BAB I

PENDAHULUAN

1.1 Latar Belakang

Kemajuan teknologi informasi terutama pada bidang komputer dan internet terbukti telah memberikan dampak positif bagi kemajuan kehidupan manusia. Perlu digaris bawahi, dibalik kelebihan dan kemudahan yang ditawarkan oleh komputer dan internet, ternyata memiliki sisi gelap yang dapat menghancurkan kehidupan dan budaya manusia itu sendiri.[1] Perkembangan teknologi informasi mengubah pola pemikiran mengenai batas wilayah, waktu, nilai-nilai, wujud benda, logika berfikir, pola kerja, dan batas perilaku sosial dari yang bersifat manual menjadi komputerisasi/digital.[2] Informasi sudah dianggap sebagai "power" yang diartikan sebagai kekuatan dan kekuasaan yang sangat menentukan nasib manusia itu sendiri.[3]

Saat ini ketergantungan masyarakat akan teknologi informasi semakin tinggi sehingga semakin tinggi pula resiko yang dihadapi. Saat ini

[1] Brisilia Tumalun, "Upaya Penanggulangan Kejahatan Komputer Dalam Sistem Elektronik Menurut Pasal 30 Undang-Undang Nomor 11 Tahun 2008," *Jurnal Lex Et Societatis* 6, No. 2 (2018) hlm 24.

[2] Dian Ekawati, "Perlindungan Hukum Terhadap Nasabah Bank Yang Dirugikan Akibat K ejahatan Skimming Ditinjau Dari Perspektif Teknologi Informasi Dan Perbankan," *Jurnal Unes Law Review* 1, No. 2 (2018), hlm 158.

[3] Lauder Siagian, Arief Budiarto, Dan Simatupang, "Peran Keamanan Siber Dalam Mengatasi Konten Negatif Guna Mewujudkan Ketahanan Informasi Nasional," *Jurnal Prodi Perang Asimetris*, Vol. 4, No (2018) hlm 2.

ketergantungan masyarakat akan teknologi informasi semakin tinggi sehingga semakin tinggi pula resiko yang dihadapi.[4]

Teknologi informasi saat ini menjadi "pedang bermata dua" karena selain memberikan kontribusi bagi peningkatan kesejahteraan, kemajuan dan peradaban manusia, sekaligus menjadi sarana efektif perbuatan melawan hukum termasuk tindak pidana (kejahatan). Berbagai bentuk tindak pidana (kejahatan) inilah yang kemudian dikenal dengan istilah "*cybercrime*".

Teknologi yang diciptakan berkembang seiring dengan kebutuhan manusia untuk memudahkan hidup dari yang sebelumnya. Perubahan pesat teknologi informasi kearah kemajuan globalisasi berdampak ke hampir semua aspek kehidupan masyarakat. Kemajuan serta perkembangan teknologi telah banyak memberikan pengaruh terhadap seluruh aspek kehidupan sosial masyarakat. Perkembangan media sosial yang sangat pesat ditandai dengan munculnya berbagai macam media sosial seperti facebook, twitter, instagram, line dan lain sebagainya. Media sosial memberikan kemudahan dalam berkomunikasi dan berinteraksi antar penggunanya tanpa harus tatap muka yang tidak dibatasi oleh ruang dan waktu.

Meike dan Young mengemukakan bahwa media sosial sebagai konvergensi antara komunikasi personal dalam arti saling berbagi diantara individu *(to be share one-to-one)* dan media publik untuk berbagi kepada siapa saja tanpa ada kekhususan individu. Sedangkan Boyd memaparkan bahwa

[4] Darmawan Napitupulu, "Kajian Peran Cyber Law Dalam Memperkuat Keamanan Sistem Informasi Nasional," *Deviance Jurnal Kriminologi*, Vol. 1 No. (2017) hlm 102.

media sosial sebagai kumpulan perangkat lunak yang memungkinkan individu maupun komunitas untuk berkumpul, berbagi, berkomunikasi, dan dalam kasus tertentu saling berkolaborasi atau bermain. Media sosial memiliki kekuatan pada *user-generated content (UGC)* atau interaksi konten yang dihasilkan oleh pengguna, bukan oleh editor sebagaimana di instansi media massa.[5] Dalam hal penulis memilih teori ini karena akan dikaitkan dengan adanya kata kunci yang ada pada judul yang maknanya adalah dalam penggunaan media social harus digunakan secara bijak dalam penggunaannya karena sudah diatur dalam UU ITE mengenai media social ini dalam implementasinya.

Ditengah maraknya penggunaan media sosial, informasi pengguna dalam media sosial dapat dengan mudah didapatkan halnya informasi data pribadi pengguna dan hal lainnya yang bersifat privasi. Hal ini tentu dapat memicu terjadinya penyalahgunaan data pribadi. Ini dapat terjadi apabila pemilik data pribadi merasa data pribadi yang tertera atau dicantumkan dalam media sosialnya digunakan oleh pihak lain tanpa seizinnya untuk tujuan yang dianggap mengganggu, menguntungkan diri sendiri, membahayakan atau mengancam orang lain yang pastinya akan memberikan kerugian bagi pemilik data.

Perkembangan media sosial yang sangat pesat ditandai dengan munculnya berbagai macam media sosial seperti facebook, twitter, instagram, line dan lain sebagainya. Media sosial memberikan kemudahan dalam berkomunikasi dan

[5] Nasrullah, Rulli, *Media Sosial; Perspektif Komunikasi, Budaya, dan Sosioteknologi*, Simbiosa Rekatama Media, Bandung, 2015, hlm. 12.

berinteraksi antar penggunanya tanpa harus tatap muka yang tidak dibatasi oleh ruang dan waktu.

Menurut Jerry Kang, data pribadi mendeskripsikan suatu informasi yang erat kaitannya dengan seseorang yang dapat membedakan karateristik masing-masing pribadi. Data dapat dikatakan data pribadi jika pada data tersebut dapat digunakan untuk mengenali atau mengidentifikasi seseorang.[6] Hak privasi seseorang sesungguhnya telah dilindungi oleh Deklarasi Hak Asasi Manusia (*Universal Declaration of Human Rights*) Pasal 12, sebagaimana yang diakomodasi dalam Undang-Undang Dasar Pasal 28 G ayat (1) yang 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."

Berdasarkan hal itu, maka dibutuhkan perlindungan terhadap data pribadi itu sendiri. Perlindungan data pribadi adalah perlindungan secara khusus tentang bagaimana undang-undang melindungi, bagaimana data pribadi dikumpulkan, didaftarkan, disimpan, dieksploitasi, dan disebarluaskan. Regulasi mengenai data pribadi ini belum diatur secara spesifik dalam satu undang-undang namun terdapat beberapa pasal yang tersebar dalam beberapa undang-undang yang mencerminkan perlindungan data pribadi.

---

[6] Radian Adi Nugraha, *Analisis Yuridis Mengenai Perlindungan Data Pribadi dalam Cloud Computing System Ditinjau dari Undang-Undang Informasi dan Transaksi Elektronik*, Rajawali Press, Jakarta, 2012, hlm. 31.

Sehubungan dengan Data Pribadi, UU ITE memang belum memuat aturan perlindungan data pribadi secara khusus. Namun dalam ketentuannya, terdapat Pasal 26 ayat (1) dan penjelasannya UU 19/2016, yang berbunyi:

> 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.

Penjelasan Pasal 26 ayat (1) UU 19/2016:

> Dalam pemanfaatan Teknologi Informasi, perlindungan data pribadi merupakan salah satu bagian dari hak pribadi (privacy rights). Hak pribadi mengandung pengertian sebagai berikut:
>
> a. Hak pribadi merupakan hak untuk menikmati kehidupan pribadi dan bebas dari segala macam gangguan.
> b. Hak pribadi merupakan hak untuk dapat berkomunikasi dengan Orang lain tanpa tindakan memata-matai.
> c. Hak pribadi merupakan hak untuk mengawasi akses informasi tentang kehidupan pribadi dan data seseorang.

Sedangkan, hal yang berkaitan dengan penjabaran tentang data elektronik pribadi, UU ITE mengamanatkannya lagi dalam Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik ("PP PSTE"). Definisi data pribadi terdapat dalam Pasal 1 angka 29 PP PSTE:

> 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.

Data Pribadi berdasarkan Pasal 1 ayat (1) Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 20 Tahun 2016 merupakan bagian informasi pribadi, dikarenakan sebagaimana yang ditegaskan pada Pasal

tersebut bahwa Data Pribadi harus dijaga kerahasiaannya, sehingga Data Pribadi merupakan hak pribadi seseorang. Melihat kembali pada *General Data Protection Regulation* pada Pasal 12 sampai 22, telah dijelaskan mengenai hak-hak pemilik Data Pribadi dalam terlaksananya Perlindungan Data pribadi, baik dari segi preventif maupun represif. Hak-hak pemilik Data Pribadi di Indonesia diatur dalam Pasal 26 Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016, yang mana ditegaskan:

"Pemilik Data Pribadi berhak:

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

Melihat pada poin b pada Pasal 26 Permenkominfo PDPSE di atas, bahwa menteri yang dimaksud dalam mengajukan pengaduan ialah Menteri Komunikasi dan Informatika. Namun, pengaduan ini hanya dapat dilakukan jika data pribadi yang disimpan dan dikelola terdapat dalam sistem elektronik.

Pada sektor kesehatan diatur Pasal 57 ayat (1) Undang-Undang Nomor 36 Tahun 2009 tentang Kesehatan menyebutkan bahwa *"Setiap orang berhak atas rahasia kondisi kesehatan pribadinya yang telah dikemukakan kepada*

penyelenggara pelayanan kesehatan." Kemudian Pasal 57 ayat (2) menambahkan bahwa

> *"Ketentuan mengenai hak atas rahasia kondisi kesehatan pribadi sebagaimana dimaksud pada ayat (1) tidak berlaku dalam hal: a. perintah undang-undang; b. perintah pengadilan; c. izin yang bersangkutan; d. kepentingan masyarakat; atau e. kepentingan orang tersebut."*

Selain itu, Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan juga mengatur perlindungan data pribadi. Pasal 1 ayat (22) mendefinisikan Data Pribadi sebagai *"data perseorangan tertentu yang disimpan, dirawat, dan dijaga kebenaran serta dilindungi kerahasiaannya."*

Dalam pemanfaatan Teknologi Informasi, perlindungan data pribadi merupakan salah satu bagian dari hak pribadi (privacy rights). Hak pribadi mengandung pengertian sebagai berikut:

1. Hak pribadi merupakan hak untuk menikmati kehidupan pribadi dan bebas dari segala macam gangguan;
2. Hak pribadi merupakan hak untuk dapat berkomunikasi dengan orang lain tanpa tindakan memata-matai;
3. Hak pribadi merupakan hak untuk mengawasi akses informasi tentang kehidupan pribadi dan data seseorang. Selanjutnya, Hak-hak pribadi (privacy rights) dalam cyberspace mencakup 3 (tiga) aspek yang perlu diperhatikan, yaitu:
    a. pengakuan terhadap hak seseorang untuk menikmati kehidupan pribadinya dan terbebas dari gangguan;
    b. adanya hak untuk berkomunikasi dengan orang lain tanpa adanya pengawasan (tindakan memata-matai dari pihak lain); dan

c. adanya hak untuk dapat mengawasi dan mengontrol informasi pribadinya yang dapat diakses oleh orang lain. Hak perlindungan data pribadi berkembang dari hak untuk menghormati kehidupan pribadi atau disebut "the right to private life". Konsep kehidupan pribadi berhubungan dengan manusia sebagai makhluk hidup. Dengan demikian orang perorangan adalah pemilik utama dari hak perlindungan data pribadi.

Berkaitan dengan data pribadi, maka terdapat beberapa kasus dimana terjadi bocornya data pribadi. Berikut beberapa insiden kebocoran data pribadi di Indonesia, yaitu:[7]

1. Electronic Health Alert Card (eHAC)

   Masyarakat belakangan dihebohkan dengan dugaan kebocoran sebanyak 1,3 juta data pribadi pengguna electronic Health Alert Card (eHAC). Persoalan tersebut menjadi perhatian banyak orang karena aplikasi tersebut selama ini digunakan untuk kepentingan pelacakan Covid-19 dalam pemenuhan persyaratan penerbangan.

   Temuan kebocoran data pengguna eHAC pertama kali ditemukan oleh peneliti vpnMentor. Dilansir dari vpnmentor.com, 1,3 juta data pengguna eHAC pertama kali ditemukan di sebuah server yang bisa diakses oleh semua orang.

[7] "6 Kasus Kebocoran Data Pribadi di Indonesia", *https://nasional.tempo.co/read/1501790/6-kasus-kebocoran-data-pribadi-di-indonesia*, diakses 23 Februari 2022

2. Kebocoran data BPJS Kesehatan

Pada Mei 2021, data sejumlah peserta Badan Penyelenggara Jaminan Sosial (BPJS) dijual di Raid Forums seharga 0,15 Bitcoin. Data tersebut dijual oleh pengguna forum dengan nama id 'Kotz'. Ada satu juta contoh data gratis untuk diuji. Totalnya 279 juta, Sebanyak 20 juta memiliki foto personal.

3. Kebocoran data Cermati dan Lazada

Kasus kebocoran data dari dua perusahaan itu beredar di situs Raidforums pada akhir tahun 2020. Di dalamnya, ada data yang diperjualbelikan dari cermati.com sebanyak 2,9 juta pengguna yang diambil dari kegiatan 17 perusahaan, sebagian besar kegiatan finansial. Sedangkan, Lazada mengalami kebocoran sebanyak 1,1 juta data.

4. Penjualan data nasabah BRI Life

Sempat ramai beredar di media sosial ihwal dugaan penjualan data dua juta nasabah BRI Life dengan harga $7.000 atau sekitar Rp 101,6 juta. Unggahan tersebut dibeberkan akun Twitter @HRock. Terdapat 463.000 dokumen yang diperjualbelikan. Dokumen yang tertera dalam tangkapan layar berupa foto KTP elektronik, nomor rekening, nomor wajib pajak, akte kelahiran, dan rekam medis nasabah BRI Life.

5. Kebocoran data Tokopedia

Pada Mei 2020 ramai jutaan akun pengguna e-commerce Tokopedia diduga telah bocor. Bahkan, pemilik akun twitter @underthebreach menyebut aktor peretas telah menjual database Tokopedia sejumlah 91 juta akun seharga US$ 5.000 di darkweb. Adapun pihaknya mengklaim aksi peretasan telah dilakukan sejak Maret 2020.

6. Kebocoran data Komisi Pemilihan Umum

Peretas mengklaim telah membobol 2,3 juta data warga Indonesia dari Komisi Pemilihan Umum (KPU). Informasi itu datang dari akun @underthebreach, Kamis malam 21 Mei 2020. "Aktor (peretas) membocorkan informasi 2.300.000 warga Indonesia. Data termasuk nama, alamat, nomor ID, tanggal lahir, dan lainnya," cuit @underthebreach. Akun itu menyebutkan dugaan data yang diretas berasal dari data 2013 hingga kini. Tidak hanya itu, peretas juga mengklaim akan membocorkan 200 juta data lainnya.

Dalam konteks media sosial, pada tahun 2021, sebanyak 214 juta data pribadi dari akun Facebook, Instagram, dan LinkedIn dikabarkan bocor di internet. Pelanggaran data besar ini diungkap oleh peneliti Safety Detectives. Data yang dicuri termasuk alamat email, nomor telepon serta nama lengkap pengguna, dan dalam beberapa kasus, data lokasi tertentu.

Akibat adanya pihak yang dirugikan atas dugaan pelanggaran data pribadi di media social maka harus adanya perlindungan data pribadi merupakan bentuk dari perlindungan privasi yang diamanatkan langsung oleh Konstitusi Negara Republik Indonesia yang mengandung penghormatan atas nilai-nilai HAM dan penghargaan atas hak perseorangan sehingga perlu diberikan landasan hukum untuk lebih memberikan keamanan privasi dan data pribadi. Sebagaimana terkandung dalam Pasal 28G Undang-Undang Dasar 1945 tentang hak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang berada di bawah kekuasaan seseorang.

Dapat dipahami bahwa data pribadi berkenaan dengan kehidupan individu dan juga dekat kaitannya dengan konsep kerahasiaan atau hak privasi seseorang yang harus dijaga dan dilindungi oleh aturan perundangundangan, maka dari itu dibutuhkan kepastian hukum untuk melindungi hal ini. Di setiap tempat dibutuhkan kepastian hukum. Kepastian hukum merupakan perlindungan yustiabel terhadap tindakan sewenang-wenang yang berarti bahwa seseorang akan dapat memperoleh sesuatu yang diharapkan dalam keadaan tertentu[8]

Instagram sebagai salah satu jejaring sosial yang populer di kalangan remaja tentu memiliki dampak. Di satu sisi, keberadaan Instagram telah mendorong remaja menjadi lebih kreatif dalam menciptakan konten- konten digital, serta mendorong adanya praktik-praktik budaya partisipatif. Di sisi lain, keberadaan Instagram telah mendorong munculnya perilaku memberikan atau

[8] Sudikno Mertokusumo, *Mengenal Hukum Suatu Pengantar*, Citra Aditya Bakti, Bandung, 2013, hlm. 160.

menyebarkan informasi pribadi kepada pihak lain. Individu memberikan atau menyebarkan informasi pribadi dalam bentuk data diri yang dicantumkan pada keterangan informasi profil atau pada tulisan, foto atau video yang kemudian diunggah. Fenomena memberikan atau menyebarkan informasi pribadi kepada pihak lain seringkali dikaitkan dengan isu privasi. Perilaku tersebut merefleksikan kurangnya kesadaran mengenai isu privasi dalam diri individu. Gejala yang menandai fenomena tersebut salah satunya tergambar dalam studi yang dilakukan oleh Aisyah Nur

Pelanggaran privasi terjadi pada remaja bernama Millendaru. Dimana foto-foto millendaru yang pernah diunggah di Instagram telah dicuri oleh pihak tak berwenang dan dipajang di situs prostitusi online. Informasi pribadi millendaru, seperti tempat tanggal lahir, usia, alamat, termasuk nomor teleponnya juga dicuri dan dicantumkan dalam situs prostitusi online tersebut. Kasus tersebut jelas merugikan remaja yang bersangkutan. Hal serupa dapat terjadi pada remaja lain yang belum menerapkan perilaku perlindungan privasi dengan baik.[9]

Permasalahan mengenai privasi di Indonesia masih belum dieksplorasi secara mendalam. Hal tersebut terjadi karena kurangnya perhatian terhadap isu privasi, baik dari pihak akademisi maupun dari pihak pemerintah. Karena belum terbukti dengan adanya regulasi yang secara khusus mengarahkan individu pada perilaku melindungi privasi di ranah virtual online, terutama pada situs jejaring

[9] "Heboh Foto Millendaru Terpampang di Situs Prostitusi Online", https://www.liputan6.com/showbiz/read/3546672/heboh-foto-millendaru-terpampang-di-situs-prostitusi-online diakses pada tanggal 13 Januari 2022 pukul 08.34

sosial. Hal lain yang turut menjadi tanda adalah kurangnya jumlah penelitian-penelitian yang mengkaji mengenai isu privasi.

Uni Eropa (UE) menyoroti kasus privasi data pengguna Facebook. Platform media sosial terbesar itu terancam dibanjiri kasus privasi data tak hanya dari satu negara anggota UE, tapi beberapa negara lainnya. UE memiliki regulasi perlindungan data umum yang bernama General Data Protection Regulation (GDPR). Regulasi itu berlaku sejak tahun 2018. Melalui GDPR, masyarakat di UE punya akses lebih luas untuk menyuarakan keluhan pelanggaran privasi dari platform media sosial manapun, termasuk Facebook.

Dalam GDPR, keluhan privasi dari platform manapun akan diproses oleh Komisioner Perlindungan Data yang kantor pusatnya berlokasi di Dublin, Irlandia. Namun ternyata, aturan itu sedikit menghambat proses penyelidikan kasus pelanggaran privasi, seperti di Belgia. Sebelumnya pada 2015, pengadilan Belgia memutuskan bahwa Facebook melanggar aturan privasi karena bisa memantau riwayat pencarian pengguna internet, meskipun pengguna tersebut tidak pernah mendaftar atau memiliki akun Facebook. Merespons itu, Facebook yang mengatakan dalam GDPR kasus pelanggaran privasi hanya bisa diproses oleh pengadilan Irlandia, karena kantor Komisioner Perlindungan Data berlokasi di Irlandia.

Tak tinggal diam, Otoritas Perlindungan Data Belgia kemudian meminta European Court of Justice (ECJ) untuk mengklarifikasi ketentuan tersebut. Advokat Jenderal ECJ mengatakan, penyelidikan keluhan pelanggaran privasi memang tidak harus dibawa ke regulator domestik. Justru, kasus itu bisa

diselidiki lebih lanjut atas keluhan pelanggaran data privasi di berbagai negara UE dan GDPR mengizinkan otoritas perlindungan data dari Negara Anggota UE untuk membawa persidangan ke pengadilan di Negara Bagian tersebut atas dugaan pelanggaran GDPR sehubungan dengan pemrosesan data lintas batas, meskipun itu bukan otoritas perlindungan data utama yang dipercayakan kepada seorang jenderal kekuasaan untuk memulai proses penyelidikan

CEO Ethyca Cillian Seorang ahli di pelanggaran data privasi sekaligus Kieran mengemukakan "apabila pengadilan suatu negara sudah memutuskan adanya pelanggaran privasi dari sebuah perusahaan media sosial justru akan semakin memperkuat penyelidikan di seluruh negara UE". Meski begitu, pendapat Advokat Jenderal ECJ tidak mengikat. Akan tetapi, kabarnya pendapat itu sedang dipertimbangkan oleh hakim ECJ yang akan memberikan putusan atas kasus pelanggaran privasi oleh Facebook di tahap selanjutnya. Sebaliknya, Associate General Counsel Facebook Jack Gilbert mengatakan, perusahaan menilai Advokat Jenderal masih memegang teguh prinsip satu pintu, dalam hal ini mengacu pada penyelidikan lebih lanjut kasus pelanggaran privasi yang menurut perusahaan hanya bisa diproses di Irlandia.[10]

Kurangnya perhatian terhadap isu privasi pada situs jejaring sosial merupakan hal yang ironis. Mengingat pemberitaan mengenai pelanggaran privasi pengguna situs jejaring sosial sudah banyak tersebar di berbagai media. Seperti pemberitaan mengenai jejaring sosial *Instagram* yang dilansir dari

[10] "Facebook Terancam Banjir Kasus Privasi Data di Uni Eropa", https://finance.detik.com/berita-ekonomi-bisnis/d-5333089/facebook-terancam-banjir-kasus-privasi-data-di-uni-eropa, diakses pada tanggal 10 Februari 2022 pukul 16.11 WIB.

laman *CNN news*. Diberitakan bahwa sejak tahun 2012 penyedia situs jejaring sosial *Instagram* mulai menjual foto-foto pengguna kepada perusahaan lain untuk kepentingan iklan korporasi. Berita lain yang dilansir dari laman huffing ton post menyebutkan adanya kelompok bernama *Doxogram* yang melakukan peretasan dan penjualan data pribadi berupa informasi kontak lebih dari 600 juta pengguna *Instagram*. Pengguna *Instagram* yang peka terhadap pemberitaan tersebut tentu mempertanyakan mengenai privasi pengguna.

Berdasarkan kasus diatas maka terindikasi adanya entuk-bentuk indikasi pelanggaran dalam media sosial yaitu kejahatan erat kaitannya dengan kegiatan forensik komputer misalnya:[11]

1. Pencurian kata kunci atau "password" untuk mendapatkan hak akses;
2. Pengambilan data elektronik secara diam-diam tanpa sepengetahuan sang empunya;
3. Pemblokiran hak akses ke sumber daya teknologi tertentu sehingga yang berhak tidak dapat menggunakannya;
4. Pengubahan data atau informasi penting sehingga menimbulkan dampak terjadinya mis-komunikasi dan/atau dis-komunikasi;
5. Penyadapan jalur komunikasi digital yang berisi percakapan antara dua atau beberapa pihak terkait;
6. Penipuan dengan berbagai motivasi dan modus agar si korban memberikan aset berharganya ke pihak tertentu;

[11] *Ibid.*

7. Peredaran foto-foto atau konten multimedia berbau pornografi dan pornoaksi ke target individu di bawah umur;
8. Penyelenggaraan transaksi pornografi anak maupun hal-hal terlarang lainnya seperti perjudian, pemerasan, penyalahgunaan wewenang, pengancaman, dan lain sebagainya;
9. Penyelundupan file-file berisi virus ke dalam sistem korban dengan beraneka macam tujuan;

Ketika korban dirugikan akibat adanya pelaku pelanggaran hukum atas data pribadi di media social yang yang di mana atas dasar perbuatan melanggar hukum maka korban bisa mengajukan gugatan perdata yang telah sesuai dengan undang-undang yang berlaku apabila ingin mengajukan gugatan terhadap penyalahgunaan data pribadi yang dilakukan oleh perseorangan ataupun korporasi dengan maksud yang tidak baik atas dasar gugatan yang lebih tepat digunakan adalah perbuatan melanggar hukum alasan yang pertama adalah korban dan pelaku itu itu tidak ada hubungan hukum atau perjanjian sebelum penyalahgunaan data itu terjadi banyak sekali kasus pelaku sebagai pihak ketiga berhasil membobol suatu data akun pribadi yang di mana biasanya perseorangan inilah yang mempunyai hubungan perjanjian dengan si korban kedua gugatan.Atas dasar perbuatan melanggar hukum yang perlu dibuktikan dengan harus terpenuhinya unsur-unsur yang ada di dalam perbuatan melawan hukum.

Kalau seandainya memakai gugatan atas dasar wanprestasi itu itu akan sangat sulit pembuktiannya dalam penyalahgunaan data pribadi karena harus dibuktikan adanya hubungan kontrak antara korban dan pelaku serta kewajiban apa saja yang dilakukan dalam melakukan perjanjian yang tidak dipenuhi sehingga bisa terjadinya wanprestasi.

Maka dari itu hal yang dapat diterapkan adalah mengajukan gugatan pada pelaku penyalahgunaan data pribadi dengan beban pembuktian sebagaimana hal ini juga diterapkan pada hukum perlindungan konsumen yang menerapkan beban pembuktian Karena pada dasarnya juga terdapat para pelaku yang melakukan penyalahgunaan data pribadi dan si korban yang dirugikan oleh karenanya pihak yang merasa dirugikan cukup untuk membuktikan adanya kerugian yang terjadi di yang terjadi di pihak-pihak yang merasa penggunaan data pribadinya digunakan tanpa izin sedangkan pihak yang tergugat harus melakukan pembuktian bahwa dirinya yang tidak bersalah dalam peristiwa itu pihak-pihak yang secara sah memperoleh data pribadi penggugat.

Di dalam pasal 26 Undang-Undang tentang informasi dan transaksi elektronik menjelaskan bahwa adanya hak yang yang dimiliki oleh perseorangan yaitu perlindungan atas data pribadinya dan terdapat juga di dalam peraturan pemerintah tentang penyelenggaraan sistem dan transaksi elektronik Nomor 82 Tahun 2012 yang dijelaskan bahwa data perseorangan tertentu yang disimpan dirawat dan dijaga kebenaran serta dilindungi kerahasiaannya.

Penyadapan merupakan segala tindakan yang tidak boleh dijalankan dan tidak termasuk golongan perseorangan yang mempunyai hak untuk itu dalam rangka upaya-upaya hukum yang diatur didalam UU ITE yang isinya mengenai perlindungan data pribadi termasuk penyadapan.Pasal 26 UU ITE dijelaskan penggunaan data pribadi melalui media elektronik harus didasari adanya persetujuan yang bersangkutan dan kerugian yang timbul akibat adanya penyalahgunaan pribadi itu dapat melewati jalur non litigasi dengan melakukan musyawarah maupun melalui jalur litigasi yang dilakukan kan di pengadilan melalui gugatan sebagai upaya untuk mengajukan ganti rugi.

Sebagaimana yang tertera pada Pasal 26 ayat 2 undang-undang tentang informasi dan transaksi elektronik ketentuan-ketentuan pidana yang ada di dalam undang-undang tersebut belum diatur oleh karena itu itu perlunya reformasi terhadap perundang-undangan dengan menambahkan berupa sanksi sanksi pidana hal itu supaya menimbulkan efek jera meskipun sanksi pidana yang itu merupakan jalan terakhir

Berdasarkan latar belakang di atas maka penulis tertarik untuk menulis tesis dengan judul "**PERLINDUNGAN HUKUM BAGI PIHAK YANG DIRUGIKAN ATAS DUGAAN PELANGGARAN DATA PRIBADI DI MEDIA SOSIAL**", yang diuji adalah pasal 26 UU ITE terhadap dugaan pelanggaran hokum atas data pribadi di media social dengan cara perlu disegarakan rancangan undang – undang data pribadi.

1.2 Rumusan Masalah

Dengan memperhatikan berbagai fenomena di atas maka penelitian tesis ini merumuskan dua permasalahan utama sebagai berikut :

1. Bagaimana ketersediaan hukum perlindungan data pribadi pelanggan?
2. Bagaimana penerapan perlindungan hukum terhadap pelanggaran data pribadi di media sosial?

1.3 Tujuan Penelitian

Penelitian ini dilakukan berkaitan dengan kehendak dan maksud yang ingin dicapai, yakni:

1. Untuk mengkaji dan menganalisis perlindungan hukum terhadap pelanggaran data pribadi di media sosial
2. Untuk mengkaji dan menganalisis penerapan perlindungan hukum terhadap pelanggaran data pribadi di media sosial

1.4 Manfaat Penelitian

Hasil penelitian ini diharapkan akan memberikan kegunaan baik dari segi teoritis maupun segi praktis, sebagai berikut:

1. Segi Teoritis

   Memberikan sumbangan pemikiran ilmiah dalam bidang hukum dan bahan rujukan dalam penyempurnaan peraturan perundang-undangan di Indonesia mengenai perlindungan hukum atas data pribadi serta evaluasi dalam pengembangan ilmu hukum terutama yang berkaitan dengan hukum siber b) Hasil penelitian ini diharapkan dapat digunakan menjadi

referensi tambahan dalam bahan pustaka bagi segala lapisan masyarakat, khususnya para akademisi maupun peneliti dalam bidang yang sama

2. Segi Praktis

Memberikan sumbangan pemikiran dan manfaat bagi masyarakat luas, terkhusus bagi kalangan remaja sebagai pengguna maupun pemerhati teknologi dan media sosial

1.5 Sistematika Penulisan

Dalam suatu karya ilmiah maupun non-ilmiah diperlukan suatu sistematika untuk menguraikan isi dari karya ilmiah ataupun non-ilmiah tersebut. Dalam menjawab pokok permasalahan, penulis menyusun penelitian ini dengan sistematika sebagai berikut :

BAB I PENDAHULUAN

Dalam bab I terdiri dari uraian mengenai latar belakang, perumusan masalah tujuan dan manfaat penelitian

BAB II TINJAUAN PUSTAKA

Pada bab ini penulis akan membahas tinjauan pustaka, yang terdiri dari kerangka konseptual dan kerangka teori dan akan membahas mengenai pihak yang dirugikan atas dugaan pelanggaran data pribadi di media social.

BAB III METODOLOGI PENELITIAN

Pada bab ini penulis menggunakan alat pengumpulan data berupa Studi dokumen dan/atau Bahan Pustaka. Studi dokumen yaitu memeriksa dokumen atas bahan hukum primer.Bahan Pustaka yaitu dengan

menggunakan bahan hukum sekunder karena sifatnya terbatas kepada sesuatu topik yang telah dipilih dalam waktu sesingkat mungkin.

BAB IV ANALISIS PENERAPAN PERLINDUNGAN HUKUM TERHADAP PELANGGARAN DATA PRIBADI DI MEDIA SOSIAL

Pada bab ini penulis akan menganalisis terkait perlindungan hukum apabila seseorang melakukan pelanggaran data pribadi di media sosial serta penerpan bagi para pelanggar di media sosial.

BAB V PENUTUP

Dalam bab ini penulis akan memasukkan kesimpulan – kesimpulan tentang yang sudah dibahas pada bab sebelumnya dan saran – saran.