi mengenai adanya dugaan kegagalan perlindungan data pribadi yang menyebar di masyarakat, bukan kepada pengguna yang bersangkutan secara langsung. Padahal di dalam peraturan perundang-undangan di Indonesia, menjadi kewajiban dari Penyelenggara Sistem Elektronik/PSE untuk memberitahukan kepada pemilik data pribadi yang bersangkutan apabila terjadi kegagalan dalam perlindungan terhadap data pribadi yang dikelolanya.

Kewajiban ini dapat kita lihat pada beberapa pengaturan di Indonesia. Pasal 14 ayat (1) Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggara Sistem dan Transaksi Elektronik memuat prinsip perlindungan data pribadi yang wajib dilaksanakan oleh PSE dalam melakukan pemrosesan data pribadi, salah satunya adalah pemrosesan Data Pribadi dilakukan dengan memberitahukan kegagalan perlindungan data pribadi. Bahkan Pasal 14 ayat (5) pada PP yang sama juga menambahkan bahwa pemberitahuan kepada pemilik data pribadi yang bersangkutan dilakukan secara tertulis.

Pada Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik yakni di Pasal 2 ayat (2) huruf f menyatakan bahwa PSE





harus Itikad baik untuk segera memberitahukan secara tertulis kepada Pemilik Data Pribadi atas setiap kegagalan perlindungan Data Pribadi menjadi salah satu asas dalam perlindungan data pribadi. Kemudian pada Pasal 28 huruf c Permekominfo yang sama juga mengatur mengenai kewajiban PSE untuk memberitahukan secara tertulis kepada Pemilik Data Pribadi jika terjadi kegagalan perlindungan rahasia Data Pribadi dalam Sistem Elektronik yang dikelolanya. Bahkan dalam pasal ini lebih dijabarkan lagi apa yang menjadi ketentuan dalam pemberitahuan tersebut, seperti substansi pemberitahuan harus disertai dengan alasan mengapa kegagalan tersebut bisa terjadi. Akan tetapi terdapat pengecualian bahwa pemberitahuan tentang kegagalan perlindungan data pribadi dapat dilaksanakan melalui media elektronik jika sudah ada persetujuan perihal tersebut sebelumnya.

Kemudian tidak hanya sekedar mengirim saja, tapi PSE harus memastikan bahwa pemberitahuan harus benar-benar diterima oleh Pemilik Data Pribadi apabila kegagalan perlindungan data pribadi tersebut terdapat potensi kerugian bagi pemilik data pribadi tersebut dan maksimal dikirimkan 14 (empat belas) hari setelah diketahui adanya kegagalan perlindungan data pribadi yang dikelola oleh PSE tersebut.

Pemberitahuan tersebut juga hendaknya disampaikan secara jujur apa adanya. Karena apabila Penyelenggara Sistem Elektronik tidak menyampaikan yang sebenarnya apabila terjadi kebocoran data pribadi, maka akan berpotensi timbul masalah kebohongan publik dan melanggar hak atas kejelasan informasi kepada pengguna/konsumen selaku pemilik data pribadi yang bersangkutan.<sup>116</sup>

Melihat betapa pentingnya pemberitahuan untuk pemilik data pribadi terkait kegagalan perlindungan data pribadi oleh PSE, maka seharusnya LinkedIn sebagai salah satu PSE mengatur di dalam *Privacy Policy*-nya mengenai bagaimana mekanisme yang akan digunakan oleh LinkedIn untuk memberitahukan jikalau terjadi kegagalan dalam melindungi data pribadi

<sup>116</sup> Edmon Makarim, Pertanggungjawaban Hukum Terhadap Kebocoran Data Pribadi, 2020, <https://www.hukumonline.com/berita/a/pertanggungjawaban-hukum-terhadap-kebocoran-data-pribadi-1t5f067836b37ef?page=1> (02 Maret 2022)



penggunanya. Namun tidak cukup hanya mencantumkannya saja di *privacy policy*, namun LinkedIn juga harus secara nyata melakukannya.

Pengakomodiran dua kewajiban tersebut menjadi penting karena dengan tidak dicantumkannya pernyataan bahwa pihak platform akan menyampaikan pemberitahuan kepada pengguna apabila terjadi kegagalan pada perlindungan data pribadinya, maka akan terjadi ketidaktahuan pengguna atas apa yang terjadi pada data pribadinya. Padahal sebagaimana yang terdapat pada Penjelasan Pasal 26 ayat (1) UU ITE, menjadi salah satu dari hak pribadi seseorang untuk mengawal akses informasi berkenaan dengan kehidupan pribadi dan data miliknya. Apabila pengguna tidak mengetahui bahwa terjadi kegagalan pada perlindungan data pribadinya, maka pengawasan juga tidak dapat terwujud dengan baik. Selain itu, apabila tidak ada pemberitahuan dari platform bahwa terjadi kegagalan pada perlindungan data pribadinya, maka pengguna tidak dapat segera melakukan tindakan guna mengamankan data pribadinya, misalnya saja segera menutup akun pengguna.

Selain itu, LinkedIn juga tidak secara tersurat menyebutkan mengenai bagaimana dan sejauh apa pertanggungjawaban LinkedIn atas adanya kegagalan perlindungan data pribadi yang dikendalikannya ataupun yang dikelola pihak ketiga, baik untuk kepentingannya sendiri dan diikat oleh kerjasama ataupun dalam rangka untuk menjalankan tugas dari LinkedIn. Padahal bagian 2. *How We Use Your Data* pada *privacy policy* banyak menyebutkan bahwa LinkedIn akan membagikan data pribadi pengguna kepada pihak ketiga; baik pihak ketiga tersebut merupakan pihak yang melakukan riset, entitas yang berafiliasi dengan LinkedIn, ataupun pihak lain yang bekerja sama dengan LinkedIn dalam hal pengembangan layanan.

Bagi penulis, hal ini menjadi penting untuk diperhatikan karena dapat menjadi celah bagi LinkedIn untuk mengelak dari pertanggungjawaban hukum apabila kegagalan perlindungan data pribadi pengguna seperti kebocoran dan lain sebagainya terjadi disebabkan oleh kesalahan dan/atau kelalaian dari pihak ketiga. Terlebih lagi, dalam hal pemanfaatan API, pertukaran data pribadi bisa dikatakan sebagai suatu keniscayaan, dan melihatkan tiga (3) pihak sekaligus; yakni LinkedIn, pihak penyedia API, dan pihak ketiga penerima data pribadi pengguna. Dengan tidak jelasnya sejauh





apa pertanggungjawaban LinkedIn atas adanya kegagalan dalam perlindungan terhadap data pribadi penggunanya yang dikelola oleh pihak ketiga, maka dapat membingungkan bagi pengguna yang akan mengajukan gugatan berkenaan dengan kerugian yang dialami akibat kegagalan perlindungan data pribadi.

Dengan demikian, maka menurut penulis terdapat dua hal penting yang seharusnya diakomodir dan dicantumkan oleh LinkedIn di dalam *Privacy Policy* platform, yakni yang pertama mengenai pernyataan bahwa LinkedIn akan menyampaikan pemberitahuan kepada pengguna apabila terjadi kegagalan pada perlindungan data pribadinya, dan yang kedua mengenai sejauh apa LinkedIn akan bertanggung jawab atas sejauh apa pertanggungjawaban LinkedIn atas adanya kegagalan pada perlindungan data pribadi penggunanya yang dikelola oleh pihak ketiga. Dengan diakomodirnya dua hal yang telah disebutkan sebelumnya, maka perlindungan data pribadi bagi pengguna LinkedIn akan lebih memenuhi asas-asas perlindungan data pribadi sebagaimana yang diamanatkan oleh ketentuan perundang-undangan di Indonesia.

#### **B. Pertanggungjawaban hukum bagi LinkedIn jika terjadi penyalahgunaan data pribadi pengguna akhir (*end-user*) melalui *Application Programming Interface (API)* platform**

Menurut Pasal 1 angka 6 UU 19/2016 menyatakan, "*Penyelenggaraan Sistem Elektronik adalah pemanfaatan Sistem Elektronik oleh penyelenggara negara, Orang, Badan Usaha, dan/atau masyarakat.*"<sup>117</sup> Pasal 1 angka 5 menyebutkan bahwa "*Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan Informasi Elektronik.*"<sup>118</sup> Oleh karena itu, maka dapat kita ketahui bahwa LinkedIn juga termasuk PSE. Hal ini

<sup>117</sup> Pasal 1 angka 6 **Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi Dan Transaksi Elektronik.**

<sup>118</sup> Pasal 1 angka 5 **Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi Dan Transaksi Elektronik.**



karena di dalam mengoperasikan platform-nya, LinkedIn akan menghimpun, mengolah, menganalisis, menyimpan dan mencadangkan, memperlihatkan, memublikasikan, mengirimkan, dan/atau mendistribusikan Informasi Elektronik; termasuk data pribadi penggunanya.

Kewajiban mengenai penyelenggaraan SE secara andal, aman, dan bertanggung jawab tidak hanya diatur pada 1 (satu) ketentuan saja, namun juga pada beberapa ketentuan, yaitu di Pasal 15 ayat (1) UUU ITE, Pasal 3 ayat (1) PP 71/2019 tentang PSTE, juga pada Pasal 9 ayat (1) Permenkominfo 5/2020 tentang PSE Lingkup Privat. Menjadi kewajiban dari Penyelenggara Sistem Elektronik, termasuk LinkedIn, untuk menyelenggarakan sistem elektroniknya secara andal, aman, dan bertanggung jawab.<sup>119</sup> "Andal", maksudnya adalah bahwa sistem elektronik mempunyai kapabilitas yang cocok dengan kebutuhan penggunanya; "aman", memiliki makna bahwa SE yang dilakukan haruslah terlindungi, baik fisik dan nonfisik; sedangkan "bertanggung jawab" maksudnya adalah PSE wajib bertanggung jawab secara hukum atas penyelenggaraan SE yang dilakukannya.<sup>120</sup>

Selanjutnya Pasal 3 ayat (2) PP 71/2019 tentang PSTE mencantumkan bahwa pada dasarnya PSE bertanggung jawab atas penyelenggaraan Sistem Elektroniknya.<sup>121</sup> Namun tanggung jawab tersebut dapat menjadi tidak berlaku apabila dapat dibuktikan adanya keadaan memaksa (*force majeure*) dan/atau adanya kesalahan maupun kelalaian dari pihak pengguna<sup>122</sup> yang menyebabkan sistem tidak dapat beroperasi dan terselenggara sebagaimana mestinya.

Pasal di atas mengandung prinsip *presumption of liability*. Hal ini karena pasal tersebut mengisyaratkan bahwa tiap PSE dianggap selalu bertanggung jawab secara hukum atas kesalahan atau kegagalan yang terjadi pada penyelenggaraan sistem elektroniknya; melainkan bisa

<sup>119</sup> Pasal 3 ayat (1) **Peraturan Pemerintah Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik.**

<sup>120</sup> Penjelasan Pasal 3 **Peraturan Pemerintah Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik.**

<sup>121</sup> Pasal 3 ayat (2) **Peraturan Pemerintah Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik**

<sup>122</sup> Pasal 3 ayat (3) **Peraturan Pemerintah Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik**





dipastikan jikalau kegagalan tersebut terjadi ditimbulkan adanya kesalahan dan/atau kelalaian dari pengguna SE, atau dikarenakan keadaan memaksa. Karena berisi prinsip *presumption of liability*, maka pembuktian dibebankan kepada PSE. Pihak PSE lah yang memiliki kewajiban untuk membuktikan jikalau kegagalan atau kesalahan dalam penyelenggaraan SE tersebut dikarenakan keadaan memaksa ataupun kesalahan dan/atau kelalaian dari pengguna. Hal ini logis, karena tentu tidak mungkin pengguna dapat membuktikan kesalahan seperti apa yang terjadi pada sistem elektronik tersebut, karena sistem tersebut adalah teknologi tinggi (*hi-tech*) yang tidak mungkin dapat dengan mudah diakses dan diketahui serta dipahami bagaimana substansi sistem tersebut sebenarnya.<sup>123</sup>

Oleh karena itu LinkedIn sebagai salah satu Penyelenggara Sistem Elektronik seharusnya dianggap selalu bertanggung jawab secara hukum atas penyelenggaraan sistem elektroniknya, apalagi ketika terjadi peretasan sistem yang menyebabkan tersebarnya data pribadi pengguna di forum peretas/*hacker*. Hal ini karena LinkedIn selaku Penyelenggara Sistem Elektronik dapat dinilai tidak cukup andal, aman, dan bertanggung jawab dalam menyelenggarakan sistem elektroniknya hingga sistem dapat diretas oleh pihak asing. Selain itu, dengan adanya insiden beredarnya data pribadi pengguna LinkedIn untuk dijual pada forum peretas/*hacker*, maka LinkedIn juga dinilai tidak bisa memenuhi kewajibannya sebagai Penyelenggara Sistem Elektronik untuk melaksanakan prinsip perlindungan data pribadi pada saat melakukan pemrosesan data pribadi sebagaimana yang diatur pada Pasal 14 ayat (1) huruf e Peraturan Pemerintah Nomor 71 Tahun 2019, yang menyatakan, "*Pemrosesan data pribadi wajib dilakukan melindungi keamanan Data Pribadi dari kehilangan, penyalahgunaan, Akses dan pengungkapan yang tidak sah, serta pengubahan atau perusakan Data Pribadi;*"<sup>124</sup>

LinkedIn dapat terbebas dari tanggung jawab apabila pihak LinkedIn dapat membuktikan bahwa kegagalan sistem elektronik yang menyebabkan

<sup>123</sup> Gerungan, Carlo A., **Tanggungjawab Penyelenggara Sistem Informasi Jika Terjadi Kegagalan Sistem**, Jurnal Hukum UNSRAT, Volume 21, Nomor 4, 2013, Fakultas Hukum Universitas Sam Ratulangi, Manado, hlm. 46.

<sup>124</sup> Pasal 14 ayat (1) huruf e **Peraturan Pemerintah Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik**





tersebar nya data pribadi pengguna tersebut disebabkan oleh kesalahan dan/atau kelalaian dari pengguna itu sendiri, ataupun terjadi kejadian yang digolongkan *force majeure*. Selain alasan tersebut, maka LinkedIn tetap dianggap bertanggung jawab atas penyelenggaraan sistem elektroniknya, termasuk ketika terjadi kegagalan operasional sistem sebagaimana mestinya.

Kebocoran data pribadi pengguna LinkedIn terjadi karena peretas menyalahgunakan API LinkedIn dengan menggunakan bot untuk mengumpulkan basis data informasi yang besar. Sebagaimana yang dilaporkan 9to5Mac, LinkedIn mengklaim bahwa mereka tak bisa menemukan bukti penyusupan ke server.<sup>125</sup>

Kemudian hal ini memunculkan pertanyaan, siapa yang akan bertanggung jawab atas terjadinya kebocoran data pribadi yang terjadi dengan cara menyalahgunakan API LinkedIn? Pihak Penyedia API, atau Pihak LinkedIn, atau keduanya? Kemudian apakah karena server LinkedIn tidak diretas secara langsung maka LinkedIn terbebas dari pertanggungjawaban atas kebocoran data pribadi penggunanya?

Tanggung jawab hukum muncul sebagai konsekuensi dari adanya hak dan kewajiban yang timbul dari adanya hubungan hukum yang terjadi diantara para pihak. Terdapat 2 (dua) hubungan hukum yang timbul antara LinkedIn, pengguna, serta penyedia API. Yakni yang pertama, terdapat hubungan hukum antara LinkedIn dengan pengguna yang didasarkan pada *user agreement* yang disajikan dalam bentuk *Click-wrap agreement*. Sedangkan hubungan hukum kedua adalah hubungan hukum antara LinkedIn dengan penyedia API yang biasanya didasarkan pada perjanjian kerja sama antara dua pihak tersebut.

Jika kita perhatikan, maka sebenarnya tidak ada hubungan hukum langsung antara Pengguna LinkedIn dengan pihak penyedia API. Namun Pada *Privacy Policy* LinkedIn bagian 3.5 *Service Providers*, LinkedIn menyatakan bahwa mereka akan mengizinkan pihak ketiga yang bekerja sama dengan LinkedIn untuk mengakses informasi pengguna dalam rangka untuk menjalankan tugasnya. Dalam hal ini, maka penyedia *Application*

<sup>125</sup> CNN Indonesia, 2021, **Data Pengguna LinkedIn Bocor, Dijual di Dark Web (online)**, <https://www.cnnindonesia.com/teknologi/20210630130302-185-661303/data-pengguna-linkedin-bocor-dijual-di-dark-web>, (06 Maret 2022)





*Programming Interface* (API) dapat termasuk ke dalam pihak ketiga yang dimaksud pada bagian 3.5 tersebut. Hal ini karena penyedia API menjalankan tugas yang diberikan oleh LinkedIn sebagaimana yang diperjanjikan guna menyediakan *Application Programming Interface* yang akan mempermudah operasional LinkedIn dalam hal *transfer* data dan sistem operasi kepada aplikasi/pihak lain.

Ketika pengguna meng-klik bergabung dengan LinkedIn dan mendaftarkan akun/keanggotaan, atau ketika menggunakan layanan dari LinkedIn, maka secara otomatis pengguna dianggap menyetujui seluruh ketentuan LinkedIn, termasuk bagian 3.5 pada *Privacy Policy*. Dengan disetujuinya ketentuan yang dinyatakan pada bagian 3.5 *Service Providers* pada *Privacy Policy* LinkedIn, maka pengguna dianggap setuju apabila LinkedIn membagikan data pribadi dan informasi mereka kepada pihak ketiga yang bekerja sama dengan LinkedIn. Dengan begitu, maka pemrosesan data pribadi pengguna LinkedIn oleh penyedia API tidak bertentangan dengan Pasal 26 ayat (1) UU 19/2016 karena telah atas persetujuan dari pengguna.

Karena kebocoran data pribadi pengguna LinkedIn terjadi dengan menyalahgunakan API, maka nampaknya pihak penyedia API yang seharusnya dibebankan pertanggungjawaban atas adanya kebocoran data pribadi tersebut. Hal ini karena sistem elektronik yang diretas bukanlah server LinkedIn, namun *Application Programming Interface* yang dibuat oleh penyedia API. API inilah yang dinilai tidak cukup andal, aman, dan bertanggung jawab dalam menyelenggarakan sistem elektroniknya serta dinilai gagal untuk melaksanakan prinsip perlindungan data pribadi pada saat melakukan pemrosesan data pribadi hingga API dapat diretas.

Kemudian, LinkedIn tetap dapat dimintai pertanggungjawaban atas adanya kebocoran data pribadi penggunanya, meskipun server LinkedIn tidak diretas, didasarkan kepada dua hal. Yang pertama adalah bahwa hubungan hukum yang dimiliki oleh pengguna LinkedIn adalah dengan pihak LinkedIn. Pihak yang mengumpulkan dan menerima data pribadi pengguna adalah LinkedIn. Maka sudah seharusnya, menjadi kewajiban LinkedIn untuk menjaga keamanan data pribadi penggunanya dan terhindar dari kehilangan,



penyalahgunaan, Akses dan pengungkapan yang tidak sah, serta perubahan atau perusakan Data Pribadi.

Alasan kedua adalah bahwa pada dasarnya penyedia *Application Programming Interface* sedang melakukan urusan yang ditugaskan oleh LinkedIn kepadanya. API juga dapat melakukan pemrosesan data pribadi pengguna atas izin dari LinkedIn sebagaimana yang telah dinyatakan pada *Privacy Policy* bagian 3.5 *Service Providers*. Berdasarkan prinsip *vicarious liability*, maka seseorang tidak hanya bertanggung gugat berkenaan dengan kerugian yang ditimbulkan oleh PMH yang ditindakan sendiri, tetapi juga bertanggung gugat atas PMH yang ditindakan oleh individu-individu yang menjadi tanggungannya.

Menurut Pasal 1367 KUH Perdata, *vicarious liability* dapat diterapkan pada hubungan orang tua/wali dengan anak-anak yang belum dewasa, majikan dengan pelayannya, guru sekolah dengan murid yang berada di bawah pengawasannya, serta antara kepala tukang dengan tukang-tukangnya. Namun pada kasus *JGE vs English Province of Our Lady of Charity and another* di Inggris, penerapan *vicarious liability* bukan hanya didasarkan atas adanya hubungan ketenagakerjaan (majikan dan pelayan) semata, tetapi juga karena adanya pendelegasian tugas-tugas pengurusan panti asuhan kepada pastur yang berbuat PMH. Karena hubungan antara kedua pihak tersebut seperti layaknya hubungan antara pemberi kerja dan pekerja (*akin of employment*), maka *court of appeal*/pengadilan banding menerapkan prinsip *vicarious liability* pada kasus tersebut.<sup>126</sup>

Kasus ini menjadi salah satu bentuk dari Teori Pendelegasian Tugas (*The Delegation of Task Theory*) sebagai salah satu teori penerapan prinsip *vicarious liability*. Menurut teori ini, prinsip *vicarious liability* dapat diterapkan apabila terdapat pendelegasian tugas, yakni pengalihan tugas yang semula merupakan tugas salah satu pihak diberikan kepada pihak lainnya.<sup>127</sup> Hal ini sama dengan yang terjadi antara LinkedIn dengan penyedia *Application*

<sup>126</sup> Reekie, Adam, 2017, *The Liability of Employers for the Acts of Their Employees: a Comparative Analysis of Section 425 of the Thai Civil and Commercial Code and Vicarious Liability in English Tort Law*, Thammasat Business Law Journal, Volume 7, Faculty of Law Thammasat University, Bangkok, hlm. 3.

<sup>127</sup> Dickinson, Jill dan Alex Nicholson, 2015, *Supreme Court Closes Another Vicarious Liability Loophole: Woodland v Swimming Teachers Association*, European Journal of Current Legal Issues, Volume 21, Nomor 2.





*Programming Interface*. Berdasarkan perjanjian, LinkedIn mengalihkan sebagian urusannya untuk dikerjakan oleh penyedia API. Penyedia API atas perintah LinkedIn menyediakan *Application Programming Interface* yang digunakan oleh LinkedIn untuk membagikan data ataupun sistem operasi yang dimiliki oleh LinkedIn kepada pihak lain sesuai dengan kebutuhan dari LinkedIn.

Maka dari itu, menurut hemat penulis, LinkedIn tetap dapat dimintai pertanggungjawaban atas kesalahan atau kelalaian dari penyedia API yang menyebabkan bocornya data pribadi pengguna didasarkan pada prinsip *vicarious liability*. Akan tetapi penerapan dari prinsip *vicarious liability* kepada LinkedIn bukan berarti meniadakan tanggung jawab dari penyedia API. Penyedia API tetap dibebankan tanggung jawab atas kesalahan atau kelalaian yang dilakukannya, termasuk atas kegagalan perlindungan Data Pribadi.

Pasal 38 Undang-Undang 11/2008 tentang ITE menyatakan bahwa tiap-tiap orang dapat mengajukan gugatan kepada pihak yang menyelenggarakan Sistem Elektronik dan/atau menggunakan Teknologi Informasi yang menyebabkan kerugian.<sup>128</sup> Pasal 32 Permenfominfo 20/2016 tentang Perlindungan Data Pribadi dalam SE juga menyatakan bahwa tiap-tiap Pemilik Data Pribadi dan PSE dapat mengajukan gugatan berkenaan dengan adanya kejadian kegagalan perlindungan rahasia Data Pribadi jikalau upaya penyelesaian sengketa dengan musyawarah atau upaya penyelesaian sengketa alternatif lainnya gagal.<sup>129</sup> Didasarkan kedua pasal itu, dapat diketahui bahwa pengguna bisa mengajukan gugatan kepada PSE, dalam hal ini ialah LinkedIn, atas adanya kegagalan perlindungan data pribadi mereka. LinkedIn dapat digugat karena Perbuatan Melawan Hukum (PMH) dengan dasar adanya kesalahan<sup>130</sup> atau kelalaian<sup>131</sup> yang menyebabkan kerugian.

Selain itu, dengan adanya kebocoran data pribadi yang terjadi pada pengguna LinkedIn, maka LinkedIn dapat dikenai gugatan dengan dasar

<sup>128</sup> Pasal 38 ayat (1) **Undang-Undang Nomor 11 Tahun 2008 tentang Informasi Dan Transaksi Elektronik**

<sup>129</sup> Pasal 32 ayat (1) **Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik**

<sup>130</sup> Pasal 1365 Kitab Undang-Undang Hukum Perdata

<sup>131</sup> Pasal 1366 Kitab Undang-Undang Hukum Perdata





PMH karena LinkedIn tidak memenuhi kewajiban-kewajibannya sebagai PSE yang dibebankan kepadanya menurut peraturan perundang-undangan, yakni:

- 1) Kewajiban di Pasal 15 ayat (1) UU ITE, Pasal 3 ayat (1) PP 71/2019 tentang PSTE, juga pada Pasal 9 ayat (1) Permenkominfo 5/2020 tentang PSE Lingkup Privat yang mewajibkan PSE untuk menyelenggarakan sistem elektroniknya secara andal, aman, dan bertanggung jawab sehubungan dengan beroperasinya sistem elektronik yang dipunyai sebagaimana mestinya;
- 2) Kewajiban di Pasal 3 ayat (2) PP 71/2019 tentang PSTE yang menyatakan bahwa PSE bertanggung jawab atas penyelenggaraan Sistem Elektroniknya; serta
- 3) Kewajiban pada Pasal 14 ayat (1) huruf e PP 71/2019 tentang PSTE yang pada intinya menyatakan bahwa PSE harus melakukan pemrosesan Data Pribadi dengan melindungi dan menjaga keamanan Data Pribadi dari ketiadaan, penyalahgunaan, Akses dan pengungkapan yang tidak sah, serta perubahan ataupun perusakan Data Pribadi.





## BAB IV

### KESIMPULAN

#### A. Kesimpulan

Berdasarkan pembahasan dan penjelasan yang telah diuraikan, didapatkan kesimpulan bahwa:

1. Berdasarkan analisis *privacy policy* LinkedIn dengan pengaturan perlindungan data pribadi di Indonesia, LinkedIn telah memuat beberapa klausula di dalam *privacy policy*-nya dalam rangka pemenuhan prinsip-prinsip perlindungan data pribadi serta kewajibannya sebagaimana yang telah diatur pada beberapa ketentuan perundang-undangan di Indonesia. Akan tetapi LinkedIn belum memenuhi kewajiban untuk "memberitahukan kepada pemilik data pribadi yang bersangkutan apabila terjadi kegagalan dalam perlindungan terhadap data pribadi yang dikelolanya" sebagaimana yang diatur pada Pasal 14 PP 71/2019 tentang PSTE serta Pasal 2 ayat (2) & Pasal 28 Permenkominfo 20/2016 tentang Perlindungan Data Pribadi dalam SE. Selain itu, walaupun pada *Privacy Policy* LinkedIn sudah mencantumkan bahwa mereka akan membagikan data pribadi pengguna di berbagai layanan dan entitas yang berafiliasi dengan LinkedIn, namun belum diatur mengenai apakah LinkedIn tetap memiliki tanggung jawab atas data pribadi pengguna yang telah dibagikan kepada pihak ketiga tersebut.
2. Berdasarkan prinsip *vicarious liability*, LinkedIn dapat dimintai pertanggungjawaban atas adanya kebocoran data pribadi penggunanya walaupun kebocoran tersebut terjadi melalui *Application Programming Interface*. LinkedIn dapat digugat dengan dalil PMH disebabkan adanya kesalahan atau kelalaian yang menimbulkan kerugian serta karena LinkedIn tidak memenuhi kewajiban-kewajibannya sebagai PSE yang dibebankan kepadanya menurut peraturan perundang-undangan, yakni kewajiban di Pasal 15 ayat (1) Undang-Undang Informasi dan Transaksi Elektronik, Pasal 3 ayat (1) Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, juga pada Pasal 9 ayat (1) Permenkominfo Nomor 5 Tahun 2020



tentang Penyelenggara Sistem Elektronik Lingkup Privat; Kewajiban di Pasal 3 ayat (2) Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik; serta kewajiban di Pasal 14 ayat (1) huruf e Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

## B. Saran

1. Hendaknya LinkedIn dapat menyempurnakan *Privacy Policy*-nya dengan menambahkan klausula mengenai mekanisme pemberitahuan kepada pengguna apabila terjadi kegagalan perlindungan data pribadi dan bagaimana pertanggungjawaban pihak ketiga atas penggunaan data pribadi pengguna LinkedIn sehingga perlindungan data pribadi pengguna LinkedIn beserta prinsip-prinsipnya dapat lebih terakomodir.
2. Diharapkan bagi pengguna LinkedIn untuk terlebih dahulu membaca *privacy policy* platform sebelum menggunakan layanan sehingga pengguna dapat mengetahui dan mengawasi sejauh apa perlindungan data pribadi yang sudah dilaksanakan.



## DAFTAR PUSTAKA

### Buku

Ahmadi Miru, **Hukum Perlindungan Konsumen**, Raja Grafindo Persada, Jakarta, 2004.

Abdulkadir Muhammad, **Hukum Perikatan**, Alumni, Bandung, 2002.

-----, **Hukum Perusahaan Indonesia**, Citra Aditya Bakti, Bandung, 2010.

I Made Pasek Diantha, **Metodologi Penelitian Hukum Normatif dalam Justifikasi Teori Hukum**. Kencana, Jakarta, 2017.

Jimly Asshiddiqie dan Ali Safa'at, **Teori Hans Kelsen Tentang Hukum**, Cetakan ke-1, Sekretariat Jenderal & Kepaniteraan Mahkamah Konstitusi RI, Jakarta, 2006.

Made Metu Dahana, **Perlindungan Hukum dan Keamanan Terhadap Wisatawan**, Paramita, Surabaya, 2021.

Peter Mahmud Marzuki, **Penelitian Hukum (edisi revisi)**, Kencana Prenada Media Group, Jakarta, 2013.

R. Setiawan, **Pokok-Pokok Hukum Perdata**, Bina Cipta, 2007

R. Subekti, **Hukum Perjanjian**, Alumni, Bandung, 1979.

Shinta Dewi, **CyberLaw: Aspek Data Privasi Menurut Hukum Internasional, Regional dan Nasional**, Refika Aditama, Bandung, 2015.

Soekidjo Notoatmojo, **Etika dan Hukum Kesehatan**, Rineka Cipta, Jakarta, 2010.

Soerjono Soekanto dan Sri Mahmudji, **Penelitian Hukum Normatif, Suatu Tinjauan Singkat**, Raja Grafindo Persada, Jakarta, 2003.

Sugeng Istanto, **Hukum Internasional**, Cetakan ke-2, Universitas Atma Jaya Yogyakarta, Yogyakarta, 2016.

Zainal Asikin dkk, **Pengantar Hukum Perusahaan**, Prenadamedia Group, Jakarta, 2016.

### Jurnal

Ari Purwadi dkk, ***From Liability Based on Fault Principle towards Presumption of Liability Principle in Medical Disputes***, *Journal*





of *Advanced Research in Law and Economics (JARLE)*, Volume 5, Issue (43), Fall 2019.

Carlo A. Gerungan, **Tanggungjawab Penyelenggara Sistem Informasi Jika Terjadi Kegagalan Sistem.** *Jurnal Hukum UNSRAT*, Vol. 21, No. 4, hlm. 42 – 51, Fakultas Hukum Universitas Sam Ratulangi, Manado, 2013.

Dickinson, Jill dan Alex Nicholson. ***Supreme Court Closes Another Vicarious Liability Loophole: Woodland v Swimming Teachers Association***, *European Journal of Current Legal Issues*, Vol 21, No. 2, *School of Law Queen's University Belfast*, Inggris, 2015.

Fransisca Stefanie Chandra. **Kepuasan Pengguna Jejaring Sosial LinkedIn sebagai Jejaring Sosial yang Berorientasi pada Dunia Bisnis dan Profesional di Indonesia**, *Jurnal E-Komunikasi (online)*, Vol. 5 No. 2, <http://publication.petra.ac.id/index.php/ilmu-komunikasi/article/view/7079> (24 Agustus 2021), Universitas Kristen Petra, Surabaya, 2017.

Guadamuz, A. ***Developing a right to be forgotten***. In: *EU Internet Law: Regulation and Enforcement*. Cham : Springer, pp 59 – 76, 2017.

Krisnadi Nasution. **Penerapan Prinsip Tanggung Jawab Pengangkut Terhadap Penumpang Bus Umum**, *Mimbar Hukum*, Vol. 26, No. 1, 54 – 69, Fakultas Hukum Universitas Gadjah Mada, Yogyakarta, 2014.

Morgan, Philips. ***Recasting Vicarious Liability***, *The Cambridge Law Journal*, Vol. 71, No. 3, Cambridge University Press, Britania Raya, November 2012

Nursapia Harahap. **Penelitian Kepustakaan**, *Jurnal Iqra'*, Vol. 08 No. 01. 2014.

Shilling, Cameron G. ***Privacy and Data Security : New Challenges of the Digital Age***, *New Hampshire Bar Journal*, Amerika Serikat, 2011.

Nur Aini Rakhmawati dkk, **Indonesia's Public Application Programming Interface (API)**, *Jurnal Penelitian Pos dan Informatika* (online), Vol. 9 No. 2, 85 – 96, <http://dx.doi.org/10.17933/jppi.2019.090201> (24 Agustus 2021), Kementerian Komunikasi dan Informatika, Jakarta, 2019.





Reekie, Adam. ***The Liability of Employers for the Acts of Their Employees: a Comparative Analysis of Section 425 of the Thai Civil and Commercial Code and Vicarious Liability in English Tort Law***, *Thammasat Business Law Journal*, Faculty of Law Thammasat University, Vol. 7, 2017.

Soemardjono B. Soedjono, **Hukum Perlindungan Konsumen dalam Transaksi Konsumen di Dunia Maya Tentang Tanggungjawab Produk**. *Ragam Penelitian Mesin*, Vol. 3, No. 2, Universitas Surakarta, Solo, 2014.

Wong, Benjamin. ***Delimiting the concept of personal data after the GDPR***, *Legal Studies*, Volume 39, Issue 3, Cambridge University Press, Britania Raya, September 2019

Jerry, Kang. ***Information Privacy in Cyberspace Transaction***, *Stanford Law Review*, Vol. 50, Issue 4, Stanford, 1998.

#### **Skripsi, Tesis, dan Disertasi**

Galuh Dwi Purnama Putra, ***Bentuk Pertanggungjawaban Hukum Orangtua Terhadap Pelaku Anak Dalam Kasus Kecelakaan Lalu Lintas***, Tesis, Surabaya, Fakultas Hukum Universitas Airlangga, 2015.

Kiki Ristanto, ***Tinjauan Yuridis Pertanggungjawaban Marketplace Online Terhadap Pelanggaran Hak Cipta Berdasarkan Undang-Undang Nomor 28 Tahun 2014 Tentang Hak Cipta***, Skripsi, Batam, Fakultas Hukum Universitas Internasional Batam, 2017.

#### **Peraturan Perundang-Undangan**

Undang-Undang Dasar Negara Republik Indonesia 1945

Kitab Undang-Undang Hukum Perdata

***Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi Dan Transaksi Elektronik***, Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251, Tambahan Lembaran Negara Republik Indonesia Nomor 5952.





*Undang-Undang Nomor 11 Tahun 2008 tentang Informasi Dan Transaksi Elektronik*, Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 8483.

*Peraturan Pemerintah Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik*, Lembaran Negara Republik Indonesia Tahun 2019 Nomor 185, Tambahan Lembaran Negara Republik Indonesia Nomor 6400.

*Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik*, Berita Negara Republik Indonesia Tahun 2016 Nomor 1829.

*Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 5 Tahun 2020 tentang Penyelenggara Sistem Elektronik Lingkup Privat*, Berita Negara Republik Indonesia Tahun 2020 Nomor 1376.

*General Data Protection Regulation 2016/679*

*Data Protection Act 1998*

### **Internet**

BRI API, **Apa Itu API: Pengertian, Cara Kerja, hingga Manfaat API**, <https://developers.bri.co.id/id/news/apa-itu-api-pengertian-cara-kerja-hingga-manfaat-api>, (01 Maret 2022), 2021.

Daniar Supriyadi, **Data Pribadi dan Dua Dasar Legalitas Pemanfaatannya**, <https://www.hukumonline.com/berita/a/data-pribadi-dan-dua-dasar-legalitas-pemanfaatannya-lt59cb4b3feba88/>, (27 Januari 2022), 2017.

Edmon Makarim, **Pertanggungjawaban Hukum Terhadap Kebocoran Data Pribadi**, <https://www.hukumonline.com/berita/a/pertanggungjawaban-hukum-terhadap-kebocoran-data-pribadi-lt5f067836b37ef?page=1>, (02 Maret 2022), 2020.

Ironclad, Inc., **User Agreements 101: What You Need to Know**, <https://ironcladapp.com/journal/contracts/user-agreements/> (13 Maret 2022), 2022.





Kementerian Komunikasi dan Informatika, **Lindungi Data Pribadi, Ada Empat Unsur Penting Pengaturan RUU PDP,**

[https://www.kominfo.go.id/content/detail/27503/lindungi-data-pribadi-ada-empat-unsur-penting-pengaturan-ruu-pdp/0/artikel,](https://www.kominfo.go.id/content/detail/27503/lindungi-data-pribadi-ada-empat-unsur-penting-pengaturan-ruu-pdp/0/artikel)

2020.

LinkedIn, **An update on report of scraped data,**

<https://news.linkedin.com/2021/june/an-update-from-linkedin> (24 Agustus 2021), 2021.

LinkedIn, **API Concepts,** [https://docs.microsoft.com/en-](https://docs.microsoft.com/en-us/linkedin/shared/api-guide/concepts?context=linkedin/consumer/context)

[us/linkedin/shared/api-guide/concepts?context=linkedin/consumer/context](https://docs.microsoft.com/en-us/linkedin/shared/api-guide/concepts?context=linkedin/consumer/context) (02 September 2021), 2021.

LinkedIn, **Authenticating with OAuth 2.0 Overview,**

<https://docs.microsoft.com/en-us/linkedin/shared/authentication/authentication?context=linkedin/consumer/context> (02 September 2021), 2021.

LinkedIn, **LinkedIn Consumer Solutions Platform,**

<https://docs.microsoft.com/en-us/linkedin/consumer/> (02 September 2021), 2021.

McCormick, Michelle, **New Privacy Legislation** (online),

<http://www.ica.bc.ca> (24 Agustus 2021). 2021.

Merriam-Webster, Diterjemahkan dari [http://www.merriam-](http://www.merriam-webster.com/dictionary/Internet)

[webster.com/dictionary/Internet](http://www.merriam-webster.com/dictionary/Internet) (24 Agustus 2021)

Red Hat, Inc., **What is a REST API?**

<https://www.redhat.com/en/topics/api/what-is-a-rest-api> (02 September 2021), 2020.

Sven Taylor, **New LinkedIn Data Leak Leaves 700 Million Users**

**Exposed,** <https://restoreprivacy.com/linkedin-data-leak-700-million-users/> (24 Agustus 2021), 2021.

TomLiner, **SELLING LinkedIn 1 Billion (1000Million) Record,**

<https://raidforums.com/Thread-SELLING-LinkedIn-1Billion-1000Million-Record> (01 Januari 2022)

We are Social, **Digital 2021** (Online), <https://wearesocial.com/digital-2021>

(24 Agustus 2021), 2021.





### Lain-Lain

3 scale, What is an API? Your guide to the Internet Business (R)evolution, 3scale Networks S.L., Barcelona, 2011.

Direktorat Jenderal IKP, Kementerian Komunikasi Dan Informatika, Dan *Cyberlaw Centre* Fakultas Hukum Univaersitas Padjadjaran, *Naskah Akademik RUU Perlindungan Data Pribadi (Penyelarasan)*, Badan Pembinaan Hukum Nasional, 2016.

Kamus Besar Bahasa Indonesia.

Rancangan Undang-Undang Perlindungan Data Pribadi.





