Penanganan Kebocoran Data Pribadi Pelanggan e-Commerce

Oleh : Deasy Kamila : 01 April 2024

Hukum Bisnis

Kemajuan teknologi telah membawa perubahan dalam keseharian masyarakat. Banyak kegiatan yang sebelumnya dilakukan secara fisik, dengan kehadiran teknologi kini beralih dilakukan secara non-fisik atau jarak jauh, salah satunya kegiatan jual beli. Hal ini tidak hanya terjadi secara global, namun juga di Indonesia. Berdasarkan data Statista Market Insights, jumlah pengguna *e-commerce* di Indonesia mengalami peningkatan setiap tahunnya terhitung sejak tahun 2018 (Ridhwan Mustajab: 2023). Kegiatan belanja *online* semakin meningkat sejak adanya pembatasan pada saat pandemi Covid-19 melanda Indonesia. Berdasarkan data dari Bank Indonesia, transaksi *e-commerce* pada tahun 2018 jumlah konsumen tercatat yaitu di angka Rp. 106 triliun sedangkan pada tahun 2020, tercatat sebesar Rp. 266 triliun (MB Dewi Pancawati: 2023). Terdapat kenaikan hampir tiga kali lipat dari tahun sebelumnya.

Berbelanja secara *online* menawarkan berbagai kemudahan bagi pelanggan, di antaranya hemat waktu dan tenaga, banyaknya penawaran promo dan harga yang bersaing yang dapat dibandingkan oleh konsumen, reviu produk yang transparan, serta ketersediaan pilihan produk dari berbagai macam *brand* (Aninda Nabilah: 2023). Keberadaan *platform e-commerce* juga didukung dengan tersedianya metode pembayaran yang mudah dan aman sehingga konsumen tidak lagi ragu untuk melakukan belanja secara *online*, berbeda dengan beberapa waktu sebelumnya di mana belanja *online* hanya dapat dilakukan dengan menggunakan kartu kredit sehingga hanya kalangan tertentu yang dapat menjangkaunya.

Namun dibalik kemudahan yang ditawarkan, nyatanya berbelanja secara *online* yang juga memiliki risiko yang perlu diperhatikan, yaitu: penipuan oleh penjual seperti dikirimkannya barang palsu atau barang tidak dikirimkan, metode pembayaran yang tidak aman, dan kebocoran data pelanggan. Secara global, kebocoran data dibagi menjadi dua yaitu *data leaked* dan *data breach*. *Data leaked* diartikan sebagai bocornya data sensitif kepada publik yang tidak diketahui penyebabnya (Edward Kost: 2023). Pada kasus *data leaked* bisa jadi merupakan akibat dari kelemahan sistem elektronik yang tidak diketahui oleh penyelenggara sistem. Sedangkan *data breach* adalah saat kebocoran data disebabkan adanya peretasan oleh pihak ketiga atau *cyberattack* (Edward Kost: 2023).

Banyaknya *platform e-commerce* mulai dari yang menjual produk *retail*, *grocery* sampai dengan *travel* semakin menjamur saat ini baik nasional maupun global. Pada bulan Maret 2020, salah satu *e-commerce* di Indonesia yaitu Tokopedia mengalami peretasan yang menyebabkan 91 juta akun pelanggan dan 7 juta akun penjual bocor dan dijual bebas di salah satu *darkweb* (CNN Indonesia: 2023). Setahun sebelumnya, yakni pada Maret 2019, Bukalapak juga mengalami kasus serupa yang menyebabkan 13 juta data pelanggan bocor. Kasus kebocoran data pelanggan tidak hanya menimpa *e-commerce* di Indonesia, China mengalami kebocoran data terbesarnya pada tahun 2019 yakni sebesar 1 milliar data pelanggan bocor akibat serangan peretas pada salah satu anak perusahaan Alibaba, Taobao (Reni Erina: 2023). Salah satu perusahaan *airlines* asal Britania Raya, British Airway, juga mengalami kebocoran data yang mengakibatkan 400.000 data pelanggan bocor pada tahun 2018 (Djairan: 2023). Akibatnya, perusahaan tersebut dinyatakan bersalah dan didenda sebesar 20 juta poundsterling atau sebesar 380 miliar rupiah.

Dalam kaitannya dengan beberapa contoh kasus seperti yang telah disampaikan di atas, Penulis bermaksud menganalisis sejauh mana kewajiban perusahaan *e-commerce* untuk menjaga data pelanggan dan tindakan apa yang perlu dilakukan apabila perusahaan *e-commerce* mendapat serangan dari peretas yang menyebabkan bocornya data pelanggan. Indonesia telah memiliki peraturan perundang-undangan terkait dengan perlindungan data pribadi yang diundangkan melalui Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU Pelindungan Data Pribadi). Berdasarkan ketentuan tersebut, pengendali data pribadi wajib melindungi data pribadi dari pemrosesan yang tidak sah sebagaimana merujuk pada Pasal 48.

Pada waktu terjadinya kasus kebocoran data Bukalapak dan Tokopedia, belum ada peraturan yang menjamin pelindungan data pribadi. Namun apabila kasus tersebut terjadi setelah berlakunya UU Pelindungan Data Pribadi, berikut hal yang perlu dilakukan kedua perusahaan tersebut selaku pengendali data pribadi berdasarkan Pasal 46, yaitu:

a. Menyampaikan pemberitahuan tertulis maksimal 3x24 jam mengenai kasus kebocoran data kepada subjek data pribadi dan lembaga pengawas;
b. Melakukan upaya penanganan dan pemulihan atas kebocoran data pelanggan;
c. Apabila kebocoran data yang terjadi mengganggu pelayanan publik dan/atau berdampak serius terhadap kepentingan masyarakat, pengendali data wajib memberitahukan kepada masyarakat mengenai kebocoran data pribadi pelanggan.

Pada saat kasus kebocoran data pribadi Tokopedia terjadi, berikut hal yang telah dilakukan oleh Tokopedia, antara lain (Fahmi Ahmad Burhan: 2023):

a. Memastikan transparansi dengan menyampaikan data apa saja yang berhasil diretas;
b. Update pengembangan penanganan kepada pengguna;
c. Upaya perbaikan sistem secara internal;
d. Berkoordinasi dengan pemerintah dan berbagai pihak yang berwenang terkait insiden kebocoran data pelanggan.

Pada masyarakat era teknologi informasi dan komunikasi, teknologi memiliki peranan yang lebih jauh dari sekedar sebagai ‘alat’ untuk membantu kehidupan manusia. Menurut Lawrence Lessig, masyarakat saat ini diatur oleh empat kekuatan, yaitu: hukum, norma sosial, mekanisme pasar dan arsitektur (dalam hal ini teknologi) (Hetty Hassanah dan Wahyudi: 2021). Berdasarkan kasus yang terjadi dan tindakan yang diambil oleh Tokopedia, dapat dikatakan bahwa sebelum hukum mengatur mengenai tata cara yang harus dilakukan dalam hal sebuah *e-commerce* gagal dalam melindungi data pelanggan, sebuah perusahaan teknologi secara tidak langsung telah diatur oleh teknologi yakni dengan harus mengambil tindakan-tindakan yang diperlukan untuk memitigasi risiko yang lebih besar terhadap serangan siber yang telah diterimanya.

Tindakan yang dilakukan oleh Tokopedia ini telah sesuai dengan ketentuan yang ditetapkan dalam UU Pelindungan Data Pribadi dan juga menjadi *best practice* secara global dalam menangani kasus kebocoran data pelanggan yang terkena peretasan. Tindakan penanganan yang tepat terhadap kasus peretasan akan membantu menumbuhkan kepercayaan pelanggan dan meningkatkan kegiatan digital sehingga secara tidak langsung akan mendorong investasi, kompetisi dan inovasi dalam ekonomi digital di Indonesia (Ajisatria Suleiman, dkk, 2022: 13).

Dalam kaitannya untuk memitigasi ancaman kebocoran data pelanggan pada *e-commerce*, berikut hal-hal yang perlu dilakukan oleh berbagai pihak terkait seperti masyarakat, perusahaan *e-commerce* itu sendiri dan Pemerintah:

Masyarakat Subjek Data Pribadi	Perusahaan *e-Commerce* Pengendali dan Pemroses Data	Pemerintah Regulator
1. Menjaga data pribadi dari permintaan/ pemrosesan data pribadi yang berlebihan; 2. Melakukan transaksi pada e-commerce yang terpercaya; 3. Mengedukasi diri mengenai pelindungan data pribadi.	1. Memastikan keamanan sistem elektronik *e-commerce;* 2. Menggunakan teknologi yang *up-to-date;* 3. Melakukan sertifikasi keandalan kebijakan privasi.	1. Melakukan pengawasan dan pembinaan terhadap *e- commerce* sebagai pengendali data pribadi; 2. Mengawasi pelaksanaan dan penegakan UU PDP dan peraturan pelaksananya; 3. Mengedukasi masyarakat akan pentingnya melindungi data pribadi.

Berdasarkan kasus tersebut, dapat dilihat bahwa sebelum adanya ketentuan yang mengatur mengenai penanganan kebocoran data pribadi yang terjadi di dunia digital, teknologi yang dalam teori Lessig disebut sebagai arsitektur telah menyiapkan kerangka penanganan yang perlu dilakukan sebagai *best practice* penanggulangan apabila kebocoran data terjadi dalam suatu sitem informasi. Namun pemerintah, selaku regulator, perlu membuat peraturan yang tegas demi menjamin kepastian hukum dalam penyelenggaraan sistem informasi, khususnya dalam ranah *e-commerce* karena terkait dengan berbagai macam data pribadi yang bersifat sensitif.