BAB I

LATAR BELAKANG DAN RUMUSAN MASALAH

Penetrasi teknologi yang semakin berkembang memudahkan individu dalam kehidupan sehari-hari dengan diikuti adanya distribusi data yang kian cepat dan masif. Data yang didistribusikan oleh individu pada sistem elektronik dalam penggunaan media elektronik dalam hal ini individu memiliki hak agar data pribadinya baik data yang bersifat umum dan spesifik tidak disalahgunakan oleh siapa pun dengan mendapatkan perlindungan hukum, sehingga kehidupan pribadi individu tersebut tidak terganggu atas intervensi dari siapa pun. Adanya percepatan teknologi pada sistem elektronik dapat menimbulkan celah adanya kebocoran data yang dapat disebabkan dari dua faktor yaitu faktor internal dari korporasi itu sendiri seperti sistem keamanan elektronik yang lemah, penempatan SDM yang kurang baik maupun korporasi tidak menjalankan ketentuan sebagai Sistem Penyelenggara Elektronik (PSE) sebagaimana diatur di dalam undang-undang serta faktor eksternal kebocoran data dipicu dari berbagai kasus *cybercrime* seperti praktik jual beli data pribadi, ancaman keselamatan diri, *hacking* (peretasan), *cracking* (pembajakan), pemerasan hingga dapat terjadinya penipuan daring.

Pelindungan data melekat erat dengan privasi dimana hal ini merupakan hal yang sangat fundamental untuk menjaga keamanan perlindungan data pribadi individu. Dalam konstitusi Indonesia, hak privasi dan hak seseorang tidak dapat diambil oleh siapa pun diatur secara tegas di dalam Pasal 28G Ayat (1) dan Pasal 28H Ayat (4) Undang-Undang Dasar NRI 1945. Dapat dikatakan, isu privasi merupakan pembatasan atau melindungi dari ancaman yang tidak diinginkan dalam kehidupan. Pelopor atau ‘ayah’ dari konsep Modern Data Privacy Law yaitu Alan Westin. Dalam bukunya yang berjudul “Privacy and Freedom”, Alan Westin menyampaikan privasi merupakan hak invidu,

organisasi(lembaga) atau kelompok untuk menentukan sendiri kapan, bagaimana dan sejauh mana informasi mengenai individu dikomunikasikan kepada orang lain(Rollenhagen, 2020).

Perlindungan privasi data menjadi topik yang diperhatikan oleh masyarakat universal. Istilah privasi data memiliki dua *terms* yang dipakai secara bergantian yakni perlindungan privasi dan data pribadi yang sesungguhnya. Dalam teoritis, privasi merujuk pada konteks abstrak yang lebih luas seperti hak untuk tidak diganggu, kontrol atas informasi pribadi dan akses terbatas. Sementara itu, perlindungan data pribadi yaitu perlindungan secara khusus mengenai cara regulasi dalam mengayomi, menghimpun, mendaftarkan, menyimpan, dieksploitasi maupun disebarluaskan terhadap data pribadi yang dimiliki oleh subjek data(Rosadi, 2015).

Korporasi sebagai *data controller* dan/atau *data processor* memegang kendali pemrosesan data pribadi dan sistem keamanan data individu dalam teknologi informasi yang dimilikinya. Namun, sayangnya sistem keamanan tidak selalu baik dan aman dalam menjaga keamanan data pribadi. Dilansir tempo.co kasus kebocoran data marak terjadi di Indonesia seperti dalam kasus kebocoran data pribadi BPJS Kesehatan dengan total 279 juta dan terdapat sebagian data yang diperjualbelikan di internet. Selain itu, kebocoran dialami oleh Cermati dengan 2,9 juta data bocor yang diperjualbelikan, Lazada dengan 1,1 juta data bocor, data pengguna Tokopedia diduga telah bocor dan pemilik akun twitter @underthebreach menyebut aktor peretas telah menjual database Tokopedia sebanyak 91 juta akun seharga US$ 5.000 di darkweb serta kebocoran data Komisi Pemilihan Umum (KPU) sebanyak 2,3 juta data warga Indonesia (Fajriadi, 2024). Selanjutnya, sejak kuartal I tahun 2020 jumlah akun yang mengalami kebocoran data fluktuatif. Klimaksnya, terdapat 39,6 juta akun yang dibobol oleh *hacker*. Terdapat 1,04 juta akun yang mengalami kebocoran data di Indonesia selama kuartal II pada tahun 2022. Jumlah tersebut meningkat 143% dari kuartal I tahun 2022 sebanyak 430,1 ribu akun berdasarkan informasi data dari perusahaan keamanan siber Surfhark. Secara global, terdapat 2,3 miliar akun yang bocor sejak awal tahun 2020 dan bahkan angkanya mencapai 5,1

miliar akun yang mengalami kebocoran data sejak 2004(Dihni, 2022). Selain kasus kebocoran data yang disebabkan oleh pihak eksternal, muncul kasus kebocoran data yang disebabkan pihak internal korporasi berdasarkan informasi yang diungkapkan pakar keamanan siber Teguh Aprianto melalui akun twitter nya @secgron pada 10 Maret 2024. Dalam cuitannya, *hacker* yang mengaku karyawan korporasi karena tidak setuju dengan *Fair Usage Policy* (FUP) yang diimplementasikan oleh Biznet. Terdapat 380 ribu akun pengguna Biznet bocor di dark web berupa nama, email, NIK, NPWP, nomor HP, alamat, dll. Pelaku juga mengancam kepada pihak manajemen Biznet apabila kebijakan FUP tidak dihapus sampai 25 Maret 2024, maka akan membocorkan data intenal Biznet Gio dan layanan *computing* milik biznet(Liputan6.com,2024).

Berkaca dari informasi data kebocoran data pribadi di Indonesia yang telah terjadi, pertanggungjawaban korporasi sangat vital karena korporasi sebagai *data cotroller* dan/atau *data processor* wajib bertanggungjawab dalam memproses data pribadi dengan membuktikan akuntabilitasnya berdasarkan pemenuhan kewajiban dalam melaksanakan prinsip perlindungan data pribadi. Mengenai pidana ekonomi dalam transaksi elektronik, memiliki isu hukum yang esensial untuk mengatasinya sebagaimana diungkapkan oleh Al Wisnubroto yaitu:

1. berkenaan teknis penerapan atau pelasaknaan hukum terhadap perbuatan kriminalitas dalam aktivitas transaksi elektronik dalam berbagai sumber hukum pidana positif khususnya dalam hukum pidana ekonomi dan Undang-Undang Informasi dan Transaksi Elektronik belum memadai;
2. berkenaan konsep regulasi *economic criminal law* dan *cyber law*, pelaku transaksi elektronik dilindungi secara hukum dalam kegiatan transaksi dari ancaman *cybercrime*; dan
3. berkenaan dalam teknis pembuktian, kejahatan yang dilakukan di dalam *cyberspace* (dunia maya) tidak tampak oleh penglihatan secara langsung dan objeknya didasarkan pada informasi data atau layanan komputer yang sifatnya *intangible object* (Wijaya, 2020).

   Korporasi dalam menyediakan media elektronik tidak menutup

kemungkinan dapat menjadi pelaku kebocoran data pribadi sehingga mengakibatkan kerugian bagi pengguna media elektronik tersebut. Hal ini yang menjadi faktor internal permasalahan kebocoran data yang diakibatkan dari kejahatan yang dikerjakan oleh korporasi itu sendiri, pengurus, individu yang menjalankan korporasi atau individu yang mengatasnamakan korporasi dengan tujuan memperoleh keuntungan bagi korporasi itu sendiri. Padahal, menjaga keamanan data pribadi sudah seharusnya menjadi prioritas yang absolut dari penyelenggara sistem elektronik. Selain itu, pertanggungjawaban pidana ekonomi khususnya dalam dalam sektor transaksi dan informasi elektronik sangat vital untuk diketahui.

Era digital mengubah pola kehidupan individu sebagai konsumen dalam bertransaksi elektronik dan aktivitas digital sehingga data informasi menjadi aset yang sangat berharga. Oleh karena itu, sepatutnya penyelenggara sistem elektronik bertanggungjawab atas privasi data individu. Kebocoran data yang diakibatkan oleh korporasi itu sendiri, pengurus, individu yang menjalankan korporasi atau individu yang mengatasnamakan korporasi untuk memperoleh keuntungan bagi korporasi dengan bentuk memperoleh atau mengumpulkan, mengungkapkan, menggunakan, membuat atau memalsukan data pribadi patut mempertanggungjawabkan secara pidana. Dengan demikian, sanksi pidana sebagai upaya terakhir (*ultimum remidium*) dibutuhkan. Berdasarkan latar belakang tersebut, peneliti tertarik untuk mengkaji kelemahan dari Undang-Undang No. 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik dimana sebelum lahirnya undang-undang pelindungan data pribadi merujuk pada undang-undang ITE, tetapi peristiwa kebocoran data pribadi masih terus terjadi dan peneliti juga tertarik mengkaji pertanggungjawaban pidana korporasi sebagai pelaku terjadi dimana dewasa ini korporasi memegang data pribadi dari subjek data pribadi untuk kepentingan dalam lingkup professional dan bisnis dengan tujuan meidentifikasi individu. Hal ini memungkinkan korporasi melakukan tindak pidana dalam membocorkan data pribadi individu serta mengkaji hak-hak yang diperoleh individu sebagai warga negara di dalam ketentuan Undang-Undang Pelindungan Data Pribadi (UU PDP) ketika menjadi korban kebcoran

data pribadi. Berdasarkan latar belakang yang telah dijelaskan, maka yang menjadi permasalahan dalam penelitian ini dirumuskan sebagai berikut:

1. Bagaimana kelemahan di dalam Undang-Undang No. 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang No. 11 Tahun 2008 tentang Informasi Transaksi dan Elektronik sehingga kebocoran data pribadi masih terjadi?
2. Bagaimana sistem pertanggungjawaban pidana bagi korporasi sehingga dapat memberikan perlindungan hak bagi subjek data pribadi?