22 DESEMBER 2020

SAFEnet
SOUTHEAST ASIA FREEDOM OF EXPRESSION NETWORK

Tim penulis:
Abu Hasan Banimal
Damar Juniarto
Ika Ningtyas

Sumber foto:
Pixabay.com
Canva Library

Daftar isi

Peningkatan Serangan Doxing dan Tantangan Perlindungannya di Indonesia

Doxing. Istilah ini semakin sering kita dengar di sejumlah pemberitaan atau linimasa media sosial. Secara awam, *doxing* dilekatkan pada tindakan yang menyebarkan data pribadi. Bisa berupa foto, alamat rumah atau nomor handphone. Istilah "*doxing*" (kependekan dari "*dropping documents*") pertama kali menjadi populer sebagai kata kerja sekitar satu dekade lalu, merujuk pada tindakan peretas dalam mengumpulkan informasi pribadi dan pribadi, termasuk alamat rumah dan nomor identitas nasional.

Namun ternyata studi mendalam tentang *doxing* menunjukkan tindakan ini lebih dari sekedar membuka data pribadi dan dibagikan di ruang publik seperti media daring/sosial, tetapi *doxing* disebut-sebut sebagai ancaman kejahatan terbaru yang difasilitasi oleh teknologi digital. Seperti apakah kasus *doxing* yang terjadi di Indonesia dan mengapa *doxing* dianggap sebagai ancaman terbaru di ranah daring?

Kasus Doxing di Indonesia

Pada 31 Juli 2020, foto profil Facebook dua jurnalis pemeriksa fakta *Tempo*, Zainal Ishaq dan Ika Ningtyas disebarkan oleh akun seorang dokter hewan, Moh. Indro Cahyono tanpa persetujuan keduanya. Selain foto, ada tiga unggahan yang disebarkan akun tersebut dengan melabeli keduanya sebagai jurnalis penyebar ketakutan dan teroris wabah.

Foto Zainal dan Ika disebarkan di media sosial setelah mereka menulis empat artikel cek fakta yang memverifikasi klaim-klaim si dokter hewan mengenai Covid-19. Hasil cek fakta menunjukkan klaim-klaim dokter hewan yang menjadi viral tersebut, tidak benar 100 persen setelah diverifikasi bersama para ahli dan data yang ada.

Jauh sebelum menimpa Zainal dan Ika, *doxing* di Indonesia sebenarnya mulai mencuat menjadi masalah ketika marak digunakan pada persekusi Efek Ahok yang terjadi pada tahun 2017. Korbannya adalah mereka yang dianggap memiliki pandangan politik berseberangan dengan kelompok yang mengidentifikasi dirinya sebagai Pembela Agama dan Ulama. Tiga kasus terjadi selama tahun 2017-2018, yang menimpa Zulfikar Akbar jurnalis *TopSkor* dan Kartika Prabarini jurnalis *Kumparan.com* dan Rolando Fransiscus jurnalis foto *Detik.com*.

Kasus yang dihadapi Zulfikar Akbar jurnalis *TopSkor* itu bermula dari pengusiran terhadap Abdul Somad ke Hongkong. Mengomentari kabar itu, Zulfikar menulis cuitan di akun twitter @zoelfick. "Ada pemuka agama rusuh ditolak di Hong Kong, alih-alih berkaca justru menyalahkan negara orang. Jika Anda bertamu dan pemilik rumah menolak, itu hak yang punya rumah. Tidak perlu teriak di mana-mana bahwa Anda ditolak. Sepanjang Anda diyakini mmg baik, penolakan itu takkan terjadi." Postingan tersebut memicu tekanan dan serangan terhadap Zulfikar di media sosial dalam bentuk *doxing* dan upaya persekusi. Puncaknya adalah dengan kemunculan tagar #BoikotTopSkor dan sempat menjadi *trending topic* di Twitter. Kasus itu berakhir dengan Manajemen *TopSkor* yang memanggil Zulfikar dan memberhentikannya pada 26 Desember 2017.

Kasus serupa juga menimpa jurnalis *Kumparan.com*, Kartika Prabarini. Ia mendapat ancaman di akun instagramnya setelah media tempatnya bekerja menurunkan liputan khusus berjudul "Menjinakkan Rizieq". Pendukung Rizieq Shihab menilai laporan khusus yang dibuat *Kumparan.com* itu tidak menghormati pemimpin mereka. Sebab, dalam laporan itu tidak menyematkan kata 'Habib' saat menulis nama Rizieq Shihab. Akun @mastermeme.id terindentifikasi melakukan *doxing* yaitu pemuatan identitas Kartika di sosial media dengan tujuan melakukan *profiling*. Akibatnya Kartika mendapat ancaman dari pengikut akun @mastermeme.id, hingga dirisak dengan

komentar yang tidak pantas karena identitas gender dan penampilannya. Bahkan Kartika dan *Kumparan.com* diancam akan dilaporkan ke polisi bila tidak meminta maaf.

Kasus ketiga yang terjadi pada 2 November 2018, seorang jurnalis foto *Detik.com* Rolando Fransiscus mengalami doxing saat meliput rapat umum yang disebut "Aksi Bela Tauhid (Bela Tauhid atau Keyakinan Islam)." Akun Facebook Tryas Ramandest dan Instagram @jasmevisback mengunggah data pribadi yang ada di KTP dan kartu pers milik jurnalis tersebut.

Kemudian selama 2019, *doxing* kembali terjadi. Pada 11 Mei 2019 juga terjadi penyebaran doxing yang berulang kali dilakukan oleh Ulin Yusron simpatisan pendukung Jokowi terhadap terduga seorang laki-laki yang berkata akan 'memenggal kepala Jokowi' di media sosial selama Pilpres 2019. Ia membagikan data pribadi Cep Yanto dan Dheva Suprayoga secara lengkap dengan foto, nama lengkap, tempat tanggal lahir, Nomor Induk Kependudukan, status, hingga alamat. Setelah Dheva memuat pernyataan lewat video bahwa itu bukan dirinya dan aksi Ulin dikecam publik, barulah ia menghapusnya. Kemudian setelah ada penangkapan oleh kepolisian terhadap Hermawan Susanto, pada 12 Mei 2019, Ulin memosting sambil meminta maaf atas kekeliruan informasi yang ia sebarkan.

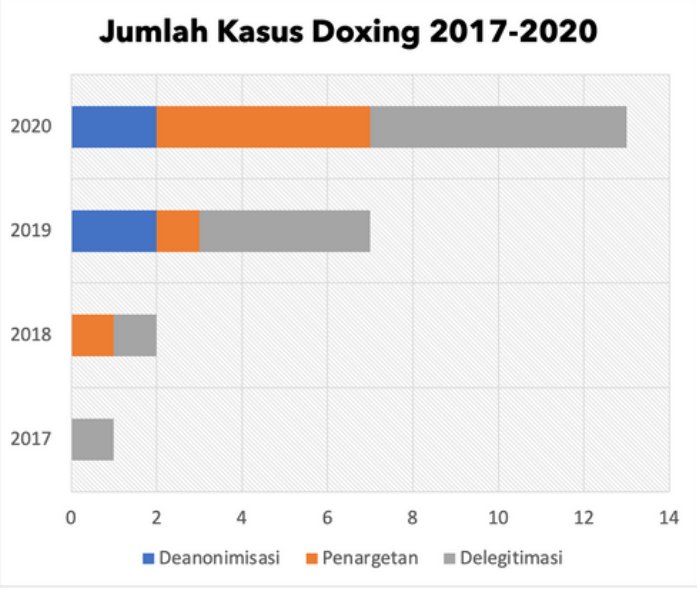
Doxing juga terjadi pada pembela HAM dan jurnalis yang terkait isu sensitif Papua. Pada 9 Oktober 2019, akun Twitter @digeeembok melakukan *doxing* terhadap pengacara pembela HAM Papua, Veronica Koman dengan memberitahu lokasi tempat tinggal kedua orang tua Veronica Koman berada.

Upaya *doxing* ini disertai dengan intimidasi bahwa Veronica Koman telah dipantau oleh akun tersebut. Selain itu, tiga orang jurnalis yang meliput isu Papua mengalami doxing. Pada Agustus 2019, akun Twitter @antilalat melakukan *doxing* terhadap tiga jurnalis lewat posting berikut:

Pemasok info dan propaganda negatif bagi Veronica Koman adl @victorcmambor yg merupakan pemred https://jubi.co.id/ dan @ArnoldBelau pemred https://suarapapua.com

@victorcmambor ini jg yg mjd penghubung antara sayap OPM di luar negeri dgn sayap OPM yg beraksi di pedalaman.

Kemudian pada September 2019, Febriana Firdaus, jurnalis *Al Jazeera*, juga mengalami doxing karena pemberitaannya terkait jumlah korban yang meninggal dalam kerusuhan di Papua.



Sumber: SAFEnet, 2020

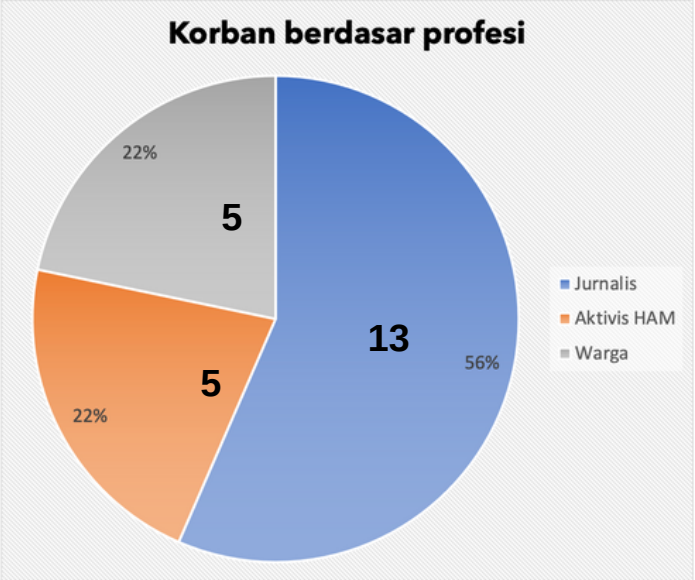
Sedangkan pada 2020, *doxing* juga kerap terjadi selain pada Zainal dan Ika, jurnalis pemeriksa fakta pada Juli 2020. Bahkan di tengah pandemi Covid-19, *doxing* kembali menimpa jurnalis dan aktivis.

Dimulai pada 6 Januari 2020 *doxing* dialami oleh editor *Kompas.com* Jessi Carina terkait pemberitaan sehari sebelumnya di *Kompas.com* berjudul "Anies Kerja Bakti Saat Hujan di Kelurahan Makasar, Warga: Gubernur DKI Rasa Presiden". Foto resepsi pernikahan Jessi Carina disandingkan dengan berita tersebut disebarluaskan oleh sejumlah akun para pendukung Jokowi seperti Romanus Sumaryo @vaiyo, @murthadaone1, @WagimanDeep dan lain-lain disertai narasi "ada kedekatan" editor *Kompas.com* dengan Anies Baswedan dan FPI dan tagar #AniesBeliBeritaMediaOnline.

Pada 15 Mei 2020, seorang jurnalis *Magdalene.co*, media yang menyuarakan hak-hak perempuan dan kelompok minoritas, mendapati dirinya menjadi korban *doxing* dan perisakan daring. Melalui media sosial, jurnalis Magdalene diberi ilustrasi *manga* telanjang serta komentar yang merendahkan martabat perempuan.

Kemudian pada 26 Mei 2020, data pribadi Isal Mawardi seorang jurnalis *Detik.com* tersebar di media sosial yang disertai opini yang menyerang jurnalis tersebut. Serangan siber itu dia alami setelah menulis soal rencana Jokowi yang akan membuka mal di Bekasi di tengah pandemi Covid-19. Jurnalis *Detik.com* itu juga menerima ancaman pembunuhan melalui pesan WhatsApp. Bahkan yang bersangkutan sampai "diserbu" pengemudi ojek online yang datang membawa makanan, padahal ia tak melakukan pemesanan. Salah satu pelaku *doxing* ini adalah Salman Faris. Dia mengunggah beberapa *screenshot* jejak digital penulis untuk mencari-cari kesalahannya, meskipun isinya tak terkait berita yang dipersoalkan.

Selain itu, penulis Niha Alif di situs *Seword* juga melakukan hal serupa dan menyebarkan opini yang menyerang penulis dan media.



Sumber: SAFEnet, 2020

Jurnalis *liputan6.com* Cakrayuri Nuralam pada 11 September 2020 mendapati dirinya menjadi korban *doxing* saat ia menemukan sejumlah akun di Instagram mencantumkan tautan yang mengarah kepada alamat rumah, foto keluarga, termasuk foto anak bayi dari jurnalis tersebut. Peristiwa *doxing* itu didahului saat pada 10 September 2020, korban mempublikasikan artikel cek fakta yang memverifikasi klaim yang menyebut politisi PDI Perjuangan, Arteria Dahlan merupakan cucu dari pendiri PKI di Sumatera Barat, Bachtaroeddin. Setidaknya ada empat akun yang teridentifikasi sebagai pelaku *doxing*, yakni akun Instagram cyb3rw0lff99.tm, d34th.5kull, cyb3rw0lff__, dan_j4ck__5on___

Pada 12 Oktober 2020 usai aksi demonstrasi menolak *Omnibus Law* di Jakarta, identitas pribadi ibu Pramudhi AW dan keluarga berupa NIK, nomor KK, alamat, disebarluaskan di media sosial disertai narasi menyudutkan bahwa ia sedang membagi logistik ke perusuh. Pelaku *doxing* adalah sejumlah akun di Twitter yang serentak membagikan yaitu @seloooooowww, @powerxbr88 dan @terkembang_4817

Terkait demonstrasi *Omnibus Law*/UU Cipta Kerja juga, pada 19 Oktober 2020 beredar konten berupa foto, video, lokasi, nomer induk mahasiswa, nomer telepon disertai narasi memframe "tokoh penggerak demo berakhir rusuh di Yogyakarta" pada mahasiswa UGM Azhar Jusardi Putra, aktivis perempuan Ernawati, aktivis buruh Ardy Syihab di WhatsApp dan diunggah akun Instagram sewordofficial dan NCI4NKRI serta akun Twitter @demoanarki dan @NCI4NKRI

Peristiwa *doxing* pada Jusardi, disusul dengan pengambilalihan akun Whatsapp Jusardi dan pada 20 Oktober 2020, ibu dari Jusardi menerima ancaman pembunuhan dari nomer telpon yang dibagikan oleh akun @demoanarki.

Dari berbagai kasus itu dapat terlihat bahwa praktik *doxing* bisa menimpa semua pengguna internet. Namun, jurnalis memiliki kerentanan yang lebih tinggi (56%). Ini menunjukkan *doxing* telah digunakan oleh pihak-pihak tertentu untuk meneror mereka yang menjadi target serangan.

Pakar teknologi dan keamanan Bruce Schneier berpendapat di kemudian hari akan melihat lebih banyak *doxing* sebagai serangan.

Semua orang mulai dari aktivis politik hingga peretas hingga pemimpin pemerintahan kini telah belajar betapa efektifnya serangan ini. Setiap orang mulai dari orang biasa hingga eksekutif perusahaan hingga para pemimpin pemerintahan sekarang khawatir hal ini akan terjadi pada mereka (Schenier, 2015).

Studi Tentang Doxing

Secara umum, *doxing* kerap dijelaskan sebagai tindakan mengumpulkan dan pengumbaran data pribadi di media sosial. *Oxford British and World English Dictionary* mendefinisikan *doxing* sebagai "mencari dan mempublikasikan informasi pribadi atau identitas tentang (individu tertentu) di Internet, biasanya dengan niat jahat".

Sedang *Cambridge Dictionary* mendefinisikan *doxing* sebagai tindakan menemukan atau menerbitkan informasi pribadi tentang seseorang di internet tanpa izin mereka, terutama dengan cara yang mengungkapkan nama, alamat, dll.

Definisi ini tidak salah karena merujuk pada bentuk-bentuk tindakan yang dilakukan oleh pelaku *doxing*. Namun definisi ini terus berkembang di kalangan akademisi.

Doxing adalah saat informasi pribadi seseorang dibagikan di Internet tanpa persetujuannya. (Lisa Bei Li, 2018). Dalam makalah "Data Privacy in the Cyber Age: Recommendations for Regulating Doxing and Swatting", Lisa Bei Li menekankan pada aspek persetujuan pemilik data sebagai bentuk indikator ketika tindakan pelanggaran hak privasi daring ini terjadi.

Ia mengelompokkan doxing sebagai bentuk tindakan perisakan secara daring (*online harrashment*) sebagai fenomena unik, sama seperti halnya *swatting* yaitu ketika seseorang membuat laporan fiktif ke polisi dengan mengarahkan pasukan bersenjata SWAT (*Special Weapon and Tactics*) untuk datang ke rumah "korban" yang tidak diketahui. Swatting membuat korban merasa tidak berkutik.

Doxing adalah serangan di mana informasi pribadi korban dirilis untuk umum secara daring (Peter Snyder, 2017). Oleh Peter, serangan *doxing* ini dirumuskan sebagai salah satu bentuk pelecehan daring.

Definisi lebih rinci tentang *doxing* bisa dibaca dalam dalam makalah penelitian Roney Matthews berjudul "A Study of Doxing, its Security Implications and Mitigation Strategies for Organizations". Ia menulis definisi *doxing* sebagai kegiatan mempublikasikan informasi individu yang ditargetkan (tanpa persetujuannya) di internet untuk konsumsi publik, dengan maksud menyebabkan rasa malu, penghinaan dan kerusakan, dengan cara tertentu yang mengancam privasi korban dan mungkin orang-orang di sekitarnya korban (teman, anggota keluarga, dll.) (Roney Matthews, 2017) Penekanan Roney pada niat jahat (*dolus malus*) yang memotivasi pelaku dengan sengaja melakukan *doxing*.

Definisi ini juga digunakan David M. Douglas dalam makalah "Doxing: a conceptual analysis". Dalam makalahnya David mengungkap *doxing* sering menjadi alat untuk 'penguntitan dunia maya' (*cyberstalking*), karena informasi tersebut mungkin dirilis dalam konteks yang akan menyebabkan orang yang berakal sehat takut akan hidupnya (Citron 2014).

Doxing juga dapat berfungsi sebagai alat untuk main-main di Internet, di mana mereka yang menentang tindakan seseorang membalas dengan mengungkapkan identitas dan informasi pribadinya, membiarkan korban terbuka menjadi ejekan publik, pelecehan, dan fitnah (Solove 2007).

Doxing mudah dilakukan karena fitur berbagi lokasi geografis tersedia di jejaring sosial, forum dan foto membantu pelaku doxing dalam membuat referensi ke alamat/lokasi saat ini, tempat yang dikunjungi, kota asal dan lain-lain, yang memungkinkan pelaku *doxing* untuk mempersempit hasil pencariannya untuk individu yang ditargetkan. *Doxing* kerap meluas ke identitas teman-teman korban, keluarga, rekan kerja, organisasi dan mereka kenal dengan target, yang akan menuju tindakan perisakan, penghinaan publik, ancaman terhadap kehidupan, pencurian identitas, penipuan dan pengungkapan gaya hidup pribadi mereka.

Doxing bukan tindakan acak. Seorang pelaku *doxing* memilih target dan mulai mengerjakan target dengan mengumpulkan informasi dasar (nama, alamat, anggota keluarga, jenis kelamin, alamat email, nama pengguna, situs web terdaftar dan sebagainya).

Pelaku *doxing* menggunakan segudang sumber seperti berita media, jejaring sosial, aplikasi yang diinstal di ponsel perangkat, atau situs web pemerintah. Aplikasi (dengan pengaturan privasi tidak aman) yang diinstal pada perangkat seluler berbagi data di antara pengguna lain dari aplikasi yang sama, dan tambahan membantu membentuk catatan informasi untuk aplikasi database pengembang.

Tindakan *doxing* ternyata dapat dilakukan oleh banyak aktor sekaligus dalam kampanye yang lebih besar untuk merisak satu subjek (Julia M. MacAllister, 2017). Kerja kolektif melakukan *doxing* ini dapat ditemukan pada kasus Efek Ahok yang melibatkan jaringan *Muslim Cyber Army* (MCA) pada kurun waktu 2017-2018. Pelaku *doxing* membuat agregat dokumen yang disebut sebagai dokumen korban.

Dokumen bisa termasuk informasi yang dipublikasikan dan komunikasi yang diretas dari situs web seperti WikiLeaks. Ini diterbitkan dalam situs web doxing seperti AnonBin, DoxBin dan PasteBin.

Dalam kasus MCA yang terjadi di tahun 2017 di Indonesia, para pelaku doxing menyimpan dokumen korban di Facebook Page Database Buronan Umat Islam.

Ada tiga jenis tipe *doxing*, yaitu: deanonimisasi, penargetan, dan delegitimasi. (Douglas, 2016).

Deanomimisasi adalah *doxing* yang dilakukan dengan cara memberikan informasi yang mengungkapkan identitas orang (atau beberapa orang) yang sebelumnya tidak disebutkan namanya (*anonim*) atau dikenal dengan nama samaran (*pseudonim*).

Contohnya adalah terungkapnya identitas orang yang diduga berada di balik nama samaran 'Satoshi Nakamoto'. Satoshi Nakamoto adalah nama yang diadopsi oleh pencipta (atau pencipta) mata uang kripto Bitcoin (Nakamoto n.d.). Identitas sebenarnya dari pencipta Bitcoin masih belum pasti.

Penargetan adalah doxing yang dilakukan untuk mengungkapkan informasi spesifik tentang keberadaan seseorang secara fisik dengan menunjukkan lokasi keberadaannya. Pelaku *doxing* membagikan lokasi GPS rumah korban atau foto depan rumah. *Doxing* jenis ini membuat seseorang yang ditarget lebih rentan terhadap serangan fisik.

Sedang delegitimasi adalah *doxing* yang dilakukan dengan cara membagikan informasi pribadi dengan tujuan merusak kredibilitas, reputasi, dan/atau karakter korban. *Doxing* jenis ini mencoba untuk mempermalukan dan merisak korban. Misalnya dengan mengungkap rahasia pribadi, atau membuka preferensi seksual korban.

Doxing termasuk dalam **Advanced Persistent Threat (APT)**

A Study of Doxing, its Security Implications and Mitigation Strategies for Organizations
Roney Simon Matthews,
Concordia University College of Alberta, Canada, 2017

Doxing sebagai Advanced Persistent Threats

Doxing dapat menjadi pintu masuk dari kejahatan dunia maya lebih lanjut termasuk pencurian identitas, kartu kredit dan/atau penipuan kartu debit, *phishing*, peretasan atau kejahatan dunia maya lainnya.

Memposting informasi pribadi secara publik dengan maksud untuk dipermalukan, mencemarkan nama baik, melecehkan atau membahayakan adalah perbuatan ilegal. Ini menempatkan individu yang mengalami *doxing* dalam situasi yang berpotensi berbahaya.

Karena pelaku *doxing* dapat menggunakan cara menanam *malware* yang sulit dideteksi oleh korban. Atas dasar itu doxing dapat dikategorikan sebagai *Advanced Persistent Threats (APT),* yakni salah satu metode serangan siber yang yang digunakan untuk melakukan pencurian data. APT sering digunakan untuk mencuri data dari gawai-gawai milik sektor pemerintah, militer atau pun perusahaan. Penyerang menggunakan metode APT harus merancang secara profesional, jadi APT bukan pekerjaan iseng atau coba-coba, tapi APT lebih serius, butuh persiapan yang lama sebelum melancarkan serangan. Korban baru sadar telah terkena serangan APT setelah beberapa lama.

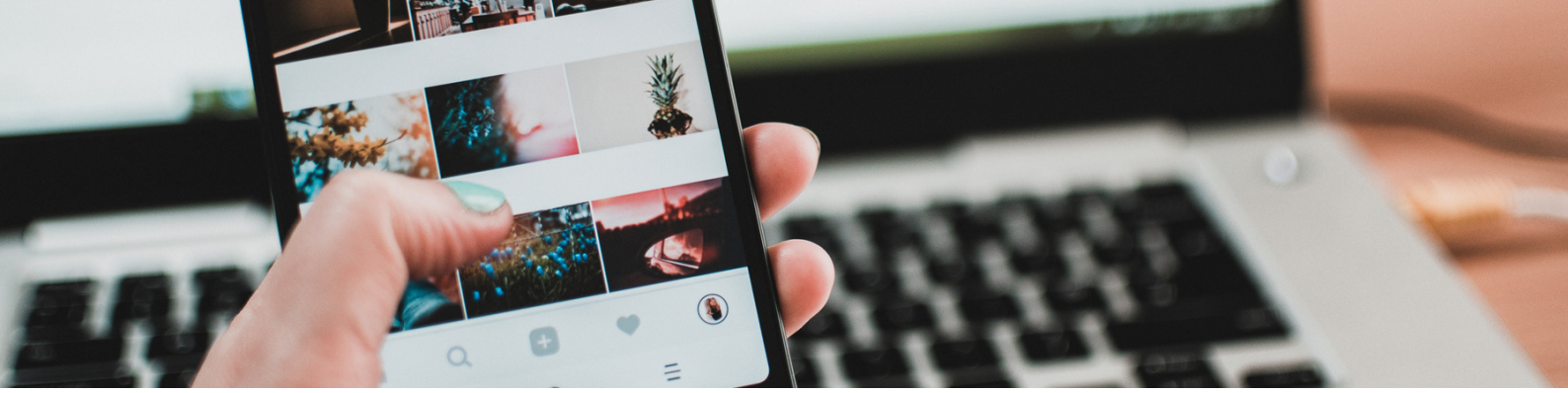
Banyak ahli keamanan siber menyebutkan untuk mendeteksi keberadaan malware APT, tidak cukup hanya mengandalkan antivirus, *proxy* atau *Virtual Private Network.* Untuk mengetahui sebuah sistem sudah dimasuki APT harus dilakukan analisa dengan beberapa tools seperti palantir, splunk, arcsight, tools siem, cybernet falcon, solera, netwitness, dan lain-lain.

Penyerangan dengan menggunakan metode APT bisa sangat membahayakan, karena si penyerang bisa dipastikan harus mengenali sistem yang diserang, berbeda dengan metode lain yang cenderung menyerang dengan langsung, *brute force* atau DDoS. APT menanamkan sebuah *malware* jinak yang tidak terdeteksi, hingga pada waktu yang ditentukan *malware* tersebut melakukan aktivitas sesuai yang diinginkan oleh yang menanam, yang dimaksud di sini adalah memanen data. Sampai *malware* itu bisa dideteksi dan dihapus dari korban, serangan *doxing* bisa terjadi sewaktu-waktu.

Risiko yang Dihadapi Korban Doxing

Apa yang dialami korban *doxing* tidak dapat disederhanakan hanya dengan mengatakan datanya dibaca oleh banyak orang karena ulah pelaku *doxing*. Meskipun *doxing* dilakukan secara daring, hal ini telah menyebabkan kerugian nyata dan serius bagi para korban dengan memindahkan perisakan dari internet ke dunia fisik.

Dalam kasus-kasus *doxing* yang terjadi, selain menghadapi *online trotlling* ternyata justru banyak yang mendapatkan teror fisik mulai dari rumahnya didatangi orang-orang tidak dikenal, dikepung dan dipersekusi, hingga menerima ancaman pembunuhan. Tidak jarang



ancaman pembunuhan yang terakhir ini justru diarahkan pada keluarga korban, orang tua hingga pasangan.

Selain itu karena merasa mendapat ancaman langsung yang diterima lewat *Direct Message*, *mention*, pesan instan, atau telepon dari nomor tidak dikenal, korban *doxing* mengalami trauma psikis, menjadi paranoid pada kondisi sekitar, menutup diri, bahkan dalam sejumlah kasus tertentu harus relokasi/pindah lokasi, entah menginap ke rumah sanak keluarga atau masuk ke rumah aman (*safe house*) untuk sementara waktu.

Resiko lain yang dihadapi oleh korban *doxing* adalah risiko hukum dengan dibawa ke kantor polisi dan dipidanakan. Kebanyakan dari korban ini dikenakan pasal penistaan agama atau pasal ujaran kebencian saat kelompok yang melakukan penjemputan di rumah korban tidak puas dengan permintaan maaf yang disampaikan oleh korban *doxing*. Praktik *doxing* disertai mobokrasi seperti ini banyak terjadi pada periode tahun 2017-2018 selama kasus-kasus Efek Ahok di Indonesia.

Pelaku doxing biasanya melibatkan sejumlah besar orang yang bekerja mencari informasi detail pribadi Anda melalui situs media sosial dan database publik online.

Mitigasi Risiko

Pelaku *doxing* biasanya melibatkan sejumlah besar orang yang bekerja mencari informasi detail pribadi Anda melalui situs media sosial dan database publik *online*. Mereka dapat menggunakan data pribadi Anda, seperti alamat rumah untuk mengancam Anda atau anggota keluarga. Untuk meminimalkan pelaku *doxing* menggunakan data pribadi untuk menyerang Anda, sebaiknya penting untuk memeriksa dan mengelola data pribadi Anda yang tersebar di internet:

1) Sebelum menggunakan platform atau aplikasi tertentu, baca Kebijakan Privasi dan Ketentuan Layanan sebelum Anda mengklik "Terima." Hal itu untuk mengetahui data apa saja yang diambil oleh platform tersebut. Beberapa kebijakan platform mungkin melebihi batas kenyamanan pribadi Anda, misalnya, beberapa situs gratis dapat mengumpulkan dan menjual data kepada pihak ketiga untuk tujuan pemasaran.

2) Tinjau informasi apa yang tersedia tentang Anda di online dan catat situs-situs tempat informasi ini disimpan.

3) Ambil langkah-langkah untuk menghapus informasi apapun di online yang membuat Anda tidak nyaman atau dapat membahayakan Anda, seperti alamat rumah atau foto anak-anak Anda.

4) Waspadai foto-foto Anda yang saat ini bisa diakses secara online dan pikirkan bagaimana mereka dapat digunakan untuk melawan Anda.

5) Pertimbangkan menghapus informasi pribadi Anda dari basis data publik. [Baca langkah menghapus informasi pribadi di layanan Google di link ini: https://s.id/hapusdatapribadi]

6) Periksa pengaturan privasi akun media sosial Anda untuk melihat informasi apa yang bisa dilihat oleh orang lain. Hapus atau batasi akses ke konten yang menurut Anda dapat digunakan untuk mendiskreditkan Anda atau yang dapat membahayakan Anda.

7) Menonaktifkan pelacakan lokasi untuk akun media sosial apapun, termasuk tidak membagikan lokasi Anda secara real-time di media sosial.

8) Hindari mengunggah KTP, tiket, foto rumah, foto anak dengan seragam sekolah, nama lengkap anak, atau informasi pribadi lain yang bisa membuka privasi Anda atau keluarga.

Strategi Advokasi

Saat menjadi target *doxing*, setiap individu harus mengetahui langkah-langkah apa yang dilakukan untuk menghadapinya. Tidak kalah penting, organisasi masyarakat sipil, termasuk organisasi jurnalis dan perusahaan media, harus mulai merancang SOP untuk mengadvokasi kasus *doxing* yang diterima oleh anggotanya.

Langkah advokasi bagi individu:

a. Jika pelaku *doxing* mengungkap alamat rumah Anda dan berpotensi membahayakan keselamatan Anda dan keluarga, pertimbangkan untuk mengungsi ke tempat yang dianggap lebih aman untuk sementara waktu hingga serangan mereda.

b. Laporkan postingan yang mengandung *doxing* ke *platform* dan blokir akun pelaku *doxing*. Fitur aduan/*report* tersedia di masing-masing *platform*.

c. Jika pelaku *doxing* mengungkap nomor telepon dan Anda menerima banyak gangguan, matikan telepon Anda sementara waktu. Pertimbangkan untuk mengganti nomor telepon di kemudian hari.

d. Jika pelaku *doxing* telah mengekspos bank, kartu kredit, atau informasi akun keuangan Anda lainnya, segera hubungi semua lembaga keuangan yang terlibat dan laporkan pelanggarannya.

e. Menutup sementara akun media sosial menjadi pilihan terbaik jika serangan pelaku *doxing* meningkat.

f. Laporkan ke polisi atas *doxing* yang Anda alami dengan membawa hasil dokumentasi dan URL-nya.

Langkah advokasi bagi organisasi:

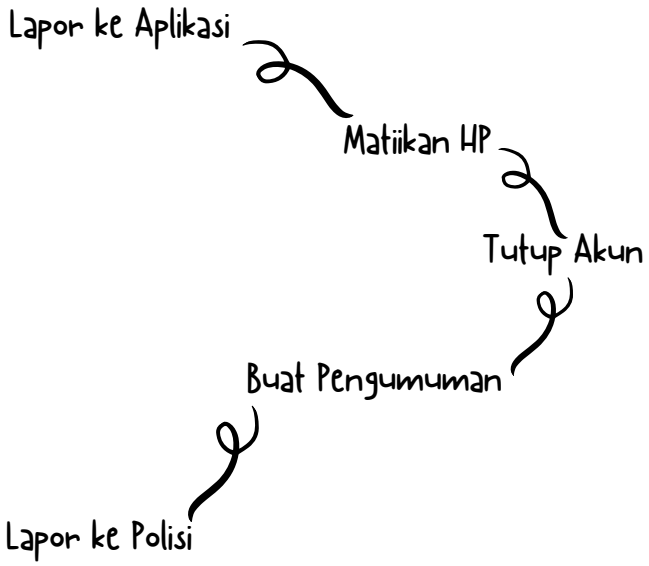
a. Setiap organisasi harus memantau perkembangan tingkat ancaman pada korban *doxing*.

b. Segera memberi respon cepat saat tingkat ancaman meningkat seperti mengeluarkan *alert* kepada publik atau siaran pers.

c. Membantu melaporkan akun pelaku dan postingan tindakan *doxing* kepada penyedia *platform*.

d. Menyediakan rumah aman bagi korban dan keluarganya apabila pelaku *doxing* membuka alamat rumah.

e. Memberikan pendampingan litigasi kepada korban untuk melapor ke aparat hukum apabila *doxing* mengancam pada keselamatan jiwa.



Penegakan hukum

Jika pelaku *doxing* menggunakan layanan seperti Facebook, Twitter, atau Google, kita dapat dengan mudah melaporkan ke *platform* pengguna dengan alasan melanggar *Community Guidelines*. Namun dalam penegakan hukum di Indonesia, ternyata tidak semudah itu.

Sekalipun demikian membawa kasus *doxing* ke ranah penegakan hukum penting mengingat *doxing* adalah serangan siber yang membahayakan.

Sebelum membawa kasus ini ke penegak hukum, Anda sebaiknya melakukan langkah-langkah berikut ini:

a. Simpan semua email, pesan, dan komunikasi lainnya sebagai bukti. Sangat penting bahwa ini tidak diubah dengan cara apa pun, dan salinan elektronik disimpan, bukan hanya cetakan.

b. Simpan semua catatan ancaman terhadap keselamatan atau nyawa korban. Ini termasuk ancaman tertulis atau direkam, dan catatan tanggal, waktu, dan keadaan ancaman verbal.

c. Laporkan ke petugas penegak hukum dengan membuat laporan tindak pidana siber.

d. Simpan catatan rinci saat melapor ke petugas penegak hukum. Penting untuk menyimpan catatan dari semua laporan yang dibuat ke lembaga atau penyedia mana pun, dan untuk mendapatkan salinan laporan resmi jika tersedia.

Di Amerika Serikat, tindakan *doxing* termasuk melanggar hak privasi. Privasi sangat dihargai dan dilindungi dengan hukum privasi. Namun belakangan *doxing* diusulkan sebagai tindakan kriminal juga. Negara bagian Utah pernah mengusulkan rancangan UU Anti-doxxing pada 2016. RUU 'anti-doxxing' Utah akan melarang penyebutan nama seseorang secara online 'dengan maksud untuk menyinggung'. *Doxing* dianggap sebagai salah satu tindakan kejahatan siber penguntitan daring (*cyberstalking*).

Kantor Pengacara AS (USAO) merilis sebuah laporan pada tahun 2016 yang menyatakan bahwa "'*cyberstalking*' mencakup segala tindakan atau serangkaian tindakan yang diambil oleh pelaku di Internet yang menempatkan korban dalam ketakutan yang wajar terhadap kematian atau cedera tubuh yang parah, atau penyebab, upaya untuk menyebabkan, atau secara wajar diperkirakan akan menyebabkan tekanan emosional yang besar bagi korban atau keluarga dekat korban. Hukum federal yang sering digunakan untuk menangani *doxing* adalah 18 U.S.C. § 2261A (Title 18, United States Code, Section 2261A) dan pelaku *doxing* dapat dihukum hingga lima tahun penjara dan denda $ 250.000.

Di Eropa, pasal 8 dari *European Convention on Human Rights*/Konvensi Eropa tentang Hak Asasi Manusia melindungi informasi pribadi yang secara wajar diharapkan untuk tidak dipublikasikan tanpa persetujuan mereka. Jenis informasi ini, misalnya, adalah nama lengkap seseorang dan alamat rumah. Oleh karena itu, *doxing* dianggap sebagai pelanggaran Pasal 8 *European Convention on Human Rights*.

Tantangan terbesar dari aspek penegakan hukum di Indonesia adalah belum diaturnya tindakan *doxing* secara spesifik dalam norma hukum. Namun yang menarik dari kasus *doxing* yang dialami oleh *influencer* Denny Siregar, polisi dapat menangkap pelaku *doxing* dalam waktu singkat usai informasi pribadi Denny Siregar seperti, nama, alamat, NIK, KK, IMEI, OS, hingga jenis perangkat di-screenshot, lalu dimuat di akun Twitter @opposite6890 pada 14 Agustus 2020.

Dalam kasus tersebut, pelaku *doxing* FPH dijerat Pasal 46 atau 48 UU nomor 11 tahun 2008 tentang ITE, atau pasal 50 UU nomor 36 tahun 1999 tentang Telekomunikasi dan atau Pasal 362 KUHP atau Pasal 95 UU nomor 24 tahun 2013 tentang Administrasi Kependudukan dengan ancaman pidana paling lama 10 tahun penjara atau denda Rp10 miliar. Sedang pemilik akun Twitter @opposite6890 masih diburu oleh aparat.

Memang menurut pasal 58 Undang-Undang Nomor 24 Tahun 2013 tentang Perubahan terhadap Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Publik (UU

Adminduk), orang yang menyebarluaskan data kependudukan akan terkena sanksi pidana penjara paling lama dua tahun dan/atau denda paling banyak Rp25 juta. Begitu pula dalam pasal 30 juncto pasal 46 UU ITE, orang yang melakukan akses dengan cara melawan hukum (ilegal) dapat dikenai pidana penjara 6-8 tahun dan denda Rp 600 hingga Rp 800 juta.

Hanya saja, tidak semua kasus *doxing* mendapat penanganan cepat seperti kasus *doxing* yang dialami Denny Siregar. Tidak jarang korban *doxing* harus pulang dengan tangan kosong ketika aparat penegak hukum kesulitan mencarikan pasal yang dapat digunakan untuk menjerat pelaku *doxing*. Hal seperti ini pernah dialami jurnalis Cakra saat hendak melaporkan peristiwa yang dialaminya. Tentu hal ini akan menjadi tantangan dari akademisi dan tugas dari ahli hukum dan pemerhati kejahatan siber untuk mendorong agar tindakan *doxing* dilarang dalam sistem hukum Indonesia. []

Referensi:

Lisa Bei Li, *Data Privacy in the Cyber Age: Recommendations for Regulating Doxing and Swatting*, Federal Communications Law Journal (FCLJ) Volume 70, Issue 3, September 2018 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3012266

Roney Matthews, A Study of Doxing, its Security Implications and Mitigation Strategies for Organizations, 2017. https://concordia.ab.ca/wp-content/uploads/2017/04/Roney_Mathews.pdf

David M. Douglas. *Doxing: a conceptual analysis. Ethics and Information Technology* 18, 3, 2016. https://link.springer.com/article/10.1007/s10676-016-9406-0

Peter Snyder, Periwinkle Doerfler, Chris Kanich, and Damon McCoy. *Fifteen Minutes of Unwanted Fame: Detecting and Characterizing Doxing*. In Proceedings of IMC '17.ACM, 2017https://www.peteresnyder.com/static/papers/fifteen-minutes.pdf

Cambridge Dictionary, meaning of doxing https://dictionary.cambridge.org/dictionary/english/doxing

Oxford British and World English Dictionary, meaning of dox https://www.lexico.com/definition/dox

The Economist Explains What Doxxing Is, and Why It Matters, THE ECONOMIST (Mar. 10, 2014), https://www.economist.com/blogs/economist-explains/2014/03/economist-explains-9

What Is an Advanced Persistent Threat (APT)? https://www.kaspersky.com/resource-center/definitions/advanced-persistent-threats

Advanced Persistent Threats https://www.fireeye.com/current-threats/apt-groups.html

Bruce Schneier, *Doxing as an attack*, 2015 https://www.schneier.com/blog/archives/2015/01/doxing_as_an_at.html

Julia M. MacAllister, *The Doxing Dilemma: Seeking a Remedy for the Malicious Publication of Personal Information*, 2017. https://ir.lawnet.fordham.edu/flr/vol85/iss5/44


SAFEnet
Anda Jadi Korban Serangan Digital?
CODE
$
Laporkan ke SAFEnet lewat saluran berikut:
s.id/laporserangan
@SAFEnetvoice
08119223375
aduan@safenet.or.id