BAB I

PENDAHULUAN

A. Latar Belakang Masalah

Perkembangan teknologi informasi yang begitu cepat serta globalisasi memberikan tantangan baru dalam upaya perlindungan data pribadi. Di mana skala pengumpulan dan berbagi (*sharing*) data pribadi meningkat secara signifikan. Teknologi juga memungkinkan perusahaan-perusahaan swasta maupun otoritas publik memanfaatkan data pribadi dalam skala besar yang belum pernah terjadi sebelumnya. Pemrosesan data pribadi terjadi di berbagai bidang kehidupan seperti kegiatan ekonomi dan social. Kemajuan teknologi informasi membuat pemrosesan dan pertukaran data tersebut jauh lebih mudah.[1]

Teknologi berperan dalam berbagai masalah privasi, karena mempermudah dalam pengumpulan maupun pemrosesan informasi. Ketika orang-orang menjelajahi web, menggunakan ponsel dan melakukan transaksi online, mereka meninggalkan jejak di mana-mana. Teknologi sendiri tidaklah melanggar privasi, tetapi aktivitas dan tujuan si pengguna teknologi yang sebenarnya dapat menciptakan pelanggaran. Kelebihan atau cacat pada teknologi tidaklah melekat dalam teknologi itu sendiri, tetapi tergantung pada bagaimana mereka digunakan dan sejauh mana penggunaannya, hal ini harus diawasi dan dipertanggungjawabkan oleh pihak-pihak yang terlibat.[2]

---

[1] Lamber paul,2017, *Understanding the new European data protection rules*, CRC Press. hal. 43.

[2] Dorraji, Seyed Ebrahim; Barcys, Mantas, *Privacy in Digital AgeDead or Alive?! Regarding the New EU Data Protection Regulations, Social*, Mykolas Romeris University, *Lithuania*. hal. 1.

Keamanan informasi sudah menjadi prioritas utama dalam organisasi modern. Keamanan informasi merupakan komponen krusial yang menjadi kunci kesuksesan teknologi modern, keamanan informasi merupakan salah satu aset yang paling penting dari tiga aset berharga dalam teknologi modern yaitu: *people*, *physical property* dan *information*.

Karakteristik informasi menjadi pondasi utama dalam konsep keamanan informasi, karena informasi merupakan salah satu aset berharga dari orang perorangan maupun organisasi yang harus dilindungi dari segala ancaman. Ancaman dimaksud dapat berasal dari eksternal maupun internal. Ancaman dari eksternal antara lain *Social engineering* (manipulasi psikologis dari peretas untuk menguak suatu informasi rahasia dari targetnya, hal ini dapat berupa meminta informasi itu langsung kepada korban atau pihak lain yang mempunyai dan mengetahui informasi itu), Sabotase dan Perusakan (tindakan yang dilakukan untuk merusak dan mengotori sebuah sistem dalam sebuah *website*), Pemerasan Informasi (tindakan ancaman yang dilakukan oleh peretas yang mengancam untuk mencuri atau menyebarkan informasi dengan tuntutan bayaran atau imbalan kepada korban), *Software Attack* (serangan yang dilakukan untuk menginfeksi komputer), maupun serangan dari *Programmer* pengembang sistem (misalnya *backdoor*, yaitu sebuah *password* yang hanya diketahui oleh penyerang yang digunakan untuk mengakses sebuah sistem komputer tanpa melalui prosedur keamanan). Sedangkan ancaman dari internal lebih kepada celah keamanan pada faktor pengguna, baik itu berupa kelalaian maupun ketidaktahuan mengenai keamanan informasi.[3]

---

[3] Kementrian keuangan 2020, *Keamanan Informasi, Sudah Saatnya Kita Peduli*, diakses tanggal 15 Oktober 2021 jam 20:00 WIB www.djkn.kemenkeu.go.id

Berdasarkan pembahasan diatas hal ini berhubungan dengan kejahatan *Phising* yang berkaitan erat dengan perlindungan data pribadi. *Phising* adalah suatu metode untuk melakukan penipuan dengan mengelabui target yang bertujuan untuk mencuri akun target. Istilah ini berasal dari kata *"fishing"* atau "memancing" korban agar terperangkap dalam jebakannya. *Phising* bisa dikatakan mencuri informasi penting dengan mengambil alih akun korban untuk maksud tertentu. Hal ini bisa saja dengan maksud mencari celah untuk beberapa akun yang terhubung dengan akun yang telah didapat. *Phising* biasanya sering digunakan pada email, dimana penyebaran melalui email ini dilakukan untuk memberikan informasi yang mengarah ke halaman palsu untuk maksud menjebak korban. Untuk menghindari *phising*, pengguna harus lebih berhati-hati dengan memperhatikan beberapa hal keamanan. Sebagai contoh, jika Anda mengakses suatu halaman *website*, maka pastikan anda berada di halaman website dengan url domain yang benar. Data yang diincar oleh pelaku *phishing* di antaranya: kata sandi, informasi kartu kredit, alamat email, dan *one-time password* (OTP). Cara kerjanya adalah dengan mengelabui target dengan berbagai tipuan yang terlihat normal bagi target. Hal ini bermaksud untuk membuat target tidak sadar bahwa data mereka baru saja dicuri. Data yang dicuri tentu saja digunakan untuk tindak kejahatan seperti pencurian, penyalahgunaan identitas pribadi, hingga pemerasan uang.[4]

Pelaku *phising* ini sering disebut dengan *hacker*. Mereka ini memanfaatkan kecanggihan teknologi untuk mendapatkan keuntungan dengan jalan "melanggar hukum. Seseorang bisa menjadi korban web *phising* ini jika meng-klik e-mail palsu. Bisa pula dengan mengklik link situs yang mengarahkan user untuk mendownload

[4] Ozora Antari,2021, *Phising; Pengertian, Ciri-Ciri dan Cara Mengatasinya*, diakses tanggal 2 desember 2021 pukul 21:00 WIB *https://www.jojonomic.com/blog/**phising***

malware. Dengan inilah maka pelaku mendapatkan akses komputer anda secara penuh tanpa anda sadari sama sekali.

Kasus kebocoran data di Indonesia sudah sering terjadi belakangan ini adalah data 279 juta WNI (Warga Negara Indonesia) yang tersebar dalam forum online pada 20 Mei 2021 berisi NIK (Nomor Induk Kependudukan), nomor ponsel, email, alamat, dan gaji yang diduga merupakan data dari BPJS (Badan Penyelenggara Jaminan Sosial) Kesehatan. Data tersebut termasuk data penduduk Indonesia yang telah meninggal dunia. Pihak BPJS hingga saat ini belum mengakui bahwa data tersebut berasal dari BPJS. Namun, mengakui data tersebut mirip dengan data yang ada pada BPJS.[5]

Kasus lain dari kebocoan yang terjadi di Indonesia adalah kasus kebocoran data pengguna Tokopedia yang terjadi Pada awal Mei 2020, sebanyak 91 juta data pengguna dan lebih dari tujuh juta data merchant Tokopeda dikabarkan dijual di situs gelap (*dark web*) dengan harga jual sebesar 5000 Dollar Amerika Serikat dan sudah di unduh oleh lebih dari 50 pengguna. Data tersebut diperjual belikan secara bebas, namun orang yang ingin mengunduh data tersebut harus menggunakan VPN karena data tersebut ada di server Amerika. Data pengguna Tokopedia yang dijual mencakup gender, lokasi, username, nama lengkap pengguna, alamat e-mail, nomor ponsel, dan password. Data tersebut kabarnya sudah dikumpulkan peretas sejak Maret 2020. Tokopedia mengklaim bahwa informasi milik pengguna tetap aman dan terlindungi. *VP of Corporate Communications* Tokopedia, Nuraini Razak mengatakan bahwa password milik pengguna telah terlindungi dan dienkripsi. Tokopedia juga

[5] Pebrianto, Fajar 2021 *Investigasi Kebocoran Data 279 Juta Penduduk Libatkan Polri, Kemenhan, hingga BIN*,15 Oktober 2021 TEMPO.CO.

menerapkan sistem kode OTP (*one-time password*) yang hanya bisa diakses secara real time oleh pemilik akun.[6]

Kasus lain yang banyak terjadi di Indonesia adalah jual beli data konsumen. Konsumen yang datanya berhasil diperoleh menjadi target pemasaran suatu produk perusahaan atau perseorangan. Tidak sedikit pula pengguna internet menawarkan jasa jual-beli akun atau pengikut. Padahal praktik tersebut membuka ruang terjadinya penyalahgunaan data seseorang untuk melakukan kejahatan. Kasus terbaru yaitu penipuan dan penggelapan kartu kredit nasabah dengan tersangka Imam Zahali (IZ), yang menyebabkan kerugikan pihak bank sekitar Rp 250 juta setelah menggunakan kartu kredit nasabah untuk transaksi gesek tunai. Hasil kejahatan itu kemudian digunakan untuk kepentingan dirinya, salah satunya menunaikan ibadah haji di Tanah Suci Mekah. Pelaku mendapatkan data nasabah dengan cara membelinya di internet sebesar Rp 800 ribu untuk 25 data. Dari data tersebut, pelaku kemudian menghubungi korban dengan mengaku sebagai sales kartu kredit dan menawarkan untuk menaikkan limit kartu kredit. Bentuk lain dari diabaikannya perlindungan terhadap privasi adalah munculnya sebuah pesan berisi iklan yang biasa disebut *Location-Based Messaging*. Pesan tersebut akan terkirim otomatis kepada seseorang jika ia berada di tempat tertentu. Padahal, belum tentu ia pernah menyetujui suatu perjanjian dengan provider dan memperbolehkan mereka merekam setiap aktivitasnya.[7]

Kasus penyalahgunaan data pribadi terus meningkat dari tahun ke tahun. Secara statistik dalam kurun waktu 2017-2019 kasus pencurian data pribadi

[6] Anggi Amanda,*2020, Analisis Kebocoran Data Pengguna Tokopedia dari Sudut Pandang Etika Bisnis*,12 November 2021. KUMPARAN

[7] Niffari, Hanifan, 2020, *"PERLINDUNGAN DATA PRIBADI SEBAGAI BAGIAN DARI HAK ASASI MANUSIA ATAS PERLINDUNGAN DIRI PRIBADI Suatu Tinjauan Komparatif Dengan Peraturan Perundang-Undangan Di Negara Lain"*. Jurnal Hukum dan Bisnis Volume VI Nomor 1 Juni 2020. hal. 1-14.

mengalami kenaikan yang signifikan. Bareskrim Polri mencatat di tahun 2017 terdapat 47 kasus, 2018 meningkat menjadi 88 kasus, dan terus meningkat pada 2019-2020 sebanyak 140 kasus. Sejauh ini kesadaran masyarakat terkait kejahatan data pribadi dinilai masih rendah. Hal ini dibuktikan dengan data hanya 278 dari total 11.777 atau hanya 2,3%.

Oleh sebab itu, perkembangan teknologi tersebut membutuhkan kerangka perlindungan data yang kuat dan lebih koheren, didukung oleh penegakan yang kuat, mengingat pentingnya menciptakan kepercayaan yang akan memungkinkan ekonomi digital berkembang di seluruh pasar internal. Orang perseorangan harus memiliki kendali atas data pribadi mereka sendiri. Kepastian hukum dan praktis bagi orang perseorangan, pelaku ekonomi dan otoritas publik harus ditingkatkan. Perlindungan hukum adalah segala upaya pemenuhan hak dan pemberian bantuan untuk memberikan rasa aman kepada saksi dan/atau korban dimana perlindungan hukum korban kejahatan sebagai bagian dari perlindungan masyarakat yang diwujudkan dalam berbagai bentuk, seperti pemberian restitusi, kompensasi, pelayanan medis, dan bantuan hukum.[8]

Berbicara tentang regulasi data yang dijadikan pedoman atau *guideline* pada saat ini adalah *European Union General Data Protection Regulation* Selanjutnya disebut sebagai EU GDPR sebagai acuan perlindungan data pribadi saat ini. Dimana dalam EU GDPR disebutkan bahwa "Pemrosesan data pribadi harus dirancang untuk melayani umat manusia. Hak atas perlindungan data pribadi adalah hak mutlak, harus diperhatikan dalam kaitannya dengan fungsinya dalam masyarakat dan diseimbangkan dengan hak-hak dasar lainnya, sesuai dengan prinsip proporsionalitas.

[8] Soerjono Soekanto, *1984, Pengantar Penelitian Hukum,* Ui Press. Jakarta, hal 133.

Regulasi ini menghormati semua hak dasar dan mematuhi kebebasan dan prinsip-prinsip yang diakui dalam Piagam sebagaimana tercantum dalam Perjanjian, khususnya penghormatan terhadap kehidupan pribadi dan keluarga, rumah dan komunikasi, perlindungan data pribadi, kebebasan berpikir, hati nurani dan agama, kebebasan berekspresi dan informasi, kebebasan untuk menjalankan bisnis, hak atas pemulihan yang efektif dan pengadilan yang adil, dan keragaman budaya, agama dan bahasa."

Selain EU GDPR, Reguliasi perlindungan data pribadi yang juga menjadi patokan dalam membuat aturan tentang perlindungan data adalah *Organization For Economic Co-Operation and Development* Tahun 1980 yang selanjutnya disebut sebagai OECD. Dimana dalam OECD ini membahas tentang prinsip perlindungan data pribadi yang kemudian dikembangkan oleh Uni Eropa menjadi regulasi perlindungan data pribadi yang kita kenal dengan EU GDPR dan ini lah yang menjadi pedoman atau patokan bagi negara-negara didunia dalam merumuskan regulasi perlindungan data pribadi untuk negaranya.

Perlindungan umum terhadap hak dan data pribadi di Indonesia termuat pada Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 Pasal 28G Ayat (1) , yang berbunyi "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."

Regulasi perlindungan data pribadi di Indonesia biasanya akan merujuk pada aturan teknis seperti Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PSTE), Penyelenggara Sistem

Elektronik dan Peraturan Menteri Kominfo Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik.

Indonesia sampai saat ini belum mempunyai Undang-Undang khusus yang mengatur perlindungan data pribadi, aturan tentang perlindungan data pribadi di Indonesia masih berbentuk rancangan undang-undang yang belum disahkan oleh pemerintah Indonesia. Disisi lain, regulasi setingkat Undang-Undang yang mengatur data pribadi masih tersebar ke beberapa peraturan perundang-undangan sesuai karakteristik sektor masing-masing, misalnya di bidang perbankan, perusahaan, telekomunikasi, administrasi kependudukan, kearsipan, kesehatan, informasi dan transaksi elektronik.

Peraturan Perundang-Undang lain di Indonesia yang juga membahas tentang pentingnya perlindungan data adalah Undang-Undang Informasi dan Transaksi Elektronik atau yag sering kita kenal dengan UU ITE juga dijelaskan tentang perlindangan data pribadi terlatak pada Pasal 32 Ayat (1) yang berbunyi "Setiap orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apapun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu informasi elektronik dan/atau Dokumen Elektronik milik orang lain atau milik publik". Pihak tersebut mendapat jerat hukum yang dijelaskan pada pasal 48 UU ITE yang berbunyi "Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32 Ayat (1) dipidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp.2.000.000.000,00 (dua milyar rupiah)"

Konsep kehidupan pribadi berhubungan dengan manusia sebagai makhluk hidup. Dengan demikian orang perorang adalah pemilik utama dari hak perlindungan

data pribadi. Dalam konteks Indonesia, Putusan No.5/PUU-VIII/2011, MK (Mahkaman Konstitusi) juga menulis bahwa *right to privacy* merupakan bagian dari hak asasi manusia (*derogable rights*) dan cakupan dari *right to privacy* meliputi informasi atau *right to information privacy*, disebut juga *data privacy (data protection)*. Peraturan delegasi dari Undang-Undang ITE, PP Nomor 82 Tahun 2012 tentang Penyelenggara Sistem dan Transaksi Elektronik, memuat definisi data pribadi yaitu data perseorangan tertentu yang disimpan, dirawat, dijaga kebenaran serta dilindungi kerahasiaannya (Pasal 1 Angka 27).

Berdasarkan uraian diatas dengan banyaknya kasus kebocoran dan penyalahgunaan data pribadi yang terjadi di Indonesia pada saat sekarang ini, maka penulis tertarik untuk melakukan penelitian yang dituangkan dalam bentuk karya ilmiah yang berjudul " **KAJIAN YURIDIS TENTANG PERLINDUNGAN DATA PRIBADI MENURUT EUROPEAN UNION GENERAL DATA PROTECTION REGULATION (EU GDPR) TAHUN 2018 DITINJAU DARI HUKUM INTERNASIONAL".**

B. Rumusan Masalah

1. Bagaimanakah Pengaturan Perlindungan Data Pribadi Menurut *European Union General Data Protection Regulation* (EU GDPR) Tahun 2018?
2. Bagaimanakah Kajian Yuridis Tentang Perlindungan Data Pribadi Menurut Hukum Internasional?

C. Tujuan Penelitian

1. Untuk menganalisis tentang perlindungan data pribadi menurut *European Union General Data Protection Regulation* (EU GDPR)

2. Untuk menganalisis tentang kajian yuridis tentang perlindungan data pribadi menurut hukum Internasional

D. Metode Penelitian

Metode Penelitian pada dasarnya merupakan cara ilmiah untuk mendapatkan data dengan tujuan dan kegunaan tertentu. Maksud dari cara ilmiah adalah kegiatan bedasarkan pada ciri-ciri keilmuan yakni rasional, sistematis dan empiris.[9]

1. Jenis Penelitian

Jenis penelitian yang digunakan dalam penulisan penelitian ini adalah jenis penelitian Yuridis Sosiologis *(Socio Legal Reserch*) atau dapat disebut pula dengan penelitian lapangan, yaitu mengkaji ketentuan hukum yang berlaku serta apa yang terjadi pada kenyatannya.**[10]**

Menurut Amiruddin dijelaskan bahwa "penelitian yuridis sosiologis adalah penelitian hukum yang menggunakan data sekunder sebagai data awalnya, yang kemudian dilanjutkan dengan data primer atau data lapangan, Meneliti efektivitas suatu Undang-Undang dan penelitian yang ingin mencari hubungan (korelasi) antara berbagai gejala atau variabel sebagai alat pengumpul datanya terdiri dari studi dokumen, dan wawancara (*interview)*"[11].

2. Sumber data

Sumber dan jenis data Sumber dan jenis data yang digunakan dalam penelitian ini adalah data primer dan data sekunder, yaitu:

a. Data Primer:

[9] Ranah Research, 2020, *Metode Penelitian dan Jenis-jenis Penelitian*, diakses pada 21 Januari 2022.

[10] Bambang Waluyo, 2002, *Penelitian Hukum Dalam Praktek*, Sinar Grafika, Jakarta, hal 15.

[11] Amiruddin dan Asikin Zainal, H, 2012. *Pengantar Metode Penelitian Hukum*, PT. Raja Grafindo Persada Jakarta, hal. 37.

Data yang langsung diperoleh dari sumber utama melalui penelitian langsung berkaitan dengan perlindungan data pribadi di Kantor Dinas Komunikasi dan Informatika Kota Padang dengan mewawancarai Ibu Fazarianti, SKM, M.Ti. Selaku Fungsional Persandian Ahli Muda Bidang Statistik Sektoral Persandian Daerah dan wawancara langsung dengan Bapak Irvi Efendi S.Kom. Selaku Administrator Database Kependudukan dan Bapak Fauzan Ibnovi S.T., M.Ti. Selaku Kepala Bidang Pengelolaan Informasi Administrasi Kependudukan Dinas Kependudukan dan Catatan Sipil Kota Padang.

b. Data Sekunder

Bahan hukum sekunder merupakan bahan hukum yang mendukung dan memperkuat bahan hukum primer memberikan penjelasan mengenai bahan hukum primer yang ada sehingga dapat di lakukan analisa dan catatan resmi, atau risalah dalam pembuatan peraturan perundang-undangan. Dan yang merupakan data yang mencangkup dokumen- dokumen resmi, buku-buku, hasil-hasil penelitian yang berwujud laporan.

Data hukum memiliki kaitan yang erat dengan bahan hukum primer yang akan membantu untuk memahami,menganalisis serta menjelaskan bagaimana hukum primer, antara lain merupakan hasil-hasil penelitian terdahulu,karya tulis dari ahli hukum dan teori dari para sarjana yang terkait dengan permasalahan penelitian ini.

Dalam penelitian ini, data sekunder terdiri dari:

1. Bahan Hukum Primer
    a. European Union- General Data Protection Regulation
    b. Undang - Undang Dasar 1945

c. Undang – Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang – Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

d. Peraturan Menteri komunikasi dan Informatika Nomor 20 Tahun 2016 Tentang Perlindungan Data Pribadi Dalam Sistem Elektronik

2. Bahan Hukum Sekunder

   a. Jurnal-Jurnal Tentang Perlindungan Data Pribadi

   b. Hasil Karya dari kalangan hukum

   c. Hasil penelitian terdahulu

3. Bahan Hukum Tersier

   a. Kamus Bahasa Indonesia

   b. Kamus Bahasa Indonesia- Inggris

3. Teknik Pengumpulan Data

Teknik pengumpulan data yang digunakan penulis dalam penelitian ini adalah:

a. Wawancara

Wawancara adalah teknik pengumpulan data untuk memperoleh keterangan dengan melakukan tanya jawab secara lisan dengan Responden. Responden adalah penjawab atas pertanyaan yang diajukan untuk kepentingan penelitian.[12] Sebelum peneliti melakukan wawancara, peneliti mempersiapkan pertanyaan berupa semi terstruktur yaitu daftar pertanyaan telah disusun secara terstruktur namun kalau ada isu berkembang dan berguna untuk peneliti

[12] Bambang Sunggono, 2006, *Metode Penelitian Hukum*, Raja Grafindo Persada, Jakarta, hal 42.

terkait dengan masalah yang di teliti maka peneliti langsung menanyakan kepada Responden yang bertugas di Kantor Dinas Komunikasi dan Informatika Kota Padang dan Kantor Dinas Kependudukan dan Pencatatan Sipil Kota Padang.

b. Studi Dokumen

Studi dokumen merupakan pengumpulan data yang dilakukan dengan cara mempelajari Literatur-Literatur, Peraturan Perundang-undangan, Hasil penelitian dan buku–buku di berhubungan dengan masalah yang diteliti untuk mendapatkan data sekunder. Dengan lokasi perpustakaan

1) Perpustakaan Universitas Bung Hatta Kampus
2) Perpustakaan Fakultas Hukum Universitas Bung Hatta

4. Analisa Data

Salah satu cara menganalisis dalam penelitian ini adalah menganalisis data yang telah diperoleh dari hasil wawancara dan menganalisis dokumen-dokumen yang berkaitan dengan penelitian ini. Cara analisis data yang dilakukan penulis adalah kualitatif, merupakan analisis data yang tidak menggunakan angka melainkan memberikan gambaran-gambaran (*deskripsi*) dengan kata-kata atas temuan-temuan dan mengutamakan mutu atau kualitas data dan bukan kuantitas.[13]

[13] Salim HS dan Erlies Septiana Nurbani, 2013, *Penerapan Teori Hukum Pada Penelitian Tesis dan Disertasi*, PT Raja Gravindo Persada, Jakarta, hal. 27