KEBOCORAN DATA, KENALI PENYEBABNYA DAN LAKUKAN PENCEGAHANNYA

Oleh : Vega Lazuardi

Credit Foto : sindonews.com

Resiko kebocoran data menjadi popular akhir – akhir ini. Dalam kurun waktu singkat berturut – turut data – data di beberapa instansi publik diberitakan bocor dan dijual di pasaran gelap. Kejadian serangan siber yang bertubi-tubi di tahun 2022 ini menjadi *shock therapy* bagi kita semua untuk melakukan evaluasi sudah seberapa amankah kita melindungi informasi pribadi kita.

Apa itu Data Pribadi dan ID?

Dalam konsep keamanan siber, terdapat dua jenis data yang berharga yang umum dikenali, yaitu "identitas digital" dan "data pribadi". Identitas digital merupakan identitas seseorang sebagai pengguna platform digital – dari identitas yang nampak seperti nama akun, foto, kata sandi (password) dan kode One Time Password (OTP). Sedangkan data pribadi adalah serangkaian informasi yang digunakan untuk mengenali seseorang, seperti nama, tanggal lahir, alamat rumah, email, dan nomor telepon. Data pribadi khusus biasanya berupa data kesehatan, keuangan, akademis, preferensi seksual, hingga pandangan politik,.

Terjadinya kebocoran data, salah satunya atau kombinasi dari kedua data tersebut, akan memungkinkan pihak – pihak yang tidak bertanggungjawab untuk melakukan pemalsuan kartu identitas, paspor, pinjaman online, dan lain – lain. Maka tak heran, data pribadi atau identitas digital bernilai jual tinggi di pasar gelap.

Modus Pembobolan Data Pribadi

Beberapa modus dan akibat yang umum muncul dalam kasus – kasus pencurian/pembobolan data pribadi/identitas digital antara lain :

1. Men-*capture* gambar diri dari platform sosmed seseorang dan digunakan untuk melakukan penipuan seolah – olah ia orang yang memiliki data yang asli. Tentunya peretas/penipu meneliti dulu lingkaran pertemanan dan lingkungan korban.
2. Manipulasi secara sosial dengan mengelabui korban. Misalnya, pelaku dapat mengirim e-mail disertai pesan genting atau manipulatif supaya korban membeberkan data pribadi dan informasi layanan bank pada suatu link atau lampiran. Modus seperti ini bahkan bisa digunakan untuk membobol dompet digital kita.
   Kasus seorang ojek online yang dibobol tabungannya oleh peretas melalui pesan penipuan yang meminta pengguna memberitahukan kode *One Time Password (OTP)* menjadi salah satu berita heboh di media sosial.
   Ada pula kasus seorang nasabah yang kehilangan saldo tabungannya karena mendapat pesan di aplikasi chat mengenai kenaikan biaya transfer di bank tempat ia menabung.
3. Manipulasi data untuk penipuan pinjaman online (pinjol) ilegal. Biasanya, peminjaman uang ini dilakukan orang lain yang berpura-pura sebagai pemilik data. Korban bahkan tidak tahu menahu soal pinjaman tersebut, dan berujung sebagai pihak yang diteror untuk pengembalian uang dan bunga. Korban pencurian data pribadi untuk pinjol tidak hanya mengalami kerugian finansial,

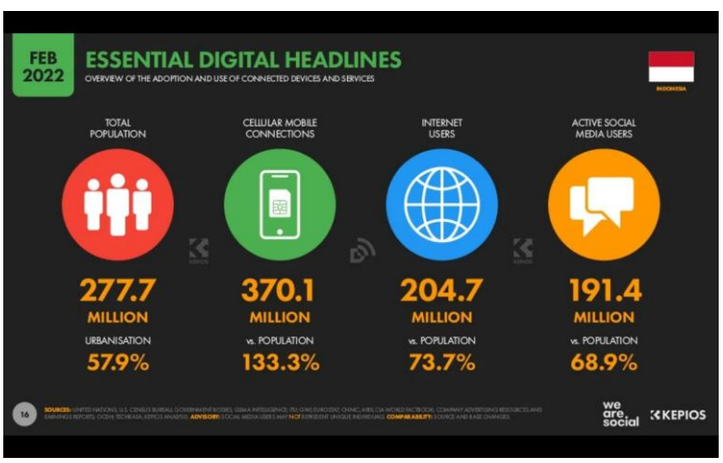
namun juga ketakutan psikologis dan menghabiskan energi karena harus berurusan dengan layanan hukum untuk mendapatkan bantuan.

4. Pemerasan secara online. Salah satu bentuk kejahatan adalah pemerasan seksual atau biasanya disebut *"sextortion"*. Misalnya, pelaku bisa mengajak kita untuk melakukan percakapan seksual, atau menawarkan layanan *video call sex (VCS)*. Aktivitas tersebut kemudian bisa direkam dan digunakan untuk memeras korban. Bahkan, gambar atau video pribadi yang diunggah di media sosial, perangkat digital, maupun layanan penyimpanan lainnya juga bisa diretas dan digunakan untuk pemerasan seksual
5. Pembobolan database badan publik secara elektronik memanfaatkan *backdoor*, Trojan, dan bantuan program – program jahat lainnya yang disusupkan dan disamarkan sebagai program baik (pembersih data, antivirus gratis, dan sebagainya), serta belum terupdatenya Firewall serta antivirus di pusat data.

Kebocoran data selain bermotif iseng atau keuangan, juga bisa digunakan untuk memetakan preferensi politik pengguna yang kemudian bisa dimanfaatkan sebagai target disinformasi. Data Daftar Pemilih Tetap (DPT) Pemilu 2014, misalnya, pernah dibobol peretas dan berisiko digunakan dengan tujuan tidak baik Di belahan lain dunia, hal yang hampir sama juga terjadi di tahun 2018 saat perusahaan data *Cambridge Analytica* terbukti menyalahgunakan data pribadi hingga 87 juta pengguna Facebook untuk keperluan politik – di antaranya untuk mendukung kampanye Donald Trump pada Pemilu Amerika Serikat 2016.

Kenali Penyebabnya

Teknologi informasi menjadi salah satu sector yang berkembang pesat di Indonesia. Pertumbuhan penetrasi teknologi tersebut tergambar dari data yang dilansir datareportal.com pada Februari 2022 :



Credit Foto : datareportal.com

Dari data tersebut diketahui bahwa pada awal tahun 2022 :

1. jumlah telepon seluler lebih banyak 92,4 juta dibanding jumlah penduduk;
2. Pengguna internet mencapai 73,7% dibanding jumlah penduduk;
3. Pengguna aktif media sosial mencapai 68,9% dibanding jumlah penduduk.

Seiring dengan makin meningkatnya kemajuan teknologi digital, maka mau tidak mau makin banyak lapisan masyarakat yang bersentuhan langsung dengannya. Saat ini tak terhitung aktivitas kita yang termonitor secara digital, mulai dari pemanfaatan aplikasi media sosial, aplikasi belanja online, transportasi online, hingga keuangan online. Semakin sering kita terkespose di dunia digital, maka semakin besar pula peluang kita terpapar pada resiko peretasan.

Munculnya berbagai peretasan tentunya tidak lepas dari kelemahan kita sendiri, seperti :

1. Mengumbar data – data pribadi dengan mudah, seperti aktivitas kita sehari – hari bersama keluarga, berpose di depan mobil pribadi atau rumah pribadi yang menampilkan plat nomor, atau nomor rumah kita lalu menguploadnya di medsos;

2. Mengaktifkan fitur *my location* pada gadget kita;
3. Menggunakan akun media sosial pengguna yang memakai sandi keamanan yang mudah ditebak seperti nama, tanggal lahir, tempat lahir, dan sebagainya;
4. Mengijinkan penggunaan *cookie* di beberapa situs. Sebagaimana kita ketahui bersama cookie dapat digunakan mengumpulkan remah – remah aktivitas digital untuk memprofile pengguna internet;
5. Tidak berpikir jernih dan tidak melakukan *check and recheck* (malu bertanya)saat menerima informasi yang secara tiba – tiba diterima dari media sosial;
6. Penerapan kebijakan perlindungan data pribadi yang kurang kuat di pelayanan umum seperti kebiasaan meminta fotocopy identitas diri di berbagai instansi untuk persyaratan pelayanan, hingga kebijakan yang kurang ketat di pusat data yang dikelola pemerintah.

Bagaimana Cara Pencegahan Peretasan Data Pribadi?

Secara hukum, beberapa akademisi berpendapat bahwa perlindungan data pribadi adalah bagian dari hak asasi manusia. Regulasi terkait seperti melalui Revisi UU ITE masih menjadi perdebatan sengit antara perlindungan data pribadi versus demokrasi dan kebebasan berpendapat.

Sembari menunggu munculnya regulasi yang lebih advance, diperlukan upaya – upaya preventif dari masing – masing individu, untuk membantu mencegah kebocoran atau peretasan data pribadi kita :

1. Mengaktifkan fitur keamanan ganda/*Two Factor Authentication* , di mana setelah memasukkan password, kita memerlukan kode tambahan yang dibuat secara acak dan hanya berlaku sekitar 30 detik. Aplikasi seperti Whatsapp dan Google, serta beberapa perbankan telah menyarankan pengguna untuk menggunakan fitur ini yang ada di dalam aplikasi mereka.
2. *Password* harus diperbaharui secara berkala, dan dibuat berbeda untuk setiap aplikasi atau platform. Selain itu, kode sementara termasuk *One Time Password* (OTP) harus selalu dirahasiakan dari orang lain. Penggunaan aplikasi password manager yang aman seperti 1Password atau LastPass juga bisa menjadi opsi – kita tinggal menghafalkan satu kata sandi utama dan aplikasi akan mengelola kata sandi yang sangat rumit dan susah ditebak untuk berbagai akun yang kita miliki.
3. Harus disiplin menjaga data diri baik milik kita sendiri, keluarga, maupun orang lain untuk tidak diumbar di media sosial.
4. Pastikan kita hanya memberi data diri pada pihak yang menjamin pengelolaan data pribadi kita dengan baik dan bertanggung jawab.
5. Meninggalkan platform “http://” dan beralih menggunakan platform https:// saat berselancar di media maya, serta hati – hati pada website yang meminta ijin menggunakan *“cookie”*.
6. Berpikir jernih dan melakukan *check and recheck* saat menerima informasi mencurigakan yang secara tiba – tiba diterima dari media sosial.
7. Generasi muda harus bersabar memberikan pendampingan bagi generasi tua untuk ikut menerapkan perlindungan data – data pribadi ini.
8. Cara terbaik adalah sebisa mungkin memilah dan memilih data mana yang bisa dishare, atau menggunakan sandi keamanan yang kuat di berbagai akun media sosial atau layanan digital lainnya, dengan menggabungkan huruf, angka dan simbol lainnya sehingga tidak mudah ditebak.

Langkah – langkah tersebut perlu dilaksanakan secara parsial oleh kita masing – masing sebagai individu, yang kemudian membentuk kewaspadaan sosial. Oleh sebab itu penekanan perluasan literasi digital menjadi wajib dan mutlak untuk terus menerus diedukasikan kepada khalayak luas, sehingga kemajuan teknologi tidak merugikan kehidupan masyarakat.

Peran Pemerintah

Bagi instansi pemerintah, serangan demi serangan yang muncul menjadi tantangan penciptaan regulasi yang kuat serta pengalokasian effort yang lebih baik pada pengamanan sistem siber yang dikelola pemerintah, baik pada Data Center, akses internet, aplikasi/database dan siatem siber

lainnya. Kewaspadaan dan jiwa besar kolaborasi dalam pengelolaan sistem siber pemerintahan menjadi tanggungjawab semua institusi.

Solusi kolaborasi menjadi langkah yang baik, seperti memanfaatkan Pusat Data Daerah/Nasional, dengan mengalokasikan satu tempat untuk penempatan data, tidak terpisah – pisah di masing – masing instansi. Tentunya kemudian muncul pertanyaan apakah pusat data pemerintah sudah lebih aman? Jawabannya juga normatif, yaitu tidak ada yang aman 100%, namun setidaknya upaya pengamanan yang terkonsentrasi akan lebih terjaga dibandingkan berjalan sendiri – sendiri.

Pada akhirnya, momentum ini bisa kita jadikan peringatan untuk melakukan evaluasi keamanan data diri masing – masing individu maupun institusi.

Disiplin perlindungan data merupakan suatu kewajiban. Dengan melakukan perlindungan data secara disiplin dan periodik, kita bisa aman dalam bermedia digital dan risiko kebocoran data pribadi bisa kita minimalisir