JURNAL HUKUM "DE'RECHTSSTAAT"
DIKELOLA OLEH FAKULTAS HUKUM UNIVERSITAS DJUANDA BOGOR P-ISSN 2549-9874 E-ISSN 2442-5303
jurnal.hukum@unida.ac.id

Cyber Profiling dalam Pengawasan Keimigrasian: Analisis Pemanfaatan Data Digital untuk Pencegahan Penyalahgunaan Izin Tinggal oleh Orang Asing

Muhamad Itsar Muqarab,[1] Sohirin,[1] Koesemoyo Ponco Aji[1]

[1]Prodi Hukum Keimigrasian, Jurusan Keimigrasian, Politeknik Pengayoman Indonesia

Volume 12 Issue 1 (Maret, 2026)
e-ISSN 2716-5191
doi: *10.30997/jhd.v12i1.21441*

ARTICLE INFO

Article history:
Received: Aug 25, 2025
Revised version received: Sept 02, 2025
Accepted: March 10, 2026
Available online: March 19, 2026

Keywords:
Cyber profiling; Digital data; Immigration oversight; Immigration violations; Residence permits.

How to Cite:
Muqarab, Muhamad Itsar, et. al., 2026. "Cyber Profiling dalam Pengawasan Keimigrasian: Analisis Pemanfaatan Data Digital untuk Pencegahan Penyalahgunaan Izin Tinggal oleh Orang Asing." *JURNAL HUKUM DE'RECHTSSTAAT*

Corresponding Author:
Muhamad Itsar Muqarab
Itsar4m@gmail.com

ABSTRAK

Perkembangan teknologi digital telah mendorong transformasi dalam sistem pengawasan keimigrasian, khususnya dalam menghadapi peningkatan penyalahgunaan izin tinggal oleh orang asing. Pendekatan konvensional dinilai belum optimal dalam mendeteksi pelanggaran yang semakin kompleks dan tersembunyi di ruang siber. Penelitian ini bertujuan untuk menganalisis penerapan *cyber profiling* dalam pengawasan keimigrasian, mengkaji dasar hukum yang melandasinya, serta menilai implikasi hukum terhadap pelanggaran izin tinggal. Metode yang digunakan adalah penelitian hukum normatif dengan pendekatan kualitatif melalui studi kepustakaan terhadap peraturan perundang-undangan dan literatur terkait. Hasil penelitian menunjukkan bahwa *cyber profiling* memiliki legitimasi hukum melalui Undang-Undang Nomor 6 Tahun 2011 tentang Keimigrasian dan Peraturan Menteri Imigrasi dan Pemasyarakatan Nomor 2 Tahun 2025, serta berperan sebagai alat deteksi dini yang efektif terhadap pelanggaran izin tinggal. Dengan demikian, diperlukan penguatan regulasi teknis, peningkatan kapasitas aparatur, serta penerapan prinsip etika dan perlindungan hak asasi manusia agar *cyber profiling* dapat diimplementasikan secara optimal, proporsional, dan akuntabel dalam sistem pengawasan keimigrasian Indonesia.

Available online at https://ojs.unida.ac.id/LAW

ABSTRACT

The advancement of digital technology has transformed immigration oversight systems, particularly in addressing the increasing misuse of residence permits by foreign nationals. Conventional approaches are considered insufficient to detect violations that are increasingly complex and concealed within cyberspace. Therefore, cyber profiling emerges as a technology-based surveillance method that utilizes digital data to identify patterns of individual online activities. This study aims to analyze the implementation of cyber profiling in immigration oversight, examine its legal basis, and assess its legal implications for residence permit violations. This research employs a normative legal method with a qualitative approach through literature review of relevant laws and academic sources. The findings indicate that cyber profiling has a strong legal foundation under Law Number 6 of 2011 concerning Immigration and Ministerial Regulation Number 2 of 2025, and serves as an effective early detection tool for identifying violations. However, its implementation also faces challenges, particularly in relation to personal data protection, the validity of digital evidence, and limitations in human resources and technological infrastructure. Therefore, strengthening technical regulations, enhancing institutional capacity, and ensuring ethical standards and human rights protection are essential to ensure that cyber profiling can be implemented effectively, proportionally, and accountably within Indonesia's immigration oversight system.

1. Pendahuluan

Globalisasi dan percepatan teknologi digital telah merevolusi dinamika mobilitas manusia lintas negara. Indonesia, sebagai negara kepulauan dengan daya tarik wisata yang tinggi serta peluang ekonomi yang berkembang, menjadi destinasi utama bagi Warga Negara Asing (WNA) untuk berbagai tujuan—mulai dari pariwisata, pendidikan, hingga kegiatan ekonomi dan profesi. Namun, peningkatan intensitas kedatangan orang asing tersebut tidak terlepas dari berbagai tantangan hukum dan administratif, khususnya dalam hal penegakan aturan mengenai izin tinggal.Salah satu persoalan yang mengemuka dalam tata kelola keimigrasian di Indonesia adalah penyalahgunaan izin tinggal, yang dapat berbentuk tinggal melebihi masa berlaku (*overstay*), pelanggaran jenis visa (seperti penggunaan visa kunjungan untuk bekerja), hingga pemberian data palsu demi memperoleh izin tinggal tertentu.

Selama ini, pengawasan terhadap orang asing dilakukan melalui pendekatan konvensional, yakni patroli lapangan, pemeriksaan dokumen di tempat-tempat strategis, atau pemanggilan ke Kantor Imigrasi. Namun, patroli lapangan dinilai tidak cukup efektif untuk mendeteksi modus yang sering dilakukan pelanggaran izin tinggal.[1] Fenomena meningkatnya penggunaan media sosial dan platform digital oleh WNA selama berada di Indonesia telah menghadirkan peluang baru bagi aparat Imigrasi.[2] Jejak digital (digital footprint) yang tertinggal dalam ruang maya seperti unggahan media sosial, aktivitas dalam forum daring, partisipasi dalam transaksi elektronik, hingga publikasi konten komersial dapat dijadikan indikator awal untuk menilai apakah seseorang menjalankan aktivitas yang selaras atau

[1] Malhotra, Anshu, Luam Totti, Wagner Meira Jr., Ponnurangam K. Kumaraguru, dan Virgilio Almeida. 2013. "Studying User Footprints in Different Online Social Networks." arXiv, Januari.

[2] Kim, Jisu, Alina Sîrbu, Fosca Giannotti, dan Lorenzo Gabrielli. 2020. "Digital Footprints of International Migration on Twitter." In *Digital Footprints of International Migration on Twitter*, 274–86. LNCS 12080.

bertentangan dengan status keimigrasiannya. Maka konsep *cyber profiling* dalam pengawasan keimigrasian mulai memperoleh relevansi strategis.

Cyber profiling merupakan istilah di keimigrasian dapat dipahami sebagai metode pengawasan berbasis teknologi yang memanfaatkan data digital terbuka untuk menyusun profil perilaku orang asing. Pendekatan ini memungkinkan keimigrasian untuk mengidentifikasi pola aktivitas digital yang mencurigakan, tanpa harus bergantung pada pengawasan fisik. Sebagai bagian dari transformasi kelembagaan menuju pengawasan berbasis informasi, praktik ini memperoleh legitimasi hukum melalui Peraturan Menteri Imigrasi Pemasyarakatan No 2 Tahun 2025 yang mengatur pengumpulan, analisis, dan pemanfaatan data digital dalam pengambilan tindakan administratif. Namun, penggunaan teknologi siber dalam pengawasan keimigrasian juga menimbulkan pertanyaan kritis, terutama terkait validitas data sebagai alat pembuktian hukum, batasan etis dalam pengumpulan informasi pribadi, serta perlindungan hak privasi individu asing yang tunduk pada yurisdiksi Indonesia.[3] Oleh karena itu, dibutuhkan kajian yang tidak hanya deskriptif tetapi juga analitis mengenai bagaimana metode cyber profiling dijalankan secara hukum, serta bagaimana konsekuensi administratif dan pidana dikenakan terhadap pelanggar yang teridentifikasi melalui data digital.Penelitian ini bertujuan mengkaji penggunaan cyber profiling dalam konteks pengawasan keimigrasian, dasar hukumnya, serta konsekuensi hukum bagi pelanggar.

Berdasarkan uraian latar belakang diatas, maka yang menjadi rumusan masalah dalam penelitian ini adalah:

1. Bagaimana penerapan metode *cyber profiling* dalam pengawasan keimigrasian di Indonesia, khususnya untuk mencegah penyalahgunaan izin tinggal oleh orang asing?
2. Apa saja dasar hukum, tantangan, dan implikasi etis yang dihadapi dalam penggunaan data digital sebagai alat pengawasan keimigrasian melalui pendekatan cyber profiling?

2. Metode Penelitian

Penelitian ini menggunakan pendekatan hukum normatif dengan metode analisis kualitatif. Pendekatan normatif dimaksudkan untuk mengkaji hukum sebagai suatu sistem norma, dengan menitikberatkan pada analisis terhadap bahan-bahan hukum sekunder. Oleh karena itu, sumber data utama diperoleh melalui studi kepustakaan, meliputi peraturan perundang-undangan, putusan pengadilan, serta literatur ilmiah yang relevan dengan permasalahan yang dikaji. Data yang terkumpul kemudian dianalisis secara deskriptif-kualitatif guna memperoleh pemahaman yang mendalam dan sistematis mengenai isu hukum yang menjadi fokus penelitian.

[3] Samad, M. Yusuf, Beta K. Ningtiyas, Fiqih Fauzy Rosny, dan Diah A. Permatasari. 2024. "Anticipating Cyber Espionage: Open Source Intelligence Investigation and Cyber Counterintelligence." Jurnal JSRCS 5 (2): 167–84.

3. Hasil dan Pembahasan

Cyber profiling merupakan metode pengawasan berbasis teknologi informasi yang melibatkan proses pengumpulan, pemetaan, dan analisis data digital untuk menyusun profil perilaku individu secara daring.[4] Dalam hal keimigrasian, pendekatan ini digunakan untuk menilai kepatuhan warga negara asing (WNA) terhadap ketentuan izin tinggal di Indonesia. Data yang menjadi objek pemantauan meliputi informasi yang secara sadar atau tidak disadari diunggah oleh individu, seperti aktivitas di media sosial (Instagram, Facebook, TikTok), platform video (YouTube), situs web pribadi, partisipasi dalam forum daring, hingga jejak transaksi dalam *e-commerce* atau aplikasi transportasi. Tujuan utama dari cyber profiling dalam sistem keimigrasian adalah untuk mendeteksi secara dini potensi pelanggaran izin tinggal oleh orang asing. Dengan meningkatnya kehadiran digital para WNA selama mereka berada di Indonesia, data yang tersedia di ruang maya dapat menjadi sumber informasi yang sah dan berguna untuk mengidentifikasi aktivitas yang bertentangan dengan jenis visa atau izin tinggal yang dimiliki. Misalnya, WNA yang memiliki visa kunjungan seharusnya tidak diperkenankan menjalankan kegiatan usaha, namun melalui penelusuran digital, petugas Imigrasi mungkin menemukan unggahan promosi layanan, testimoni pelanggan, atau rincian transaksi yang menunjukkan keterlibatan dalam kegiatan ekonomi.[5]

Penerapan cyber profiling dalam pengawasan keimigrasian telah memperoleh legitimasi hukum melalui Peraturan Menteri Hukum dan HAM Republik Indonesia Nomor 2 Tahun 2025 tentang Pengawasan Keimigrasian Berbasis Teknologi Informasi. Pasal 6 hingga Pasal 10 dalam regulasi tersebut secara tegas mengatur bahwa data digital orang asing dapat dikumpulkan dari berbagai sumber terbuka—termasuk media sosial, forum komunitas, serta platform digital lainnya—untuk dianalisis oleh petugas keimigrasian. Informasi tersebut dapat digunakan untuk menilai apakah aktivitas individu sesuai dengan status izin tinggal yang diberikan.Salah satu contoh konkret penerapan metode *cyber profiling* dalam pengawasan keimigrasian dapat ditemukan pada kasus warga negara asing (WNA) pemegang visa wisata yang secara aktif mempromosikan kegiatan komersial melalui media sosial, seperti Instagram.[6] Dalam kasus tersebut, WNA yang bersangkutan menawarkan jasa pelatihan yoga, kelas meditasi, atau konsultasi bisnis kepada masyarakat luas, lengkap dengan jadwal kegiatan, tarif layanan, serta testimoni dari klien. Aktivitas semacam ini secara kasatmata mungkin tidak mengganggu ketertiban umum atau keamanan nasional.[7] Namun, dari sudut

[4] Zulkiflee, E.F. 2024. "Digital Era OSINT: Formulating Special ..." Journal of Management & Intelligence 17 (2): 50–67.

[5] Yusila, Anggina, Mabruri Andatu, Fatimatuzzahra, and Sal Sabila Alamsyah. 2025. "Protection Of Human Rights For Workers In The Job Creation Law From An Islamic Legal Perspective". *DE'RECHTSSTAAT*, February, 157-70. https://ojs.unida.info/index.php/LAW/article/view/17147.

[6] Nugroho, F. 2023. "Analisis Penerapan OSINT dalam Pengawasan WNA di Indonesia." Jurnal Keamanan Digital 3 (2): 101–15.

[7] Riswanih, Ira, Nurwati, and M. Rendi Aridhayandi. 2025. "Effectiveness Of The Ministry Of Communication And Information In Handling The Misuse Of Personal Data". *De'rechtsstaat*, February, 83-89. https://ojs.unida.info/index.php/LAW/article/view/18393.

pandang keimigrasian, tindakan tersebut jelas menunjukkan adanya pelanggaran terhadap ketentuan izin tinggal, karena visa wisata tidak memberikan izin bagi pemegangnya untuk melakukan kegiatan ekonomi atau memperoleh penghasilan di wilayah Indonesia.

Cyber profiling memainkan peran sentral sebagai alat pendeteksi dini terhadap penyalahgunaan izin tinggal yang tidak terjangkau oleh pengawasan fisik tradisional. Petugas Imigrasi tidak perlu menunggu laporan masyarakat atau melakukan operasi lapangan untuk mengidentifikasi pelanggaran, karena data yang tersedia secara terbuka di internet telah memberikan cukup bukti awal. Aktivitas promosi, interaksi dengan calon pelanggan, serta transaksi yang terekam secara digital dapat dijadikan dasar untuk mengkaji ulang status izin tinggal yang dimiliki oleh WNA tersebut.Penggunaan data digital dalam pengawasan keimigrasian di Indonesia telah mendapatkan legitimasi hukum melalui Permenimipas No. 2 Tahun 2025. Pasal 14 ayat (2) menyatakan bahwa "Petugas Imigrasi dapat melakukan pengawasan secara siber terhadap orang asing berdasarkan informasi digital."[8] Hal ini menunjukkan bahwa pengawasan tidak lagi terbatas pada interaksi fisik, tetapi telah meluas ke ruang siber.Lebih lanjut, Pasal 16 dari peraturan yang sama menegaskan bahwa hasil cyber profiling dapat menjadi dasar bagi tindakan administratif, seperti pemanggilan, pemeriksaan, hingga deportasi.[9] Ketentuan ini memberikan landasan bagi keimigrasian untuk menindak WNA berdasarkan informasi digital yang valid dan terverifikasi.

Selain itu, UU No. 6 Tahun 2011 memberikan kekuatan hukum bagi pejabat Imigrasi untuk melakukan tindakan administratif maupun pidana. Pasal 75 ayat (1) menyebutkan bahwa pejabat Imigrasi berwenang mengambil tindakan terhadap orang asing yang mengganggu keamanan dan ketertiban atau tidak mematuhi peraturan perundang-undangan.Dalam konteks ini, penggunaan data digital sebagai dasar tindakan dianggap sah selama data tersebut dikumpulkan dari sumber yang terbuka dan digunakan sesuai prosedur hukum.[10]

3.1 Sanksi Pidana dan Administratif terhadap Pelanggaran Izin Tinggal

Cyber profiling tidak hanya berfungsi sebagai alat deteksi dini, tetapi juga sebagai bukti awal untuk menindak pelanggaran. Berdasarkan UU No. 6 Tahun 2011, terdapat beberapa ketentuan hukum yang mengatur sanksi bagi orang asing yang menyalahgunakan izin tinggal:

- **Pasal 119**: Menyebutkan bahwa orang asing yang menyalahgunakan izin tinggal dapat dikenakan pidana penjara paling lama 5 (lima) tahun dan/atau denda paling banyak Rp500.000.000.
- **Pasal 122 huruf a**: Mengatur bahwa setiap orang yang memberikan data palsu atau tidak benar untuk memperoleh izin tinggal dapat dipidana penjara paling lama 5 (lima) tahun dan/atau denda paling banyak Rp500.000.000.

[8] Sahdewa, M Farhas, Henny Nuraeny, and Rizal Syamsul Ma'arif. 2025. "Applying of the Concept of the Death Penalty in Indonesia and Malaysia". *DE'RECHTSSTAAT* 11 (2):236-47. https://doi.org/10.30997/jhd.v11i2.18691.

[9] Nurkumalawati, Intan, dan M. Syaroni Rofii. 2023. "Public Review of M-Paspor Application in Indonesia: Mobile Government, Digital Resilience, Cyber Security." In AICoBPA 2022, 404–12.

[10] Lestari, Siti. 2022. "Ethical Limits of Cyber Surveillance: Balancing National Interest and Privacy Rights." *Jurnal Etika Hukum dan Masyarakat* 6 (1): 66–80.

- **Pasal 75 ayat (1)**: Memberikan kewenangan kepada pejabat Imigrasi untuk mengenakan tindakan administratif berupa deportasi, pencantuman dalam daftar cekal, hingga pencabutan izin tinggal.

Dalam praktiknya, *cyber profiling* memungkinkan petugas Imigrasi mengidentifikasi pelanggaran dengan lebih cepat dan akurat. Misalnya, melalui postingan media sosial, petugas dapat mengetahui bahwa seorang pemegang visa pelajar ternyata bekerja penuh waktu, yang jelas melanggar ketentuan izin tinggalnya. Namun, penggunaan data digital sebagai bukti juga harus memperhatikan prinsip kehati-hatian, validitas data, dan privasi individu.[11] Prosedur pengumpulan dan analisis harus transparan, proporsional, dan sesuai dengan ketentuan hukum yang berlaku agar tidak menimbulkan pelanggaran hak asasi manusia.

3.2 Implikasi dan Tantangan

Penerapan *cyber profiling* dalam pengawasan keimigrasian menandai pergeseran paradigma dalam manajemen keamanan dan ketertiban terhadap keberadaan orang asing. Namun, meskipun strategi ini menjanjikan efisiensi dan deteksi dini terhadap pelanggaran izin tinggal, implementasinya tidak terlepas dari sejumlah implikasi krusial dan tantangan struktural yang perlu dicermati secara serius.

3.2.1. Perlindungan Data Pribadi

Salah satu tantangan utama dalam penerapan *cyber profiling* adalah terkait perlindungan data pribadi. Pengumpulan, penyimpanan, dan analisis data digital harus dijalankan dalam koridor hukum yang menghormati hak privasi individu. Dalam konteks Indonesia, keberadaan Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) menjadi fondasi normatif yang tidak dapat diabaikan. Imigrasi harus memastikan bahwa setiap aktivitas pengawasan siber dilakukan dengan persetujuan yang sah (jika diperlukan), prinsip proporsionalitas, serta sistem keamanan data yang kuat untuk mencegah penyalahgunaan atau kebocoran informasi. Ketidakhati-hatian dalam aspek ini dapat menimbulkan pelanggaran HAM serta menggugurkan legitimasi tindakan hukum berbasis data digital.

3.2.2. Kemampuan Teknologi dan Sumber Daya Manusia

Tantangan berikutnya adalah kesenjangan kapasitas teknologi dan kompetensi sumber daya manusia (SDM) antar wilayah. Tidak semua Kantor Imigrasi di Indonesia memiliki infrastruktur teknologi informasi yang memadai, apalagi personel yang terlatih dalam teknik *open-source intelligence (OSINT)*, data mining, atau analisis perilaku daring. Untuk itu, dibutuhkan strategi penguatan kelembagaan, mulai dari peningkatan kapasitas SDM melalui pelatihan teknis, hingga pengadaan perangkat lunak pendukung yang dapat mengolah data secara akurat dan efisien. Tanpa dukungan tersebut, *cyber profiling* akan berisiko menjadi prosedur administratif semata, bukan alat deteksi yang efektif.

[11] Walkow, Marcus, dan Daniela Pöhn. 2024. "Systematically Searching for Identity-Related Information in the Internet with OSINT Tools." *arXiv*, Juli.

3.2.3. Etika dan Batasan Pengawasan Siber

Di luar aspek teknis dan hukum, pengawasan siber juga membawa konsekuensi etis. *Cyber profiling* harus dijalankan sebagai instrumen pengawasan yang berbasis bukti dan proporsional, bukan sebagai alat kontrol sosial yang represif. Pemantauan digital yang bersifat invasif atau sewenang-wenang justru berpotensi menimbulkan ketidakpercayaan publik dan memperburuk citra institusi keimigrasian. Oleh karena itu, perlu adanya pedoman etis dan mekanisme pengawasan internal agar praktik ini tetap berada dalam batas kewajaran dan akuntabilitas.[12]Dengan demikian, meskipun *cyber profiling* menawarkan berbagai keunggulan dalam mendukung pengawasan keimigrasian modern, keberhasilannya sangat ditentukan oleh integrasi antara aspek hukum, teknologi, sumber daya manusia, dan komitmen etis dari aparat yang menjalankannya.

4. Kesimpulan

Cyber profiling merupakan salah satu inovasi strategis dalam pengawasan keimigrasian di era digital yang memungkinkan deteksi dini terhadap penyalahgunaan izin tinggal oleh orang asing melalui pemanfaatan data digital yang tersedia di ruang siber. Penerapan metode ini tidak hanya meningkatkan efektivitas pengawasan, tetapi juga memperluas jangkauan deteksi pelanggaran yang sebelumnya sulit diidentifikasi melalui pendekatan konvensional. Secara yuridis, penggunaan cyber profiling memiliki dasar hukum yang kuat, sebagaimana diatur dalam Undang-Undang Nomor 6 Tahun 2011 tentang Keimigrasian dan Peraturan Menteri Imigrasi dan Pemasyarakatan Nomor 2 Tahun 2025, yang memberikan kewenangan kepada petugas imigrasi untuk melakukan pengumpulan, analisis, dan pemanfaatan data digital sebagai dasar tindakan administratif maupun pidana. Hal ini menunjukkan bahwa pengawasan keimigrasian telah bertransformasi menuju pendekatan berbasis teknologi informasi yang adaptif terhadap perkembangan zaman.

Namun demikian, implementasi cyber profiling tidak terlepas dari berbagai tantangan, terutama yang berkaitan dengan perlindungan data pribadi, validitas data digital sebagai alat pembuktian hukum, serta keterbatasan kapasitas sumber daya manusia dan infrastruktur teknologi di berbagai wilayah. Oleh karena itu, diperlukan penguatan kebijakan teknis melalui penyusunan Standar Operasional Prosedur (SOP) yang komprehensif, peningkatan kompetensi aparatur, serta pengembangan sistem teknologi yang andal dan terintegrasi. Keberhasilan penerapan cyber profiling sangat bergantung pada keseimbangan antara efektivitas pengawasan dan perlindungan hak asasi manusia. Apabila dikelola secara proporsional, transparan, dan akuntabel, metode ini berpotensi menjadi pilar utama dalam sistem pengawasan keimigrasian Indonesia yang modern, responsif, dan berkelanjutan di masa depan.

5. Ucapan Terima kasih

Penulis mengucapkan terima kasih kepada Politeknik Pengayoman Indonesia yang telah memberikan dukungan institusional, fasilitas, serta lingkungan akademik yang kondusif sehingga penelitian ini dapat terlaksana dengan baik. Penulis juga menyampaikan apresiasi kepada semua

[12] Anjani, N. H. 2021. *Cybersecurity Protection in Indonesia*. Policy Brief CIPS-PB09. CIPS/Econstor.

pihak yang telah memberikan kontribusi, baik secara langsung maupun tidak langsung, dalam proses penyusunan artikel ini.

Referensi

Buku

Anjani, N. H. 2021. Cybersecurity Protection in Indonesia. Jakarta: CIPS/Econstor.

Artikel Jurnal

Kim, Jisu, Alina Sîrbu, Fosca Giannotti, dan Lorenzo Gabrielli. 2020. "Digital Footprints of International Migration on Twitter." Lecture Notes in Computer Science 12080: 274–286.

Lestari, Siti. 2022. "Ethical Limits of Cyber Surveillance: Balancing National Interest and Privacy Rights." Jurnal Etika Hukum dan Masyarakat 6, no. 1: 66–80.

Malhotra, Anshu, Luam Totti, Wagner Meira Jr., Ponnurangam K. Kumaraguru, dan Virgilio Almeida. 2013. "Studying User Footprints in Different Online Social Networks." arXiv.

Nugroho, F. 2023. "Analisis Penerapan OSINT dalam Pengawasan WNA di Indonesia." Jurnal Keamanan Digital 3, no. 2: 101–115.

Nurkumalawati, Intan, dan M. Syaroni Rofii. 2023. "Public Review of M-Paspor Application in Indonesia: Mobile Government, Digital Resilience, Cyber Security." Proceedings of AICoBPA 2022: 404–412.

Riswanih, Ira, Nurwati, dan M. Rendi Aridhayandi. 2025. "Effectiveness of the Ministry of Communication and Information in Handling the Misuse of Personal Data." De'Rechtsstaat, February, 83–89. https://ojs.unida.info/index.php/LAW/article/view/18393.

Sahdewa, M. Farhas, Henny Nuraeny, dan Rizal Syamsul Ma'arif. 2025. "Applying of the Concept of the Death Penalty in Indonesia and Malaysia." De'Rechtsstaat 11, no. 2: 236–247. https://doi.org/10.30997/jhd.v11i2.18691.

Samad, M. Yusuf, Beta K. Ningtiyas, Fiqih Fauzy Rosny, dan Diah A. Permatasari. 2024. "Anticipating Cyber Espionage: Open Source Intelligence Investigation and Cyber Counterintelligence." Jurnal JSRCS 5, no. 2: 167–184.

Walkow, Marcus, dan Daniela Pöhn. 2024. "Systematically Searching for Identity-Related Information in the Internet with OSINT Tools." arXiv.

Yusila, Anggina, Mabruri Andatu, Fatimatuzzahra, dan Sal Sabila Alamsyah. 2025. "Protection of Human Rights for Workers in the Job Creation Law from an Islamic Legal Perspective."

De'Rechtsstaat, February, 157–170. https://ojs.unida.info/index.php/LAW/article/view/17147.

Zulkiflee, E. F. 2024. "Digital Era OSINT: Formulating Special Surveillance Model for Non-Traditional Threats." Journal of Management & Intelligence 17, no. 2: 50–67.