

BAB I

PENDAHULUAN

1.1. Latar Belakang Masalah

Kehadiran revolusi digital di era globalisasi dalam kehidupan sehari-hari kita telah berhasil menempatkan peranan teknologi informasi. Hal ini menciptakan adanya dunia tanpa batas, jarak, ruang, dan waktu dan menempati posisi yang sangat strategis serta menambah efisiensi dan produktivitas. Pola hidup masyarakat yang berubah karena adanya inovasi dalam bidang Teknologi Informasi secara cepat menjadikan dunia kita yang sangat dan semakin bergantung pada produk digital dalam kehidupan sehari – hari dan pekerjaan, di mana ini adalah sebagai titik awal bagi Manusia untuk dapat melakukan suatu refleksi dan percakapan mengenai topik terkait etika digital, kejahatan siber. Terdapat 2 (dua) hal yang tidak dapat dipisahkan, yaitu Teknologi dan Masyarakat. Dewasa ini dalam perkembangan teknologi yang mempengaruhi berbagai Sektor, termasuk Pendidikan, Kesehatan, Publik, Perdagangan hingga Keuangan. Kehidupan manusia dalam seluruh sektor sangat terdampak dengan adanya Teknologi Informasi, sektor Perbankan juga merupakan salah satu sektor yang terdampak. Saat ini ketergantungan masyarakat akan teknologi informasi semakin tinggi di mana semakin tinggi juga risiko yang akan dihadapi oleh Masyarakat. Dalam halnya didunia Perbankan yang saat ini sangat terpengaruh dengan adanya perkembangan teknologi informasi ini, sehingga ada anggapan bahwa untuk menyelenggarakan kegiatan usahanya, sektor ini dapat melakukan inovasi baru. Kemajuan teknologi, pemerataan

digital, penggunaan internet oleh masyarakat memberikan kontribusi yang baik dan sekaligus menjadi sarana yang memadai dalam perbuatan melawan hukum termasuk tidak pidana (kejahatan). Dari berbagai contoh kasus tindak pidana yang terjadi inilah yang dikemudian dikenal dengan pada era ini yaitu “*cybercrime*” atau kejahatan siber¹.

Menelisik dari permasalahan dalam Teknologi Informasi yang saat ini terjadi di mana salah satunya terkait keamanan Data Pribadi yang telah menjadi sebuah isu global yang sangat penting di zaman sekarang dapat dikatakan era “*Web of The World*”. Praktik yang dilakukan oleh manusia sekarang dengan kemajuan yang amat mutakhir dalam melakukan komunikasi antar individu yang menggunakan komunikasi bergerak (*mobile communication*) seperti *smartphone* dan super-komputer yang terhubung dengan internet², yang mana internet menghubungkan dunia fisik ke dalam satu jaringan yang disebut dengan dunia maya (*cyberspace*). Terjadinya serangan siber atas Pelindungan Data dan atau Pengelolaan Data Pribadi juga akan dapat terjadi secara efektif dari kejahatan siber. Dalam hal ini, dengan kemajuan Teknologi Informasi yang saat ini berkembang dengan sangat cepat memuat batas antara Privasi semakin tipis, sehingga berbagai macam informasi pribadi serta Data Pribadi masyarakat semakin mudah untuk tersebar luas.

Di Indonesia pelanggaran Data Pribadi pada tahun 2023 terdapat pada setidaknya 10 kasus di mana aplikasi Pemerintah atau institusi Negara menjadi sumber bocornya data. Dari 10 kasus yang tercatat, Bjorkä berandil pada sebagian besarnya

¹ Lauder Siagian, *Peran Keamanan Siber Dalam Mengatasi Konten Negatif Guna Mewujudkan Ketahanan Informasi Nasional*, Jurnal Asimetris, Vol. 4, No (2018): hal. 3

² Sinta Dewi Rosadi, 2015, *Cyber Law: Aspek Data Pribadi Menurut Hukum Internasional, Regional, Dan Nasional*, Refika Aditama, Bandung, hlm.1.

yaitu bocornya Data Pelanggan IndiHome, PLN, Data MyPertamina, serta kebocoran Data Nasabah yang disebabkan oleh *ransomware lockbit*³. Ditahun yang sama, terdapat juga kasus yang serupa di mana terdapat kebocoran sebanyak 15 juta Data Pribadi nasabah dan karyawan pada Bank Syariah Indonesia (BSI)⁴. Surfshark selaku perusahaan keamanan siber melalui hasil kajiannya menunjukkan bahwa dalam jangka waktu Kuartal-II tahun 2022 terdapat adanya kebocoran data dalam 1,04 juta akun di Negara Indonesia yang jumlahnya melonjak menjadi 143% dari Kuartal-I 2022.⁵

Ransomware biasanya menginfeksi sistem dengan mengeksploitasi celah keamanan yang belum diperbaiki. Contoh yang sering menjadi sasaran adalah akses jarak jauh komputer pribadi yang terhubung ke Internet, yang kemudian dimanfaatkan untuk mengakses jaringan internal Bank. Interaksi ini berhasil mendapatkan akses ke *server remote access* secara menyusup ke jaringan korban, dan *ransomware* dapat berbalik dan menjual akses tersebut atau menggunakannya untuk menyebarkan *ransomware* secara langsung. Modus penyalahgunaan Data Pribadi juga semakin bervariasi salah satunya dengan cara mengirimkan pesan melalui Short Message Service (SMS), e-mail, maupun push notification yang berisikan narasi hadiah, tips, undian, hingga bantuan dari Pemerintah yang menyertakan tautan penipuan (phising

3 Ransomware Lockbit adalah ransomware yang dikendalikan oleh operator, di mana saat menjalankan aksinya maka operator tersebut akan meninggalkan jejak dan tanda tangan Lockbit pada data atau komputer yang datanya berhasil dienkripsi, diakses dari <https://www.kompas.com/tren/read/2023/05/14/170000665/apa-itu-ransomware-lockbit-dan-apabedanya-dengan-ransomware-lainnya-?page=all> pada tanggal 10 Mei 2023 pukul 13.12

⁴ Fahmi Ahmad Burhan, "Data Pribadi Nasabah Bank Syariah Indonesia (BSI) Diduga bocor, OJK Turun Tangan!", diakses dari <https://finansial.bisnis.com/read/20230516/90/1656624/data-pribadi-nasabah-bsi-bris-diduga-bocor-ojk-turun-tangan> pada tanggal 10 Mei 2024

⁵ Vika Azkiya Dihni, "Kasus Kebocoran Data di Indonesia Melonjak 143% pada Kuartal II 2022," Databoks, 2022" diakses dari <https://databoks.katadata.co.id/datapublish/2022/08/09/kasus-kebocorandata-di-indonesia-melonjak-143-pada-kuartal-ii-2022> pada 10 Mei 2024

link). Dampaknya bagi Masyarakat yang terlanjur membuka tautan itu sendiri dapat menyebabkan pencurian Data Pribadi korban yang membuka tautan tersebut dan memungkinkan untuk digunakan untuk tindak kejahatan seperti penjualan Data secara ilegal, penipuan yang mengatas namakan nama korban, Organisasi, atau Pihak tertentu.

Phishing adalah salah satu tindakan kejahatan siber melalui tautan yang mengatasnamakan Organisasi, Perusahaan, atau Pihak tertentu. Tautan dibuat seolah-olah berasal atau dikirimkan oleh Pihak yang kredibel untuk menarik perhatian korban⁶. Tindakan tersebut dianggap sebagai kejahatan yang dapat merusak reputasi baik individu maupun perusahaan. Meskipun pemulihan data yang hilang mungkin dilakukan, namun reputasi yang telah tercemar akibat penyebaran data pribadi sulit untuk dipulihkan. Dampaknya bisa sangat luas, mulai dari kebocoran data sensitif hingga hilangnya kepercayaan publik. Hal ini tentunya akan mengurangi tingkat kepercayaan masyarakat terhadap bank, di mana indikator yang digunakan oleh konsumen untuk menilai layanan yang diterima (*perceived service*) dan yang diharapkan (*expected service*) berdasar kepada kualitas layanan (Kotler, 2000). Supancana menyatakan bahwa pelanggaran terhadap Pelindungan Data pribadi banyak terjadi dalam dunia bisnis. Oleh karena itu, pemerintah bersama pelaku usaha perlu mengembangkan sistem hukum yang melindungi privasi, baik melalui *soft law* maupun *hard law*. Di samping itu, setiap individu juga perlu mengambil langkah-langkah preventif untuk melindungi data pribadinya sendiri (Supancana, 2009:34).

⁶ Andrian W Finaka, “Mengenali Tanda Link Penipuan”, 2023 diakses dari <https://indonesiabaik.id/infografis/mengenali-tanda-link-penipuan-1> pada tanggal 10 Mei 2024

Penggunaan teknologi informasi, terutama dalam pengumpulan data melalui internet, memungkinkan Data Pribadi seseorang terkumpul dengan sangat mudah tanpa sepengetahuan individu yang bersangkutan. Hal ini memberi risiko terhadap subjek data pribadi yaitu ancaman bagi hak-hak konstitusional yang mereka miliki, yang pada gilirannya membuka celah bagi terjadinya tindak kejahatan. Dari implementasi Teknologi Informasi yang digunakan untuk mengumpulkan data melalui jaringan internet, mempermudah dalam akses terhadap Data Pribadi seseorang tanpa sepengetahuan mereka. Praktik ini dapat memberikan ancaman pada data pribadi dalam perlindungan hak konstitusional mereka, bahkan berpotensi menimbulkan tindak kejahatan yang merugikan pihak yang bersangkutan.

Apabila kita terikat oleh pemikiran yang dibentuk oleh peraturan yang lama, sulit untuk berpikir sesuai dengan kondisi yang dibutuhkan ke depan. Selama tiga tahun terakhir, telah terjadi berbagai perubahan peraturan oleh regulator terkait sistem keuangan, yang dalam pertimbangan dasarnya dijelaskan bahwa perubahan tersebut dilakukan untuk menghadapi tantangan yang ditimbulkan oleh perkembangan digital⁷. Pelanggaran terhadap penggunaan data pribadi terjadi dalam beberapa sektor di Indonesia, dalam dunia Perbankan penggunaan data pribadi dilakukan secara ditukar yang menggunakan sistem *sharing* atas informasi pribadi yang ditukar antara pada pengguna kartu kredit, memberikan informasi terkait hubungan dengan pemegang kartu kredit itu sendiri dari dan/atau pihak ketiga atau diperjual belikan di antara Bank maupun pihak ketiga yang termasuk halnya ini adalah transaksi.

⁷ DR. dr. Bayu Prawira Hie, MBA, 2021, Panduan Transformasi Digital Bank di Indonesia, hlm. v

Secara tradisional, Perbankan dituntut untuk terus berhadapan dengan Hukum dan Peraturan yang sangat ketat, di mana Otoritas Jasa Keuangan (“OJK”) dan Bank Indonesia (“BI”) sebagai Regulator memiliki peran penting dalam sistem keuangan Indonesia, dan kolaborasi antara kedua Lembaga ini sangat krusial untuk menjaga stabilitas dan integritas sektor Keuangan. Dengan hadirnya ekonomi digital gelombang keempat, Bank menyadari bahwa transaksi yang dilakukan oleh nasabah selama bertahun-tahun mengandung Data yang berharga, tetapi penggunaan Informasi Data Pribadi dan penyimpanan Data ini juga tidak luput oleh aturan yang mengikat. Selain itu, Bank juga dihadapkan pada dilema bahwa mereka ingin menggunakan peluang dan kemungkinan komersial ini dengan cara yang fleksibel dan cepat, tetapi di sisi lain Bank juga harus meminimalkan risiko penyalahgunaan Data Pribadi. Pada akhirnya kepercayaan dan reputasi adalah nilai inti bank dan karenanya tidak boleh dirusak maupun dilanggar.

Kesadaran tiap-tiap individu terkait pentingnya menjaga data pribadi dapat mendukung upaya Pemerintah dalam perlindungan terhadap Data Pribadi Masyarakat dengan cara menumbuhkan kesadaran masing-masing. Hal ini telah dijamin dalam konstitusi Undang-Undang Dasar 1945, terkait Hak Asasi Manusia, di mana Hak Asasi Manusia di atur pada Pasal 28G ayat (1) UUD 1945 yang berbunyi:

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

Di mana Indonesia, sebagai negara hukum harus melindungi dan menjamin HAM dari masyarakatnya terutama konstitusinya. Tercerminnya dari beberapa kasus

yang terjadi di Indonesia, Pelindungan dan Pembentukan hukum dari Pemerintah juga harus berperan aktif dalam melindungi Privasi dan Data Pribadi masyarakat, melalui beberapa kali Rapat Paripurna DPR RI yang diselenggarakan di Jakarta, hingga muncul urgensi dalam Peraturan yang mengatur secara khusus terkait Pelindungan Data Pribadi yang disahkan pada tahun 2022 yaitu Undang – Undang No. 27 Tahun 2022 tentang Pelindungan Data Pribadi (“UU PDP”).

Penggunaan internet memberikan kemudahan dalam berbagai bidang, namun di sisi lain, hal ini juga menciptakan keadaan serta tantangan baru yang perlu diatur oleh Negara untuk memastikan bahwa Hak Privasi masyarakat Indonesia terlindungi dari berbagai ancaman atau serangan siber. Pelindungan Data Pribadi harus diperhatikan agar Masyarakat Indonesia tidak menjadi korban penyalahgunaan yang dapat merugikan masyarakat dalam bentuk materi maupun secara sosial.

Lahirnya Peraturan baru ini sejalan dengan Konsep–konsep Hukum yang bertumbuh dan berkembang sampai satu momentum yuridis yang menjadi suatu dasar argumentasi rasional yang dapat diterima oleh warga. Pembentukan hukum yang tegas, komprehensif, dan efektif akan menjadi salah satu pandangan hukum tersebut dapat dipahami sebagai sesuatu yang benar, konstruksi teoritis akan bergeser ke arah bentuk baru yang dapat disebut sebagai suatu teorema hukum⁸. Disini dapat terlihat bahwa UU PDP lahir berisikan tentang bagaimana pemegang Hak atas Privasi dapat melakukan kontrol atas Data Pribadi⁹. Dan bagi Konsumen yang mengalami kerugian bisa

⁸ Dr. P.M. Rondonuwu “Dari Eksistensi ke Rekonstruksi”, RajaGrafindo Persada, 2023, Hlm 17

⁹Unpar, “RUU Perlindungan Data Pribadi Perlu Atur Saksi bagi Pengumpul Data Jika Bocor”, <https://unpar.ac.id>, dikunjungi pada tanggal pada tanggal 10 Mei 2024 pukul 18.00

menuntut pihak yang lalai dalam menjaga kerahasiaan Data Pribadi Konsumen. Karena itu, individu harus ditempatkan sebagai fokus utama oleh hukum, sehingga memastikan Pelindungan Data Pribadi, tanpa memandang apakah dalam hukum Pelindungan Data Pribadi tersebut juga mempertimbangkan Hak Privasi seseorang, baik yang bersifat universal maupun peraturan tertulis pada undang-undang atau aturan moral yang tidak tertulis.

Data Pribadi merupakan informasi baik melalui sistem elektronik maupun non-elektronik yang berupa data perorangan serta dapat diidentifikasi secara terpisah maupun bersama-sama dengan langsung atau tidak langsung.¹⁰ Selama ini Perbankan telah mengutamakan aspek Pelindungan Konsumen bagi Masyarakat, misalnya terdapat halaman persetujuan untuk Nasabah pada formulir Syarat dan Ketentuan yang mengizinkan atau tidak mengizinkan Bank dalam memberikan Informasi atau penawaran produk yang sifatnya opsional bagi Nasabah itu sendiri. Hal ini juga sejalan dengan ketentuan Pasal 38 UU PDP yang mewajibkan Pengendali Data Pribadi untuk memastikan perlindungan terhadap data pribadi dari pemrosesan yang tidak sah.

Data Pribadi Nasabah yang biasa digunakan oleh Bank ini berisi tentang informasi-informasi penting milik nasabah seperti Nama, NIK, Alamat, Usia, Nama Ibu, Pekerjaan, Catatan Keuangan. Dalam konteks ini Nasabah dapat disebut juga sebagai Konsumen. Definisi Konsumen merujuk pada setiap individu yang perlu mendapat perlindungan, asalkan mereka tidak memiliki kapasitas atau bertindak

¹⁰ Indonesia (1), Undang-Undang tentang Pelindungan Data Pribadi, UU No. 27 Tahun 2022, Pasal 1.

sebagai produsen atau pelaku usaha¹¹. Permasalahan yang timbul dari sebuah Pemrosesan Data Pribadi pada Perbankan adalah penggunaan Data yang tidak sesuai untuk tujuannya. Dalam konteks dunia Perbankan masalah Pelindungan Data Pribadi menjadi semakin kompleks.

Pelindungan di bidang perbankan terhadap keamanan serta kerahasiaan data diatur dalam Pasal 19 ayat (1) POJK No.22 Tahun 2023 mengenai Perlindungan Konsumen dan Masyarakat di Sektor Jasa Keuangan, yang mengharuskan Yang memberikan Pelaku Usaha Jasa Keuangan (PUJK) kewajiban dalam pengelolaan data serta informasi pribadi milik konsumen agar menggunakan teknologi informasi, Kewajiban bagi PUJK adalah menggunakan teknologi informasi yang andal untuk melakukan pengkajian dan/atau ke mana secara berkala untuk menjamin keamanan dan/atau informasi pribadi konsumen. Selanjutnya pada Pasal 36 menegaskan bahwa menjaga keamanan aset konsumen dan/atau dana yang merupakan tanggung jawab PUJK juga menjadi kewajiban PUJK. Keseluruhan peraturan ini menunjukkan bahwa ada urgensi bagi negara Indonesia untuk memperhatikan Pelindungan Data Pribadi. Pengendali Data Pribadi¹², Dalam hal ini Perbankan dapat mengumpulkan, memproses, sesuai untuk tujuannya dan didapatkan secara sah. Pengawasan yang dilakukan oleh Otoritas yang berwenang pada Sektor Jasa Keuangan terhadap perbankan serta kepatuhan Bank dan Tata Kelola yang baik merupakan tanda bahwa adanya

¹¹ Zulham, Hukum Perlindungan Konsumen, Cetakan 1, Kencana Perenda Media Group, Jakarta, 2013, hlm. 15.

¹² Pengendali Data Pribadi adalah adalah setiap orang, badan publik, dan organisasi internasional yang bertindak sendiri-sendiri atau bersama-sama dalam menentukan tujuan dan melakukan kendali pemrosesan Data Pribadi, Pasal 1 angka (4), UU No. 27 Tahun 2023 tentang Undang-Undang Pelindungan Data Pribadi

Pelaksanaan atas perlindungan hukum terhadap Data Pribadi serta pengawasan dari setiap kegiatan dan aktivitas Bank secara efektif. Sebagai bentuk kesadaran atas pentingnya peningkatan dan/atau kualitas pelayanan kepada Nasabah, Bank perlu menempatkan perhatian yang sungguh-sungguh terhadap Pelindungan Data Pribadi.

Dampak negatif dari lemahnya Pelindungan Data Pribadi antara lain adalah terjadinya penyalahgunaan informasi pribadi Konsumen secara ilegal, pencurian data yang digunakan untuk tindak kriminal lainnya, pemalsuan dalam berbagai bentuk, serta kesulitan dalam penanganan dan pembuktian kejahatan. Selain itu, hal ini juga menyebabkan kendala dalam pelacakan, penyelidikan, penyidikan, penuntutan, dan pembuktian suatu kejahatan. Karena informasi pribadi telah menjadi komoditas utama dalam ekonomi informasi, perlindungan privasi atas data pribadi akan menciptakan rasa aman dan nyaman dalam proses transaksi.

Berangkat dari latar belakang dan di atas, menarik untuk mengkaji lebih mendalam khususnya tentang bagaimana penulis ingin mengkaji lebih dalam terkait permasalahan ini dengan judul **“Kajian Prinsip – Prinsip Hukum Pada Pelindungan Data Pribadi Sebagai Bentuk Pelindungan Konsumen Pada Perbankan Berdasarkan Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi”**.

1.2. Rumusan Masalah

Mengacu pada latar belakang masalah dalam tulisan yang telah diuraikan sebelumnya terhadap Peraturan UU No. 27 Tahun 2023 tentang Pelindungan Data Pribadi (“UU PDP”) dapat diformulasikan sebagai berikut:

1. Bagaimana pengaturan hukum pada Perbankan serta Tanggung Jawab Bank Terhadap Pelindungan Data Pribadi nasabah Bank berdasarkan UU PDP?
2. Bagaimana pelaksanaan Undang-Undang Pelindungan Data Pribadi dalam hal pemrosesan Data Pribadi oleh Perbankan?

1.3. Tujuan Penelitian

Tujuan dari penelitian ini adalah:

1. Untuk mengetahui pengaturan menurut ketentuan peraturan perundang-undangan yang berlaku mengenai Pelindungan Data Pribadi Nasabah.
2. Untuk memperdalam dan melakukan terhadap analisis bentuk tanggung jawab Bank selaku Pengendali Data Pribadi terhadap dalam hal terjadinya Pelanggaran Data Pribadi nasabah Bank.

1.4. Manfaat Penelitian

1. Manfaat Teoritis

Dalam konteks teori, penelitian ini diharapkan dapat menambah wawasan dan dapat mengembangkan pemahaman ilmu hukum, khususnya tentang Pelindungan Data Pribadi sebagai bentuk Pelindungan Konsumen pada Sektor Perbankan.

2. Manfaat Praktis

Manfaat secara Praktis diharapkan dapat memberikan kontribusi yang bermanfaat serta sumbangan pikiran dan gagasan baru khususnya yang bekerja dalam profesi Perbankan dalam melakukan *best practice* Pelindungan Data Pribadi agar terhindar dari Sanksi oleh Pemerintah.

1.5. Sistematika Penulisan

BAB I PENDAHULUAN

Dalam bab ini, akan dipaparkan secara ringkas isi dari bab-bab yang akan dibahas selanjutnya, yang kemudian akan diikuti dengan pembahasan tesis yang memiliki hubungan yang saling terkait untuk menyoroti tema utama topik ini. Bab ini juga bertujuan untuk menyajikan pembahasan secara sistematis yang dimulai dari latar belakang masalah penelitian, perumusan masalah penelitian, tujuan penelitian, manfaat penelitian, dan struktur penelitian yang akan diikuti.

BAB II TINJAUAN PUSTAKA

Pada tinjauan pustaka ini, terdapat dua aspek yang diperhatikan, yakni landasan teori dan landasan konseptual. Bagian landasan teori akan membahas berbagai teori yang relevan dengan penelitian, khususnya teori Kepastian hukum yang akan diuraikan dan diterapkan dalam konteks penelitian ini. Sedangkan, dalam landasan konseptual, akan dijelaskan definisi dan penjelasan kata-kata yang digunakan peneliti dalam menyusun tesis ini.

BAB III METODE PENELITIAN

Dalam bab metode penelitian hukum ini, peneliti akan menjelaskan tentang jenis penelitian yang dipilih, jenis data

yang akan digunakan, teknik pengumpulan data yang akan diterapkan, pendekatan yang digunakan dalam menganalisis data, serta proses analisis data yang akan dilakukan.

BAB IV HASIL PENELITIAN DAN ANALISIS

Dalam bab ini, peneliti akan menguraikan jawaban atas permasalahan pada tesis ini, yaitu (i) pengaturan hukum pada Perbankan serta Tanggung Jawab Bank Terhadap Pelindungan Data Pribadi nasabah Bank berdasarkan UU PDP (ii) pelaksanaan Undang-Undang Pelindungan Data Pribadi dalam hal pemrosesan Data Pribadi oleh Perbankan.

BAB V PENUTUP

Bab ini merupakan bagian akhir yang mengemukakan rangkuman dari temuan dan analisis yang telah dibahas dalam bab-bab sebelumnya, serta memberikan rekomendasi dan saran untuk penelitian selanjutnya.