

BAB I PENDAHULUAN

A. Latar Belakang

Perkembangan teknologi di Indonesia semakin maju dan pesat dari masa ke masa sehingga dengan adanya perkembangan teknologi di Indonesia tentu dapat berdampak pada kegiatan yang dilakukan oleh manusia seperti pada kegiatan transaksi jual beli, dengan adanya perkembangan teknologi dampak yang diberikan tidak hanya dampak positif melainkan ada juga dampak negatif yang dapat merugikan masyarakat.¹ Sebelum adanya perkembangan teknologi ini kegiatan jual beli hanya dapat dilakukan secara langsung antar pedagang dan pembeli harus berinteraksi secara tatap muka namun dengan adanya perkembangan teknologi seperti saat ini kegiatan transaksi jual beli tidak harus dilakukan secara tatap muka namun dapat melalui transaksi elektronik dimana baik penjual maupun pembeli dapat melakukan kegiatan tersebut melalui media elektronik yang terhubung dengan internet. Perdagangan elektronik menjadi salah satu bagian dari transaksi elektronik yang dapat menjadi tempat yang efektif bagi pelaku usaha untuk memperkenalkan dan menjual barang atau jasa ke calon konsumen dari seluruh dunia.

Perdagangan elektronik atau *e-commerce* meliputi seluruh proses dari pengembangan, pemasaran, penjualan, pengiriman, pelayanan, dan pembayaran para pelanggan, dengan dukungan dari jaringan para mitra bisnis di seluruh dunia. Sistem *e-commerce* sangat bergantung pada sumber daya internet dan banyak teknologi informasi lainnya untuk mendukung setiap

¹ Novi Purnama, "Dampak Perkembangan Teknologi Komunikasi Terhadap Kehidupan Sosial Budaya", *Jurnal Gema Eksos*, Vol. 5, No. 1, (2009), hlm. 40

proses ini.² Berdasarkan data dari Global Web Index, sebanyak 90 persen dari pengguna internet berusia 16 hingga 64 tahun di Indonesia pernah melakukan pembelian produk dan jasa secara online.³

Dalam transaksi yang dilakukan melalui *e-commerce* ini tentu memerlukan data seperti alamat email, nomor telepon, hingga alamat tempat tinggal guna memudahkan penjual mengirimkan barang yang telah dibeli oleh pembeli yang dimana jenis data diatas merupakan data yang bersifat pribadi. Selain adanya dampak positif dalam perkembangan teknologi maka ada juga dampak negatifnya. 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*.⁴ Tidak hanya itu suatu tindak pidana (*cybercrime*) yang berpotensi dilakukan dengan mudah dan efektif dengan memanfaatkan perkembangan teknologi dan informasi juga pada sektor pengelolaan data dan informasi khususnya pada pengelolaan data pribadi yang membutuhkan perlindungan data. Sebab dengan kemajuan teknologi informasi dan komunikasi tersebut membuat batas privasi makin tipis sehingga berbagai data-data pribadi semakin mudah untuk

² Mujiyana, Ingge Elissa, “Analisis Faktor-Faktor yang Mempengaruhi Keputusan Pembelian Via Internet pada Toko Online” *Jurnal Teknik Industri*, Vol. 8, No. 3, (2013), hlm. 144

³ Safir Makki, 2020, *Trend dan Peluang Industri E-Commerce di Indonesia 2020*, <https://www.cnnindonesia.com/teknologi/20200205204206-206-472064/tren-dan-peluang-industri-e-commerce-di-indonesia-2020>, (diakses pada 22 September 2023, 20:06)

⁴ A. Aco Agus dan Riskawati, “Penanganan Kasus Cybercrime Di Kota Makassar (Studi Pada Kantor Kepolisian Resort Kota Besar Makassar)”, *Jurnal Supremasi*, Vol. 10, No. 56, (2016), hlm. 56

tersebar.⁵ Resiko bocornya data pribadi pengguna *e-commerce* semakin mencuat dengan pesatnya perkembangan sektor ini di Indonesia. Aksi seribu start up yang diresmikan oleh Presiden Republik Indonesia Joko Widodo, merupakan salah satu pondasi berkembangnya ekonomi digital. Sejauh ini dapat mendorong 4 startup unicorn nasional dengan sangat pesat seperti, Bukalapak, Traveloka, Go-Jek, Dan Tokopedia. Pengumpulan data pribadi pelanggan secara gencar dipicu oleh tumbuhnya startup digital ini, serta mempengaruhi perilaku belanja dari pelanggan/konsumen. Merujuk pada istilah layanan pada beberapa *e-commerce* yang ada di Indonesia, mereka menghimpun data pribadi pelanggan. Bahkan, setiap pengguna di setiap aplikasi dipaksa untuk memberikan akses ke data lainnya untuk menjalankan aplikasi oleh calon penggunanya, contohnya daftar kontak, akses terkait dengan identitas diri, SMS, kontak hingga media foto dan file lainnya. Sehingga, tidak ada pilihan lain untuk pengguna apabila betul-betul ingin mengoperasikan aplikasi tersebut kecuali dengan menyetujui izin pemberian akses terhadap data-data yang dimaksud.⁶ Seperti kasus yang terjadi pada Mei 2020 lalu dimana 91 juta data pengguna Tokopedia dijual disitus gelap (*dark web*) oleh pihak yang tidak bertanggungjawab, adapun data pengguna yang dijual mencakup *gender*, alamat, *username*, nama lengkap pengguna, alamat email, nomor ponsel, dan *password*.⁷ Data pribadi yang disebutkan diatas

⁵ Normand Edwin Elnizar, 2019, *Perlindungan Data Pribadi Tersebar di 32 UU, Indonesia Perlu Regulasi Khusus*, <https://money.kompas.com/read/2019/07/27/201200426/penyalahgunaan-data-pribadi-konsumensudah-masuk-kategori-gawat-darurat?page=all>, (diakses pada 13 Desember 2023, 17.18)

⁶ Djafar W, 2019, *Hukum Perlindungan Data Pribadi di Indonesia*, <https://law.ugm.ac.id/wp-content/uploads/sites/1043/2019/08/Hukum-Perlindungan-Data-Pribadi-di-Indonesia-Wahyudi-Djafar.pdf>, (diakses pada 14 Desember 2023, 20.00)

⁷ Conney Stephanie, 2021, *7 Kasus Kebocoran Data Yang Terjadi Sepanjang 2020*, <https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=>

merupakan data pribadi bersifat umum namun, data pribadi yang bersifat umum juga dapat menimbulkan akibat fatal apabila disalahgunakan oleh pihak yang tidak bertanggung jawab. Berikut adalah potensi kejahatan yang dapat terjadi akibat penyalahgunaan data pribadi yang bocor berdasarkan jenis data pribadi yang dipakai:

1. Nama, Alamat, dan Nomor Induk Kependudukan

Kebocoran data pribadi yang mencakup data pribadi umum seperti nama, alamat, serta nomor induk kependudukan dapat berakibat konsumen mengalami kejahatan keuangan seperti transfer uang illegal, pemerasan, serta penipuan pajak. Adapun dengan data pribadi yang dimiliki, pihak yang tidak bertanggung jawab tersebut dapat melakukan penyamaran atau mengaku sebagai orang lain agar dapat bantuan sosial, layanan kesehatan, dan sebagainya.

2. Email dan Nomor Telepon

Email dan nomor telepon yang dimiliki pihak lain yang tidak bertanggung jawab dapat menyebabkan terbukanya akses akun online yang berimbas iklan spam/telemarketing, dan menjadi sasaran phising via email dan nomor telepon. Walaupun iklan spam tidak membahayakan namun iklan spam yang diterima bisa sangat mengganggu dan merugikan karena dapat menyebabkan penyimpanan email atau sms penuh. Kejahatan phising dilakukan melalui komunikasi secara elektronik yang dilakukan dalam bentuk meniru sebuah entitas yang dapat dipercaya / *legitimate organization*

[2ahUKEwjModzugIeCAxXnbWwGHRPAAPYQFnoECBIAQ&url=https%3A%2F%2Ftekno.kompas.com%2Fread%2F2021%2F01%2F01%2F14260027%2F7-kasus-kebocoran-data-yang-terjadi-sepanjang-2020%3Fpage%3Dall&usg=AOvVaw13busNaA3EH7Ph-f9zFh3&opi=89978449](https://kompas.com/read/2021/01/14/260027%2F7-kasus-kebocoran-data-yang-terjadi-sepanjang-2020%3Fpage%3Dall&usg=AOvVaw13busNaA3EH7Ph-f9zFh3&opi=89978449), (diakses pada 16 Oktober 2023, 16.00)

untuk mengambil suatu username, password dan setil kartu kredit yang merupakan informasi yang sangat sensitif dan rahasia.⁸

Dengan bocornya data pribadi pengguna *e-commerce*, maka ada hak pengguna *e-commerce* yang menjadi korban penyalahgunaan data pribadi tersebut yang dilanggar, seperti hak untuk mendapat kenyamanan, keamanan, dan keselamatan. Dalam kasus ini pelanggaran yang merugikan konsumen atau pengguna *e-commerce* tidak hanya berakibat pada hilangnya rasa nyaman tetapi juga keamanan dan keselamatannya sebagai pengguna tidak sepenuhnya terjamin. Pelaksanaan perlindungan data pribadi juga berkaitan erat dengan tugas penyelenggara sistem elektronik dalam mengumpulkan informasi pribadi pengguna, baik secara daring ataupun luring. Lebih lanjut, tugas yang dimaksud bahwa setiap penyelenggara sistem elektronik wajib memiliki aturan internal tentang perlindungan data pribadi sebagai upaya pencegahan terjadinya penyalahgunaan dalam operasional. Namun, fakta yang terjadi adalah banyak data digital milik pengguna yang diperjualbelikan tanpa izin atau disalahgunakan guna tujuan illegal, hingga dicuri oleh pihak ketiga.

Penyalahgunaan data pribadi tersebut mengisyaratkan bahwa adanya kelemahan sistem dalam faktor kesadaran hukum masyarakat, faktor kurang efektifnya regulasi, pengawasan yang kurang ketat, serta praktik penegakan hukum sehingga timbul kerugian bagi individu yang bersangkutan.⁹ Dalam Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi, Pasal 1 ayat (2) menyatakan bahwa “Perlindungan Data Pribadi adalah

⁸ Fanny Priscyllia, “Perlindungan Privasi Data Pribadi Perspektif Perbandingan Hukum”, *Jatiswara*, Vol. 34, No. 3, (2019), hlm. 23

⁹ Sahat Maruli Tua Situmeang, “Penyalahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna Dalam Perspektif Hukum Siber”, *Sasi*, Vol. 27, No. 1, (2021), hlm. 38

keseluruhan upaya untuk melindungi Data Pribadi dalam rangkaian pemrosesan Data Pribadi guna menjamin hak konstitusional subjek Data Pribadi.”¹⁰ Dalam Undang-Undang Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, yang selanjutnya disebut UU ITE menyatakan bahwa “Transaksi Elektronik adalah perbuatan hukum yang dilakukan dengan menggunakan komputer, jaringan komputer, dan atau media elektronik lainnya.”¹¹ Transaksi melalui *e-commerce* termasuk ke dalam pengaturan UU ITE. Berdasarkan pernyataan menurut UU ITE diatas, maka transaksi melalui *e-commerce* harus mempunyai kontrak yang telah disepakati berdasarkan Pasal 19 UU ITE yang berbunyi “Para pihak yang melakukan Transaksi Elektronik harus menggunakan sistem elektronik yang disepakati”¹² agar mengikat para pihak dan kedua belah pihak memiliki perlindungan dan kekuatan hukum yang sama seperti yang tercantum pada pasal 18 ayat (1) UU ITE yang berbunyi “Transaksi Elektronik yang dituangkan ke dalam Kontrak Elektronik mengikat para pihak.”¹³

B. Rumusan Masalah

1. Bagaimana peraturan mengenai perlindungan data pribadi bagi pengguna *e-commerce* di Indonesia?
2. Apa sanksi bagi perusahaan *e-commerce* selaku penyelenggara sistem elektronik jika terjadi kebocoran data pribadi pengguna?

¹⁰ Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi

¹¹ Undang-Undang Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik

¹² *Ibid*

¹³ *Ibid*

C. Tujuan Penelitian

Berdasarkan rumusan masalah tersebut, adapun tujuan penelitian yang ingin dicapai yaitu:

1. Untuk menguraikan bagaimana aturan mengenai perlindungan data pribadi pengguna *e-commerce* di Indonesia.
2. Untuk menguraikan bagaimana sanksi yang diberlakukan kepada perusahaan *e-commerce* selaku penyelenggara sistem elektronik jika terjadi kebocoran data pribadi pengguna.

D. Manfaat Penelitian

Dalam penelitian ini diharapkan dapat bermanfaat bagi perkembangan ilmu hukum terkhusus ilmu hukum yang mengenai perlindungan data pribadi, adapun manfaat lainnya yaitu:

1. Manfaat Teoritis

Dengan adanya penelitian ini diharapkan dapat membantu perkembangan dalam ilmu hukum terkhusus dalam bidang hukum bisnis mengenai perlindungan data pribadi secara lebih rinci lagi kedepannya.

2. Manfaat Praktis

- a. Bagi masyarakat, penelitian ini dapat menumbuhkan kesadaran kepada masyarakat supaya bijak terhadap segala ketentuan dalam bertransaksi melalui *e-commerce*.
- b. Bagi perusahaan *e-commerce* selaku penyelenggara sistem elektronik, dengan adanya penelitian ini agar penyelenggara sistem elektronik sebagai pengelola data pribadi dapat lebih meningkatkan keamanan data pribadi para penggunanya.