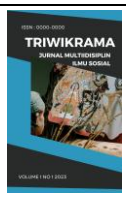
Triwikrama: Jurnal Ilmu Sosial
Volume 11 No 9 2025
E-ISSN: 2988-1986
Open Access:



LEGAL ADVICE: PERLINDUNGAN KORBAN DOXING DAN ONLINE SHAMING BERBASIS APLIKASI KONSULTASI MELALUI "AKSARA"

Ziilaan Kamal[1], Zaenal Fahad[2], Muhammad Adhymas Hikal [3]
Departemen Hukum, Fakultas Hukum, Universitas Negeri Semarang

ARTICLE INFO

Article history:
Received Desember 2025
Revised Desember 2025
Accepted Desember 2025
Available online Desember 2025

Email:
kuzilan637@students.unnes.ac.id,
zaenalfahad@students.unnes.ac.id,
Hikal@mail.unnes.ac.id

Abstrak

Eskalasi Kekerasan Berbasis Gender Online (KBGO), khususnya fenomena doxing dan online shaming, telah mencapai titik kritis seiring masifnya penetrasi digital di Indonesia. Di Kota Semarang, para korban menghadapi dampak psikologis serius, namun sering kali terhambat dalam mengakses keadilan akibat kompleksitas pembuktian elektronik dan tingginya biaya litigasi. Penelitian ini bertujuan untuk mengonstruksi model aplikasi bantuan hukum digital "AKSARA" yang mengintegrasikan layanan konsultasi hukum, pendampingan psikososial, dan preservasi bukti elektronik. Penelitian ini menggunakan metode Research and Development (R&D) dengan pendekatan socio-legal untuk menjamin kepatuhan sistem terhadap UU No. 1 Tahun 2024 tentang ITE dan UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP). Hasil penelitian menunjukkan bahwa AKSARA mampu menjembatani kesenjangan antara kondisi psikologis korban dan rigiditas standar hukum melalui fitur Legal First Aid dan Secure Evidence Vault. Dengan menerapkan algoritma hashing SHA-256 dan standar forensik ISO/IEC 27037, aplikasi ini menjamin integritas alat bukti elektronik agar memiliki nilai pembuktian (probative value) yang sah di pengadilan, sekaligus memitigasi risiko reviktimisasi melalui prinsip Privacy by Design.

Kata kunci: AKSARA, Doxing, Online Shaming, Bukti Elektronik, Bantuan Hukum Digital.

Abstract

The escalation of Online Gender-Based Violence (OGBV), particularly doxing and online shaming, has reached a critical point alongside massive digital penetration in Indonesia. In Semarang City, victims suffer severe psychological impacts yet face significant barriers in accessing justice due to the complexity of electronic evidence and high litigation costs. This study aims to construct "AKSARA," a digital legal aid application model that integrates legal consultation, psychosocial support, and electronic evidence preservation. Utilizing a Research and Development (R&D) method combined with a socio-legal approach, the application is designed to comply with the ITE Law No. 1/2024 and the Personal Data Protection Law (UU PDP) No. 27/2022. The results indicate that AKSARA effectively bridges the gap between victim psychology and legal rigidity through "Legal First Aid" and "Secure Evidence Vault" features. By implementing SHA-256 hashing algorithms and ISO/IEC 27037 forensic standards, the system ensures the integrity of electronic evidence to possess valid probative value in court, while simultaneously mitigating the risk of revictimization through Privacy by Design principles.

Keywords: *AKSARA, Doxing, Online Shaming, Electronic Evidence, Digital Legal Aid.*

PENDAHULUAN

Peningkatan kejahatan digital di Indonesia telah mencapai titik kritis yang memerlukan perhatian serius dari berbagai pemangku kepentingan. Ruang siber, yang semula dimaksudkan untuk berfungsi sebagai media untuk demokrasi informasi, seringkali berubah menjadi arena intimidasi. Menurut laporan terbaru dari Southeast Asia Freedom of Expression Network (SAFEnet), tren serangan digital meningkat secara signifikan sejak 2024. SAFEnet juga mencatat bahwa doxing, yaitu penyebaran data pribadi tanpa izin, masih digunakan secara sistematis sebagai alat represi terhadap aktivis, jurnalis, dan warga sipil. Fenomena ini diperparah oleh banyaknya budaya shaming online, yang merupakan situasi di mana korban dipermalukan secara

massal oleh warganet, biasanya disebabkan oleh narasi palsu atau tuduhan yang belum terbukti benar, yang menghasilkan penghakiman sosial tanpa proses peradilan yang sah.

Tingkat lokal merasakan dampak anomali ruang siber ini. Angka kerentanan terhadap kejahatan siber di Jawa Tengah meningkat, terutama di Kota Semarang. Menurut data dari Legal Resource Center untuk Keadilan Jender dan Hak Asasi Manusia (LRC-KJHAM, 2024), ada 102 kasus kekerasan terhadap perempuan sepanjang tahun 2024. Sebagian besar kasus tersebut memiliki dimensi siber atau diklasifikasikan sebagai Kekerasan Berbasis Gender Online (KBGO). Korban di wilayah ini sering kali tidak memiliki cara untuk mendapatkan keadilan; upaya mereka untuk melapor ke polisi sering dihalangi oleh kekurangan bukti digital yang dianggap sah. Sementara itu, gangguan psikologis seperti depresi dan kecemasan akut terus mengganggu korban tanpa bantuan atau perawatan yang memadai.

Secara normatif, Indonesia telah memiliki undang-undang yang progresif untuk menangani masalah ini, seperti yang ditunjukkan oleh Undang-Undang Pelindungan Data Pribadi (UU PDP) Nomor 27 Tahun 2022 dan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) Nomor 1 Tahun 2024, yang merupakan revisi terbarunya. Namun, hukum yang ditulis (law in books) dan yang diterapkan di lapangan sangat berbeda. Orang awam seringkali kesulitan memahami batas-batas delik hukum dan prosedur pengamanan bukti digital yang sah (*digital forensics*). Akibatnya, bukti yang mereka ajukan seringkali tidak lengkap di mata hukum.

Urgensi peralihan menuju mekanisme bantuan hukum berbasis teknologi ini semakin tak terelakkan ketika meninjau karakteristik kejahatan siber yang bersifat *volatile* (mudah berubah) dan *transborder* (lintas batas). Pendekatan konvensional yang mengandalkan konsultasi tatap muka dinilai memiliki latensi waktu yang terlalu tinggi, sehingga sering kali gagal menyelamatkan 'Golden Hour' atau masa kritis preservasi bukti digital. Hal ini sejalan dalam kajian forensik digital pasca-revisi UU ITE, yang menegaskan bahwa integritas alat bukti elektronik sangat bergantung pada kecepatan akuisisi sebelum metadata terkontaminasi atau dihapus oleh pelaku. Lebih lanjut, studi mengenai kebijakan kriminal siber di Indonesia menyoroti bahwa hambatan terbesar akses keadilan (*access to justice*) saat ini bukan lagi sekadar biaya, melainkan literasi teknis masyarakat dalam mengonversi peristiwa hukum menjadi alat bukti yang *admissible* (dapat diterima) di pengadilan.[1] Oleh karena itu, kehadiran AKSARA bukan sekadar mendigitalkan layanan hukum manual, melainkan merekayasa ulang (*re-engineering*) proses advokasi agar responsif terhadap kecepatan delik siber yang terjadi secara *real-time*

Pengembangan aplikasi "AKSARA" menjadi sangat penting untuk mengatasi perbedaan antara peraturan dan kenyataan sosial. Aplikasi ini muncul sebagai jembatan teknologi hukum (*Legal Tech*) yang dimaksudkan untuk memfasilitasi akses mudah ke layanan konsultasi hukum dan memastikan bukti digital aman sesuai standar forensik. Akibatnya, diharapkan bahwa AKSARA dapat membantu korban mendapatkan perlindungan hukum yang memadai di tengah arus kejahatan digital yang cepat.

METODE PENELITIAN

Penelitian ini menggunakan desain campuran (*mixed-method*) yang menggabungkan metode Research and Development (R&D) untuk pengembangan sistem aplikasi, dengan metode penelitian hukum Socio-Legal untuk menganalisis efektivitas hukum di masyarakat. Pendekatan socio-legal digunakan untuk membedah efektivitas hukum bukan hanya dari teks undang-undang

[1] H. S. Disemadi, "Lenses of Legal Policy on Cybercrime in Indonesia," *Jurnal Hukum dan Peradilan* (2022).

(*law in books*), melainkan bagaimana hukum tersebut bekerja atau gagal bekerja saat berhadapan dengan psikologis korban dan kesiapan aparat di lapangan (*law in action*).

1. Tahap pertama, **analisis kebutuhan**, memadukan pendekatan yuridis melalui studi UU ITE 2024, UU PDP 2022, dan Perpol No. 8/2021 untuk menyelaraskan algoritma dengan hukum acara, serta pendekatan empiris partisipatif via wawancara mitra LBH Semarang dan analisis kasus *doxing* 2023–2024 guna memetakan hambatan pembuktian.
2. Hasil analisis ditranslasikan ke tahap **perancangan sistem** (Prototyping) "AKSARA" berbasis *Privacy by Design* (ISO/IEC 27001 & 27701), yang memprioritaskan keamanan data dan integritas forensik bukti digital agar valid dalam proses litigasi maupun non-litigasi.[2]
3. Terakhir, tahap **pengujian** dilakukan melalui *System Usability Scale* (SUS) untuk mengukur aspek *usability* publik di Semarang, serta *User Acceptance Testing* (UAT) oleh praktisi hukum guna memvalidasi logika konsultasi dan fitur pengamanan bukti.

HASIL DAN PEMBAHASAN

Integrasi Kerangka Hukum dan Validitas Bukti dalam Arsitektur AKSARA

Pengembangan aplikasi AKSARA menggunakan pendekatan legal engineering untuk menyelesaikan masalah integrasi kerangka hukum ke dalam desain teknologi. Metode ini mengubah aturan abstrak yang ditemukan dalam UU ITE dan UU PDP menjadi logika algoritma yang dapat diterapkan. Dua mekanisme utama terdiri dari integrasi ini: (1) Nasihat Hukum (*Legal Advice*) yang diotomatisasi melalui klasifikasi delik; dan (2) Pengamanan Bukti Elektronik (Evidence Preservation) yang didasarkan pada standar forensik.

A. Transformasi UU PDP

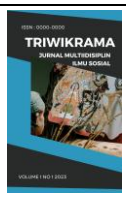
Integrasi fitur Legal Triage dalam aplikasi AKSARA menunjukkan kepatuhan terhadap peraturan perlindungan data di Indonesia. Sistem ini tidak hanya berperan sebagai pemisah kasus hukum, tetapi juga berfungsi sebagai alat manajemen risiko yang wajib dimiliki oleh Penyelenggara Sistem Elektronik (PSE). Dengan mengikuti prinsip Pasal 4 Undang-Undang Nomor 27 Tahun 2022 mengenai Perlindungan Data Pribadi, sistem secara otomatis memisahkan data untuk mengidentifikasi tingkat keamanan yang dibutuhkan. otomatis berdasarkan jenis data yang dimasukkan korban atau mitra. Sesuai dengan Pasal 4 UU PDP, algoritma aplikasi membagi data menjadi tiga kategori:

1. Data Pribadi Umum

Dalam struktur Legal Triage AKSARA, tahap awal adalah pengenalan subjek hukum melalui Data Pribadi Umum. Berdasarkan Pasal 4 ayat (3) UU PDP, data ini mencakup informasi seperti nama lengkap, jenis kelamin, kewarganegaraan, serta agama. Walaupun dianggap sebagai data umum, pengelolaan informasi ini di dalam aplikasi bantuan hukum sangat penting, karena berfungsi sebagai alat verifikasi identitas pelapor. Jika data umum tidak dilindungi dengan baik, hal ini dapat mengakibatkan konsekuensi hukum administratif serta denda, sehingga AKSARA perlu melaksanakan prinsip pemrosesan data yang terbatas dan spesifik sesuai dengan tujuannya.

[2] Robere & Associates Indonesia, "Privacy by design dan privacy by default dalam UU PDP dan ISO/IEC 27001: Strategi proaktif pelindungan data pribadi", https://robere.co.id/id/privacy-by-design-dan-privacy-by-default-dalam-uu-pdp-dan-iso-iec-27001-strategi-proaktif-pelindungan-data-pribadi/.

Triwikrama: Jurnal Ilmu Sosial
Volume 11 No 9 2025
E-ISSN: 2988-1986
Open Access:



2. Data Pribadi Spesifik

Analisis mendalam diperlukan ketika algoritma mendeteksi input data pribadi spesifik dalam konteks aplikasi layanan hukum, di mana data tersebut sering kali mencakup riwayat kesehatan fisik atau psikologis korban, data genetika atau biometrik, informasi kehidupan seksual, atau data terkait anak. Berdasarkan analisis dari Jurnal Hukum & Pembangunan (Universitas Indonesia), data spesifik ini bersifat sensitif, sehingga kebocorannya dapat menimbulkan kerugian yang lebih besar, termasuk diskriminasi sosial dan stigmatisasi seumur hidup bagi korban.[3] Oleh karena itu, fitur Legal Triage pada aplikasi AKSARA harus secara otomatis mengaktifkan protokol enkripsi yang lebih tinggi ketika data jenis ini diinput, serta membatasi akses hanya kepada konselor yang tersertifikasi, guna memastikan kepatuhan terhadap prinsip Data Minimization dan Confidentiality dalam Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP). Dengan demikian, mekanisme ini berfungsi ganda, memperkuat integritas data sekaligus meminimalisasi risiko reviktimisasi, menjadikan aplikasi ini instrumen perlindungan yang etis.[4]

Penerapan klasifikasi ini dalam fitur triage juga menegaskan perlindungan Hak Asasi Manusia (HAM), di mana Lembaga Studi dan Advokasi Masyarakat (ELSAM) menyoroti bahwa pelindungan data pribadi merupakan bagian integral dari hak atas privasi.[5] Dalam kasus kekerasan seksual atau pidana anak yang ditangani aplikasi AKSARA, data kesehatan dan pandangan politik jika relevan dengan motif kejahatan menjadi aset yang sangat rentan. Dengan memisahkan penyimpanan dan akses "Data Spesifik" (seperti data anak) dari "Data Umum", aplikasi AKSARA mencegah reviktimisasi yang mungkin terjadi akibat penyalahgunaan data oleh pihak internal maupun eksternal, sehingga memastikan kepatuhan terhadap prinsip-prinsip HAM dan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP). Implementasi protokol privasi tersebut berfungsi ganda, memperkokoh integritas data sekaligus mereduksi potensi reviktimisasi. Hal ini memosisikan aplikasi AKSARA sebagai instrumen perlindungan hukum yang tidak hanya efektif, tetapi juga etis dan berorientasi pada pemulihan korban.

Tanggungjawab Pengendalian Data (*Data Controller*)

Secara operasional, klasifikasi otomatis ini memfasilitasi aplikasi AKSARA dalam memenuhi tanggung jawabnya sebagai Pengendali Data Pribadi (Data Controller) berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP). Kajian dari Jurnal Legislasi Indonesia menunjukkan bahwa pemisahan kategori data ini mempermudah pemenuhan hak subjek data, seperti ketika pengguna meminta penghapusan data (*right to be forgotten*). Sistem ini memungkinkan pelacakan yang lebih efisien untuk menentukan data sensitif yang harus dimusnahkan secara permanen dan data umum yang mungkin masih diperlukan untuk arsip administrasi hukum, sesuai dengan periode retensi yang diatur oleh regulasi. Secara normatif, klasifikasi data otomatis ini tidak sekadar memenuhi standar kepatuhan UU PDP, melainkan juga meningkatkan akuntabilitas penyelenggara sistem elektronik. Implikasi lanjutannya adalah terjaminnya perlindungan hak-hak subjek data dalam ekosistem layanan hukum digital.[6]

---

[3] Dewi, S., *"Konsep Perlindungan Hukum Atas Privasi dan Data Pribadi Di Indonesia: Perspektif Undang-Undang No. 27 Tahun 2022"*, Jurnal Hukum & Pembangunan 53, no. 1 (2023): 1–22.
[4] Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, Pasal 67 ayat (2).
[5] ELSAM, *Perlindungan Data Pribadi di Indonesia: Tantangan dan Peluang Pasca Pengesahan UU PDP* (Jakarta: Lembaga Studi dan Advokasi Masyarakat, 2022).
[6] G. Greenleaf dan K. Kemp, "Indonesia's Personal Data Protection Act (PDP Law): A generic model for ASEAN?" *Privacy Laws & Business International Report* (2022).

Triwikrama: Jurnal Ilmu Sosial
Volume 11 No 9 2025
E-ISSN: 2988-1986
Open Access:

B. Penjaminan Validitas Bukti Melalui Standar ITE dan Forensik Digital

Dalam lanskap hukum siber pasca-pengesahan Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), status alat bukti elektronik (ABE) menjadi semakin krusial, namun memerlukan standar validitas yang ketat. Meskipun Pasal 5 ayat (1) UU ITE mengakui informasi elektronik sebagai alat bukti hukum yang sah, tantangan utamanya terletak pada sifat digital yang rentan terhadap perubahan atau manipulasi. Aplikasi AKSARA menjawab tantangan "kadar pembuktian" (*probative value*) ini melalui fitur *Secure Evidence Vault*, yang mengintegrasikan prinsip hukum acara pidana dengan standar forensik digital global, sehingga memastikan integritas bukti elektronik dalam proses penegakan hukum. Integrasi standar forensik tersebut secara simultan memperkuat legitimasi alat bukti di muka persidangan serta menjamin keamanan data korban. Langkah ini selaras dengan dinamika regulasi terkini yang menempatkan validitas dan keamanan informasi elektronik sebagai prioritas utama.[7]

1. Integritas Data (Hashing SHA-256)

Fondasi utama agar bukti elektronik dapat diterima di pengadilan adalah aspek "Keutuhan" sebagaimana diamanatkan dalam Pasal 6 Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). Dalam konteks ini, tangkapan layar biasa tidak memadai karena piksel dapat disunting tanpa jejak yang kasat mata.

Aplikasi AKSARA mengatasi tantangan ini dengan menerapkan algoritma kriptografi SHA-256 (*Secure Hash Algorithm 256-bit*), di mana saat korban mengambil bukti melalui aplikasi, sistem langsung menghasilkan digest atau kode unik (hash) dari file tersebut. Jika satu bit saja dari gambar tersebut diubah misalnya, chat diedit kode hash akan berubah total, sehingga dalam persidangan, ini berfungsi sebagai pembuktian matematis bahwa bukti yang disajikan adalah otentik dan identik dengan kondisi saat diambil (originality), memenuhi syarat formil dan materiil bukti elektronik yang tidak terbantahkan (*non-repudiation)*.

Penerapan algoritma kriptografi ini menutup celah penyangkalan (*non-repudiation*), sehingga alat bukti elektronik memiliki kekuatan pembuktian yang setara dengan dokumen otentik.[8] Kontribusi teknis ini secara langsung meningkatkan efisiensi penegakan hukum pidana ITE dan menjamin kepastian hukum.[9]

2. Akuntabilitas Metadata (Stamping Metadata):

Kelemahan utama dari bukti tangkapan layar biasa adalah bahwa mereka tidak memiliki konteks waktu dan lokasi yang terverifikasi. Pelaku sering menggunakan celah ini untuk menafikan kebenaran bukti dengan mengubah tanggal pada perangkat korban. Studi mengenai tantangan forensik dalam kasus kekerasan berbasis gender online menunjukkan bahwa bukti visual semacam ini sering dikategorikan lemah dalam praktik peradilan karena tidak memenuhi persyaratan formal tentang "integritas data" yang diatur dalam Pasal 6 UU ITE. Tanpa adanya jaminan teknis terhadap keaslian data, tangkapan layar hanya dianggap sebagai indikasi awal

[7] Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Pasal 5 ayat (1).
[8] D. Situngkir, "Aspek Hukum Kemanfaatan dan Kepastian Hukum Alat Bukti Elektronik dalam Tindak Pidana ITE," *Jurnal Kertha Semaya* 9, no. 2 (2021).
[9] H. Santhos Wachjoe P., "Penggunaan informasi elektronik dan dokumen elektronik sebagai alat bukti persidangan", *Jurnal Hukum dan Peradilan* 5, no. 1 (2016): 1–18.

yang mudah dipatahkan (*presumption rebuttable*), bukan sebagai bukti surat atau bukti yang memiliki kekuatan pembuktian yang sempurna.

Aplikasi AKSARA menggunakan *Network Time Protocol* (NTP) sebagai komponen penting untuk menghindari kerentanan hukum tersebut. Mekanisme Metadata Stamping otomatis mengunci Time-Stamp dan Geo-Tagging. Protokol ini menghindari pengaturan waktu lokal perangkat pengguna yang dapat diubah secara manual. Sebaliknya, sistem menyinkronkan waktu kejadian (tempus delicti) secara real-time dengan server waktu internet global atomik. Menggabungkan akurasi waktu, pencatatan URL khusus, dan alamat IP ini menghasilkan konstruksi hukum yang stabil tentang dimensi temporal dan spasial (locus delicti) peristiwa siber. Mekanisme ini sejalan dengan penelitian Dewi dan Winarko (2023), yang menyatakan bahwa untuk *menjamin Chain of Custody* agar bukti kompatibel dengan pemeriksaan penyidikan, standardisasi penanganan bukti digital melalui penguncian metadata adalah perlu. Implikasi hukum dari arsitektur teknis ini sangat signifikan. Mekanisme penguncian metadata mencegah kelemahan alami bukti digital, menjamin proses peradilan yang adil, dan meningkatkan nilai pembuktian laporan di mata penyidik.[10]

3. Preservasi Bukti Melalui *Chain of Custody* (Standar ISO 27037)

Dalam perspektif forensik digital, integritas prosedural yang melingkupi metode perolehan dan penyimpanan alat bukti memiliki urgensi yang ekuivalen dengan substansi materiil bukti itu sendiri. Guna menjamin hal tersebut, AKSARA mengimplementasikan fitur *Chain of Custody* yang dikonstruksikan berdasarkan standar internasional ISO/IEC 27037:2012, sebuah pedoman komprehensif yang mengatur tata kelola identifikasi, pengumpulan, akuisisi, hingga preservasi bukti digital.

Kepatuhan terhadap standar ini dimanifestasikan melalui penciptaan jejak audit (*audit trail*) yang bersifat *immutable*, di mana sistem merekam secara presisi setiap interaksi dan akses yang dilakukan oleh subjek hukum, baik pengunggah maupun verifikator. Keberadaan log aktivitas yang transparan ini berfungsi vital untuk memitigasi risiko kontaminasi data maupun dalil fabrikasi bukti, sehingga menjamin otentisitas dan validitas alat bukti elektronik mulai dari tahap pelaporan hingga proses pembuktian di persidangan.

C. Mitigasi Risiko Hukum Melalui Legal First Aid

Dalam ekosistem penanganan Kekerasan Berbasis Gender Online (KBGO), teridentifikasi adanya dikotomi kritis antara respons psikologis korban dengan rigiditas standar pembuktian hukum. Korban yang mengalami trauma cenderung melakukan tindakan impulsif berupa pemutusan komunikasi atau pemblokiran pelaku demi mereduksi kecemasan (*coping mechanism*). Namun, tindakan yang wajar secara psikologis ini berimplikasi fatal secara yuridis karena memicu terjadinya *Spoliation of Evidence* atau perusakan alat bukti. Laporan Situasi Hak Digital Indonesia oleh SAFEnet pada tahun 2022 mengonfirmasi pola ini, di mana penghapusan riwayat percakapan (*chat logs*) secara prematur mengakibatkan hilangnya metadata dan URL asli yang tersimpan dalam server platform. Ketiadaan akses terhadap jejak digital primer ini menyebabkan laporan korban kerap mengalami penolakan di tahap penyelidikan karena tidak memenuhi syarat formil dan materiil sebagaimana diatur dalam Surat Keputusan Bersama (SKB) 3 Menteri tentang Pedoman Implementasi UU ITE (2021). Tanpa bukti yang utuh, unsur *mens*

[10] S. Yuniarti dan A. Ristyawati, "Keabsahan Alat Bukti Elektronik dalam Pembuktian Tindak Pidana ITE," *Jurnal Pembangunan Hukum Indonesia* 4, no. 1 (2022).

rea (niat jahat) dan *actus reus* (perbuatan pidana) menjadi kabur (*obscuur*), sehingga verifikasi forensik mustahil dilakukan.[11]

Merespons kerentanan tersebut, modul *Legal First Aid* pada AKSARA mengimplementasikan mekanisme intervensi perilaku (*behavioral intervention*) melalui sistem peringatan dini (*early warning system*). Fitur ini berfungsi menahan impuls korban untuk tidak memusnahkan bukti secara serta-merta dengan memberikan edukasi persuasif mengenai urgensi preservasi metadata. Pendekatan ini disandarkan pada karakteristik bukti elektronik yang bersifat *volatile* (mudah berubah/hilang). Sebagaimana ditegaskan dalam riset Jurnal Teknologi dan Sistem Komputer (2021) serta amanat Pasal 6 UU ITE, integritas data merupakan syarat mutlak bagi validitas informasi elektronik. Oleh karena itu, jeda waktu yang diciptakan oleh intervensi sistem ini dimanfaatkan oleh AKSARA untuk melakukan proses *crawling* dan penguncian bukti (*hashing*) secara komprehensif. Mekanisme ini menjamin bahwa bukti yang diakuisisi memiliki nilai pembuktian (*probative value*) yang kuat di hadapan pengadilan, sebelum akses terhadap pelaku benar-benar diputus oleh korban.

Signifikansi intervensi teknis tersebut menemukan relevansinya yang paling krusial ketika ditinjau dari perspektif *digital evidence reliability*. Pergeseran paradigma pembuktian dari *visual-based* menuju *metadata-based* menuntut adanya jaminan bahwa bukti tidak terkontaminasi oleh *human error* korban yang sedang berada di bawah tekanan psikologis. Hal ini selaras dengan kajian hukum pidana teknologi informasi pasca-revisi UU ITE, yang mempostulasikan bahwa validitas alat bukti elektronik sangat bergantung pada prinsip *non-repudiation* (nirsangkal), artinya sistem harus mampu membuktikan asal-usul data secara presisi tanpa celah penyangkalan. Dengan memitigasi risiko modifikasi manual melalui automasi *crawling*, AKSARA mentransformasi data mentah menjadi alat bukti yang bersifat *self-authenticating*. Keunggulan metodologis ini secara langsung menjawab tantangan bahwa tingginya angka *dismissal* (penolakan) kasus siber di Indonesia sering kali bukan disebabkan oleh ketiadaan fakta hukum, melainkan akibat degradasi kualitas bukti yang gagal memenuhi standar *Chain of Custody* sejak tahap pelaporan awal.[12]

Model Aplikasi dan Uji Kelayakan di Kota Semarang

Konstruksi arsitektural AKSARA tidak sekadar merepresentasikan digitalisasi layanan bantuan hukum, melainkan sebuah transformasi paradigmatik menuju *LegalTech* yang menginternalisasi prinsip *Privacy by Design* (PbD) sebagai fundamen utama. Selaras dengan mandat Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi serta standar ISO/IEC 27001, sistem ini menerapkan prinsip minimalisasi data guna memitigasi risiko eksposur informasi sensitif milik korban. Integrasi aspek keamanan dan privasi tersebut disempurnakan melalui pendekatan *Computational Law* dalam modul *Legal Triage*, yang mentransformasikan norma abstrak dalam peraturan perundang-undangan termasuk KUHP, UU ITE, dan UU TPKS menjadi logika algoritmik berbasis *decision tree*. Transformasi logika normatif menjadi algoritma komputasi ini secara substantif merefleksikan kapasitas teknologi dalam mendemokratisasi akses keadilan (*access to justice*). Melalui simplifikasi digital, kesenjangan kognitif masyarakat awam terhadap terminologi hukum yang rigid dan kompleks (*legalese*) dapat dijembatani secara efektif.[13]

[11] Arsa Ilmi Budiarti, Gladys Nadya Arianto, dan Marsha Maharani, *Indonesia's Sexual Violence Data and Facts 2021* (Jakarta: Indonesia Judicial Research Society, 2022)
[12] A. R. Pradana dan R. Njatrijani, "Analisis Yuridis Terhadap Kekuatan Pembuktian Alat Bukti Elektronik Dalam Tindak Pidana Siber," *Jurnal Pembangunan Hukum Indonesia* 5, no. 1 (2023): 58–74.
[13] R. A. Nugroho dan A. A. Ilma, "Digitalisasi Hukum: Tantangan dan Peluang dalam Pembangunan Hukum Nasional," *Jurnal Penelitian Hukum De Jure* 21, no. 3 (2021).

Urgensi fitur keamanan pada AKSARA tidak hanya bersifat reaktif, melainkan juga preventif melalui modul *Legal First Aid*. Dalam ekosistem penanganan kasus siber, teridentifikasi kerentanan di mana korban yang mengalami trauma cenderung melakukan tindakan impulsif memblokir pelaku atau menghapus percakapan (*chat logs*) demi mereduksi kecemasan sesaat. Tindakan ini memicu fenomena *Spoliation of Evidence* atau perusakan alat bukti, yang mengakibatkan hilangnya metadata URL dan jejak digital primer di server. Merujuk pada Laporan Situasi Hak Digital Indonesia (SAFEnet, 2022), hilangnya akses terhadap jejak digital asli menjadi penyebab utama laporan korban ditolak di tahap penyelidikan karena gagal memenuhi syarat formil pembuktian. Oleh karena itu, AKSARA mengimplementasikan mekanisme intervensi perilaku (*behavioral intervention*) berupa peringatan dini (*early warning*) yang menahan impuls korban, memberikan jeda waktu bagi sistem untuk melakukan *crawling* dan penguncian bukti secara utuh sebelum akses diputus.

Defisiensi dalam pembuktian tindak pidana siber, khususnya pada kasus Kekerasan Berbasis Gender Online (KBGO), kerap berakar pada deviasi prosedural dalam akuisisi bukti digital. Merespons urgensi tersebut, modul *Secure Evidence Vault* pada AKSARA dikembangkan dengan menginternalisasi standar forensik ISO/IEC 27037 guna menjamin *admissibility* alat bukti di muka pengadilan. Validitas ini diperkuat melalui arsitektur keamanan berlapis yang meliputi *hashing* (SHA-256), *metadata stamping*, serta *immutable audit trail*. Hal ini menegaskan bahwa absennya integritas data pada bukti tangkapan layar (*screenshot*) konvensional sering kali mendegradasi nilai pembuktian pada tahap penyelidikan akibat kerentanan terhadap rekayasa. Oleh karena itu, kapabilitas sistem dalam mempreservasi *tempus delicti* dan lokus digital secara presisi dan nirmipulasi menjadi instrumen strategis dalam memperkuat posisi hukum korban.

Lebih jauh, signifikansi arsitektur forensik AKSARA menemukan relevansinya dalam aspek *digital evidence reliability*. Kelemahan fatal bukti tangkapan layar konvensional terletak pada ketiadaan validasi waktu yang independen, sehingga pelaku sering kali menyangkal (*repudiation*) dengan dalih manipulasi tanggal perangkat. Memitigasi celah ini, AKSARA tidak mengambil referensi waktu dari perangkat pengguna, melainkan menyinkronkan *tempus delicti* menggunakan *Network Time Protocol* (NTP) yang terhubung dengan server waktu atomik global. Konsep ini berkorelasi dengan paradigma hukum siber pasca-revisi UU ITE, yang mempostulasikan bahwa alat bukti elektronik wajib bersifat *self-authenticating* guna mencapai kekuatan pembuktian yang optimal. Implikasi praktisnya, sistem ini mampu menghasilkan alat bukti dengan integritas tinggi yang resisten terhadap uji forensik maupun sanggahan teknis di muka persidangan

Penetapan Kota Semarang sebagai *locus* uji kelayakan dilandasi oleh urgensi sosiologis yang merujuk pada laporan *Legal Resource Center* untuk Keadilan Jender dan Hak Asasi Manusia (LRC-KJHAM) tahun 2024, di mana wilayah ini teridentifikasi sebagai zona dengan tingkat eskalasi tinggi dalam kasus *doxing* dan kekerasan digital. Validasi penerimaan sistem dilakukan melalui evaluasi *System Usability Scale* (SUS) yang melibatkan 57 responden, menghasilkan skor rata-rata 78,6. Mengacu pada skala interpretasi Bangor, Kortum, dan Miller, capaian tersebut menempatkan AKSARA pada kategori *"Good"* dengan tendensi menuju *"Excellent"* (Grade B). Indikator kuantitatif ini merefleksikan efektivitas arsitektur antarmuka aplikasi dalam menjembatani kesenjangan pemahaman hukum bagi pengguna non-yuris. Secara spesifik, responden menggarisbawahi signifikansi fitur klasifikasi delik otomatis sebagai instrumen yang paling berdampak, mengingat kapabilitasnya dalam memberikan kepastian yuridis awal yang krusial di tengah disorientasi psikologis yang dialami oleh korban.[14]

[14] LRC-KJHAM Jawa Tengah, *Catatan Tahunan Kekerasan Terhadap Perempuan di Jawa Tengah* (LRC-KJHAM Jawa Tengah, 2024).

Triwikrama: Jurnal Ilmu Sosial
Volume 11 No 9 2025
E-ISSN: 2988-1986
Open Access:

Guna melengkapi validasi pengguna, tahap pengujian dilanjutkan dengan validasi kulminatif melalui mekanisme *User Acceptance Testing* (UAT) yang melibatkan pilar strategis dalam sistem peradilan pidana, yakni Advokat dari LBH Semarang dan Penyidik Unit Tipidter Polrestabes Semarang. Temuan fundamental pada fase ini mengerucut pada urgensi aspek interoperabilitas data. Meskipun fitur *Chain of Custody* dinilai efektif dalam mempreservasi otentisitas bukti, para praktisi hukum menggarisbawahi imperatifnya standardisasi luaran (*output standardization*). Secara spesifik, penyidik mensyaratkan laporan yang diekspor dalam format *Portable Document Format* (PDF) yang tidak sekadar menyajikan visualisasi bukti, melainkan juga menginkorporasikan data forensik berupa *checksum hash* dan metadata secara eksplisit. Temuan empiris ini berkorespondensi dengan literatur terdahulu yang mempostulasikan bahwa kompatibilitas format bukti digital dengan infrastruktur teknologi aparat penegak hukum merupakan prasyarat mutlak guna mengakselerasi efisiensi penyusunan Berita Acara Pemeriksaan (BAP).[15]

Secara holistik, serangkaian pengujian di atas mengonfirmasi bahwa AKSARA telah memenuhi parameter kelayakan baik dari dimensi teknis maupun sosiologis untuk diimplementasikan di wilayah Kota Semarang sebagai instrumen *first-response* bagi korban kejahatan siber. Keunggulan distingtif sistem ini termanifestasi pada kapabilitasnya dalam mengharmonisasikan antinomi antara perlindungan privasi (*privacy*) dengan rigiditas standar pembuktian (*forensics*). Sebagai konsekuensi logis, arah pengembangan strategis selanjutnya mutlak difokuskan pada penyempurnaan format ekspor data guna menjamin interoperabilitas penuh dengan arsitektur Sistem Peradilan Pidana Terpadu Berbasis Teknologi Informasi (SPPT-TI) nasional.

Rekomendasi Penanganan dan Implementasi Kebijakan

Fenomena doxing dan penghinaan online yang semakin meningkat menandakan pentingnya pendekatan yang komprehensif dan fokus pada perlindungan para korban. Berdasarkan studi dan analisis terhadap kerangka hukum di Indonesia, salah satu rekomendasi utama yakni memperkuat mekanisme pelaporan dan dukungan yang memanfaatkan teknologi hukum (*legal-tech*).[16] Dengan adanya pengembangan aplikasi AKSARA, proses pelaporan dapat diarahkan ke sistem yang mudah diakses, aman, dan terstandarisasi sehingga setiap bukti digital yang diajukan oleh korban tetap sesuai dengan hukum yang berlaku, seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), UU No. 1 Tahun 2024 tentang Perubahan Kedua UU ITE, dan Peraturan Mahkamah Agung No. 4 Tahun 2016 tentang pembuktian elektronik. Oleh karena itu, aplikasi ini tidak hanya berfungsi sebagai platform konsultasi, tetapi juga sebagai alat hukum yang memastikan keabsahan bukti elektronik untuk memperkuat proses penegakan hukum.[17] Selain itu, sistem konsultasi hukum digital harus mematuhi kerahasiaan informasi berdasarkan prinsip attorney-client privilege serta mengintegrasikan mekanisme perlindungan data yang berhubungan dengan Privacy by Design yang sejalan dengan UU Perlindungan Data Pribadi Tahun 2022, sehingga para korban dapat mengakses layanan hukum tanpa khawatir akan reviktimisasi atau kebocoran data.[18]

Di sisi lain, penanganan kekerasan digital tidak bisa hanya mengandalkan aspek hukum, tetapi juga harus memperhatikan faktor psikososial. Beragam studi telah menunjukkan bahwa individu yang menjadi korban doxing dan penghinaan daring berisiko mengalami masalah emosional seperti kecemasan, depresi, merasa tidak aman, hingga trauma berkepanjangan. Oleh karena

[15] R. Dewi dan A. Winarko, "Digital Evidence Handling and Forensic Standardization in Indonesian Cybercrime Investigations," *Jurnal Teknologi Informasi dan Hukum* 5, no. 1 (2023): 44–58.
[16] Pew Research Center. (2023). *The state of online harassment 2023*. Pew Research Center.
[17] Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 tentang Perubahan Kedua atas UU ITE.
[18] ICT Watch Indonesia. (2023). *Laporan Tahunan Perlindungan Data dan Kebebasan Digital di Indonesia 2023*. ICT Watch.

itu, pendekatan kebijakan harus menyeluruh, termasuk menyediakan dukungan psikologis, seperti merujuk pada psikolog klinis, konselor, atau layanan dukungan emosional berbasis komunitas. Pendekatan yang fokus pada korban (*victim-centered approach*) sangatlah krusial untuk memastikan intervensi yang dilakukan mempertimbangkan keadaan emosional korban dan menjaga agar proses pemulihan tidak menambah beban bagi mereka. Model dukungan ini sejalan dengan saran dari Komnas Perempuan pada tahun 2022 yang menegaskan pentingnya pengintegrasian layanan hukum dan psikososial dalam penanganan kekerasan digital, serta teori pertumbuhan pascatrauma (*post-traumatic growth*) yang menekankan pentingnya pemulihan emosional dalam rehabilitasi korban.

Selanjutnya, penguatan kebijakan perlindungan data pribadi merupakan langkah strategis untuk mencegah praktik doxing di level institusi, khususnya pada instansi pemerintah, pusat data publik, lembaga pendidikan, serta platform digital. Kebijakan keamanan data yang lebih ketat harus diterapkan berdasarkan prinsip-pinsip UU PDP, termasuk pembatasan akses terhadap informasi sensitif, audit keamanan rutin, prosedur operasional standar untuk manajemen insiden kebocoran data, serta kewajiban untuk memberi tahu publik jika terjadi pelanggaran data. Sesuai dengan laporan ICT Watch, banyaknya kebocoran data di Indonesia disebabkan oleh rendahnya pengelolaan informasi, sehingga sangat penting untuk membentuk satuan tugas keamanan digital di setiap lembaga guna memantau potensi ancaman, menangani laporan pengaduan, dan memberikan edukasi tentang keamanan siber secara berkala. Kebijakan ini bukan hanya bersifat preventif melainkan juga responsif untuk memastikan bahwa institusi memiliki kesiapan menghadapi serangan digital yang semakin kompleks.[19]

Dalam rangka mencegah, peningkatan pemahaman terhadap hukum serta literasi digital merupakan langkah kunci untuk mengurangi angka kekerasan yang terjadi di dunia maya. Banyak individu yang mengalami kekerasan tidak melaporkan insiden yang dialaminya karena ketidaktahuan mengenai hak-hak hukum mereka dan cara untuk melaporkan, sehingga penyuluhan kepada masyarakat menjadi komponen penting dalam rekomendasi kebijakan ini. Instansi pemerintah, lembaga pendidikan, dan organisasi masyarakat harus mengintegrasikan materi mengenai literasi digital ke dalam kurikulum atau program edukasi berkesinambungan, mencakup pemahaman tentang pelanggaran privasi, etika digital, cara aman menggunakan media sosial, dan prosedur untuk melaporkan kejahatan digital. Aplikasi AKSARA dapat memberikan kontribusi dengan menawarkan modul pendidikan berbasis gamifikasi yang lebih interaktif dan mudah dipahami. Hal ini menunjukkan bahwa interaksi dalam pendidikan digital dapat memaksimalkan kesadaran serta mengubah perilaku pengguna internet secara signifikan.[20]

Di samping itu, suksesnya penerapan kebijakan untuk menangani kekerasan digital sangat bergantung pada kerjasama antara berbagai pihak. Sinergi yang solid antara pemerintah lokal, aparat penegak hukum, universitas, lembaga bantuan hukum (LBH), platform media sosial, dan organisasi masyarakat sipil perlu diperkuat melalui penciptaan ekosistem perlindungan di dunia maya. Kerja sama ini dapat terwujud melalui perjanjian kerjasama, pembentukan pusat layanan terintegrasi, dan pengembangan SOP antar lembaga untuk mempercepat penanganan laporan mengenai doxing serta penghinaan secara online. Model kolaborasi tersebut sejalan dengan praktik internasional yang direkomendasikan oleh Pew Research Center (2023), di mana

[19] ICT Watch Indonesia. (2023). *Laporan Tahunan Perlindungan Data dan Kebebasan Digital di Indonesia 2023*. ICT Watch.
[20] Khairunnisa, N. (2023). "Tingkat Pelaporan Korban Kekerasan Digital dan Hambatan dalam Akses Keadilan." *Jurnal Komunikasi Digital Indonesia*, 5(2), 112–124.

penanganan kejahatan digital yang efektif selalu melibatkan koordinasi antara negara, penyedia platform, dan komunitas yang mendukung korban.[21]

Sejalan dengan penguatan kolaborasi, aspek krusial yang sering terabaikan adalah standardisasi kompetensi penyidik di tingkat daerah. Kesenjangan kapabilitas antara unit siber di tingkat Mabes Polri dengan tingkat Polres sering kali menjadi penghambat utama dalam pemrosesan bukti yang dihasilkan oleh aplikasi bantuan hukum seperti AKSARA. 'Digital Forensic Readiness atau kesiapan institusi dalam mengumpulkan, memelihara, dan menganalisis bukti digital masih belum merata, yang berakibat pada tingginya angka penghentian penyidikan (SP3) karena bukti dianggap tidak cukup (insufficient evidence). Oleh karena itu, rekomendasi kebijakan harus mencakup mandat pelatihan sertifikasi forensik digital dasar bagi penyidik di sentra pelayanan kepolisian terpadu (SPKT). Dengan demikian, laporan berbasis metadata yang diekspor dari aplikasi AKSARA dapat langsung diproses tanpa hambatan teknis akibat ketidakpahaman aparat terhadap protokol *Chain of Custody* bukti digital.

Selain penegakan hukum yang bersifat punitif, kerangka kebijakan juga perlu mengarusutamakan pendekatan *Restorative Justice* (Keadilan Restoratif), khususnya untuk kasus penghinaan daring atau delik aduan yang tidak melibatkan kekerasan fisik atau ancaman terhadap keamanan nasional. Berdasarkan Surat Edaran Kapolri Nomor SE/2/II/2021, penyelesaian perkara ITE harus mengedepankan prinsip *ultimum remedium* (hukum pidana sebagai upaya terakhir).[22] Institute for Criminal Justice Reform dalam kajian evaluasinya menegaskan bahwa mekanisme mediasi penal jauh lebih efektif dalam memulihkan hak korban dibandingkan pemidanaan penjara yang sering kali tidak menyentuh akar konflik.[23] Dalam konteks ini, aplikasi AKSARA dapat dikembangkan lebih lanjut untuk menyertakan fitur 'Pra-Mediasi', di mana korban dapat memilih opsi penyelesaian sengketa alternatif yang terhubung langsung dengan mediator bersertifikat, sehingga beban penumpukan perkara di pengadilan dapat direduksi secara signifikan

Secara regulatoris, diperlukan pula pembaruan dan penyusunan aturan turunan dari UU PDP dan UU ITE yang lebih spesifik terkait penanganan doxing serta kejahatan privasi digital. Hal ini mencakup definisi operasional doxing, mekanisme perlindungan saksi dan korban dalam konteks kejahatan digital, standar keamanan data lembaga publik, serta pedoman teknis penanganan kasus oleh aparat penegak hukum. Friedman (1975) menekankan bahwa sistem hukum harus adaptif terhadap dinamika sosial dan perubahan teknologi; oleh karena itu, pembaruan kebijakan di area ini menjadi keharusan agar negara mampu memberikan perlindungan maksimal kepada masyarakat. Dengan adanya rekomendasi komprehensif ini, diharapkan Indonesia dapat mengembangkan model kebijakan yang lebih responsif, integratif, dan humanis dalam menghadapi tantangan kekerasan digital di era informasi.[24]

SIMPULAN

Secara agregat, penelitian ini mengonfirmasi bahwa eskalasi kasus *doxing* dan *online shaming* di Indonesia, khususnya di Kota Semarang, telah menciptakan urgensi mendesak akan mekanisme bantuan hukum yang responsif. Temuan studi menunjukkan bahwa aplikasi AKSARA

[21] Pew Research Center. (2023). *The State of Online Harassment 2023*. Pew Research Center.
[22] *Surat Edaran Kepala Kepolisian Negara Republik Indonesia Nomor SE/2/II/2021 tentang Kesadaran Budaya Beretika untuk Mewujudkan Ruang Digital Indonesia yang Bersih, Sehat, dan Produktif*.
[23] Institute for Criminal Justice Reform, "Peluang dan Tantangan Penerapan *Restorative Justice* di Indonesia," Institute for Criminal Justice Reform.
[24] Nilan, P., & Utari, P. (2020). Gendered Violence Online on Social Media in Indonesia. *Asian Journal of Women's Studies*, 26(1), 62–82.

berhasil diformulasikan sebagai instrumen *LegalTech* yang efektif dalam menjembatani kesenjangan antara rigiditas standar pembuktian hukum (*law in books*) dengan keterbatasan literasi teknis serta kondisi psikologis korban di lapangan (*law in action*).

Keunggulan distingtif AKSARA termanifestasi dalam tiga dimensi fundamental. **Pertama**, dari aspek yuridis-teknis, aplikasi ini telah memenuhi standar kepatuhan terhadap UU No. 1 Tahun 2024 tentang ITE dan UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP). Implementasi fitur *Secure Evidence Vault* yang mengintegrasikan algoritma *hashing* SHA-256 dan *Metadata Stamping* berbasis *Network Time Protocol* (NTP) terbukti mampu menjamin integritas, otentisitas, dan nirsangkal (*non-repudiation*) alat bukti elektronik sesuai standar forensik ISO/IEC 27037. **Kedua**, dari aspek psikososial, fitur *Legal First Aid* berfungsi krusial sebagai mekanisme intervensi perilaku (*behavioral intervention*) yang mencegah terjadinya perusakan bukti (*spoliation of evidence*) oleh korban yang mengalami trauma, sehingga peluang keberhasilan litigasi dapat dipertahankan.

Validitas sistem ini diperkuat oleh hasil uji kelayakan empiris. Skor *System Usability Scale* (SUS) sebesar 78,6 mengindikasikan penerimaan yang tinggi dari masyarakat (kategori *Good/Excellent*), sementara *User Acceptance Testing* (UAT) memvalidasi bahwa logika aplikasi selaras dengan kebutuhan penyidikan, dengan catatan perlunya standardisasi format luaran (PDF ber-metadata) untuk menjamin interoperabilitas.

Sebagai implikasi kebijakan, keberhasilan implementasi AKSARA tidak dapat berdiri sendiri sebagai solusi teknis semata. Diperlukan orkestrasi kebijakan yang meliputi: (1) Peningkatan kapabilitas forensik digital (*Digital Forensic Readiness*) aparat penegak hukum di tingkat daerah; (2) Integrasi sistem pelaporan digital dengan arsitektur Sistem Peradilan Pidana Terpadu Berbasis Teknologi Informasi (SPPT-TI); serta (3) Pengarusutamaan pendekatan *Restorative Justice* dan perlindungan data pribadi yang komprehensif. Dengan demikian, AKSARA dapat bertransformasi dari sekadar purwarupa aplikasi menjadi pilar strategis dalam ekosistem perlindungan korban kejahatan siber yang berkeadilan dan humanis.

UCAPAN TERIMAKASIH

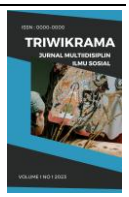
Penulis mengucapkan terima kasih kepada Rekan-rekan atas dukungan akademik yang diberikan sehingga penyusunan rancangan aplikasi AKSARA dapat terlaksana dengan baik. Aplikasi ini pada tahap saat ini masih berupa rancangan konseptual yang dituangkan dalam artikel untuk diajukan ke Program Kreativitas Mahasiswa bidang Pengabdian Masyarakat (PKM-PM). Apabila proposal ini disetujui dan memperoleh pendanaan, maka implementasi aplikasi AKSARA akan dijalankan sebagai bentuk kontribusi nyata dalam mendukung transformasi digital di bidang hukum dan perlindungan korban kejahatan siber.

DAFTAR PUSTAKA

Budiarti, A. I., G. N. Arianto, dan M. Maharani. *Indonesia's Sexual Violence Data and Facts 2021*. Jakarta: Indonesia Judicial Research Society, 2022.

Christina, A. I. "Indonesian Online Gender-Based Violence Victims' Empowerment and Support via Instagram." *Jurnal Audiens* 6, no. 3 (2025): 395–407.

Dewi, R., dan A. Winarko. “Digital Evidence Handling and Forensic Standardization in Indonesian Cybercrime Investigations”. *Jurnal Teknologi Informasi dan Hukum* 5, no. 1 (2023): 44–58.



Disemadi, H. S. "Lenses of Legal Policy on Cybercrime in Indonesia." *Jurnal Hukum dan Peradilan* (2022).

ELSAM. *Perlindungan Data Pribadi di Indonesia: Tantangan dan Peluang Pasca Pengesahan UU PDP*. Jakarta: Lembaga Studi dan Advokasi Masyarakat, 2022.

Greenleaf, G., dan K. Kemp. "Indonesia's Personal Data Protection Act (PDP Law): A generic model for ASEAN?" *Privacy Laws & Business International Report* (2022).

Hudhana, A. F., D. Arifianto, dan M. Yulianto. "Usability Evaluation of Legal Aid Mobile Applications Using System Usability Scale". *Jurnal Sistem Informasi* 18, no. 3 (2022): 245–258.

ICT Watch Indonesia. *Laporan Tahunan Perlindungan Data dan Kebebasan Digital di Indonesia 2023*. ICT Watch, 2023.

Institute for Criminal Justice Reform. "Peluang dan Tantangan Penerapan *Restorative Justice* dalam Sistem Peradilan Pidana di Indonesia." Institute for Criminal Justice Reform. Diakses 5 Desember 2025. https://icjr.or.id/peluang-dan-tantangan-penerapan-restorative-justice-dalam-sistem-peradilan-pidana-di-indonesia/.

Khairunnisa, N. "Tingkat Pelaporan Korban Kekerasan Digital dan Hambatan dalam Akses Keadilan." *Jurnal Komunikasi Digital Indonesia* 5, no. 2 (2023): 112–24.

Kn, M., M. Adymas, & H. Fikri (1960). *Implementasi hak ulayat terhadap pengaturan tanah adat lampung pepadun berdasarkan uu no 5 tahun 1960 tentang uupa*. *5*, 1–13

Komisi Nasional Anti Kekerasan terhadap Perempuan (Komnas Perempuan). *Catatan Tahunan Kekerasan terhadap Perempuan 2022*. Komnas Perempuan, 2022.

LRC-KJHAM Jawa Tengah. *Catatan Tahunan Kekerasan Terhadap Perempuan di Jawa Tengah*. LRC-KJHAM Jawa Tengah, 2024.

Nilan, P., dan P. Utari. "Gendered Violence Online on Social Media in Indonesia". *Asian Journal of Women's Studies* 26, no. 1 (2020): 62–82.

Nugroho, Y., dan A. Z. Ilma. "Legal Informatics and the Integration of Statutory Norms into Algorithmic Systems". *Indonesian Journal of Law and Technology* 4, no. 2 (2021): 112–125.

Pew Research Center. *The State of Online Harassment 2023*. Pew Research Center, 2023.

Pradana, A. R., dan R. Njatrijani. "Analisis Yuridis Terhadap Kekuatan Pembuktian Alat Bukti Elektronik Dalam Tindak Pidana Siber." *Jurnal Pembangunan Hukum Indonesia* 5, no. 1 (2023): 58–74.

Prasetyo, A. "Forensic Challenges in Handling Gender-Based Online Violence Cases in Indonesia". *Jurnal Keamanan Siber Nasional* 3, no. 2 (2022): 97–110.

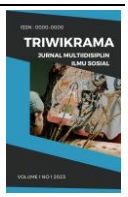
Robere & Associates Indonesia. "Privacy by design dan privacy by default dalam UU PDP dan ISO/IEC 27001: Strategi proaktif pelindungan data pribadi". https://robere.co.id/id/privacy-by-design-dan-privacy-by-default-dalam-uu-pdp-dan-iso-iec-27001-strategi-proaktif-pelindungan-data-pribadi/

Satria, M. K., dan H. Yusuf. "Analisis Yuridis Tindakan Kriminal Doxing Ditinjau Berdasarkan Undang Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi". *Jurnal Intelek Dan Cendikiawan Nusantara* 1, no. 2 (2024): 2442–2456.

Wachjoe P., H. S. "Penggunaan informasi elektronik dan dokumen elektronik sebagai alat bukti persidangan." *Jurnal Hukum dan Peradilan* 5, no. 1 (2016): 1–18.

Yuniarti, S., dan A. Ristyawati. "Keabsahan Alat Bukti Elektronik dalam Pembuktian Tindak Pidana ITE." *Jurnal Pembangunan Hukum Indonesia* 4, no. 1 (2022): 97–111.

Peraturan Perundang-undangan



Indonesia. *Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi*. Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196, Tambahan Lembaran Negara Republik Indonesia Nomor 6820.

Indonesia. *Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*. Lembaran Negara Republik Indonesia Tahun 2024 Nomor 10, Tambahan Lembaran Negara Republik Indonesia Nomor 6909.

Kepolisian Negara Republik Indonesia. *Surat Edaran Kepala Kepolisian Negara Republik Indonesia Nomor SE/2/II/2021 tentang Kesadaran Budaya Beretika untuk Mewujudkan Ruang Digital Indonesia yang Bersih, Sehat, dan Produktif*.

Mahkamah Agung Republik Indonesia. *Peraturan Mahkamah Agung Nomor 4 Tahun 2016 tentang Tata Cara Penyelesaian Perkara Pelanggaran Administrasi dalam Pemilihan Umum*.