



Data peribadi bukan lagi sekadar maklumat asas seperti nama atau nombor kad pengenalan, sebaliknya menjadi kaedah yang turut menentukan cara seseorang menggunakan pelbagai perkhidmatan dalam talian.

Ramai masih kurang menyedari bahawa setiap maklumat yang dikongsi di platform digital berpotensi disalahgunakan sekiranya jatuh ke tangan pihak tidak bertanggungjawab.

Wartawan **ZHAHIRAH SAZALI** mendapatkan Pesuruhjaya Perlindungan Data Peribadi, **SHARIFFAH RASHIDAH SYED OTHMAN**, bagi mengupas isu keselamatan data peribadi khususnya di negara ini.

Apakah sebenarnya peranan Jabatan Perlindungan Data Peribadi (JPDP)?

JPDP ialah agensi di bawah Kementerian Digital yang bertanggungjawab menguatkuasakan Akta Perlindungan Data Peribadi 2010 (Akta 709). Sejak akta itu dikuatkuasakan, jabatan berkenaan berperanan memastikan organisasi yang memproses data peribadi menguruskan maklumat pengguna secara bertanggungjawab.

Hari ini, hampir semua urusan dilakukan secara digital. Data menjadi komponen utama kepada pelbagai teknologi termasuk AI. Tanpa data yang berkualiti, teknologi tidak mampu menghasilkan keputusan yang tepat. Sebab itu perlindungan data menjadi semakin penting berbanding dahulu.

Mengapa masyarakat perlu lebih berhati-hati ketika berkongsi maklumat di media sosial?

Ramai pengguna berkongsi lokasi semasa, gambar keluarga, nombor telefon, malah salinan kad pengenalan tanpa memikirkan kesannya.

Setiap individu perlu bertanya kepada diri sendiri sama ada maklumat yang diminta benar-benar perlu diberikan.

Semakin banyak maklumat yang dikongsi secara sukarela, semakin luas jejak digital seseorang. Maklumat itu boleh digunakan untuk membina profil individu, sekali gus memudahkan pihak tertentu mengenali tabiat, lokasi dan rutin harian seseorang.

Apakah risiko sekiranya data peribadi jatuh ke tangan pihak tidak bertanggungjawab?

Kebocoran data bukan sekadar menyebabkan maklumat peribadi tersebar, malah boleh menjadi 'modal' kepada sindiket jenayah.

SEMAKIN banyak maklumat yang dikongsi secara sukarela, semakin luas jejak digital seseorang.



USAH MUDAH KONGSI DATA PERIBADI!

Setiap maklumat yang dikongsi di platform digital berpotensi disalah guna

Data yang dicuri daripada pangkalan data sesebuah organisasi boleh dijual kepada pihak lain sebelum digunakan untuk melakukan penipuan yang lebih tersasar kepada mangsa.

Dengan bantuan teknologi semasa, *scammer* mampu menghasilkan mesej yang kelihatan begitu meyakinkan kerana mereka sudah mengetahui identiti, nombor telefon, alamat atau maklumat tertentu mengenai mangsa.

Keadaan itu menyebabkan ramai pengguna sukar membezakan antara mesej tulen dan penipuan.

Adakah organisasi bebas menggunakan data pelanggan sesuka hati?

Tidak. Organisasi yang tertakluk di bawah Akta 709 hanya boleh memproses data bagi tujuan asal ia dikumpulkan.

Sebagai contoh, syarikat telekomunikasi hanya boleh menggunakan maklumat pelanggan bagi tujuan menyediakan perkhidmatan berkaitan telekomunikasi dan bukannya menjual data kepada pihak lain.

Pengguna juga mempunyai hak untuk meminta organisasi menghentikan penghantaran bahan promosi sekiranya tidak lagi mahu menerimanya. Jika arahan itu tidak dipatuhi, aduan boleh dibuat kepada JPDP.

Kanak-kanak juga terdedah kepada risiko. Mengapa ibu bapa perlu lebih berhati-hati?

Akta 709 turut memberi perhatian terhadap perlindungan data membabitkan kanak-kanak dan remaja.

Sebarang pemprosesan data membabitkan individu bawah umur memerlukan persetujuan ibu bapa atau penjaga yang sah.

Ibu bapa dinasihatkan supaya tidak terlalu terbuka dengan berkongsi maklumat anak-anak di media sosial kerana tanpa disedari, ia boleh membuka ruang kepada pihak tidak bertanggungjawab mengeksploitasi maklumat tersebut.

Apakah langkah paling penting untuk melindungi data



Data menjadi komponen utama kepada pelbagai teknologi termasuk AI. Tanpa data yang berkualiti, teknologi tidak mampu menghasilkan keputusan yang tepat"

Shariffah Rashidah



peribadi?

Perlindungan data peribadi perlu bermula dengan sikap pengguna sendiri. Beliau menyarankan orang ramai menggunakan peranti dan aplikasi yang sah serta mengelakkan penggunaan perisian cetak rompak kerana ia lebih mudah dijangkiti perisian berbahaya.

Pengguna juga digalakkan untuk mengaktifkan ciri pengesahan dua faktor (2FA) atau pengesahan berbilang faktor pada semua akaun penting sebagai lapisan keselamatan tambahan. Walaupun proses berkenaan mungkin sedikit leceh, ia mampu mengurangkan risiko akaun diceroboh.

Selain itu, masyarakat perlu memahami tetapan privasi setiap platform media sosial yang digunakan dan menghadkan perkongsian maklumat hanya kepada individu yang benar-benar dikenali.

Di samping itu, perkara yang paling penting ialah membiasakan diri berfikir sebelum memuat naik gambar, berkongsi lokasi atau menekan sebarang pautan kerana setiap tindakan di alam digital mempunyai risikonya yang tersendiri.