

ANALISIS YURIDIS PENGGUNAAN OPEN SOURCE INTELLIGENCE SEBAGAI METODE PEMROSESAN DATA PRIBADI MENURUT HUKUM POSITIF INDONESIA

Cindy Fibiana Putri¹, Benny K. Heriawanto², Ahmad Syaifudin³

Fakultas Hukum Universitas Islam Malang
Jalan Mayjen Haryono No 193 Malang 65144, Telepon (0341) 551932,
Fax (0341) 552249
Email : 22101021071@unisma.ac.id

ABSTRACT

The advancement of information technology has enabled open data access, which is utilized by various parties. The use of Open Source Intelligence (OSINT) in processing personal data must comply with legal regulations. This study examines: 1) the legal perspective on OSINT-based personal data processing in Indonesia, and 2) its implications under data protection law. Using a normative method, the findings indicate that OSINT is lawful if it adheres to the Personal Data Protection Law (UU PDP), the Electronic Information and Transactions Law (UU ITE), and related regulations. OSINT must follow data processing principles and avoid legal violations. Compared to the GDPR, Indonesia imposes lighter administrative sanctions, with fines up to 2% of annual revenue, while the GDPR may impose fines of up to 20 million euros or 4% of turnover.

Key words: Open Source Intelligence; OSINT; personal data processing.

ABSTRAK

Perkembangan teknologi informasi memungkinkan akses data terbuka yang dimanfaatkan oleh berbagai pihak. Penggunaan Open Source Intelligence (OSINT) sebagai metode pemrosesan data pribadi harus sesuai dengan hukum. Karya ini mengkaji: 1) Bagaimana penggunaan OSINT sebagai metode pemrosesan data pribadi menurut hukum positif Indonesia? 2) Apa akibat hukum penggunaan OSINT sebagai metode pemrosesan data pribadi menurut hukum perlindungan data pribadi? Penelitian ini menggunakan metode normatif. Hasil menunjukkan bahwa meski belum ada aturan spesifik, penggunaan OSINT sah selama sesuai dengan UU PDP, UU ITE, PP PSTE, Peraturan BSSN, dan ISO/IEC 27001. OSINT harus mematuhi prinsip pemrosesan data pribadi dan tidak melanggar hukum. Dibandingkan dengan GDPR, sanksi administratif di Indonesia lebih ringan, dengan denda hingga 2% pendapatan tahunan perusahaan, sedangkan GDPR dapat mengenakan denda hingga 20 juta Euro atau 4% dari omset tahunan.

Kata kunci: Open Source Intelligence; OSINT; pemrosesan data pribadi

¹ Mahasiswa Program Studi Hukum Fakultas Hukum Universitas Islam Malang

² Dosen Program Studi Hukum Universitas Islam Malang

³ Dosen Program Studi Hukum Universitas Islam Malang

PENDAHULUAN

Digitalisasi yang semakin meresapi berbagai aspek kehidupan telah mendorong penggunaan teknologi informasi untuk mengakses, mengelola, dan menganalisis data. Salah satu metode yang berkembang pesat adalah *Open Source Intelligence* (OSINT), yaitu teknik pengumpulan data dari sumber terbuka yang tersedia di ruang publik.⁴ OSINT telah berkembang dari metode manual melalui media tradisional, seperti radio dan televisi, menjadi alat canggih yang memanfaatkan internet, media sosial, web scraping, kecerdasan buatan (AI), dan big data. Kini, OSINT digunakan oleh berbagai pihak, termasuk pemerintah, perusahaan, aktivis, hingga jurnalis, untuk mendukung keamanan, investigasi, intelijen bisnis, hingga pelaporan investigatif.

Pemanfaatan OSINT memberikan banyak manfaat strategis, seperti analisis ancaman, investigasi kriminal, dan pengumpulan wawasan pasar.⁵ Namun, kemampuannya untuk mengakses dan menganalisis data dalam skala besar juga menimbulkan kekhawatiran, khususnya terkait perlindungan data pribadi. Informasi yang dikumpulkan dari sumber terbuka sering kali melibatkan data pribadi tanpa persetujuan subjek data, sehingga berpotensi melanggar privasi individu. Praktik ini menuntut kehati-hatian dalam mematuhi prinsip-prinsip perlindungan data pribadi, seperti transparansi, batasan tujuan, dan minimalisasi data.

Di Indonesia, perlindungan data pribadi diatur dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Undang-Undang ini mengharuskan setiap pemrosesan data dilakukan secara sah dan dengan persetujuan eksplisit dari pemilik data. Meskipun OSINT memanfaatkan informasi publik, pengumpulan tanpa persetujuan langsung sering kali terjadi, meningkatkan risiko penyalahgunaan data untuk keuntungan ekonomi atau tujuan ilegal.⁶ Hal ini menunjukkan perlunya pengaturan yang lebih jelas mengenai batasan legalitas OSINT dalam konteks perlindungan data pribadi.

Oleh karena itu, penelitian mengenai legalitas OSINT dalam perspektif UU PDP menjadi penting untuk memahami bagaimana teknik ini dapat digunakan secara sah tanpa melanggar hak privasi individu. Penelitian ini diharapkan mampu memberikan panduan praktis bagi pihak-

⁴ Daniel Eduardo Daud, "Open-Source Intelligence (OSINT)", Binus University, 16 April 2022, <https://student-activity.binus.ac.id/csc/2022/04/open-source-intelligence-osint/>

⁵ Ferry Gunawan dan TM Mirza Keumala. "Analisis Information Gathering Target Daftar Pencarian Orang Menggunakan Metode open Source Intelligence Pada Kejaksaan Tinggi Aceh." *Jurnal Sistem Komputer (SISKOM)* 4.1 (2024): 10-21.

⁶ Putri, "Open Source Information (OSINT): Way we collect information in the age of no privacy", Integrity Indonesia, 25 juni 2019, <https://www.integrity-indonesia.com/id/blog/2019/06/25/open-source-information-osint-eksploitasi-informasi-di-era-tanpa-privasi/>

pihak yang terlibat dalam pemanfaatan OSINT, baik untuk investigasi maupun kepentingan bisnis. Dengan pendekatan yang sesuai, OSINT dapat menjadi alat yang efektif tanpa mengorbankan perlindungan data pribadi dan hak-hak subjek data di era digital yang semakin terbuka.

Berdasarkan hal tersebut maka penting untuk mengkaji; 1) Bagaimana penggunaan OSINT sebagai metode pemrosesan data pribadi menurut hukum positif Indonesia? 2) Apa dampak OSINT sebagai metode pemrosesan data pribadi menurut hukum perlindungan data pribadi? Penelitian ini, merupakan penelitian hukum normatif dengan menggunakan pendekatan perundang-undangan, pendekatan konseptual, dan pendekatan perbandingan. Pengumpulan bahan hukum melalui studi literatur dengan bahan hukum primer, skunder, dan tersier. Selanjutnya bahan hukum dikaji dan dianalisis dengan pendekatan yang dipergunakan untuk menjawab isu hukum dalam penelitian ini.

Penggunaan Open Source Intelligence Menurut Hukum Positif Indonesia

Open Source Intelligence (OSINT) adalah metode pengumpulan dan analisis data dari sumber terbuka seperti internet, media sosial, dan dokumen publik.⁷ Awalnya digunakan oleh lembaga pemerintah seperti intelijen dan militer, OSINT kini berkembang berkat kemajuan teknologi informasi, termasuk kecerdasan buatan dan machine learning. Perangkat seperti Maltego dan Shodan mempermudah pengumpulan serta analisis data untuk berbagai keperluan, termasuk keamanan siber, investigasi hukum, dan strategi bisnis.⁸ Namun, perkembangan OSINT juga menghadirkan tantangan terkait privasi dan legalitas pemrosesan data pribadi.

Penggunaan OSINT dalam pemrosesan data pribadi memiliki manfaat, seperti mendeteksi ancaman siber, mendukung investigasi hukum, dan menyediakan wawasan bisnis tanpa melanggar privasi jika dilakukan sesuai hukum. Namun, tanpa pengawasan yang tepat, OSINT berpotensi melanggar hak privasi melalui pengumpulan data tanpa izin, penyalahgunaan informasi, atau diskriminasi berbasis profil.⁹ Publikasi data di ruang terbuka, seperti media sosial, tidak menghapus hak privasi pemilik data sesuai dengan ketentuan UU Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) dan Pasal 26 UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE).

⁷ Daniel Eduardo Daud, "Open-Source Intelligence (OSINT)", Binus University, 16 April 2022, <https://student-activity.binus.ac.id/csc/2022/04/open-source-intelligence-osint/>

⁸ *Ibid.*

⁹ Surya Dwi Putra, Bhernedetha Nindya Kusumastuti, and Nasrul Ma'arif. "Potensi Ancaman Penggunaan OSINT Menyebabkan Kegagalan Pengambilan Keputusan Akibat Informasi Hoax." *Jurnal Kajian Stratejik Ketahanan Nasional* 6.2 (2023): 4.

Di Indonesia, regulasi seperti Undang-Undang Nomor 27 Tahun 2022 (UU PDP), Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), PP Nomor 71 Tahun 2019, dan Peraturan Badan Siber dan Sandi Negara Nomor 8 Tahun 2020 tentang tentang Sistem Pengamanan dalam Penyelenggaraan Sistem Elektronik menjadi landasan hukum untuk praktik OSINT. UU PDP menegaskan bahwa pemrosesan data pribadi memerlukan persetujuan eksplisit, sementara UU ITE melarang pengumpulan data pribadi secara melawan hukum. Standar internasional seperti ISO/IEC 27001 juga relevan dalam memastikan keamanan informasi yang diperoleh melalui OSINT. Hal ini menunjukkan bahwa pemanfaatan OSINT harus memperhatikan legalitas dan etika untuk menghindari konsekuensi hukum dan dampak negatif terhadap individu.

Untuk mendukung penerapan OSINT yang sah dan efektif, diperlukan kerangka hukum yang komprehensif, termasuk pengaturan batasan dan perlindungan hak privasi. Regulasi yang berlaku di Indonesia dapat memberikan landasan yang kuat untuk memanfaatkan OSINT secara etis dan legal. Dengan pendekatan yang tepat, OSINT dapat menjadi alat strategis dalam keamanan siber dan pengelolaan informasi tanpa mengorbankan hak privasi individu, menciptakan keseimbangan antara eksploitasi informasi dan perlindungan hukum.

Prinsip-prinsip perlindungan data pribadi dalam UU PDP meliputi transparansi, legalitas, dan tujuan spesifik pemrosesan data. Transparansi menuntut pengendali data untuk memberikan informasi yang jelas kepada subjek data mengenai tujuan dan proses pengumpulan serta penggunaan data pribadi mereka. Legalitas memastikan pemrosesan data dilakukan sesuai hukum, tanpa melanggar hak individu. Tujuan pemrosesan harus spesifik dan sah untuk mencegah penyalahgunaan data. Prinsip-prinsip ini dirancang untuk menjaga kepercayaan publik dan melindungi hak privasi individu.

Pasal 20 UU PDP mengharuskan persetujuan eksplisit dari pemilik data sebelum pemrosesan dilakukan. Persetujuan ini harus diberikan tanpa paksaan, dengan pemahaman penuh atas tujuan pemrosesan, dan dapat ditarik kembali kapan saja. Ketentuan ini memberikan kontrol kepada individu atas data mereka, memastikan pemrosesan dilakukan secara etis dan sesuai hukum.

UU ITE juga mendukung perlindungan privasi dan data digital di Indonesia. Undang-undang ini menekankan pentingnya menjaga kerahasiaan data pribadi dalam transaksi elektronik dan mengatur tanggung jawab penyelenggara sistem elektronik untuk melindungi data dari akses ilegal atau penyalahgunaan. Pelanggaran privasi dapat dikenakan sanksi pidana sesuai ketentuan yang berlaku.

Dalam OSINT, praktik yang tidak menghormati hak asasi manusia, terutama privasi, dapat menimbulkan konflik hukum. Pengumpulan dan analisis data tanpa persetujuan dianggap melanggar hak privasi yang dilindungi oleh konstitusi dan hukum internasional. Praktisi OSINT harus memastikan metode dan tujuannya sesuai dengan prinsip transparansi, akuntabilitas, dan penghormatan terhadap privasi individu, sebagaimana diatur dalam Pasal 5-15 UU PDP.

Data yang dapat digunakan dalam OSINT meliputi informasi publik seperti artikel berita, postingan media sosial publik, dokumen resmi, dan data visual yang dipublikasikan secara terbuka. Sebaliknya, data pribadi seperti nomor KTP, rekam medis, atau informasi yang bersifat rahasia tidak boleh digunakan tanpa persetujuan. Namun, data yang tidak dapat dipergunakan diatas dalam praktik OSINT dapat menjadi sah untuk dimanfaatkan apabila data tersebut telah diunggah secara publik dengan tujuan untuk kepentingan umum. Dalam hal ini, publikasi data oleh individu atau lembaga menunjukkan adanya persetujuan implisit bahwa informasi tersebut dapat diakses oleh khalayak luas, selama penggunaannya sesuai dengan tujuan publikasi awal dan tidak melanggar prinsip hukum yang berlaku, seperti hak atas privasi atau perlindungan data pribadi. Dengan demikian, batasan pada penggunaan data pribadi dapat dikesampingkan jika data tersebut secara sadar dipublikasikan untuk memenuhi kebutuhan informasi publik, asalkan pengolahannya tetap dilakukan secara etis dan proporsional.

Prinsip minimalisasi data menekankan pengumpulan data yang relevan dan diperlukan untuk tujuan tertentu, mengurangi risiko pelanggaran privasi dan penyalahgunaan data.¹⁰

Pengendali data memiliki kewajiban, sebagaimana diatur dalam UU PDP, untuk memastikan pemrosesan data sesuai hukum, melindungi keamanan data, dan menghentikan pemrosesan atas permintaan subjek data. Penerapan teknologi seperti enkripsi, kontrol akses, dan audit rutin sangat penting untuk mencegah kebocoran data.

Reliabilitas sistem informasi dalam OSINT merupakan elemen krusial untuk memastikan integritas data dan mencegah informasi salah atau tidak akurat. Sistem yang andal harus mampu memverifikasi data dari sumber publik dan melindungi data dari akses ilegal.¹¹ Kegagalan reliabilitas sistem dapat melanggar ketentuan UU ITE terkait privasi dan perlindungan data, sehingga penting bagi pengembang sistem untuk memperhatikan aspek teknis dan hukum.

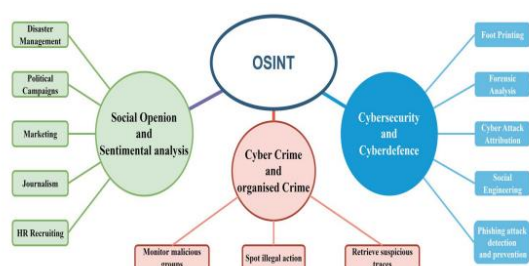
¹⁰Tiara Almira Raila, Sinta Dewi Rosadi, and Rika Ratna Permata, "Perlindungan data privasi di Indonesia dan Singapura terkait penerapan digital contact tracing sebagai upaya pencegahan covid-19 serta tanggungjawabnya." *Jurnal Kepastian Hukum dan Keadilan* 2.1 (2021): 1-18.

¹¹Firdi Gunawan, Ahmad Fadhillah, dan Essy Malays Sari Sakti. "Membangun Benteng Digital Untuk Memperkuat Etika Cyber Security Melawan Ancaman Cyber Crime." *Jurnal Ilmiah Teknik Informatika (TEKINFO)* 25.1 (2024): 154-167.

Dengan memastikan kepatuhan terhadap hukum, OSINT dapat digunakan secara efektif untuk mendukung kepentingan strategis tanpa mengorbankan hak-hak fundamental individu. Integrasi antara praktik OSINT dan kerangka hukum yang berlaku akan menjaga kepercayaan publik serta menghindari konflik hukum.

Berikut merupakan gambar pemanfaatan OSINT:¹²

Open Source Intelligence (OSINT) adalah metode pengumpulan dan analisis informasi dari sumber-sumber publik yang hasil pemanfaatannya dapat digunakan di berbagai sektor. Dalam keamanan dan intelijen, OSINT memantau aktivitas ekstremis dan teroris melalui media sosial,



Gambar 1 Pemanfaatan OSINT

forum online, dan publikasi lain, membantu identifikasi ancaman serta perancangan strategi perlindungan.¹³

Di sektor penegakan hukum, OSINT menjadi alat investigasi kriminal yang efektif. Data dari internet sering kali memberikan petunjuk tentang aktivitas dan hubungan tersangka, memfasilitasi penyelidikan yang lebih cepat.¹⁴ Dalam dunia bisnis, OSINT digunakan untuk menganalisis pesaing dan memahami tren pasar, sementara di sektor keuangan, OSINT mendukung due diligence dan prediksi pasar.

Sektor teknologi dan siber memanfaatkan OSINT untuk keamanan siber, mengidentifikasi risiko lebih awal, dan mengikuti perkembangan teknologi terkini. Di hubungan internasional, OSINT membantu merumuskan strategi diplomatik berdasarkan analisis kebijakan luar negeri lain.

Indonesia menghadapi tantangan dalam merumuskan regulasi perlindungan data pribadi secara komprehensif. Meskipun telah diberlakukan UU ITE (Undang-Undang Informasi dan

¹² Ashok Yadav, Atul Kumar, dan Vrijendra Singh. "Open-source intelligence: a comprehensive review of the current state, applications and future perspectives in cyber security." *Artificial Intelligence Review* 56.11 (2023): 12407-12438.

¹³ Nia Lavinia dan Puspitasari Puspitasari. "Urgensi Pemanfaatan Open Source Intelligent (Osint) Dalam Upaya Pencegahan Aksi Terorisme di Indonesia." *Jurnal Sosial Humaniora Terapan* 6.1 (2022): 3.

¹⁴ Ferry Gunawan dan TM Mirza Keumala. "Analisis Information Gathering Target Daftar Pencarian Orang Menggunakan Metodeopen Source Intelligence Pada Kejaksaan Tinggi Aceh." *Jurnal Sistem Komputer (SISKOM)* 4.1 (2024): 10-21.

Transaksi Elektronik) dan UU PDP (Perlindungan Data Pribadi), terdapat kekosongan hukum dan ambiguitas yang menghambat pelaksanaan regulasi secara efektif. Keterbatasan sumber daya, infrastruktur, serta ketidakselarasan kebijakan di berbagai sektor menyebabkan perlindungan data tidak konsisten.

Pemrosesan data pribadi melalui OSINT untuk tujuan komersial harus memenuhi ketentuan UU PDP, termasuk persetujuan eksplisit dari subjek data. Pasal 28 UU PDP menegaskan penggunaan data pribadi harus sesuai dengan tujuan yang diinformasikan kepada subjek data. Di sisi lain, Pasal 26 UU ITE mengatur perlunya persetujuan dalam penggunaan data pribadi. Ambiguitas muncul ketika data yang digunakan berasal dari sumber terbuka, yang sering kali dianggap tidak dilindungi.

Namun, prinsip-prinsip pemrosesan data seperti transparansi dan akuntabilitas harus tetap dipatuhi. Anonimisasi data hasil penggunaan OSINT dapat menjadi solusi untuk menghindari pelanggaran hukum, asalkan dilakukan secara menyeluruh hingga tidak dapat dilakukan *re-identifikasi*.

Individu juga memiliki tanggung jawab besar dalam melindungi data pribadi mereka.¹⁵ Kesadaran akan privasi data dan risiko yang menyertainya perlu ditingkatkan. Langkah-langkah seperti membatasi informasi yang dibagikan di media sosial, menggunakan perangkat lunak keamanan, dan berhati-hati terhadap serangan *phishing* sangat penting untuk melindungi data dari penyalahgunaan.¹⁶

Akibat Hukum Penggunaan *Open Source Intelligence* sebagai Metode Pemrosesan Data Pribadi menurut Hukum Perlindungan Data Pribadi

Open Source Intelligence (OSINT) adalah metode pengumpulan dan pengolahan data pribadi yang tersedia secara publik melalui sumber terbuka seperti media sosial, situs web, dan dokumen publik. Legalitas penggunaan OSINT sangat bergantung pada kepatuhan terhadap regulasi privasi dan perlindungan data pribadi.¹⁷ Meskipun data bersifat publik, pengumpulan dan penggunaannya harus mematuhi hukum untuk menghindari pelanggaran hak privasi individu. Di Indonesia, Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) menegaskan bahwa pemrosesan data harus berdasarkan persetujuan subjek

¹⁵ Sekaring Ayumeida Kusnadi. "Perlindungan Hukum Data Pribadi Sebagai Hak Privasi." *Al Wasath Jurnal Ilmu Hukum* 2.1 (2021): 9-16.

¹⁶ *Ibid.*

¹⁷ Mulkan Fadhlil. "Analisis Komprehensif terhadap Framework dan Alat Penetration Testing: Tren, Tantangan, dan Peluang: Comprehensive Analysis of Penetration Testing Frameworks and Tools: Trends, Challenges, and Opportunities." *Indonesian Journal of Electrical Engineering and Renewable Energy (IJEERE)* 4.1 (2024): 15-22.

data, kecuali dalam kondisi tertentu yang diatur undang-undang. Oleh karena itu, praktisi OSINT wajib memastikan aktivitas mereka tidak melanggar hukum dan norma etika.

Penggunaan data publik ini dapat menimbulkan isu privasi, terutama jika dilakukan tanpa persetujuan pemilik data. Contohnya, pengumpulan data media sosial untuk tujuan komersial atau pengawasan tanpa izin dapat dianggap melanggar privasi.¹⁸ General Data Protection Regulation (GDPR) di Uni Eropa mengharuskan pengumpulan data dilakukan secara sah, transparan, dan berdasarkan persetujuan yang jelas dari subjek data. Regulasi ini menekankan pentingnya kepatuhan terhadap prinsip perlindungan data untuk menghindari konsekuensi hukum dan etika.

Regulasi Indonesia dan GDPR memiliki perbedaan dalam konteks OSINT. Di Indonesia, UU PDP berfokus pada perlindungan data pribadi dalam negeri, sedangkan GDPR menetapkan standar internasional untuk privasi dan kontrol data individu. GDPR mendefinisikan data pribadi secara luas, mencakup informasi seperti alamat IP, data lokasi, dan biometrik, sementara definisi UU PDP lebih sempit. Kedua regulasi sama-sama menuntut transparansi, legalitas, dan tujuan jelas dalam pengumpulan data, namun GDPR lebih ketat dalam mekanisme persetujuan.

UU PDP mengatur prinsip transparansi, legalitas, dan tujuan spesifik dalam pengolahan data pribadi, serta memberikan sanksi administratif dan pidana bagi pelanggaran. Sementara itu, UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) melarang pengumpulan data tanpa izin dan mengatur konsekuensi hukum atas pelanggaran privasi. Ketentuan ini diperkuat oleh regulasi lain seperti KUHP dan UU Telekomunikasi, yang memberikan perlindungan tambahan terhadap informasi pribadi.

GDPR, dengan prinsip-prinsip legalitas, keadilan, dan transparansi, menuntut dasar hukum yang sah untuk setiap pemrosesan data. GDPR juga memberikan hak-hak individu seperti "right to be forgotten" dan akses penuh terhadap data pribadi mereka. Dalam implementasinya, otoritas perlindungan data di Uni Eropa dapat menjatuhkan denda yang signifikan untuk pelanggaran, hingga 20 juta euro atau 4% dari pendapatan tahunan perusahaan. Sementara itu, UU PDP Indonesia memperkenalkan sanksi serupa, namun dengan skala yang lebih kecil.

UU PDP, meskipun lebih fleksibel, masih dalam tahap implementasi dengan lembaga pengawas yang sedang berkembang. Kedua regulasi ini memiliki kesamaan tujuan dalam

¹⁸ Hanifan Niffari. "Perlindungan Data Pribadi Sebagai Bagian Dari Hak Asasi Manusia Atas Perlindungan Diri Pribadi (Suatu Tinjauan Komparatif Dengan Peraturan Perundang-Undangan Di Negara Lain)." *Jurnal Yuridis* 7.1 (2020): 105-119.

melindungi hak privasi individu di era digital, namun pendekatan dan tingkat kepatuhannya bervariasi sesuai konteks hukum dan budaya masing-masing wilayah.

Perbandingan regulasi penggunaan OSINT antara Hukum Positif Indonesia dan *General Data Protection Regulation* (GDPR) mencakup beberapa aspek penting. Kedua regulasi ini mengatur pengumpulan, pemrosesan, dan penggunaan data pribadi, termasuk yang diperoleh melalui OSINT. Namun, perbedaannya terletak pada cakupan dan struktur hukum yang berlaku. GDPR berlaku di seluruh Uni Eropa dengan regulasi tunggal, sementara Indonesia mengatur melalui beberapa undang-undang terpisah, yaitu UU Perlindungan Data Pribadi (UU PDP) dan UU ITE. Dalam hal definisi data pribadi, keduanya mengakui bahwa data yang dapat mengidentifikasi individu baik langsung maupun tidak langsung merupakan data pribadi, namun GDPR lebih rinci dengan mencakup kategori data sensitif yang tidak secara eksplisit diatur dalam UU PDP.

Kedua regulasi ini juga melarang pengumpulan data tanpa persetujuan, kecuali untuk tujuan tertentu seperti keamanan nasional atau penegakan hukum, meskipun GDPR memberikan ruang lebih luas untuk "kepentingan yang sah" sebagai dasar hukum dibandingkan dengan UU PDP yang lebih terbatas. Terkait pemrosesan data anonim, baik GDPR maupun UU PDP mengecualikan data anonim dari perlindungan hukum, namun GDPR memberikan penjelasan lebih rinci mengenai kriteria anonimisasi dan pseudonimisasi. Mengenai hak subjek data, keduanya memberikan hak yang serupa bagi individu untuk mengakses, memperbaiki, menghapus, dan menarik persetujuan atas data pribadi mereka, namun GDPR juga mencakup hak portabilitas data yang tidak diatur dalam UU PDP.

Sanksi atas pelanggaran data pribadi juga menjadi salah satu perbedaan signifikan antara kedua regulasi ini. GDPR menetapkan denda administratif yang jauh lebih tinggi, yakni hingga €20 juta atau 4% dari pendapatan tahunan global, sedangkan UU PDP menetapkan denda administratif hingga 2% pendapatan tahunan perusahaan dan sanksi pidana berdasarkan UU ITE. Dalam hal penggunaan untuk penegakan hukum, kedua regulasi mengizinkan penggunaan OSINT tanpa persetujuan. Terakhir, meskipun keduanya memiliki otoritas untuk mengawasi pelaksanaan regulasi, otoritas pengawasan GDPR melalui *Data Protection Authorities* (DPA) sudah aktif di Uni Eropa, sedangkan otoritas pengawasan UU PDP masih dalam tahap pembentukan di Indonesia.

KESIMPULAN

Berdasarkan hasil penelitian dan pembahasan atas permasalahan di atas, maka dapat ditarik beberapa kesimpulan sebagai berikut, yakni:

1. Open Source Intelligence (OSINT) sebagai metode pemrosesan data pribadi belum diatur secara khusus mengenai penggunaannya, namun penggunaan dan pemanfaatannya harus mematuhi ketentuan dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) dan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). Pengembangan sistem, pengambilan, pengolahan dan penggunaan hasil data pribadi harus sesuai dengan pemenuhan hak subjek data pribadi dan kewajiban pengendali data pribadi serta prosesor data pribadi dalam pemrosesan data pribadi dapat dilaksanakan menurut UU PDP, selain itu Pasal 26 angka 1 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) juga menyebutkan bahwa penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan orang yang bersangkutan. Kewajiban sebagai pengendali data pribadi juga melekat pada pengguna OSINT sesuai dengan kewajiban pengendali data pribadi yang termuat dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Monetisasi data hasil pemrosesan data menggunakan metode OSINT tidak boleh melanggar Pasal 5 dan 28 Undang-Undang Nomor 27 Tahun 2022 dan Pasal 26 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Pelanggaran terhadap ketentuan ini dapat mengakibatkan sanksi administratif dan pidana, sehingga menjadi keharusan untuk menciptakan batasan yang ketat terhadap praktik OSINT yakni data yang boleh dilakukan pemrosesan adalah data-data umum yang dapat diakses semua orang dan/atau data pribadi yang bersifat khusus yang memang sengaja diupload untuk suatu kepentingan yang bersifat umum.
2. Indonesia dan Uni Eropa memlaui Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi dan *General Data Protection Regulation* (GDPR) memiliki prinsip serupa dalam melindungi data pribadi, termasuk di dalamnya persyaratan persetujuan, pengecualian untuk anonim, dan larangan pemrosesan data tanpa dasar hukum yang sah. Apabila dibandingkan, regulasi di Indonesia cenderung belum sekomprehensif dan seketat *General Data Protection Regulation* GDPR Uni Eropa mencakup sanksi administratif yang lebih tegas dengan denda yang bisa mencapai 20 juta Euro atau 4% dari omset tahunan perusahaan, sedangkan di Indonesia sanksi administratif dan pidana ada namun dengan skala denda yang lebih rendah yakni hingga 2% pendapatan tahunan perusahaan. Selain itu, GDPR memberikan pengawasan lebih efektif melalui *Data Protection Authorities* (DPA). Sementara itu, UU PDP masih dalam tahap implementasi

dengan lembaga pengawasan yang baru berkembang, sehingga pelaksanaannya memerlukan penguatan lebih lanjut.

SARAN

Berdasarkan kesimpulan diatas terdapat beberapa saran, yakni:

1. Pemerintah Indonesia perlu mempertimbangkan penyusunan regulasi khusus yang mengatur pemanfaatan Open Source Intelligence (OSINT), terutama dalam kaitannya dengan pemrosesan data pribadi. Regulasi ini harus mencakup pedoman yang jelas tentang pengumpulan, pemrosesan, dan pemanfaatan data dari sumber terbuka, serta batasan yang melindungi hak privasi subjek data sesuai dengan prinsip-prinsip dalam UU PDP dan UU ITE. Hal ini penting untuk memastikan bahwa pelaku OSINT memiliki panduan hukum yang jelas dan tidak melakukan pelanggaran.
2. Praktisi OSINT perlu diberikan edukasi dan pelatihan yang memadai tentang kewajiban sebagai pengendali data pribadi dan pentingnya mendapatkan persetujuan subjek data sesuai dengan ketentuan dalam Pasal 26 UU ITE dan UU PDP. Selain itu, sosialisasi tentang pemrosesan data yang etis dan sah harus dilakukan untuk mencegah praktik yang melanggar hukum, seperti monetisasi data tanpa persetujuan.
3. Pemerintah perlu segera mempercepat persiapan lembaga pengawasan yang efektif sesuai amanat UU PDP, sehingga pengawasan terhadap pemrosesan data pribadi, termasuk melalui OSINT, dapat berjalan dengan optimal. Selain itu, perlu diadakan upaya penguatan mekanisme pengaduan dan penegakan hukum bagi subjek data yang merasa haknya dilanggar. Audit reguler dan evaluasi terhadap praktik-praktik OSINT dapat membantu memastikan kepatuhan terhadap aturan dan etika yang berlaku, serta identifikasi dan penanganan dampak negatif yang mungkin timbul.
4. Sanksi administratif dan pidana di Indonesia terkait pelanggaran perlindungan data perlu diperkuat, baik dari segi nominal denda maupun bentuk hukumannya. Hal ini bertujuan untuk menciptakan efek jera bagi pelanggar, sejalan dengan standar yang diterapkan oleh GDPR Uni Eropa. Selain itu, pengawasan terhadap penerapan sanksi harus dilakukan secara transparan dan konsisten.

DAFTAR PUSTAKA

Peraturan Perundang-Undangan

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE)

Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik

Jurnal

- Ashok Yadav, Atul Kumar, dan Vrijendra Singh. "Open-source intelligence: a comprehensive review of the current state, applications and future perspectives in cyber security." *Artificial Intelligence Review* 56.11 (2023): 12407-12438.
- Ferry Gunawan dan TM Mirza Keumala. "Analisis Information Gathering Target Daftar Pencarian Orang Menggunakan Metodeopen Source Intelligence Pada Kejaksaan Tinggi Aceh." *Jurnal Sistem Komputer (SISKOM)* 4.1 (2024): 10-21.
- Firdi Gunawan, Ahmad Fadhilah, dan Essy Malays Sari Sakti. "Membangun Benteng Digital Untuk Memperkuat Etika Cyber Security Melawan Ancaman Cyber Crime." *Jurnal Ilmiah Teknik Informatika (TEKINFO)* 25.1 (2024): 154-167.
- Hanifan Niffari. "Perlindungan Data Pribadi Sebagai Bagian Dari Hak Asasi Manusia Atas Perlindungan Diri Pribadi (Suatu Tinjauan Komparatif Dengan Peraturan Perundang-Undangan Di Negara Lain)." *Jurnal Yuridis* 7.1 (2020): 105-119.
- Mulkan Fadhli. "Analisis Komprehensif terhadap Framework dan Alat Penetration Testing: Tren, Tantangan, dan Peluang: Comprehensive Analysis of Penetration Testing Frameworks and Tools: Trends, Challenges, and Opportunities." *Indonesian Journal of Electrical Engineering and Renewable Energy (IJEERE)* 4.1 (2024): 15-22.
- Nia Lavinia dan Puspitasari Puspitasari. "Urgensi Pemanfaatan Open Source Intelligent (Osint) Dalam Upaya Pencegahan Aksi Terorisme di Indonesia." *Jurnal Sosial Humaniora Terapan* 6.1 (2022): 3.
- Sekaring Ayumeida Kusnadi. "Perlindungan Hukum Data Pribadi Sebagai Hak Privasi." *Al Wasath Jurnal Ilmu Hukum* 2.1 (2021): 9-16.
- Surya Dwi Putra, Bhernedetha Nindya Kusumastuti, and Nasrul Ma'arif. "Potensi Ancaman Penggunaan OSINT Menyebabkan Kegagalan Pengambilan Keputusan Akibat Informasi Hoax." *Jurnal Kajian Stratejik Ketahanan Nasional* 6.2 (2023): 4.
- Tiara Almira Raila, Sinta Dewi Rosadi, and Rika Ratna Permata, "Perlindungan data privasi di Indonesia dan Singapura terkait penerapan digital contact tracing sebagai upaya pencegahan covid-19 serta tanggungjawabnya." *Jurnal Kepastian Hukum dan Keadilan* 2.1 (2021): 1-18.

Internet

- Putri, "Open Source Information (OSINT): Way we collect information in the age of no privacy", Integrity Indonesia, 25 juni 2019, <https://www.integrity-indonesia.com/id/blog/2019/06/25/open-source-information-osint-eksploitasi-informasi-di-era-tanpa-privasi/>, diakses 5 September 2024
- Daniel Eduardo Daud, "Open-Source Intelligence (OSINT)", Binus University, 16 April 2022, <https://student-activity.binus.ac.id/csc/2022/04/open-source-intelligence-osint/>, diakses 5 September 2024