Indonesia telah memasuki era global, dimana segala aspek kehidupan telah terhubung dengan teknologi digital. Dimulai dari aspek kehidupan yang paling sederhana sekalipun, saat ini tidak lepas dari teknologi digital. Sebagai contoh, untuk pembayaran apapun saat ini bisa dilakukan secara non tunai atau cashless menggunakan berbagai metode yang sudah tersedia saat ini, dan juga berbagai aplikasi sudah bisa memfasilitasi pengguna untuk melakukan pembayaran secara online. Selain pembayaran online, pemesanan makanan dan transportasi online pun sudah menjadi bagian kehidupan yang cukup esensial. Demikian juga untuk berbagai aplikasi sudah cukup mudah didapatkan melalui gawai secara gratis.

Untuk memenuhi penggunaan semua layanan tersebut, tentunya pengguna harus memiliki akun. Dilansir oleh laman resmi liputan6.com, akun atau account dapat diartikan sebagai representasi digital dari identitas seseorang atau entitas dalam suatu sistem atau platform. Akun biasanya dilengkapi dengan informasi pribadi yang bersifat kredensial untuk akses (seperti username dan password), dan juga berbagai pengaturan dan preferensi yang terkait dengan penggunaan layanan tertentu. Akun sendiri biasanya memuat data-data dan informasi pribadi, seperti nama, tempat tanggal lahir, nomor ponsel, alamat e-mail, dan tidak jarang memerlukan alamat tempat tinggal bahkan nomor identitas seperti NIK (Nomor Induk Kependudukan), nomor paspor, atau nomor KITAS/KITAP menyesuaikan dengan informasi pemilik akun.

Dengan berbagai informasi pribadi yang masuk ke dalam suatu sistem tersebut, yang mana kemudian data-data tersebut akan diolah untuk menjadi akun itu sendiri yang nantinya akan memberi akses kepada pengguna untuk menggunakan sistem atau aplikasi terkait. Dalam era digital saat ini yang memudahkan semua orang mampu mengakses semua hal melalui jaringan internet, tidak menutup kemungkinan segala data berkaitan dengan informasi pribadi dapat dengan mudah diakses oleh pihak-pihak yang kurang bertanggung jawab. Dengan terjadinya hal tersebut, sehingga menyebabkan terancamnya keamanan siber yang berisiko akan terjadi kebocoran data atau tersebarnya informasi pribadi.

Kejahatan Siber di Indonesia

Selain memberikan kemudahan bagi seluruh pihak, ternyata adanya kemajuan dan pemutakhiran teknologi pun tidak menutup kemungkinan akan terjadi hal-hal yang menyimpang atau kejahatan di dunia maya. Kejahatan siber atau kejahatan yang dilakukan dalam dunia maya, semakin marak terjadi seiring terus berkembangnya teknologi digital. Hal ini telah menjadi perhatian bagi semua pihak baik dari lapisan masyarakat yang paling bawah maupun bagi pemerintah pusat. Kejahatan siber yang terjadi tidak hanya menyerang individu atau masyarakat saja, namun dapat menembus pertahanan organisasi besar hingga sistem pemerintahan nasional. Berikut contoh kasus-kasus kejahatan siber yang menjadi perhatian utama:

a. Phising; merupakan tindakan penipuan online yang bertujuan mencuri informasi pribadi seperti kata sandi, nomor kartu kredit, nomor kartu identitas, serta data sensitive dan kredensial lainnya.

b. Ransomware; merupakan serangan yang bertujuan mengenkripsi data korban dan pelaku meminta tebusan untuk membuka enkripsi tersebut.

c. Malware; merupakan perangkat lunak berbahaya yang dapat mencuri data, merusak sistem, atau mengganggu kinerja perangkat dan komputer.

d. Data Forgery; merupakan tindakan pemalsuan data, termasuk pemalsuan dokumen elektronik atau data pribadi.

Dalam ruang lingkup yang lebih sederhana di kehidupan sehari-hari pun kejahatan siber sudah cukup marak. Seperti panggilan telepon yang berasal dari nomor tidak dikenal yang menyampaikan informasi data pribadi seperti nama lengkap atau alamat yang mengarah ke terjadinya indikasi penipuan. Dalam hal ini telah terjadi adanua kebocoran data yang mana pelaku sudah melakukan pencurian data yang kemudian data tersebut digunakan untuk merugikan orang lain. Kasus seperti ini sudah cukup banyak ditemui secara umum dalam kehidupan bermasyarakat.

Contoh diatas merupakan beberapa jenis kejahatan siber yang umum terjadi. Masih banyak jenis kasus kejahatan lainnya yang juga semakin meningkat seiring berkembangnya teknologi. Peningkatan kasus ini juga merujuk kepada data penindakan yang dilakukan oleh pihak kepolisian, dengan jumlah kasus yang meningkat secara signifikan pada tahun 2022 dibandingkan dengan tahun-tahun sebelumnya. Kejahatan siber ini cenderung tidak kasat mata, namun kerugian yang ditimbulkan cukup signifikan. Kerugian akibat kejahatan siber ini tidak hanya berbentuk finansial saja, namun juga dapat merusak kepercayaan serta reputasi publik terhadap suatu instansi atau lembaga yang menjadi pihak korban. Dengan maraknya kejahatan siber yang banyak terjadi di negara ini mendorong digitalisasi sistem semakin digalakkan dengan tujuan supaya lebih meningkatkan kewaspadaan serta dapat mengambil langkah dan tindakan preventif.

UU Nomor 27 Tahun 2022 Sebagai Pedoman Pelindungan Data Pribadi

Secara hukum, aspek pelindungan data pribadi telah diatur dalam suatu undang-undang yaitu pada Undang-undang Nomor 27 Tahun 2022 yang selanjutnya disebut sebagai UU PDP. Disebutkan dalam UU PDP Pasal 1 Ayat (1), data pribadi merupakan data tentang orang perseorangan yang teridentifikasi atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik atau nonelektronik. Dalam pasal tersebut menjelaskan bahwa dalam penggunaan data pribadi dalam sistem elektronik saat ini bervariasi dan terdiri dari beberapa unsur sehingga masyarakat sebagai pemilik data peribadi tersebut pun wajib bersikap concern dan aware akan hal tersebut. disebutkan juga dalam UUPDP Pasal 1 Ayat (4),

Pengendali Data Pribadi adalah setiap orang, badan publik, dan organisasi internasional yang bertindak sendiri-sendiri atau bersama-sama dalam menentukan tujuan dan melakukan kendali pemrosesan Data Pribadi.

Disampaikan secara tegas dalam UU PDP Pasal 47, Pengendali Data Pribadi wajib bertanggungjawab atas pemrosesan Data Pribadi dan menunjukkan pertanggung jawaban dalam pemenuhan kewajiban pelaksanaan prinsip Pelindungan Data Pribadi. Dalam hal ini, ada beberapa hal yang dapat dilakukan oleh masyarakat selaku pengendali data pribadi dalam melindungi dan memastikan keamanan data pribadi yang diprosesnya sesuai yang tercantum pada UU PDP Pasal 35, dengan cara:

a. Menyusun dan menerapkan langkah teknis operasional untuk melindungi data pribadi dari gangguan pemrosesan data pribadi; masyarakat bisa menentukan sendiri langkah keamanan yang dilakukan, sebagai contoh, dengan menghindari nama lengkap atau tanggal lahir untuk digunakan sebagai kata sandi, atau memastikan nomor seluler tidak digunakan untuk hal-hal yang memiliki resiko penyebaran data.

b. Menentukan tingkat keamanan data pribadi dengan memperhatikan sifat dan resiko dari data pribadi yang harus dilindungi; saat ini sudah banyak fitur yang menyediakan tingkat keamanan berlapis untuk menjaga dan melindungi data pribadi, sebagai contoh, penggunaan verifikasi dua- langkah saat masuk ke email atau mengaktifkan fitur biometrik saat akan melanjutkan proses transaksi.

Dalam UU PDP Pasal 36, Pasal 37 dan Pasal 38, disebutkan bahwa pengendali data pribadi wajib menjaga kerahasiaan data pribadi tersebut serta melakukan pengawasan terhadap setiap pihak yang terlibat dalam pemrosesan data pribadi tersebut. Masyarakat selaku pengendali data pribadi wajib memperhatikan setiap detail informasi yang digunakan saat melakukan hal-hal yang memberikan data pribadi. Pengendali data pribadi bisa melakukan penggantian kata sandi secara berkala, mencatat kemudian menyimpan informasi tersebut sebagai bentuk menjaga kerahasiaan data pribadi. Selanjutnya, pengendali data pribadi juga wajib memperhatikan layanan digital yang akan digunakan dan memastikan informasinya bahwa layanan tersebut tidak memiliki resiko kebocoran data serta aman dalam penerapannya.

Dengan adanya dasar hukum dan undang-undang yang mengikat dalam aspek pelindungan data pribadi, masih membuka kemungkinan yang cukup besar akan terjadinya kebocoran data pribadi. Dimuat dalam UU PDP Pasal 46 Ayat 1 dan (2), apabila terjadi adanya kegagalan pelindungan data pribadi, pengendali data pribadi wajib melaporkan atau menyampaikan pemberitahuan secara tertulis kepada subjek data pribadi dan lembaga dalam kurun waktu paling lambat 3 x 24 jam dengan menyerahkan kelengkapan sekurang-kurangnya:

a. Data pribadi yang terungkap;

b. Waktu dan kronologi terjadinya data pribadi tersebut terungkap;

c. Upaya penanganan dan pemulihan yang sudah dilakukan oleh pengendali data pribadi atas terungkapnya data pribadi tersebut.

Maka dari hal tersebut, baik dari masyarakat selaku pengendali data pribadi ataupun pemerintah dan lembaga pusat khususnya di bagian hukum dan pembinaan data siber wajib bersinergi bersama dalam penguatan dan pelindungan data pribadi di era digital masa kini untuk satu tujuan bersama, yaitu mencegah meluasnya kasus kejahatan siber akibat adanya kebocoran data pribadi oleh pihak-pihak yang kurang bertanggung jawab. Sebagai generasi muda masa kini juga wajib turut aktif berperan dalam mewujudkan teknologi dan inovasi untuk penguatan pelindungan data pribadi sebagai tindakan preventif untuk mencegah terjadinya hal-hal yang kurang diinginkan berkaitan dengan lemahnya pelindungan data pribadi dalam era digital masa kini. Dengan banyaknya fitur pelindungan data pribadi yang bisa digunakan secara mandiri untuk penguatannya, besar harapan di masa depan angka kasus-kasus kejahatan siber dapat berkurang secara bertahap dan masyarakat selaku pengendali data pribadi dapat lebih berhati-hati dan bertanggung jawab dalam setiap pemrosesan data pribadi sebagai langkah awal dalam penegakan hukum.