Antara *Facebook* dan *Cyber Threat*

Oleh: M. Syaprin Zahidi

DALAM beberapa pekan ini kita cukup dikejutkan dengan adanya be-rita tentang kebocoran data pribadi pengguna *facebook*. Hal ini pertama kali diungkapkan oleh Christopher Wylie yang merupakan mantan kepala riset Cambridge Analytica (Perusa-haan konsultan politik asal Inggris).

Cambridge Analytica sendiri merupakan perusahaan konsultan politik yang berperan dalam peme-nangan Trump pada Pemilihan Presiden Amerika Serikat tahun 2016 lalu. Menurut Christopher Wylie perusahaannya membeli data para pengguna *facebook* dari peneliti di University of Cambridge, Aleksandr Kogan yang menggunakan aplikasi survei kepribadian dan berhasil mendapatkan data pribadi pengguna *facebook* yang jumlahnya tidak main-main sekitar 87 juta.

Data-data pribadi pengguna face-book tersebut digunakan untuk kepen-tingan kelompok tertentu. sebagai contoh data tersebut digunakan oleh Cambridge Analytica untuk kepenti-ngan penyebaran berita hoaks. Peng-gunaan data pribadi pengguna *face-book* yang diperoleh secara illegal ini tentunya membuat kita was-was ja-ngan -jangan kedepannya kita juga akan menjadi korban dari pengambil-an data secara illegal ini karena sampai dengan berita mengenai kebocoran data pribadi pengguna facebook ini diturunkan disinyalir ada sekitat 1 juta data pribadi pengguna *facebook* asal Indonesia yang bocor ke tangan pihak ketiga.

Bocornya data pengguna facebook ini dalam kajian hubungan internasio-nal dapat dikategorikan sebagai kajian non-traditional security khususnya *cyber threat* dimana intinya adalah isu keamanan bukan lagi hanya bicara pada tataran perang antar negara se-bagaimana dibahas dalam *traditional security* namun isu keamanan telah melebar kepada isu-isu diluar fokus negara seperti terorisme, peredaran obat terlarang dan lain-lain termasuk didalamnya adalah *cyber threat*.

Cyber threat sendiri dapat dimaknai sebagai ancaman yang menyusup me-lalui penggunaan komputer, internet dan termasuk juga didalamnya adalah pen-curian data penting yang bisa digunakan untuk kegiatan-kegiatan illegal. kondisi ini menurut penulis memang tidak bisa dilepaskan dari *life style* masyarakat dunia saat ini yang sangat tergantung pada teknologi informasi sehingga hampir semua data pribadi tersimpan secara on-line. Masyarakat dunia saat ini dapat dikategorikan sebagai *infor-mation based society* dimana kehidupan-nya digerakkan oleh sistem teknologi informasi mulai dari bangun tidur sampai tidur lagi.

Di Indonesia sendiri menurut data dari Asosiasi Penyelenggara Jasa Inter-net Indonesia (APJII) pengguna internet jika dibandingkan dengan jumlah pen-duduk Indonesia secara keseluruhan ber-jumlah hampir 50% yaitu dari 262 juta penduduk Indonesia pada tahun 2017 sekitar 143 juta merupakan pengguna internet aktif sehingga bisa kita ba-yangkan ketergantungan masyarakat In-donesia pada sistem teknologi informasi memang telah menjadi *life style*.

Namun yang menjadi masalah, ketergantungan masyarakat saat ini pada teknologi kadang tidak dibarengi dengan keamanan sistem teknologi informasi itu sendiri yang seharusnya menjadi prioritas utama. Sebagaimana yang terjadi pada *facebook*, bisa kita simpulkan berarti sistem di *facebook* pun ternyata sangat rawan dari upaya-upaya pencurian data pribadi karena aspek keamanan jika dianggap akan mengganggu berjalannya sistem in-fomasi kadang tidak selalu menjadi prioritas utama sehingga terjadilah kebocoran data pribadi para *user facebok* di Indonesia.

Cyber Threat sendiri jika kita kategorisasikan dapat dibagi menjadi empat yaitu *Cyber Espionage*, *Cyber Warfare*, *Cyber Crime* dan *Cyber Terrorism* dimana masing-masing term ini memiliki pengertiannya sen-diri. *Cyber Espionage* dapat dimaknai sebagai pencurian data rahasia dalam format digital baik di computer atau jaringan IT. Adapun *Cyber Warfare* memiliki pengertian serangan dunia maya yang dilakukan oleh aktor ne-gara atau non-negara kepada jaringan IT di negara lain.

Sedangkan *Cyber Crime* mendes-kripsikan tentang tindakan-tindakan kriminal yang berkaitan dengan jaringan IT dan komputer seperti hac-king, telemarketing, phishing dan lain-lain. Terakhir, *Cyber Terrorism* men-jelaskan tentang penyebaran-penye-baran ideologi terorisme yang meng-gunakan perangkat IT dan berdampak pada munculnya jaringan-jaringan te-roris baru di beberapa negara yang diakibatan oleh pengaruh penyebaran ideologi tersebut sebagai contoh ISIS yang getol menggunakan perangkat teknologi untuk merekrut anggota-anggota baru dari berbagai negara

Berdasarkan penjabaran mengenai *Cyber Threat* dan varian dari *Cyber Threat* di atas dapat kita simpulkan bahwa saat ini memang telah menjadi era sistem teknologi informasi yang telah memberikan peluang dan juga ancaman pada saat yang bersamaan.

Pada aspek peluang ini tentunya dapat dilihat pada semakin menjamur-nya penggunaan jasa yang berbasis IT seperti *Gojek*, *Traveloka* dan *Grab*. Lalu bermunculannya *market place* yang bisa dikatakan menggantikan fungsi dari mall atau bisnis ritel lain-nya seperti *Lazada*, *Shopee*, *Tokope-dia* dan masih banyak lagi yang lain-nya. Belum lagi ditambah dengan se-makin menjamurnya *Online Shop*.

Contoh-contoh di atas menunjuk-kan bahwa peluang di era digital se-perti saat ini sangat banyak bak kacang goreng namun jangan lupa juga an-caman yang muncul juga semakin banyak. Sebagai contoh seperti ko-bocoran data pribadi, *hacking*, *phis-hing* dan masih banyak lagi kejahatan-kejahatan siber lainnya yang sangat mengancam kita. Kata kuncinya untuk menghindari itu semua adalah kita harus semakin bijak dalam mengguna-kan data-data pribadi kita dan tentunya dibarengi dengan tuntutan kepada penyedia jasa IT untuk semaking concern pada sisi keamanan para pengguna IT saat ini. ***

Penulis Dosen Prodi Hubungan Internasional Universitas Muhammadiyah Malang