

# **BAB I**

## **PENDAHULUAN**

### **1.1 Latar Belakang**

Indonesia bersama dengan ratusan negara di dunia telah memasuki era revolusi industri 4.0 dimana teknologi internet digunakan secara masif dan menjadi kebutuhan bagi seluruh masyarakat dalam melangsungkan kegiatan sehari-hari. Kehadiran revolusi industri 4.0 di Indonesia sendiri merupakan hal yang tidak dapat dibantahkan maupun ditunda, hal ini dikarenakan tingkat perkembangan TIK (Teknologi Informasi dan Komunikasi) semakin canggih serta dikehendaknya proses digitalisasi secara meluas oleh pemerintah, sebagaimana pemerintah mengenalkan istilah Dilan yakni “Digital Melayani”<sup>1</sup> dalam memberikan pelayanan publik yang diwujudkan dengan beberapa hal dimulai dengan hal sederhana seperti proses pendaftaran antrian puskesmas hingga pelayanan pelaksanaan hak tanggungan secara elektronik. Tindakan pemerintah tersebut merupakan salah satu wujud keseriusan pemerintah untuk melazimkan teknologi digital ditengah kehidupan masyarakat luas yang berasal dari berbagai latar belakang golongan, tentunya kebijakan tersebut sejalan dengan kehidupan mayoritas masyarakat yang perlahan menjadi praktis dan

---

<sup>1</sup>Agus Budiawan, “Menuju Pemerintahan Digital”,  
<https://www.djkn.kemenkeu.go.id/artikel/baca/13266/Menuju-Pemerintahan-Digital.html>, diakses pada 25 Oktober 2020 pukul 14.15 WIB

efisien dengan mengandalkan teknologi. Namun proses digitalisasi tidak hanya berkembang pada sektor publik saja, ruang lingkup privat baik individu maupun badan usaha telah melakukan gebrakan digital terlebih dahulu dengan berbagai macam inovasi teknologi berupa benda seperti *smartphone* dan komputer tablet, hingga pembuatan sistem elektronik yang menjadi fitur dalam *smartphone* ataupun komputer para penggunanya.

Sistem elektronik sendiri merupakan sebuah raga dari segala kegiatan manusia dalam melakukan kegiatan elektronik, hal ini dikarenakan sistem elektronik memiliki beragam fungsi terhadap informasi elektronik yang dipunya, apakah sistem tersebut dipergunakan untuk mengumpulkan informasi saja, mengirimkan informasi, ataupun mengolah informasi yang dipunya. Buah karya manusia dalam menciptakan sistem elektronik yang umum diketahui ialah pembuatan situs maupun aplikasi, dimana kedua hal tersebut senantiasa digunakan oleh masyarakat luas untuk melakukan berbagai hal seperti mencari informasi, bersosialisasi maupun melakukan kegiatan jual-beli. Kedua jenis sistem elektronik tersebut merupakan amat dikenal dimasyarakat dikarenakan baik situs maupun aplikasi mudah untuk diakses menggunakan internet, bahkan beberapa jenis aplikasi seluler (*mobile application*) tidak memerlukan bantuan internet untuk diakses sehingga dengan mudah dapat dijangkau untuk seluruh orang hanya dengan bermodalkan *smartphone*.

Sebagian besar masyarakat Indonesia merupakan pengguna internet aktif dimana pada tahun 2021 sejumlah 202.6 juta jiwa masyarakat Indonesia dari 274,9 juta jiwa merupakan pengguna aktif internet, dari jumlah tersebut 195.3 juta jiwa penduduk Indonesia mengakses internet dengan perangkat *mobile*,<sup>2</sup> data tersebut menunjukkan bahwa banyak masyarakat lebih nyaman mengakses internet menggunakan *smartphone* dikarenakan lebih praktis dan mudah untuk digunakan oleh banyak kalangan. Salah satu sistem operasi paling dikenal di Indonesia dan dunia ialah Android, sistem operasi Android hadir didalam berbagai macam merek *smartphone* maupun *tablet* yang dibangun dengan fitur menarik dan mudah untuk digunakan oleh berbagai kalangan. Disaat menggunakan perangkat berbasis sistem Android maka pengguna akan disuguhkan berbagai aplikasi yang dengan sendirinya terdapat pada ponsel, selain itu pengguna *smartphone* berbasis Android dapat mengunduh berbagai macam aplikasi lain yang menarik melalui fitur Google Play Store.

Google Play Store sendiri menyajikan berbagai macam konten aplikasi yang dibuat oleh beragam pihak yang mengembangkan konten aplikasi seperti aplikasi mengedit foto dan permainan yang bersifat hiburan, pinjaman *online* atau *fintech* yang merupakan aplikasi keuangan, ataukah berbagai macam aplikasi *e-commerce* atau toko *online* yang memudahkan masyarakat bertransaksi

---

<sup>2</sup> Simon Kemp, “ Digital 2021 : Indonesia”, <https://datareportal.com/reports/digital-2021-indonesia>, diakses pada 10 Juli 2021 Pukul 19.20 WIB

jual-beli secara instan tanpa perlu bertatap muka. Kegiatan yang semula memerlukan keterlibatan ataukah bantuan orang lain dalam bentuk fisik beralih tergantikan dengan bantuan aplikasi yang berbasis teknologi, hal tersebut menjadikan suatu dinamika kehidupan berupa kemudahan dalam melakukan berbagai hal yang telah menjadi gaya hidup masyarakat.

Sebagaimana dipahami kehidupan dunia digital telah mencapai era *big data* dimana dunia menghadapi lonjakan jumlah data elektronik secara luar biasa yang dapat dimanfaatkan untuk berbagai tujuan. Perusahaan yang menjadi pelopor pemberdayaan data ialah Google yang menggunakan data penggunanya untuk memilihkan konsep yang relevan terhadap iklan untuk penggunanya sehingga target pemasaran sesuai dengan tujuan dan mempermudah pengguna sebagai target konsumen perusahaan atau barang yang diiklankan. Bentuk pemanfaatan data oleh Google tersebut merupakan bentuk pemanfaatan yang positif baik dari pihak yang ingin memasang iklan maupun pengguna, namun terdapat resiko lain atas pemanfaatan data pribadi jika tidak dikelola secara hati-hati.

Faktor keamanan yang menjadi perhatian ialah keamanan dari data yang dihimpun oleh aplikasi tertentu yang mensyaratkan pencantuman berbagai data pribadi seperti nama, alamat *e-mail*, nomor telepon, alamat, ataupun data nomor rekening bank jika melakukan transaksi pembayaran pada aplikasi *e-commerce*. Pencantuman beberapa data pribadi tersebut memiliki berbagai risiko tinggi terkait pelanggaran data (*data breach*) seperti kebocoran data kepada dunia luas

baik sengaja maupun tidak sengaja ataukah pemanfaatan data yang tidak sesuai dengan tujuan awal dihimpunnya data tersebut.

Permasalahan terkait keamanan data pribadi di Indonesia dan dunia cukup banyak terjadi, salah satunya di Indonesia pada aplikasi Cermati yang merupakan aplikasi teknologi finansial mengalami kebocoran data yang dilakukan oleh pihak eksternal untuk dijual.<sup>3</sup>Penyalahgunaan data tidak hanya dapat terjadi pada aplikasi milik perusahaan *start up* saja tetapi juga dapat terjadi pada aplikasi milik perusahaan dunia, Facebook sebagai pelopor media sosial pada awal tahun 2018 mengakui bahwa terjadi pemanfaatan informasi data privasi pengguna dengan memberikan informasi pengguna pada konsultan politik Cambridge Analytica untuk dapat menargetkan iklan kampanye yang disesuaikan berdasarkan profil psikologis pengguna Facebook dan dituntut dengan denda senilai \$5.000.000.000,- (lima miliar dollar).<sup>4</sup> Selain itu kejadian yang cukup baru terjadi terkait keamanan data pribadi dialami oleh aplikasi Zoom dimana pada bulan April 2020 aplikasi tersebut dinilai memiliki celah besar terjadinya pelanggaran data pribadi penggunanya, dimana pakar keamanan siber data Pratama Persadha mengkhawatirkan terjadinya praktik penyalahgunaan data

---

<sup>3</sup> Bill Clinton, "Data Pengguna Aplikasi Pinjaman Online Cermati.com Disebut Bocor dan Dijual di Internet", <https://tekno.kompas.com/read/2020/11/02/08050067/>, diakses pada 14 November 2020 pukul 11.25 WIB

<sup>4</sup> Christine Cridle, "Facebook sued over Cambridge Analytica data scandal", <https://www.bbc.com/news/technology-54722362>, diakses pada 14 November 2020 pukul 11.40 WIB

pemetaan wajah. Data pemetaan wajah tersebut dikhawatirkan digunakan untuk dapat membuka sandi perangkat elektronik dengan wajah.<sup>5</sup>

Pemerolehan rasa aman dalam pemakaian suatu aplikasi harus didapatkan oleh pengguna saat menggunakan aplikasi tersebut, salah satunya ialah dengan cara mencantumkan secara jelas bagaimana data yang diperoleh akan digunakan yang dituliskan dalam bentuk kebijakan privasi ataukah *privacy policy*. Hadirnya kebijakan privasi tersebut sebagai bentuk pengakuan pengembang aplikasi dengan dilindunginya data pengguna saat mencantumkan informasi pribadinya sebagaimana amanat dalam Pasal 3 Ayat (1) Peraturan Pemerintah No 71 Tahun 2019 yakni, setiap penyelenggara sistem elektronik harus menyelenggarakan sistem elektronik secara andal dan aman serta bertanggung jawab terhadap beroperasinya sistem elektronik sebagaimana mestinya. Kenyataan yang terjadi tidak semua pengembang aplikasi memerhatikan hal tersebut, dimana masih ditemukan pengembang aplikasi yang tidak mencantumkan kebijakan privasi ataupun tidak menyelenggarakan aplikasi yang memenuhi standar keamanan pengguna sehingga pengguna tidak mendapatkan jaminan atas keamanan informasi data pribadinya yang seharusnya ia peroleh sebagai hak yang patut didapatkan. Fenomena ini menjadi perhatian utama penulis untuk melakukan penelitian yang dituangkan kedalam bentuk penelitian dengan judul

---

<sup>5</sup>Rizky Karo Karo dan Teguh Prasetyo.. *Pengaturan Perlindungan Data Pribadi di Indonesia : Perspektif Teori Keadilan Bermartabat*. Bandung : Nusa Media. 2020. Hlm. 168

## **“TINJAUAN YURIDIS PERBUATAN MELANGGAR HUKUM (PMH) PENYALAHGUNAAN DATA PRIBADI DI GOOGLE PLAY STORE”**

### **1.2 Rumusan Masalah**

- 1 Bagaimana kriteria perbuatan melanggar hukum (PMH) terkait penyalahgunaan data pribadi?
- 2 Bagaimana upaya penyelesaian sengketa bagi pengguna aplikasi pada Google Play Store yang mengalami penyalahgunaan data pribadi?

### **1.3 Tujuan Penelitian**

1. Untuk mengetahui bentuk perbuatan melanggar hukum (PMH) yang dialami oleh pengguna aplikasi di Google Play Store terkait keamanan data pribadi pengguna.
2. Untuk mengetahui mekanisme penyelesaian sengketa yang dialami oleh pengguna aplikasi di Google Play Store terkait keamanan data pribadi pengguna.

### **1.4 Manfaat Penelitian**

Melalui proposal penelitian ini diharapkan dapat memberikan manfaat baik secara teoritis maupun praktis, yakni :

#### **1. Manfaat Teoritis**

Diharapkan dengan adanya penulisan proposal ini dapat dijadikan sebagai kajian tambahan dalam memahami hukum terkait data pribadi di Indonesia, khususnya mengenai perlindungan hukum terhadap data pribadi pengguna konten aplikasi.

## 2. Manfaat Praktis

Diharapkan dengan adanya penulisan proposal ini dapat diketahui bagaimana bentuk perlindungan hukum terkait data pribadi di Indonesia serta memberi manfaat bagi pelaku usaha yang ingin melakukan tahap digitalisasi melalui pembuatan aplikasi, pengguna konten aplikasi *mobile*, kawan pelajar yang sedang menekuni program studi ilmu hukum, serta masyarakat secara umum.

## 1.5 Kajian Pustaka

### 1.5.1 Data Pribadi

#### 1.5.1.1 Klasifikasi data pribadi

Cangkupan pembahasan mengenai privasi terdiri dari dua hal yakni data dan juga informasi, data merupakan fakta berupa symbol, gambar, kata, huruf maupun angka yang menunjukkan suatu ide maupun objek tertentu. Sedangkan informasi dipahami sebagai penerangan dari data yang telah melalui proses pemrosesan yang memiliki arti nilai nyata bagi penerima<sup>6</sup>. Berdasarkan pemahaman atas konsep tersebut dapat diketahui mengenai data pribadi, yakni informasi yang dapat dilihat, didengar, maupun dibaca mengenai seseorang ataukah badan hukum yang dimana informasi tersebut ditampung dalam sistem elektronik dengan maksud untuk digunakan sesuai

---

<sup>6</sup>Shinta Dewi . *Cyber Law 1 : Perlindungan Privasi Atas Informasi Pribadi dalam E-Commerce Menurut Hukum Internasional*. Bandung : Widya Padjadjaran. 2009. Hlm.36

tujuan yang disepakati sebelumnya.<sup>7</sup>Data pribadi memuat informasi yang memiliki nilai pribadi bagi pemiliknya, menurut Simson Garfunkel Informasi pribadi diklasifikasikan kedalam 5 jenis, antarlain:

1. *Personal Information*

Merupakan informasi yang berkaitan dengan informasi pribadi seseorang secara generic semisal nama, tanggal lahir, umur, dan nama orang tua.

2. *Private Information*

Merupakan informasi yang berkaitan dengan informasi seseorang yang tidak diketahui secara umum semisal catatan perbankan dan transkrip akademik.

3. *Personally Identifiable Information*

Merupakan informasi yang telah disimpulkan oleh seseorang berupa kebiasaan ataupun hal yang digemari.

4. *Anonymized Information*

Merupakan informasi yang telah ditransformasi sedemikian rupa sehingga informasi yang diperoleh bukan informasi yang sebenarnya.

5. *Aggregate Information*

Merupakan gabungan dari beberapa informasi individu.<sup>8</sup>

#### 1.5.1.2 Pengaturan data pribadi di Indonesia

---

<sup>7</sup>Rizky Karo, *op.cit.*Hlm. 4

<sup>8</sup>Shinta Dewi, *op.cit.*,Hal 38.

Perlindungan atas data pribadimerupakan perlindungan atas hak pribadi (*privacy rights*) seseorang, dimana hak pribadi sendiri berdasarkan penjelasan Pasal 26 Ayat (1) Undang-Undang Informasi dan Transaksi Elektronik Tahun 2008 sebagai hak untuk menikmati kehidupan yang bebas dari segala macam gangguan, hak untuk berkomunikasi dengan orang lain tanpa adanya tindakan memata-matai maupun hak untuk mengawasi akses informasi tentang kehidupan pribadi seseorang. Data pribadi milik masyarakat Indonesia yang berkaitan dengan kependudukan layaknya NIK, E-KTP maupun KK memiliki arti yang sangat penting sehingga wajib dilindungi dari segala bentuk penyalahgunaan data seperti *profiling*, tindakan spionase ataukah tujuan perdagangan. Atas hal tersebut ketersediaan aturan sebagai tindakan pengamanan atas data pribadi sangat diperlukan.<sup>9</sup>

Secara garis besar data pribadi di Indonesia diatur dalam Undang-Undang No 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang No 8 Tahun 2011 Tentang Informasi dan Transaksi Elektronik (UU ITE) dan dibahas lebih lanjut dalam instrumen hukum berupa Peraturan Pemerintah seperti Peraturan Pemerintah No 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP STE) dan Peraturan Menteri seperti Peraturan Menteri Komunikasi dan Informatika Nomor 7 Tahun 2018

---

<sup>9</sup>Lia Sautunnida.2018. “Urgensi Undang-Undang Perlindungan Data Pribadi di Indonesia : Studi Perbandingan Hukum Inggris dan Malaysia”.  
<http://www.jurnal.unsyiah.ac.id/kanun/article/view/11159>, *Kanun Jurnal Ilmu Hukum*, Vol.20 No. 2. Hlm. 370. Diakses pada tanggal 12 November 2020 Pukul 19.25 WIB.

Tentang Pelayanan Perizinan Berusaha Terintegrasi Secara Elektronik Bidang Komunikasi dan Informatika. Pengaturan mengenai data pribadi di Indonesia tersebut masihlah bersifat umum dimana data pribadi masih dibahas secara *general* dan tidak diatur secara komprehensif dimana peraturan tersebut masih terletak pada peraturan perundang-undangan yang berbeda dan tidak menjadi suatu kesatuan.<sup>10</sup>

Data pribadi milik pengguna yang hendak melakukan transaksi elektronik diberikan jaminan perlindungan oleh hukum, dimana data tersebut bersifat konfidensial dimana informasi tersebut hanya dapat diketahui oleh kedua belah pihak (pengirim dan penerima) dan penggunaan data pribadi tersebut haruslah melalui persetujuan pemilik data terlebih dahulu. Jikalau terdapat pelanggaran atas hal tersebut maka pemilik dapat mengajukan gugatan hukum sesuai apa yang ditegaskan dalam Pasal 26 Ayat (2) Undang-Undang ITE.<sup>11</sup>

#### 1.5.1.3 Pengaturan data pribadi di Eropa

Privasi sebagai hak dasar manusia sangat dilindungi terutama dalam negara-negara di Eropa dan dianggap sebagai salah satu hak dasar dalam Hak Asasi Manusia. Hal ini dapat dilihat dengan diadakannya Konvensi Eropa Tentang Hak Asasi Manusia (*European Convention of Human Rights*) yang

---

<sup>10</sup>*Ibid*, hlm. 381

<sup>11</sup>Dhanang Widijawan.. *E-Logistic Contract : Tanggung Jawab Pelaku Usaha Terhadap Malfunction, Keamanan Siber, dan Data Pribadi*. Bandung : Keni Media. 2017. Hlm. 36.

diadakan pada tahun 1950, dimana pada Pasal 8 ditekankan bahwa pemerolehan hak tiap manusia untuk mendapatkan pengakuan terhadap kehidupan pribadinya termasuk dengan kehidupan rumah tangganyamerupakan hak yang tidak dapat dicampurtangani oleh pemerintah.<sup>12</sup>

Perkembangan pengaturan mengenai data pribadi pada tahun 1995 mengalami pengkhususan lebih lanjut dengan pengadaan instrumen ataukah *directive* terkait perlindungan data pribadi yakni *The Data Protection Directive on The Protection of Individuals with Regard to The Processing of Personal Data and The Free Movement of Such Data(The General Directive)*.*Directive* tersebut selanjutnya disebut dengan *The General Directive* menegaskan keberadaan data privasi sebagai bagian dari hak asasi manusia sehingga perlu diatur lebih lanjut, salah satu pengaturan penting dalam *directive* tersebut ialah 6 prinsip kualitas data yakni :

1. Prinsip adil dan sah (*fair and lawfully*)

Prinsip tersebut menekankan bahwa data harus dikumpulkan, diproses, atau digunakan secara adil dan sah dimana data yang diperoleh haruslah sesuai peruntukannya sesuai dengan maksud tujuan semula.

2. Prinsip minimalitias(*minimality*)

---

<sup>12</sup>Shinta Dewi,op.cit. Hlm.27.

Prinsip tersebut menekankan bahwa akses terhadap data pribadi haruslah seminimal mungkin yakni hanya sesuai dengan tujuan awal semula dan setelahnya data tersebut harus segera dihapus,

3. Prinsip pembatasan tujuan (*purpose limitation*)

Prinsip tersebut menekankan bahwa data pribadi yang diperoleh dan dikumpulkan haruslah layak, relevan dan hanya untuk tujuan tertentu yang sah secara langsung berkaitan dengan fungsi pengelola data,

4. Prinsip akurat dan selalui diperbarui (*accurate and kept up to date*)

Prinsip tersebut menekankan bahwa pemilik data haruslah dapat memeriksa kembali data yang diberikan berkaitan dengan akurasi maupun relevansi data sesuai dengan perkembangan.

5. Prinsip pengawasan dari pemilik data (*data subject participation and control*)

Prinsip tersebut menekankan bahwa data pribadi yang dikumpulkan sesuai dengan maksud tertentu tidak dapat dikelola untuk persetujuan lain tanpa disertai persetujuan pemilik data.

6. Prinsip integritas dan kerahasiaan (*Integrity and confidentiality*)

Prinsip tersebut menekankan bahwa kerahasiaan data pribadi yang telah dikumpulkan harus dijunjung tinggi dan data tersebut tidak boleh dibuka tanpa persetujuan pemilik data, jika pengungkapan data diperlukan maka harus disesuaikan dengan tujuan pengumpulan data semula.<sup>13</sup>

---

<sup>13</sup>Shinta Dewi. *Cyber Law 2 : Praktik Negara-Negara dalam Mengatur Privasi dalam E-Commerce*. Bandung : Widya Padjadjaran. 2009. Hlm. 35-38.

*The General Directive* memberikan kebebasan bagi negara-negara anggota Uni Eropa untuk menafsirkan cakupan arahan isi dari *directive* tersebut sehingga penerapannya tidak seragam antar satu negara dengan negara lainnya yang tergabung dalam Uni Eropa. Hal tersebut menumbuhkan adanya keinginan baru untuk mengharmonisasikan regulasi mengenai perlindungan data privasi, sehingga pada tahun 2018 *The General Directive* resmi digantikan dengan GDPR yang merupakan singkatan dari *General Data Protection Regulation*. GDPR diterapkan sebagai regulasi yang menyelaraskan hukum privasi informasi di Uni Eropa dan disepakati seluruh negara anggota sehingga menjadi suatu unifikasi hukum. GDPR selain berlaku untuk subjek hukum di Eropa jugalah berlaku kepada perusahaan di luar Eropa yang menawarkan barang maupun jasa di Uni Eropa sehingga GDPR dikatakan memiliki pengaruh *extra territorial* dari wilayah negara Uni Eropa<sup>14</sup>

### 1.5.2 Perbuatan Melanggar Hukum (PMH)

#### 1.5.2.1 Pengertian Perbuatan Melanggar Hukum

Perbuatan melanggar hukum (*onrechtmatige daad*) merupakan terminologi yang dapat ditemukan dalam Pasal 1365 Kitab Undang-Undang Hukum Perdata dimana tiap orang yang merugikan orang lain

---

<sup>14</sup> Mark Burdon..*Digital Data Collection and Information Privacy Law*. Amerika Serikat : Cambridge University Press. 2020. Hlm. 147.

dengan melakukan perbuatan melanggar hukum diwajibkan untuk mengganti kerugian yang dialami. Makna dari perbuatan melawan hukum mulanya hanya terbatas pada perbuatan-perbuatan yang melanggar undang-undang ataupun hak subjektif orang lain saja, namun seiring berjalannya waktu istilah tersebut mengalami perluasan makna dimana sejak adanya putusan tertanggal 31 Januari 1919 *Hoge Road* memberikan pengertian lebih luas atas istilah *onrechtmatige daad*, dimana tidak saja merupakan perbuatan yang melanggar hukum ataupun orang lain melainkan juga terhadap perbuatan yang bertentangan dengan kepatutan yang dianggap pantas oleh lingkungan pergaulan masyarakat. Perluasan makna tersebut memberikan perlindungan bagi banyak perbuatan untuk dapat digugat pada pengadilan asalkan dapat dibuktikan timbulnya kerugian atas perbuatan yang dilakukan.<sup>15</sup>

#### 1.5.2.2 Unsur Perbuatan Melanggar Hukum

Berdasarkan ketentuan dalam Pasal 1365 Kitab Undang-Undang Hukum Perdata perbuatan melanggar hukum wajib memenuhi unsur sebagai berikut :

1. Adanya suatu perbuatan

Perbuatan yang dimaksudkan meliputi perbuatan dalam arti aktif yakni berbuat sesuatu maupun dalam arti pasif yakni

---

<sup>15</sup> Subekti, *Pokok-Pokok Hukum Perdata*, Jakarta : PT Intermasa, 2003, Hlm. 133

tidak berbuat sesuatu seperti tidak mengindahkan kewajiban yang timbul dari ketentuan hukum yang ada.

2. Perbuatan merupakan perbuatan melanggar hukum

Istilah perbuatan melanggar hukum sejak adanya putusan pada tahun 1919 telah mengalami perluasan makna, adapun perbuatan melanggar hukum tersebut meliputi perbuatan yang melanggar undang-undang, perbuatan yang melanggar hak orang lain, perbuatan yang bertentangan dengan kewajiban hukum pelaku, perbuatan yang bertentangan dengan kesusilaan dan perbuatan yang bertentangan dengan sikap baik dalam lingkungan masyarakat.

3. Terdapat kesalahan

Unsur kesalahan (*schuldelement*) menjadi syarat wajib untuk dapat diklasifikasikan dalam perbuatan melanggar hukum, dimana kesalahan tersebut harus memenuhi syarat adanya kesengajaan atau adanya kelalaian (*culpa*) yang dimana kesengajaan atau kelalaian tersebut tidak terdapat alasan pembenar diantaranya seperti *force majeure*, membela diri dan sakit jiwa.

4. Terdapat kerugian

Kerugian yang timbul atas suatu perbuatan melanggar hukum meliputi kerugian materiil seperti biaya yang dirugikan maupun

imateeril seperti ketakutan dan rasa kecewa, hal ini menjadi pembeda dengan kerugian akibat wanprestasi yang hanya mengenal kerugian materiil saja.

5. Terdapat hubungan kausal antar perbuatan dengan kerugian

Hubungan kausal antar perbuatan dengan kerugian yang dialami memiliki arti bahwa perbuatan seseorang menjadi sebab atas kerugian orang lain dikarenakan kerugian tidak akan terjadi tanpa penyebab.<sup>16</sup>

### 1.5.3 *Privacy Policy*

#### 1.5.3.1 Penyediaan *Privacy Policy*

*Privacy Policy* ataukah yang dikenal dengan sebutan kebijakan privasi di Indonesia merupakan salah satu jenis sertifikat keandalan yang memberikan jaminan keandalan berupa kepastian atas perlindungan data pribadi konsumen agar dilindungi kerahasiaannya sebagaimana mestinya sesuai dengan penjelasan Pasal 76 Ayat (1) Huruf C Peraturan Pemerintah No 71 Tahun 2019. *Privacy Policy* jugalah dapat diadakan dengan *sistem self-regulation* atau upaya sepihak yang dapat dilakukan oleh penyelenggara sistem elektronik yang melakukan layanan melalui media internet. Namun dalam praktiknya masih banyak ditemukan

---

<sup>16</sup> Nudirman Munir, *Pengantar Hukum Siber Indonesia*, Depok : PT Rajagrafindo Persada, 2017, Hlm. 405-408

penyelenggara sistem elektronik dibidang portal web maupun perangkat digital lain tidak menyantumkan *privacy policy* sehingga memungkinkan kedepannya kepentingan pengguna akan dirugikan.<sup>17</sup>

Praktik penggunaan *privacy policy* bagi bisnis maupun organisasi publik ataukah swasta tidak perlu menunggu dorongan dari pemerintah untuk menampilkan kebijakan privasi dihalaman beranda situs ataukah aplikasi, dikarenakan OECD (*Organisation for Economic Co-operation and Development*) telah memberikan alat dalam bentuk situs yang dapat mempermudah bagi pihak-pihak yang berkepentingan untuk membuat *privacy policy*-nya sendiri.<sup>18</sup>

#### 1.5.3.2 Ketentuan Pembuatan *Privacy Policy*

Upaya yang dapat dilakukan pihak penyedia situs ataukah aplikasi untuk memberikan informasi apakah terdapat data pribadi pengguna yang dikumpulkan maupun digunakan ialah melalui penyediaan kebijakan privasi (*privacy policy*), syarat dan ketentuan (*terms and conditions*) serta label digital.<sup>19</sup> Adapun penyediaan *privacy policy* sendiri haruslah mencerminkan prinsip yang telah disepakati bersama untuk dunia

---

<sup>17</sup> Agus Bud Riswandi.. “Perlindungan Hukum Terhadap Privacy di Internet”. <https://www.yumpu.com/id/document/read/36582968/perlindungan-hukum-terhadap-privacy-di-internet-database->, *Fenomena : Jurnal Penelitian Sosial*, Vol. 3 No. 2. Hlm. 103. Diakses pada tanggal 14 November 2020 Pukul 14.00. 2005

<sup>18</sup>Tim, Penyusun.. *Privacy Online : OECD Guidance on Policy and Practice*. Prancis : OECD Publications. 2003. Hlm. 16

<sup>19</sup>*Ibid*, hlm 91

internasional oleh OECD (*Organisation for Economic Co-operation and Development*) sejak 1998, yakni :

1. Pembatasan penghimpunan (*Collection Limitation*), dimana harus terdapat pembatasan mengenai data apa saja yang dihimpun;
2. Kualitas data (*Data quality*), dimana data yang dihimpun haruslah sesuai dengan tujuan penghimpunan, akurat, tetap utuh dan terbaru;
3. Pengkhususan tujuan (*Purpose specification*), dimana data yang ditujukan untuk dihimpun haruslah sesuai dengan tujuan yang disepakati dan tidak digunakan untuk tujuan lainnya.;
4. Pembatasan penggunaan (*Use limitation*), dimana data tidak boleh diungkapkan, disediakan atau digunakan untuk tujuan selain yang ditentukan sesuai dengan tujuan awal kecuali:mendapatkan persetujuan subjek data atau demi kepentingan hukum;
5. Perlindungan keamanan (*Security safeguards*), dimana data haruslah dilindungi dengan keamanan yang memadai dari segala risiko keamanan seperti kehilangan data atautkah adanya akses yang tidak dikehendaki;

6. Keterbukaan (*Openness*), dimana data yang dihimpun haruslah didampingi dengan informasi keterbukaan mengenai keberadaan data yang dihimpun dan tujuannya;
7. Keterlibatan perorangan (*Individual participation*), dimana individu/perorangan haruslah mendapat hak untuk untuk mendapatkan konfirmasi atas data yang berkaitan dengannya, dapat melakukan komunikasi telah berkaitan dengan datanya dalam waktu dan cara yang masuk wajar serta dalam bentuk yang mudah dipahami olehnya, diberi alasan jika permintaan yang dibuat ditolak, dan untuk dapat menggugat penolakan tersebut serta dapat meminta agar data dihapus, diperbaiki atau diubah;
8. Akuntabilitas (*Accountability*), dimana pengontrol data harus bertanggung jawab untuk mematuhi langkah-langkah yang mempengaruhi prinsip-prinsip yang disebutkan di atas.<sup>20</sup>Dengan melakukan tindakan yang mengakui dan memastikan informasi pribadi melalui kebijakan privasi yang dilakukan oleh perusahaandapat meningkatkan reputasinya, baik secara internal maupun eksternal.<sup>21</sup>

---

<sup>20</sup>*Ibid*, Hlm. 243

<sup>21</sup>Jacques Ophoff dan Marc Pelteret. 2016. "A Review of Information Privacy and Its Importance to Consumers and Organizations".  
[https://www.researchgate.net/publication/312577391\\_A\\_Review\\_of\\_Information\\_Privy\\_and\\_Its\\_Impo](https://www.researchgate.net/publication/312577391_A_Review_of_Information_Privy_and_Its_Impo)

Berdasarkan prinsip tersebut maka dalam pembuatan *privacy policy* setidaknya meliputi hal dasar diantaranya pemberitahuan mengenai informasi apa saja yang dihimpun seperti email, pelacakan lokasi, ataukah alamat IP, jika menggunakan *cookie* bagaimana cara untuk menyisihkannya serta bagaimana data privasi yang dihimpun digunakan oleh pengelolabeserta bentuk pengamanannya.<sup>22</sup>

#### 1.5.4 Sistem Elektronik

##### 1.5.4.1 Pengaturan sistem elektronik di Indonesia

Sistem berasal dari bahasa Yunani yakni *Systema*, yang memiliki pengertian sebagai suatu hubungan yang berlangsung dari komponen-komponen yang secara teratur membentuk sebuah kesatuan.<sup>23</sup> Sedangkan sistem elektronik sendiri merupakan rangkaian perangkat dan prosedur elektronik yang memiliki fungsi untuk mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan menyebarkan Informasi dalam bentuk Elektronik sebagaimana yang dijelaskan dalam Pasal 1 Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

---

[rtance to Consumers and Organizations](#), *Informing Science: the International Journal of an Emerging Transdiscipline*, Vol.19. Hlm. 292. Diakses pada tanggal 5 Januari 2021 Pukul 18.00

<sup>22</sup>Anonim. "What is a Privacy Policy & Why it's Important to Have it on Your Site".

<https://www.websitepolicies.com/blog/what-is-privacy-policy>. Diakses pada tanggal 5 Januari 2021 Pukul 17.00

<sup>23</sup> Abdul Kadir Adys, *Sistem Hukum dan Negara Hukum: Telaah Kritis Penegakan Hukum di Indonesia*, Yogyakarta: Suluh Media, 2019, hlm.5

Praktik penyelenggaraan sistem elektronik sendiri tidak hanya dapat dilakukan oleh lingkup publik melainkan termasuk juga dengan lingkup privat, yang dimana penyelenggaraan sistem elektronik privat merupakan pihak yang memiliki situs ataukah aplikasi yang terkoneksi dengan internet untuk dapat digunakan dalam mengelola barang ataukah jasa, layanan transaksi keuangan, mengoperasikan layanan komunikasi elektronik, layanan penyedia informasi elektronik (*search engine*), pemrosesan data pribadi terkait aktivitas elektronik maupun perdagangan barang dan jasa dan keuangan. Hal tersebut berdasarkan Pasal 2 Ayat (2) dan Ayat (5) Peraturan Pemerintah Nomor 71 Tahun 2019.

Pihak penyelenggara sistem elektronik baik publik maupun privat wajib melakukan pendaftaran pada sistem *Online Single Submission* (OSS) yang merupakan sistem pendaftaran terintegrasi<sup>24</sup>, pendaftaran tersebut berdasarkan Pasal 73 Ayat (1) dan (2) Peraturan Menteri Komunikasi dan Informatika Nomor 7 Tahun 2018 dilakukan dengan cara mengisi formulir pendaftaran beserta melampirkan dokumen berupa nama, alamat, nomor induk kependudukan, nomor telepon, alamat *e-mail*, nomor pokok wajib pajak (NPWP), gambaran umum pengoperasian sistem elektronik, sertifikat

---

<sup>24</sup>Pratiwi Agustini. "Pendaftaran Penyelenggara Sistem Elektronik (PSE). <https://aptika.kominfo.go.id/2020/01/pendaftaran-penyelenggara-sistem-elektronik-pse/>, diakses pada 3 Januari 2021 Pukul 16.45

keamanan informasi dan bagi badan hukum dilengkapi bentuk badan hukum lengkap dengan akta perusahaan.

#### 1.5.4.2 Pengamanan Sistem Elektronik

Penyelenggara sistem elektronik baik lingkup publik maupun privat berdasarkan Pasal 23 Peraturan Pemerintah Nomor 71 Tahun 2019 diwajibkan untuk melakukan pengamanan terhadap sistem komponen elektronik, dimana menurut penjelasan atas Pasal A *Quo* terdiri dari perangkat lunak, perangkat keras, tenaga ahli, sistem pengamanan sistem elektronik dan tata kelola sistem elektronik. Atas hal tersebut maka dilakukanlah Standarisasi keamanan informasi berupa pengendalian risiko yang dengan cara menmperkuat manajemen risiko serta pengidentifikasian asset maupun celah keamanan.<sup>25</sup>

Upaya tersebut diwujudkan dengan persyaratan penyelenggaraan transaksi elektronik dimana penyelenggaranya wajib menggunakan sertifikat elektronik serta disarankan memiliki sertifikat keandalan seperti yang dimuat dalam Pasal 42 Peraturan Pemerintah Nomor 71 Tahun 2019. Sertifikat elektronik tersebut harus didapatkan melalui penyelenggara sertifikasi di Indonesia, yang dimana terdapat 6 perusahaan penyelenggara sertifikasi elektronik di Indonesia yakni PrivyID, Perum Peruri, Vida, Balai Sertifikasi

---

<sup>25</sup>Ahmad Budi Setiawan.. “Studi standardisasi Sertifikat Elektronik dan Keandalan dalam Penyelenggaraan Sistem Transaksi Elektronik”. [https://www.researchgate.net/publication/276108709\\_Studi\\_Standardisasi\\_Sertifikat\\_Elektronik\\_dan\\_Keandalan\\_dalam\\_Penyelenggaraan\\_Sistem\\_Transaksi\\_Elektronik](https://www.researchgate.net/publication/276108709_Studi_Standardisasi_Sertifikat_Elektronik_dan_Keandalan_dalam_Penyelenggaraan_Sistem_Transaksi_Elektronik), *Buletin Pos dan Telekomunikasi*, 2014Vol.12 No.2. Hlm. 126. Diakses pada tanggal 20 Desember 2020 Pukul 21.15.

Elektronik Badan Siber dan Sandi Negara, DigiSign serta Badan Pengkajian dan Penerapan Teknologi (BPPT)<sup>26</sup>. Sedangkan sertifikat keandalan dikenal juga dengan sebutan *trustmark* meliputi registrasi identitas, keamanan sistem elektronik dan kebijakan privasi sesuai dengan Pasal 76 Ayat (1) Peraturan Pemerintah Nomor 71 Tahun 2019. Tujuan digunakannya Sertifikat Keandalan adalah untuk melindungi konsumen dalam transaksi elektronik. Dengan disertakannya sertifikat keandalan dalam sistem elektronik maka keamanan semakin terjamin, adapun jenis keamanan yang dijamin melalui sertifikat keandalan meliputi:

- Pengamanan atas identitas (*identity seal*)
- Pengamanan terhadap pertukaran data (*security seal*)
- Pengamanan terhadap kerawanan (*vulnerability seal*)
- Peningkatan konsumen (*consumer rating seal*)
- Pengamanan atas data pribadi (*privacy seal*)<sup>27</sup>

## 1.6. Metodologi Penelitian

### 1.6.1 Jenis Penelitian

---

<sup>26</sup>Tempo. “Diresmikan Kominfo, Penyelenggara Sertifikasi Elektronik Siap Tancap Gas”, <https://nasional.tempo.co/read/1274496/diresmikan-kominfo-penyelenggara-sertifikasi-elektronik-siap-tancap-gas>, diakses pada 3 Januari 2021 Pukul 19.00

<sup>27</sup>Priowirjanto, Enni Soerjati. *Trustmark Sebagai Jaminan Perlindungan Bagi Konsumen Internet Banking di Indonesia*. Bandung : Keni Media. 2019. Hlm. 195.

Penyusunan skripsi dilakukan oleh penyusun menggunakan jenis penelitian penelitian Yuridis-Normatif yang merupakan penelitian hukum dengan mengkaji bahan pustaka ataukah data sekunder sebagai acuan utama.<sup>28</sup> Penerapan jenis penelitian Yuridis Normatif dimaksudkan untuk pemerolehan gambaran yang jelas mengenai perlindungan terkait data privasi menurut Peraturan Pemerintah No 71 Tahun 2019.

#### 1.6.2 Sumber Data

Sumber data yang digunakan dalam penelitian hukum Yuridis-Normatif ialah data sekunder yang merupakan data yang diperoleh oleh penyusun melalui penelitian terhadap dokumen ataukah buku-buku yang tersedia. Data sekunder sendiri terdiri dalam tiga bahan, diantaranya adalah:

##### a. Bahan Hukum Primer

Bahan hukum primer merupakan bahan hukum yang tertulis dan ditegakkan oleh negara.<sup>29</sup> Bahan hukum primer bersifat mengikat yang terdiri dari norma hukum ataupun peraturan perundang-undangan yang terkait, antara lain:

##### 1) Kitab Undang-Undang Hukum Perdata

---

<sup>28</sup> Bambang Waluyo, Penelitian Hukum dalam Praktek, Jakarta : Sinar Grafika, 2008, Hlm.15

<sup>29</sup> I Made Pasek Diantha, Metodologi Penelitian Hukum Normatif, Jakarta : Prenada Media Group, 2016, Hlm 142

- 2) Peraturan Menteri Komunikasi dan Informatika Nomor 7 Tahun 2018 Tentang Pelayanan Perizinan Berusaha Terintegrasi Secara Elektronik Bidang Komunikasi dan Informatika
- 3) Peraturan Menteri Komunikasi dan Informatika Nomor 36 Tahun 2014 Tentang Tata Cara Pendaftaran Penyelenggaraan Sistem Elektronik
- 4) Peraturan Pemerintah Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik
- 5) Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik
- 6) Undang-Undang Nomor 30 Tahun 1999 Tentang Arbitrase dan Alternatif Penyelesaian Sengketa

b. Bahan Hukum Sekunder

Bahan hukum sekunder merupakan bahan hukum yang memberikan penjelasan atas bahan hukum primer, penjelasan tersebut termasuk dengan Rancangan Undang-Undang (RUU), hasil penelitian hukum maupun hasil karya ilmiah hukum seperti buku-buku hukum, jurnal, skripsi dan tesis.<sup>30</sup>

c. Bahan Hukum Tersier

---

<sup>30</sup>Bambang Sunggono, Metode Penelitian Hukum, Jakarta: Raja Grafindo, 2016, Hlm. 114

Bahan hukum tersier merupakan bahan hukum yang memberikan petunjuk atas bahan hukum primer dan sekunder agar diperoleh informasi yang relevan terhadap topik penelitian melalui kamus hukum, indeks kumulatif maupun ensiklopedia.<sup>31</sup>

### 1.6.3 Metode Pengumpulan Data

Teknik pengumpulan data dengan cara menggunakan metode penelitian kepustakaan (*library research*) yang data nya dapat diperoleh melalui bahan hukum primer, bahan hukum sekunder dan bahan hukum tersier, termasuk dengan peraturan perundang-undangan, buku-buku maupun publikasi ilmiah layaknya jurnal. Data yang telah diperoleh tersebut disusun dan dianalisa guna mendapatkan pemahaman lebih dalam mengenai perlindungan terkait data privasi.

### 1.6.4 Metode Analisis Data

Praktik yang dilakukan setelah mengumpulkan data ialah melakukan proses analisis data dimana dalam penulisan ini menggunakan metode analisis data analisis deskriptif-kualitatif. Proses analisis deskriptif-kualitatif merupakan proses yang menganalisis berbagai sumber data sekunder yang digunakan dengan cara mendeskripsikan data dalam bentuk kata maupun kalimat sehingga diperoleh kesimpulan.

---

<sup>31</sup>*Ibid.*

### 1.6.5 Sistematika Penulisan

Bab pertama, merupakan bab pendahuluan yang berisikan uraian mengenai pokok pembahasan secara keseluruhan, dalam bab ini terdapat latar belakang yang merupakan penjelasan mengenai penelitian, rumusan masalah yang merupakan pokok permasalahan, uraian mengenai tujuan penelitian maupun manfaat penelitian, kajian pustaka yang berisi dasar-dasar pemikiran hukum atas obyek permasalahan serta metodologi penelitian yang membahas mengenai jenis data, sumber data, metode pengumpulan data, metode analisis data beserta sistematika penulisan.

Bab kedua, merupakan bab yang akan membahas mengenai bentuk kriteria perbuatan melanggar hukum (PMH) terkait penyalahgunaan data pribadi.

Bab ketiga, merupakan bab yang akan membahas bagaimana upaya penyelesaian sengketa bagi pengguna aplikasi pada Google Play Store yang mengalami penyalahgunaan data pribadi dengan sub bab pertama mengenai bentuk upaya penyelesaian sengketa yang membahas mengenai bentuk-bentuk penyelesaian sengketa yang dapat dilakukan oleh para pengguna aplikasi yang mengalami kerugian terhadap data pribadinya, serta sub bab kedua mengenai tanggung jawab hukum bagi Google Play Store sebagai penyedia layanan aplikasi digital.

Bab keempat, merupakan bab terakhir dalam penelitian ini yang memuat kesimpulan dari seluruh pembahasan dan menyajikan saran atas permasalahan yang terjadi. Kesimpulan membahas mengenai uraian yang telah dijelaskan secara ringkas. Pada saran membahas mengenai saran-saran yang dianggap perlu.