BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Seiring perkembangan zaman, manusia memiliki kebutuhan yang semakin bertambah dan semakin kompleks. Hal ini membuat manusia terdorong untuk mencari atau menciptakan hal baru guna untuk mempermudah aktivitasnya. Salah satu dari hasil dari kecerdasan manusia tersebut adalah teknologi informasi. Teknologi informasi sendiri merupakan sebuah sistem yang melakukan pengumpulan, proses, menyimpan, dan mengirim sebuah informasi kepada subjek penerima dengan waktu yang sangat singkat sehingga menghasilkan sebuah keefisienan dan keefektifitasan dalam melakukan komunikasi.[1] Akibat dari Teknologi Informasi ini juga menciptakan budaya baru khususnya pola hidup manusia yang lebih mudah dan cepat.[2] Salah satu dari contoh kemudahan tersebut adalah manusia dapat melakukan komunikasi dimanapun dan kapanpun tanpa dibatasi ruang atau wilayah tempat suatu subjek berada.

Teknologi yang paling banyak dikenal masyarakat, dan paling banyak digunakan adalah internet. Internet sendiri merupakan media komunikasi yang

[1] Edmon Makarim, *Tanggung Jawab Hukum Penyelenggara Sistem Elektronik*, (Jakarta: Raja Grafindo Persada, 2010), hal. 2

[2] Melkior Nikolar Ngalumsine Sitokdana, *Strategi Pembangunan Pemerintahan Berbasis Elektronik*, (Yogyakarta: PT Kanisius, 2017), hal. 16

perkembangannya sangat pesat, dimana internet saling menghubungkan puluhan juta manusia di seluruh dunia, bahkan tanpa mengetahui keberadaan lawan komunikasinya. Informasi dapat dikirimkan dalam berbagai macam bentuk seperti suara, gambar, teks, dan kombinasi lainnya.[3] Menurut Sutarman, internet merupakan hubungan antar berbagai jenis komputer dan jaringan di dunia yang berbeda sistem operasi maupun aplikasinya, di mana hubungan tersebut memanfaatkan kemajuan media komunikasi (telepon dan satelit) yang menggunakan protokol standar dalam berkomunikasi, yaitu protokol TCP/IP.[4] Dikarenakan semakin bertambahnya pengguna internet yaitu hampir seluruh lapisan masyarakat dari bawah hingga atas, maka terbentuk sebuah pola kehidupan baru di jejaring internet yang biasa disebut sebagai dunia siber atau *cyber space*. Hal ini merupakan sebuah fakta baru yang dianggap sebagai dunia komunikasi berbasis komputer.[5]

Dibalik sisi positif tersebut, teknologi informasi juga diibaratkan sebagai pedang bermata dua dimana teknologi memberikan kemudahan bagi para pengguna dan memberikan ruang bagi kejahatan untuk berkembang.[6] Berdasarkan klasifikasinya kejahatan melalui Teknologi dapat dikategorikan sebagai berikut:

---

[3] Sutarman, *Pengantar Teknologi Informasi*, (Jakarta: Bumi Aksara, 2012), hal. 64
[4] Andi Abdul Muis, *Indonesia di Era Dunia Maya Teknologi Informasi dalam Dunia Tanpa Batas*, (Bandung: PT Remaja Rosdakarya Offset, 2001), hal. 32
[5] Maskun, *Kejahatan Siber (Cybercrime) Suatu Pengantar*, (Jakarta: Prenada Media Group, 2013), hal. 46
[6] Pejelasan Atas Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik

1. *Unauthorized Sccess To Computer System and Service*, yaitu kejahatan yang dilakukan ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin, atau tanpa pengetahuan dari pemilik sistem jaringan komputer yang dimasukinya.
2. *Illegal Contents*, yaitu kejahatan dengan memasukkan data atau informasi ke internet tentang sesuatu hal yang tidak benar, tidak etis, dan dianggap melanggar hukum atau mengganggu ketertiban umum.
3. *Data Forgery*, yaitu kejahatan dengan memalsukan data pada dokumen-dokumen penting yang tersimpan sebagai *scriptless document* melalui internet. Kejahatan ini biasanya ditujukan pada dokumen-dokumen *e-commerce* dengan membuat seolah-olah terjadi "salah ketik" yang pada akhirnya akan menguntungkan pelaku.
4. *Cyber Espionage*, yaitu kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer (*computer network system*) pihak sasaran. Kejahatan ini biasanya ditujukan terhadap saingan bisnis yang dokumen ataupun data-data pentingnya tersimpan dalam suatu sistem komputerisasi.
5. *Cyber Sabotage and Extortion*, yaitu kejahatan yang dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang tersambung dengan internet. Biasanya kejahatan ini dilakukan dengan menyusupkan suatu logic bomb, virus komputer atau suatu program tertentu sehingga data, program

komputer atau sistem jaringan komputer tidak dapat digunakan, tidak berjalan sebagaimana mestinya, atau berjalan sebagaimana yang dikehendaki oleh pelaku.

6. *Offence Against Intellectual Property*, yaitu kejahatan yang ditujukan terhadap hak kekayaan intelektual yang dimiliki seseorang di internet. Sebagai contoh yaitu peniruan tampilan *web page* suatu situs milik orang lain secara ilegal, penyiaran suatu informasi di internet yang ternyata merupakan rahasia dagang orang lain, dan sebagainya.
7. *Infringements of Privacy*, yaitu kejahatan yang ditujukan terhadap informasi yang terkait dengan hal yang sangat pribadi dan rahasia. Kejahatan ini biasanya ditujukan terhadap keterangan pribadi seseorang yang tersimpan pada formulir data pribadi dan tersimpan secara komputerisasi. Apabila informasi ini diketahui oleh orang lain, maka tentunya dapat merugikan orang yang bersangkutan secara materiil maupun immateriil, seperti contohnya yaitu nomor kartu kredit, nomor PIN ATM, keterangan tentang cacat atau penyakit tersembunyi, dan sebagainya.[7]

Selain macam-macam diatas, adapun istilah–istilah yang tetap digunakan tersebut juga diarahkan pada pengertian kejahatan terhadap komputer (*Crime directed at compute*r), kejahatan dengan mendayagunakan komputer (*Crimes utilizing computers*), atau kejahatan yang berkaitan dengan komputer (*Crimes related to computer*)[8]. Salah satu fenomena yang kerap terjadi di antara

[7] Maskun, *Op.cit*, hal. 51
[8] Barda Nawawi Arief, *Tindak Pidana Mayantara dan Perkembangan Kajian Cyber Crime di Indonesia*, (Jakarta: Rajawali Pers, 2006), hal. 25

kejahatan teknologi adalah pencurian data pribadi, dimana data-data pribadi dari seseorang akan dicuri dan setelah itu akan diperjual-belikan. Data pribadi ini sendiri juga dapat digunakan oleh pihak-pihak yang tidak bertanggung jawab untuk melakukan pinjaman online dengan menggunakan identitas dari data yang dicuri, membuat kartu kredit, dijual di *dark web*, dan masih banyak lainnya.[9] Beberapa contoh dari pencurian data yang baru terjadi akhir-akhir ini di Indonesia berasal dari Tokopedia, Bukalapak, Twitter, Sephora, dan Facebook.

Tabel 1.1 Beberapa Kasus Pencurian Data Pribadi Di Indonesia

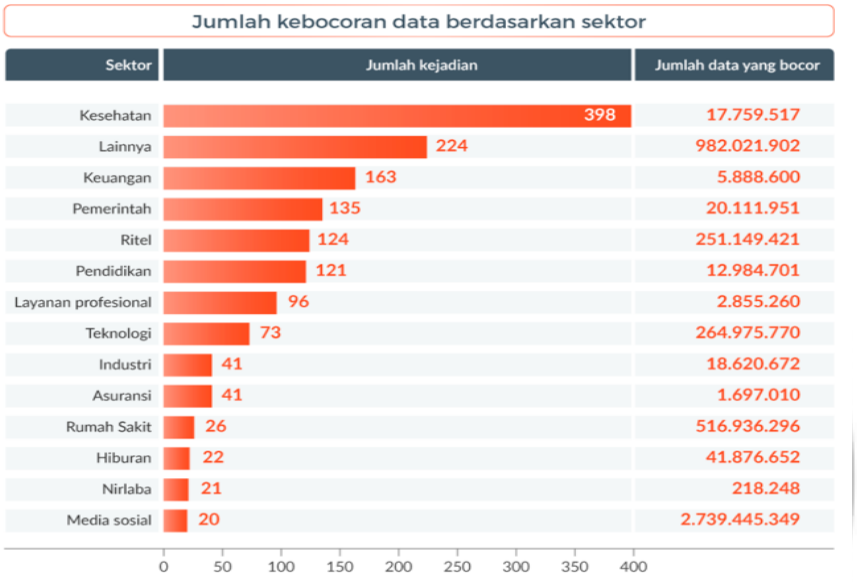
No	Pencurian Data	Tahun	Keterangan	Sumber
1	Tokopedia	2020	Peretas telah berhasil membobol 91 juta akun pengguna dan 7 juta akun *merchant* dari Tokopedia, dan menjualnya senilai US$5.000 / sebesar Rp 75 juta rupiah di *Raid Forums* dan *Empire Market* (*dark web*). Peretas ini menjual *user* ID, email, nama lengkap, tanggal lahir, jenis	CNN Indonesia dan CNBC Indonesia

[9] "Risiko Ketika Data Pribadi Dicuri", <https://www.cnnindonesia.com/teknologi/20181226210103-185-356593/risiko-ketika-data-pribadi-dicuri>, diakses 1 Oktober 2020

			kelamin, nomor telepon, dan kata sandi.	
2	Bukalapak	2020	Peretas telah berhasil mendapatkan 13 juta akun Bukalapak dan diperjualkan di forum *RaidForums*. Data yang dijual berupa *email*, nama pengguna, kata sandi, *salt, last login, email* Facebook dengan *hash*, alamat pengguna, tanggal lahir, dan nomor telepon. Setahun sebelumnya, data dari bukalapak juga telah dijual oleh peretas Pakistan yaitu Gnosicplayers dengan total nilai sebesar 1.2431 Bitcoin atau sekitar US$5.000 yang setara dengan Rp 70,5 juta (kurs US$1 = Rp 14.100).	CNN Indonesia
2	Twitter	2020	Twitter menyatakan bahwa para *hacker* telah berhasil membobol 130 akun dari Indonesia dan berhasil melihat	CNBC Indonesia

			data pribadi pengguna termasuk alamat *email* dan nomor telepon. Mereka dapat mengganti kata sandi akun pengguna, tetapi tidak dapat melihat kata sandi akun sebelumnya.	
3	Sephora	2019	*Group*-IB selaku perusahaan keamanan dunia maya internasional mengungkapkan bahwa sebanyak 500.000 *database* dari pelanggan Indonesia dan Thailand dijual pada tanggal 6 dan 17 Juli 2019 sebesar US$1.900. Namun Sephora menegaskan bahwa tidak ada informasi kartu kredit pengguna yang diakses.	Internasional Kontan.co.id
4	Facebook	2018	Facebook Indonesia menyatakan bahwa terdapat lebih dari 1 juta pengguna media sosial Facebook (1,3%)	Kompas

			yang mengalami kebocoran data pribadinya ke *Cambridge Analytica*.	



Gambar 1.1 Jumlah Kebocoran Data Tahun 2018. [10]

Kemudian, contoh kedua adalah jumlah kebocoran data pribadi yang dibagi berdasarkan sektor pada tahun 2018. Selain itu, Gemalto melaporkan bahwa sejak 2013 – 2018, laporan pencurian data pribadi mencapai 14,6 miliar dan hanya sebesar 4 persen diantaranya yang dilindungi enkripsi oleh pemiliknya. Secara statistik, kehilangan data pribadi paling banyak berasal dari perusahaan media sosial yaitu sebanyak 56,11%.[11]

[10] Ririn Aswandi, Putri Rofifah Nabilah M, dan Muhammad Sultan, "*Perlindungan Data Dan Informasi Pribadi Melalui Indonesian Data Protection System (IDPS)"*, Legislatif, Vol 3, Nomor 2 Januari 2020, hal. 173

[11] *Ibid*.

Melihat fakta hukum sebagaimana yang telah dipaparkan sebelumnya, dampak perkembangan teknologi yang telah disalahgunakan sebagai sarana kejahatan ini menjadi teramat penting untuk diantisipasi bagaimana kebijakan hukumnya, sehingga dapat melakukan penanggulangannya untuk *cybercrime* yang terjadi dengan hukum pidana, yang termasuk dalam hal ini adalah mengenai sistem pembuktiannya. Dikatakan teramat penting karena dalam penegakan hukum pidana dasar pembenaran seseorang dapat dikatakan bersalah atau tidak melakukan tindak pidana, di samping perbuatannya dapat dipersalahkan atas kekuatan undang-undang yang telah ada sebelumnya (asas legalitas), juga perbuatan mana didukung oleh kekuatan bukti yang sah dan kepadanya dapat dipertanggungjawabkan (unsur kesalahan). Pemikiran demikian telah sesuai dengan penerapan asas legalitas dalam hukum pidana (KUHP) kita, yakni sebagaimana dirumuskan secara tegas dalam Pasal 1 ayat (1) KUHP:

> "*Nullum delictum nulla poena sine praevia lege poenali*" atau dalam istilah lain dapat dikenal, "tiada tindak pidana, tidak ada pidana, tanpa adanya aturan hukum pidana terlebih dahulu".[12]

Maka, pemerintah membntuk suatu regulasi yang dapat menjangkaunya dengan prinsip kepastian hukum, sehingga pemerintah secara khusus mengundang-undangkan Undang-undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik dan berbagai peraturan perundang-undangan lainya. Dimana dalam

[12] Sudaryono dan Natangsa Surbakti, *Hukum Pidana*, (Surakarta: Fakultas Hukum UMS, 2005), hal. 58

undang-undang tersebut mengatur berbagai macam tindakan yang dilarang oleh hukum positif di Indonesia.

Terlepas dari adanya peraturan yang telah mengatur mengenai kejahatan tersebut, terdapat hak dan kewajiban yang wajib dilakukan oleh penyelenggara sistem elektronik maupun pengguna sistem elektronik tersebut. Hal ini merupakan langkah preventif untuk menjaga data pribadi milik subjek hukum dan juga menjaga keadilan bagi seluruhnya, sehingga apabila terdapat kesalahan yang berasal dari pengguna, pengguna pun tidak dapat menyalahkan dan meminta ganti rugi kepada pihak penyelenggara sistem elektronik, atau dengan kata lain seluruh elemen masyarakat baik itu pengguna maupun penyelenggara sistem elektronik harus melaksanakan kewajiban demi terselenggaranya penggunaan teknologi yang bersifat adil. Hal ini juga sesuai dengan pengimplementasian Teori Keadilan Bermartabat (*The Dignified Justice Theory*) sebagai salah satu Teori Hukum.[13]

Teori Keadilan Bermartabat merupakan suatu Grand Teori Hukum yang berfungsi untuk menjelaskan dan memberi justifikasi suatu sistem hukum yang berlaku, dengan menggambarkan tujuan hukum dalam negara Indonesia yaitu berdasarkan Pancasila. Keadilaan Bermartabat menekankan mengenai konsepsi memanusiakan manusia (*nguwongke uwong*), yang menjelaskan mengenai pengertian keadilan, kepastian, dan kemanfaatan yang ada di dalam setiap asas

[13] Teguh Prasetyo, *Keadilan Bermartabat: Perspektif Teori Hukum*, (Bandung: Penerbit Nusa Media, 2015), hal. 1

dan kaidah hukum.[14] Oleh karena itu, Teori ini dapat diimplementasikan terhadap tindakan yang tergolong merugikan orang lain, seperti pencurian dan jual-beli data pribadi yang merupakan suatu tindakan tidak terpuji dan melanggar hak-hak orang lain dengan menodai keadilan itu sendiri. Dengan menerapkan teori ini juga kita dapat menganalisis susunan dari undang-undang yang telah berlaku maupun rancangan undang-undang demi tercapainya suatu yang bermartabat.

Berkaitan dengan hal-hal yang telah penulis paparkan diatas, perlindungan data pribadi merupakan hal terpenting yang menjadi prioritas di era 4.0 ini, dimana terdapat banyak pencurian maupun jual-beli data pribadi yang dilakukan oleh oknum-oknum yang tidak bertanggung jawab, yang telah mencoreng nama keadilan dengan merenggut hak-hak privasi orang lain di negara ini. Oleh karena itu, Negara berdasarkan asas legalitas harus mengatur mengenai hal tersebut sesuai dengan Teori Keadilan Bermartabat dengan menjamin kepastian, kemanfaatan, dan keadilan yang menjunjung tinggi setiap nilai-nilai Pancasila. Maka, penulis menuangkan sebuah penulisan hukum dengan judul, "**Perlindungan Hukum Terhadap Data Pribadi Masyarakat yang Diperjual-belikan Berdasarkan Teori Keadilan Bermartabat**".

[14] Teguh Prasetyo dan Rizky P. P. Karo Karo, *Pengaturan Perlindungan Data Pribadi Di Indonesia; Perspektif Teori Keadilan Bermartabat*, (Bandung: Nusa Media, 2020), hal. 40-41

1.2 Rumusan Masalah

Rumusan Masalah dalam sebuah penelitian dimaksudkan untuk mempermudah penulis dalam membatasi masalah yang akan diteliti sehingga tujuan dan sasaran dari penelitian ini dapat sesuai yang diharapkan, sehingga rumusan masalah dalam penelitian ini yaitu:

1. Bagaimana perlindungan hukum terhadap data pribadi di Negara Indonesia?
2. Bagaimana perlindungan hukum terhadap data pribadi berdasarkan Teori Keadilan Bermartabat?

1.3 Tujuan Penelitian

Tujuan dari penelitian ini berdasarkan rumusan masalah yang ada adalah:

1. Untuk menganalisis dan meneliti mengenai perlindungan hukum terhadap data pribadi di Negara Indonesia.
2. Untuk menganalisis dan meneliti mengenai perlindungan hukum terhadap data pribadi berdasarkan Teori Keadilan Bermartabat.

1.4 Manfaat Penelitian

1.4.1 Manfaat teoritis

Manfaat penelitian secara teoritis diharapkan dapat menjadi referensi dalam ilmu pengetahuan tentang perlindungan data pribadi khususnya ditinjau berdasarkan perspektif Teori Keadilan Bermartabat,

dan diharapkan dapat memberikan wawasan baru mengenai perlindungan data pribadi.

1.4.2 Manfaat praktis

Manfaat penelitian secara praktis yaitu memberikan wawasan bagi para pengguna dan penyelenggara sistem elektronik maupun setiap orang yang memiliki kepentingan untuk memahami perlindungan data pribadi berdasarkan hukum yang berlaku di Indonesia.

1.5 Sistematika Penulisan

Untuk memudahkan pemahaman dan alur yang logis dalam penelitian ini, penulis akan memberikan gambaran umum sistematis dalam makalah ini. Adapun susunannya adalah sebagai berikut:

BAB I: PENDAHULUAN. Bab ini menguraikan mengenai Latar Belakang Masalah, Rumusan Masalah, Tujuan dan Manfaat Penelitian, dan Sistematika Penelitian.

BAB II: TINJAUAN PUSTAKA. Bab ini menguraikan mengenai Kerangka Teori dan Kerangka Konseptual yang digunakan sebagai dasar teori dan konsep pemecahan masalah penelitian.

BAB III: METODE PENELITIAN. Bab ini menguraikan mengenai Jenis Penelitian, Jenis Data, Pendekatan Penelitian, dan Sifat Analisis Data.

BAB IV: HASIL PENELITIAN DAN ANALISIS. Bab ini akan menguraikan hasil penelitian dan Analisa dari rumusan masalah yang telah penulis paparkan secara mendalam.

BAB V: PENUTUP. Bab ini menguraikan mengenai kesimpulan dan saran dari penulisan yang telah dibuat secara keseluruhan.