

## Cyber Crime Menjelang Pilkada

Tahun 2018 adalah tahun yang panas menjelang pilkada serentak di seluruh Indonesia. Menurut Hwian Christianto, S.H., M.H. selaku Dosen Fakultas Hukum Ubaya, pemilihan Gubernur, Bupati dan Walikota menjadi satu ajang kompetisi yang banyak diberitakan hampir di seluruh media. Penggunaan teknologi informasi yang beragam menjadi salah satu strategi bagi masing-masing tim sukses pasangan kandidat untuk mendapatkan dukungan dari masyarakat. Di sisilain, teknologi dapat bermanfaat positif, tapi berdampak negatif bila digunakan tidak secara bijak. Penggunaan teknologi informasi yang tidak bijak kemudian memicu memunculkan cybercrime.

Q : Kalau boleh tau apa itu sebenarnya cybercrime?

A : Istilah 'cybercrime' sendiri ada yang memaknainya dengan 'kejahatan mayantara' atau 'kejahatan dunia maya'. Jika diartikan secara sederhana, cybercrime adalah perbuatan yang merugikan kepentingan umum dan juga merupakan tindakan tercela yang dilakukan dengan menggunakan jaringan internet. Modus yang dipakai oleh pelaku yaitu dengan menggunakan keunggulan yang ditawarkan internet antara lain kecepatan, murah, canggih, tidak terikat waktu dan tempat, praktis (nirkabel), update (selalu baru dan diperbarui tiap detik) plus menyentuh kehidupan personal.

Q : Menurut Bapak mengapa menjelang pilkada cybercrime selalu bermunculan?

A : Masa yang berbeda perlu pendekatan yang berbeda pula.

Pilkada memiliki kepentingan untuk meraih suara dari masyarakat yang bersifat personal. Internet memfasilitasi kebutuhan ini! Keunggulan internet menjadi modal utama dalam penyebaran informasi (kampanye) bagi Paslon, bukan lagi kepada masyarakat secara umum tetapi lebih personal. Tidak heran jika tim sukses dari tiap calon sangat mempertimbangkan 'suara netizen' mengingat 132,7 Juta (51,8%) dari 256,2 Juta penduduk Indonesia merupakan pengguna internet (hasil survey APJII 2016). Angka 132,7 juta itu pun berdasarkan statistik pengguna internet sebanyak 110,5 juta merupakan pengguna dengan usia 20 &ndash; 44 tahun (hasil survey APJII 2016). Cybercrime pun muncul sebagai bagian dari black campaign dari pendukung yang fanatic terhadap satu paslon dan menginginkan elektabilitas paslon lain menurun. Disinilah sangat rawan muncul informasi tidak benar/hoax yang cenderung merugikan paslon lain bahkan informasi yang sesat bagi masyarakat.

Q : Siapa sasaran dari pelaku cybercrime saat menjelang pilkada?

A : Dalam situasi pilkada sebenarnya ada 2 (dua) pihak yang memiliki kepentingan, Pertama, paslon untuk memperoleh elektabilitas masyarakat dan kedua, masyarakat sebagai pemegang hak suara. Tujuan utama dari pelaku adalah membuat elektabilitas paslon lawan menjadi turun dan berdampak pada meningkatnya elektabilitas paslon pilihan. Sasaran pada pihak pertama biasanya dilakukan oleh pelaku dengan menghembuskan informasi yang berdampak negatif atau berupa informasi yang bersifat mengganggu akun dari paslon atau tim sukses paslon lawan. Bentuk perbuatan pada pihak kedua sangat beraneka ragam, misalnya saja dengan mengirimkan pesan berupa ancaman atau spam pada email secara berkala atau sengaja membuat alamat website palsu dengan tujuan menyesatkan masyarakat dalam mencari informasi (cybersquatting). Saya ambil kasus cybersquatting pernah terjadi pada Dennis Kucinich yang mengajukan diri sebagai anggota kongres Amerika Serikat memiliki alamat website kucinich.net. Lawan politiknya justru membuat alamat palsu berupa kucinich.com dan kucinich.org untuk menyebarkan gerakan anti kucinich.

Q : Apakah pendukung dan kandidat berpotensi menjadi pelaku cybercrime?

A : Mereka sangat berpotensi menjadi pelaku. Berdasarkan keunggulan dari internet, maka setiap orang yang memiliki akses dan

menyalahgunakan akses tersebut sangat berpotensi menjadi pelaku, ikut menyebarkan informasi palsu juga bisa dikatakan cybercrime. Hal tersebut didukung dengan kondisi sosial, budaya dan struktural warganet. Model masyarakat yang ditawarkan adalah warganet yang serba mudah membagikan informasi. Budaya yang ditawarkan warganet pun berupa kebebasan informasi tanpa batas yang acapkali dipahami 'kebablasan' melanggar ketentuan hukum. Pengguna internet pun semakin hari semakin belajar untuk memahami kecanggihan teknologi informasi dengan berbagai macam cara sehingga bisa berpotensi menjadi pelaku jika ingin menyalahgunakannya.

Q : Menurut bapak adakah cara mengatasi cybercrime di saat menjelang pilkada ini?

A : Upaya mengatasi cyber crime pada dasarnya ada 2 (dua) bentuk:

Pencegahan dengan Waspada! Mulai menyaring informasi yang kita peroleh dengan tidak memercayai informasi tanpa memastikan sumber informasi dan mengkonfirmasi kebenaran informasi. Penanggulangan &ndash; membuat laporan pada pihak berwajib atas tampilan situs atau informasi yang merugikan cybercrime@polri.go.id

Q : Jika ada, UU apa yang pantas di berikan kepada pelaku cybercrime?

A : Ada undang-undang mengenai cybercrime yaitu UU No. 11 Tahun 2008 tertulis tentang Informasi dan Transaksi Elektronik jodan UU No. 19 Tahun 2016 tentang Perubahan UU ITE telah memberikan larangan terhadap perbuatan apa saja yang dilarang beserta sanksinya.

Q : Menurut bapak untuk mencegah cybercrime hal apa saja yang harus di lakukan oleh penegak hukum?

A: parat penegak hukum perlu koordinasi dengan lembaga penyedia jasa internet terutama dalam memfilter konten atau website atau informasi yang merugikan masyarakat. Upaya preventif paling efektif justru dengan melibatkan peran individu dalam melakukan 'patroli' untuk melakukan pengawasan, umpan balik dan laporan.

Demikian wawancara singkat redaksi dengan Hwian Christiano, S.H., M.H.tentang cybercrime jelang pilkada.