WARTAWAN

OSINT: Pedang Bermata Dua yang Mengancam Privasi di Era Digital

Octavia Ramadhani - BEKASI.WARTAWAN.ORG

Mar 10, 2026 - 11:03

Surabaya - Di era keterbukaan informasi yang bergerak secepat kilat hari ini, kita hidup dalam ekosistem di mana data adalah mata uang baru yang paling berharga.

Di tengah hiruk-pikuk ini, muncul sebuah instrumen yang sangat kuat dan sering kali disalahpahami, yakni Open Source Intelligence (OSINT).

Secara definisi, OSINT bukanlah sihir, melainkan sebuah metode sistematis

dalam pengumpulan, analisis, dan penyajian data yang diambil secara eksklusif dari sumber-sumber yang tersedia secara publik, mulai dari media sosial yang kita gunakan sehari-hari, basis data registrasi domain, catatan properti, hingga citra satelit resolusi tinggi dari Google Earth.

Bagi kalangan jurnalis investigasi yang berjuang menyingkap tabir korupsi, atau bagi aparat penegak hukum yang memburu jejak pelaku kriminal lintas batas, OSINT adalah sebuah "tambang emas" informasi yang tak ternilai harganya.

Ia mampu merangkai kepingan teka-teki yang berserakan menjadi sebuah narasi utuh yang membuka kebenaran. Namun, seperti halnya teknologi pada umumnya, OSINT bersifat netral.

Ketika alat yang sama jatuh ke tangan yang salah yakni para peretas, penguntit (stalker), atau penjahat siber, tanpa adanya kompas moral yang membimbing, OSINT berubah wujud menjadi senjata pemusnah privasi yang sangat mematikan dan berbahaya.

Mengapa OSINT Menjadi Ancaman Nyata?.
Bahaya utama dari OSINT tidak terletak pada satu potong data saja, melainkan pada fenomena yang disebut sebagai agregasi data.

Sering kali kita merasa aman karena berpikir, "Siapa yang peduli dengan foto kopi pagi saya?", atau "Apa bahayanya membagikan lokasi kantor?". Namun, dalam dunia OSINT, satu potongan informasi yang tampak sepele, jika dikumpulkan, dianalisis, dan digabungkan dengan ribuan potongan kecil lainnya menggunakan teknik algoritma, dapat memetakan profil lengkap, pola perilaku, bahkan prediksi masa depan seseorang dengan akurasi yang menakutkan.

Ada beberapa risiko krusial yang harus kita pahami sebagai ancaman nyata.

Pertama, OSINT memudahkan pelaku untuk menemukan alamat rumah, nomor telepon pribadi, riwayat pendidikan, hingga daftar anggota keluarga hanya dengan satu foto unggahan yang terlihat tidak berbahaya di Instagram.

Kedua, penjahat siber menggunakan remah-remah data publik untuk membangun profil psikologis korban. Dengan informasi ini, mereka bisa membangun kepercayaan, melakukan penipuan phishing, hingga membobol rekening bank atau data perusahaan dengan sangat meyakinkan.

Ketiga, informasi lokasi rutin yang tersebar di aplikasi kebugaran (seperti Strava atau Garmin) atau fitur check-in lokasi dapat memberikan jadwal akurat kepada pelaku kejahatan mengenai kapan rumah Anda kosong atau kapan Anda berada di lokasi yang rentan untuk dijadikan target tindakan kriminal.

Contoh Kasus, Dari Foto Sederhana Menjadi Petaka.
Mari kita bedah secara praktis bagaimana OSINT beroperasi. Sering kali, kita merasa cukup dengan tidak menuliskan lokasi saat mengunggah foto. Padahal, tanpa disadari, kita meninggalkan jejak digital yang masif melalui Analisis Metadata Foto.

Saat seseorang mengunggah foto makanan di sebuah restoran, meski ia tidak melakukan tagging lokasi, seorang praktisi OSINT dapat mengunduh foto

tersebut dan memeriksa data EXIF (Exchangeable Image File Format). Di sana, sering kali tersimpan koordinat GPS presisi di mana foto itu diambil.

Geolokasi Berdasarkan Landmark. Ada kasus ekstrem di mana seorang idola di Jepang ditemukan alamat rumahnya oleh penguntit hanya dengan menganalisis pantulan pemandangan pada kornea mata sang idola saat ia melakukan swafoto.

Penguntit menggunakan detail kecil dari pantulan cahaya tersebut, lalu mencocokkannya dengan citra satelit dan foto Google Street View. Ini adalah bentuk ekstrem dari OSINT visual yang menunjukkan bahwa privasi kita jauh lebih tipis dari yang kita bayangkan.

Pelacakan Aset melalui Nopol. Cukup dengan mengunggah foto mobil dengan plat nomor (Nopol) yang terlihat jelas, pelaku bisa melacak status pajak, merek, tahun pembuatan, hingga dalam beberapa kasus, identitas pemiliknya melalui basis data publik yang bocor atau aplikasi pemerintah yang kurang aman pengelolaannya.

Sebagai insan pers, saya menyadari bahwa OSINT adalah kemajuan teknologi yang tidak bisa dibendung, bahkan menjadi alat bantu demokrasi yang penting. Namun, masyarakat harus mulai memiliki kesadaran kritis akan "Jejak Digital". Setiap komentar, setiap foto, dan setiap check-in adalah titik koordinat yang sedang Anda berikan kepada dunia secara sukarela.

Pemerintah memang harus memperkuat regulasi pelindungan data pribadi agar kebocoran data tidak lagi menjadi konsumsi publik yang lazim. Namun, kita sebagai pengguna juga harus lebih "pelit" dalam membagikan informasi.

Jangan sampai transparansi informasi yang kita agungkan justru menjadi jerat yang mencekik privasi kita sendiri di masa depan.

Lindungi Privasi Anda dari "Intai" Digital (OSINT)
Sebagai bentuk kepedulian atas keamanan data masyarakat, Media Sindikat Post merangkum langkah krusial agar jejak digital Anda tidak disalahgunakan oleh pihak yang tidak bertanggung jawab.

Pertama, matikan "GPS Metadata" (Geo-Tagging).
Setiap foto yang Anda ambil dengan ponsel pintar biasanya menyimpan koordinat lokasi secara otomatis ke dalam berkas foto tersebut.

Caranya, masuk ke Settings Kamera ponsel Anda, cari dan matikan fitur "Save Location" atau "Location Tags". Ini adalah langkah pencegahan paling dasar untuk menghindari orang lain melacak lokasi rumah atau kantor Anda melalui metadata foto yang diunggah.

Kedua, "Audit" Profil Media Sosial Anda.
Akun media sosial seringkali menjadi "buku harian" terbuka bagi pelaku OSINT untuk memanen data pribadi Anda.

Tindakan, atur akun menjadi Private (khusus keluarga dan teman dekat). Lakukan pembersihan secara berkala, jangan tampilkan informasi sensitif di bio, seperti nomor telepon, alamat rumah, nama anggota keluarga, atau detail tempat kerja yang spesifik.

Ketiga, hati-hati dengan "Pamer" Identitas.
Jangan pernah mengunggah dokumen pribadi ke media sosial dalam bentuk apa pun.

Hindari Foto KTP, SIM, NPWP, Tiket Pesawat (Boarding Pass), atau Ijazah. Data ini sangat mudah disalahgunakan untuk pengajuan pinjaman online ilegal, pembukaan rekening fiktif, hingga aksi penipuan perbankan yang merugikan secara finansial.

Keempat, waspadai Social Engineering.
Pelaku OSINT sering memulai dengan "memancing" informasi melalui pertanyaan yang terlihat tidak berbahaya.

Tanda Bahaya, jangan sembarangan menjawab kuis di media sosial yang menanyakan detail pribadi seperti "nama kecil ibu", "sekolah pertama", atau "tempat lahir". Data ini sering digunakan oleh peretas untuk menebak atau mereset kata sandi akun Anda melalui security question.

Kelima, berhenti mengunggah Real-time Location.
Hindari kebiasaan melakukan check-in lokasi secara langsung atau membagikan aktivitas rutin (seperti lokasi gym atau sekolah anak).

Tips. Jika ingin membagikan momen berharga, unggahlah foto atau video tersebut setelah Anda meninggalkan lokasi. Penundaan unggahan adalah cara sederhana untuk mengacaukan upaya pelacakan lokasi real-time.

Pesan Redaksi:
Internet tidak pernah benar-benar lupa. Apa yang Anda bagikan hari ini bisa menjadi ancaman di masa depan. Menjadi cerdas di ruang digital bukan berarti Anda harus menutup diri dari dunia, namun lebih kepada memahami apa yang pantas untuk dibagikan ke ruang publik dan apa yang harus tetap menjadi privasi Anda. Tetaplah waspada, karena keamanan Anda dimulai dari apa yang Anda unggah.@Dedik.

Oleh: Dedik Sugianto (Pemred Media Sindikat Post)