Verdict: Journal of Law Science
E-ISSN: 2985-3680
Journal Homepage:
https://www.ojs.wahanapublikasi.com/index.php/vjlaws

Kesiapan Hukum untuk Deteksi Dini Risiko KDRT Berbasis Teknologi melalui Pendekatan Normatif-Empiris untuk Penguatan Tafsir oleh Aparat Penegak Hukum

Endah Rizki Ekwanto[1], Vicky Ibrahim[2], Yeti S. Hasan[3], Parmin Ishak[4]*, Syalfadilah Kahar[5], Putry Rahayu Pakaya[6]

[1-6] Fakultas Hukum, Universitas Ichsan Gorontalo Utara, Gorontalo Utara, Gorontalo 96252, Indonesia

Legal Readiness for Technology-Based Early Detection of Domestic Violence Risks through a Normative-Empirical Approach to Strengthening Legal Interpretation by Law Enforcement Officials

ARTICLE INFO

Received:
15 August 2026

Accepted:
17 October 2026

Published:
05 November 2026

Keywords:

Technology-facilitated domestic violence, Legal readiness, Digital evidence, Law enforcement interpretation, Artificial intelligence

ABSTRACT

Technology-facilitated domestic violence challenges legal systems because everyday digital tools can extend surveillance, intimidation, and coercive control beyond physical encounters. This study examines Indonesia's legal readiness for early detection of technology-facilitated domestic violence, identifies interpretive gaps faced by law enforcement officers, and formulates an operational framework for accountable risk screening. Using a normative-empirical socio-legal approach, the study combines doctrinal analysis of relevant Indonesian laws with thematic analysis of verified interviews involving a Protection of Women and Children police officer, a legal counsel, and a survivor in Gorontalo. The findings show that the principal problem is not an absolute legal vacuum but fragmented legal readiness: relevant norms exist across several legal regimes, while frontline interpretation, digital evidence preservation, institutional capacity, and rapid victim protection remain weakly integrated. The study also identifies procedural fatigue as a factor that may affect survivors' willingness to continue legal processes. Artificial intelligence is positioned as an emerging risk and potential decision-support instrument, not an autonomous legal decision-maker. The study proposes a Five-Dimensional Legal Readiness Framework (KKH-5): normative recognition, interpretive integration, evidentiary readiness, institutional capacity, and protective responsiveness. The framework supports pattern-based interpretation, human oversight, due process, and survivor-centred early intervention.

Copyright © 2026 The Author(s)
Published by CV Wahana Publikasi.
This article is an open access article under the CC BY-NC 4.0 License.

* Corresponding Author: parminishak72@gmail.com
DOI: https://doi.org/10.59011/vjlaws.5.4.2026.862-879

1. Pendahuluan

Kekerasan dalam rumah tangga (KDRT) mengalami transformasi seiring kehidupan domestik yang semakin terhubung dengan telepon seluler, media sosial, layanan pesan, perangkat pelacak, kamera, penyimpanan awan, dan perangkat rumah pintar. Kekerasan tidak lagi hanya hadir melalui kontak fisik, ancaman verbal, atau penelantaran ekonomi, tetapi dapat diperpanjang melalui pengawasan akun, pelacakan lokasi, akses tanpa persetujuan terhadap komunikasi, penyebaran informasi yang mempermalukan korban, serta tekanan psikologis melalui kanal digital. Perubahan medium tersebut penting bagi hukum karena teknologi membuat kontrol dapat berlangsung terus-menerus, lintas ruang, dan bahkan ketika pelaku tidak berada bersama korban. Komnas Perempuan juga menempatkan perkembangan teknologi dan kecerdasan buatan sebagai faktor yang dapat memperluas bentuk diskriminasi dan kekerasan di ruang digital yang beririsan dengan kehidupan privat.[1]

Literatur internasional menggunakan beragam istilah, seperti technology-facilitated abuse, technology-facilitated intimate partner violence, digital coercive control, dan technology-enabled coercive control. Meskipun terminologinya beragam, penelitian menunjukkan karakter yang konsisten: teknologi berfungsi sebagai sarana untuk mengawasi, mengintimidasi, membatasi, mengisolasi, mempermalukan, atau mempertahankan dominasi dalam relasi intim. Scoping review dan systematic review terbaru memperlihatkan bahwa bentuk kekerasan tersebut meliputi penyalahgunaan telepon seluler, aplikasi pengawasan, spyware, media sosial, kamera, pelacakan lokasi, dan beragam teknologi sehari-hari, dengan dampak pada kesehatan mental, relasi sosial, kondisi ekonomi, serta rasa aman korban.[2]

Dalam penelitian ini, deteksi dini risiko (early risk detection) dimaknai sebagai proses identifikasi pada tahap awal pelaporan atau penanganan terhadap pola tindakan, indikator kerentanan, dan tanda eskalasi yang menunjukkan kemungkinan berlanjut atau meningkatnya KDRT berbasis teknologi. Secara operasional, deteksi dini dilakukan dengan menelusuri pola pengawasan, pembatasan, ancaman, akses tanpa persetujuan, pelacakan, atau penyebaran konten; menilai dampaknya terhadap rasa takut, ketidakberdayaan, dan otonomi korban; memetakan bukti elektronik yang perlu segera dipreservasi; serta menentukan kebutuhan perlindungan atau rujukan. Deteksi dini dalam penelitian ini bukan prediksi otomatis mengenai kesalahan pidana, melainkan skrining awal untuk mendukung penilaian APH yang tetap tunduk pada asas legalitas, due process, dan human oversight.

Cuomo dan Dolci menyebut fenomena tersebut sebagai "new tools, old abuse": teknologi tidak selalu menciptakan motif kekerasan yang baru, tetapi meningkatkan efisiensi, jangkauan, dan persistensi kontrol yang sudah ada. Teknologi memungkinkan pelaku memperpanjang kehadirannya secara spasial dan temporal sehingga korban dapat merasa diawasi setiap saat.[3] Temuan lain menunjukkan bahwa media sosial, GPS, perangkat komunikasi, dan teknologi yang terhubung dapat memperbesar efek kekerasan serta menghambat pemulihan korban bahkan setelah relasi berakhir.[4] Perkembangan Internet of Things (IoT) memperluas risiko karena perangkat rumah pintar dapat disalahgunakan untuk memantau, mengintimidasi, mengubah lingkungan rumah, atau melakukan gaslighting,

[1] Komisi Nasional Anti Kekerasan terhadap Perempuan, "Siaran Pers Memperingati Hari Kebangkitan Teknologi Nasional 2025: Membangun Ruang Aman Dunia Digital."

[2] Rogers et al., "Technology-Facilitated Abuse in Intimate Relationships: A Scoping Review"; Kim and Ferraresso, "Examining Technology-Facilitated Intimate Partner Violence: A Systematic Review of Journal Articles."

[3] Cuomo and Dolci, "New Tools, Old Abuse: Technology-Enabled Coercive Control (TECC)."

[4] Woodlock et al., "Technology as a Weapon in Domestic Violence: Responding to Digital Coercive Control"; Bailey et al., "The Networking of Abuse: Intimate Partner Violence and the Use of Social Technologies."

sehingga desain keamanan teknologi perlu mempertimbangkan kerentanan korban kekerasan domestik.[5]

Di Indonesia, penelitian mengenai KDRT dan teknologi masih berkembang. Penelitian terdahulu oleh Ekwanto, Ibrahim, dan Ishak telah membahas penyalahgunaan artificial intelligence dalam kekerasan rumah tangga melalui perspektif kriminologi dan menunjukkan kebutuhan penguatan sistem hukum.[6] Penelitian kriminologis di Gorontalo juga telah menunjukkan bahwa relasi kuasa, kondisi korban, dan efektivitas penegakan hukum merupakan elemen penting dalam memahami kekerasan terhadap perempuan.[7] Namun, masih terdapat ruang penelitian yang belum cukup dijelaskan, yaitu bagaimana aparat penegak hukum (APH) pada lini pertama menafsirkan rangkaian tindakan digital, memilih dasar hukum, mengamankan bukti elektronik, menilai risiko eskalasi, dan menghubungkan proses pembuktian dengan perlindungan korban.

Masalah tersebut tidak tepat direduksi menjadi klaim bahwa Indonesia sama sekali tidak memiliki norma untuk KDRT berbasis teknologi. Perkembangan hukum menunjukkan adanya beberapa titik masuk yang tersebar dalam Undang-Undang Penghapusan Kekerasan dalam Rumah Tangga (UU PKDRT), Undang-Undang Tindak Pidana Kekerasan Seksual (UU TPKS), Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), Undang-Undang Pelindungan Data Pribadi (UU PDP), serta hukum acara pidana yang kini secara eksplisit mengakui bukti elektronik. Pertanyaan yang lebih mendasar adalah apakah norma-norma tersebut telah membentuk sistem yang operasional bagi APH ketika menghadapi satu peristiwa domestik yang memuat sekaligus unsur kekerasan psikis, pengawasan digital, akses elektronik, ancaman, kerentanan data, dan kebutuhan perlindungan segera. Literatur tentang kriminalisasi kekerasan digital juga mengingatkan bahwa pembentukan delik baru tidak selalu menjadi satu-satunya jawaban; kualitas interpretasi, koherensi regulasi, dan kemampuan sistem hukum menerapkan norma yang tersedia sama pentingnya.[8]

Persoalan interpretasi beririsan dengan persoalan institusional. Penelitian di Australia dan Inggris menunjukkan bahwa penanganan technology-facilitated domestic abuse menghadapi hambatan berupa kurangnya pengenalan kekerasan digital sebagai bagian dari coercive control, keterbatasan pelatihan, keterbatasan waktu dan personel, serta kesulitan pengumpulan bukti. Studi lain menunjukkan bahwa korban dapat enggan melapor atau memiliki pengalaman negatif ketika laporan digital tidak dipandang serius.[9] Kondisi tersebut relevan bagi Indonesia, terutama di daerah yang tidak selalu memiliki akses langsung terhadap laboratorium digital forensik, ahli, atau prosedur preservasi bukti yang seragam.

Meskipun studi Australia dan Inggris telah mengidentifikasi hambatan pengenalan, pelatihan, sumber daya, dan pembuktian dalam penanganan technology-facilitated domestic abuse, penelitian terdahulu belum secara khusus menjelaskan bagaimana hambatan tersebut beroperasi dalam konteks hukum Indonesia yang tersebar pada beberapa rezim sekaligus.

[5] Brown, Harkin, and Tanczer, "Safeguarding the 'Internet of Things' for Victim-Survivors of Domestic and Family Violence: Anticipating Exploitative Use and Encouraging Safety-by-Design."

[6] Ekwanto, Ibrahim, and Ishak, "Penguatan Sistem Hukum atas Penyalahgunaan Artificial Intelligence dalam Kekerasan Rumah Tangga melalui Perspektif Kriminologi."

[7] Ekwanto and Ibrahim, "Pendekatan Kriminologi dalam Penanggulangan Tindak Pidana Kekerasan terhadap Perempuan di Kota Gorontalo"; Bakue et al., "Criminological Review of Domestic Violence Against Wife: Case Study of Boalemo Police Station."

[8] Polyzoidou, "Digital Violence Against Women: Is There a Real Need for Special Criminalization?"

[9] Douglas et al., "Policing Technology-Facilitated Domestic Abuse (TFDA): Views of Service Providers in Australia and the United Kingdom"; Flynn, Powell, and Hindes, "Policing Technology-Facilitated Abuse."

Kebaruan penelitian ini terletak pada sintesis normatif-empiris yang menghubungkan fragmentasi norma, penguatan tafsir APH, kesiapan pembuktian digital, respons perlindungan korban, dan batas akuntabel penggunaan AI ke dalam kerangka kesiapan hukum yang operasional untuk deteksi dini risiko KDRT berbasis teknologi.

Penelitian ini menggunakan pendekatan normatif-empiris untuk menghubungkan hukum sebagai norma dengan hukum sebagai praktik. Pendekatan socio-legal diperlukan karena persoalan teknologi tidak hanya ditentukan oleh bunyi norma, tetapi juga oleh nilai, kebiasaan institusional, kapasitas teknis, dan cara aparat menerjemahkan teknologi ke dalam kategori hukum.[10] Perkembangan artificial intelligence (AI) semakin memperkuat urgensi tersebut. AI dapat meningkatkan kemampuan analitik dan mendukung penilaian risiko, tetapi juga membawa persoalan akuntabilitas, bias, transparansi, privasi, dan kemungkinan ketergantungan berlebihan pada keluaran algoritmik.[11] Karena itu, kesiapan hukum penggunaan AI dalam penelitian ini ditempatkan dalam kerangka human oversight dan due process, bukan sebagai otomatisasi penentuan kesalahan pidana.

1.1 Kesiapan Hukum, Kontrol Koersif Digital, dan Penguatan Tafsir APH

Kesiapan hukum dalam penelitian ini dimaknai sebagai kapasitas sistem hukum untuk mengenali risiko, menyediakan dasar normatif yang dapat diterapkan, menjamin pembuktian yang sah, menyediakan kapasitas kelembagaan, dan mengaktifkan perlindungan korban secara tepat waktu. Kesiapan hukum tidak identik dengan jumlah peraturan. Suatu sistem dapat memiliki banyak norma, tetapi tetap tidak siap apabila norma tersebut terfragmentasi, aparat tidak memiliki pedoman interpretasi, bukti mudah hilang, atau mekanisme perlindungan berjalan terlambat. Oleh sebab itu, penelitian membedakan normative availability dari operational readiness.

Konsep kontrol koersif digunakan sebagai kerangka untuk membaca fungsi tindakan digital. Fokusnya bukan pada satu perangkat atau aplikasi, melainkan pada pola tindakan yang mengurangi otonomi korban melalui pengawasan, ancaman, isolasi, pembatasan, dan produksi rasa takut. Pendekatan ini membantu menghindari dua kekeliruan. Pertama, menganggap semua penggunaan teknologi antara pasangan sebagai kekerasan. Kedua, memisahkan setiap tindakan digital sehingga pola dominasi tidak terlihat. Dengan demikian, penguatan tafsir APH perlu bergerak dari incident-based interpretation menuju pattern-based interpretation, tanpa mengurangi kewajiban pembuktian setiap unsur tindak pidana.

Berdasarkan permasalahan tersebut, penelitian ini menjawab tiga pertanyaan. Pertama, bagaimana kesenjangan tafsir APH dalam konstruksi perbuatan, pemilihan pasal, pembuktian digital, dan perlindungan data korban pada KDRT berbasis teknologi? Kedua, bagaimana kesiapan hukum penggunaan AI untuk deteksi dini risiko KDRT yang akuntabel dan tetap menjaga due process? Ketiga, perangkat penguatan tafsir apa yang dapat dirumuskan agar penanganan KDRT berbasis teknologi lebih konsisten, cepat, dan berorientasi pada perlindungan korban? Tujuan penelitian adalah memetakan kesiapan hukum, mengidentifikasi kesenjangan interpretatif dan operasional, serta merumuskan kerangka penguatan tafsir APH yang dapat dikembangkan menjadi pedoman skrining risiko digital.

[10] Dizon, "Socio-Legal Study of Technology: A Norms and Values Approach to Hacking and Encryption Law and Policy."
[11] Qian, Siau, and Nah, "Societal Impacts of Artificial Intelligence: Ethical, Legal, and Governance Issues."

2. Metode dan Bahan Hukum

Penelitian menggunakan metode hukum normatif-empiris dengan desain socio-legal eksploratif. Pendekatan normatif digunakan untuk menganalisis struktur norma, hubungan antarrejim hukum, dan persyaratan pembuktian; pendekatan empiris digunakan untuk memahami bagaimana persoalan tersebut dialami dan diterjemahkan dalam praktik penanganan KDRT. Pilihan metode ini mengikuti pemahaman bahwa penelitian hukum dapat menggabungkan analisis doktrinal dengan fakta sosial ketika efektivitas dan penerapan norma menjadi bagian dari pertanyaan penelitian.[12]

Bahan hukum primer terdiri atas Undang-Undang Nomor 23 Tahun 2004 tentang Penghapusan Kekerasan dalam Rumah Tangga, Undang-Undang Nomor 12 Tahun 2022 tentang Tindak Pidana Kekerasan Seksual, Undang-Undang Nomor 1 Tahun 2024 sebagai perubahan kedua atas Undang-Undang Informasi dan Transaksi Elektronik, Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, dan Undang-Undang Nomor 20 Tahun 2025 tentang Kitab Undang-Undang Hukum Acara Pidana. Bahan hukum sekunder meliputi artikel jurnal internasional dan nasional mengenai technology-facilitated abuse, coercive control, digital evidence, risk assessment, AI governance, dan perlindungan korban.

Data empiris yang digunakan dalam manuskrip ini berasal dari wawancara terverifikasi pada tahap penelitian yang berjalan dengan tiga informan kunci di Provinsi Gorontalo. Informan dipilih secara purposive berdasarkan keterlibatan langsung atau pengalaman relevan dengan penanganan KDRT. Untuk menjaga kerahasiaan, identitas disamarkan sebagai APH-01 untuk Kanit/penyidik Unit Perlindungan Perempuan dan Anak (PPA), ADV-01 untuk pengacara/pendamping hukum, dan KOR-01 untuk korban KDRT. Keterlibatan korban dilakukan dengan prinsip informed consent, kerahasiaan, pembatasan pertanyaan yang berpotensi memicu distres, dan orientasi trauma-informed sebagaimana ditetapkan dalam protokol penelitian.

Rincian sumber data empiris, posisi atau peran masing-masing informan, serta fokus informasi yang digali melalui wawancara disajikan pada Tabel 1.

Tabel 1. Sumber Data Empiris Penelitian

Kode	Posisi/Peran	Fokus Informasi
APH-01	Kanit/penyidik Unit PPA	Praktik penerimaan laporan, bentuk kekerasan berbasis teknologi, bukti elektronik, SDM, infrastruktur, dan kebutuhan reformasi.
ADV-01	Pengacara/pendamping hukum	Pengalaman pendampingan korban, posisi unsur teknologi dalam perkara, dan hambatan membawa dimensi digital ke dalam proses hukum.
KOR-01	Korban KDRT	Dampak terhadap rasa aman, pengalaman dengan proses hukum, dukungan pemulihan, dan kebutuhan perlindungan cepat.

Sumber: Data primer penelitian, 2026, diolah peneliti.

Analisis data dilakukan melalui transkripsi, anonimisasi, reduksi, pengodean tematik, kategorisasi, dan sintesis normatif-empiris. Kode awal mencakup bentuk kekerasan, dampak,

[12] Marzuki, Penelitian Hukum: Edisi Revisi; Sumarna and Kadriah, "Penelitian Kualitatif terhadap Hukum Empiris."

kerentanan, pembuktian digital, kekosongan atau fragmentasi hukum, kapasitas aparat, perlindungan korban, dan rekomendasi. Analisis tidak dimaksudkan untuk menghitung prevalensi, melainkan mengidentifikasi mekanisme, pola interpretasi, dan titik lemah kesiapan hukum. Validitas diperkuat melalui triangulasi antara data wawancara, regulasi, dan literatur. Karena data empiris pada manuskrip ini bersifat eksploratif dan terbatas pada informan kunci, temuan dibaca sebagai dasar konseptual yang masih memerlukan validasi lebih luas pada tahap lanjutan penelitian.

3. Hasil dan Pembahasan

3.1 Kesenjangan Tafsir APH dalam Konstruksi Perbuatan, Pemilihan Pasal, Bukti Digital, dan Perlindungan Korban

Temuan pertama adalah adanya under-recognition terhadap dimensi teknologi dalam KDRT. APH-01 menjelaskan bahwa masyarakat masih cenderung memahami KDRT sebagai kekerasan fisik. Padahal, dalam praktik, satu peristiwa dapat sekaligus mengandung kekerasan fisik, psikis, verbal, seksual, dan kontrol melalui teknologi. Informan menyebut tekanan melalui status, foto, video, ancaman di media sosial, tindakan membuntuti, pelacakan, penyadapan komunikasi, CCTV, dan GPS. ADV-01 juga menyatakan pernah mendampingi korban yang mengalami unsur kontrol digital, tetapi perkara yang diajukan tetap berfokus pada kekerasan fisik. Data tersebut menunjukkan bahwa ketiadaan label "KDRT berbasis teknologi" dalam laporan tidak selalu berarti ketiadaan unsur teknologi dalam relasi kekerasan.

> *"KDRT berbasis teknologi itu sebenarnya banyak ditemui apabila ditelusuri lebih dalam, karena kebanyakan mengetahui bahwa KDRT itu hanya kekerasan fisik."* (APH-01)

Fenomena tersebut sejalan dengan penelitian yang menunjukkan bahwa technology-facilitated abuse sering merupakan perluasan dari pola kekerasan yang sudah ada, bukan insiden yang terpisah. Kuo, Zhang, dan Chang menemukan bahwa pelaku menggunakan teknologi untuk harassment, monitoring, stalking, isolasi, dan penyebaran pesan yang merendahkan korban.[13] Bailey dan kolega juga menunjukkan bahwa penggunaan media sosial, telepon, dan GPS dapat memperluas kekerasan melampaui kehadiran fisik dan menghambat pemulihan korban.[14] Dengan demikian, tantangan interpretatif pertama bagi APH adalah mengenali fungsi tindakan digital di dalam relasi kekuasaan, bukan sekadar mengidentifikasi perangkat yang digunakan.

Temuan kedua adalah bahwa hukum Indonesia lebih tepat digambarkan sebagai fragmented legal readiness daripada legal vacuum. UU PKDRT telah mengatur kekerasan fisik, psikis, seksual, dan penelantaran. Pasal 7 merumuskan kekerasan psikis melalui akibat berupa ketakutan, hilangnya rasa percaya diri, hilangnya kemampuan bertindak, rasa tidak berdaya, atau penderitaan psikis berat.[15] Rumusan berbasis akibat ini secara interpretatif memungkinkan tindakan pengawasan, ancaman, atau kontrol digital dinilai sebagai bagian dari kekerasan psikis apabila hubungan kausal dan dampaknya dapat dibuktikan. Kelemahannya, undang-undang tidak menyediakan indikator eksplisit mengenai pengawasan digital, pelacakan, kontrol akun, atau pola coercive control.

UU TPKS memberikan jembatan yang lebih eksplisit untuk dimensi seksual melalui

[13] Kuo, Zhang, and Chang, "Technology-Facilitated Abuse in the Context of Intimate Partner Violence: A Qualitative Study of Women Survivors in Taiwan."

[14] Bailey et al., "The Networking of Abuse: Intimate Partner Violence and the Use of Social Technologies."

[15] Undang-Undang Nomor 23 Tahun 2004 tentang Penghapusan Kekerasan dalam Rumah Tangga, khususnya Pasal 5 dan Pasal 7.

pengaturan kekerasan seksual berbasis elektronik serta mekanisme penanganan, perlindungan, dan pemulihan korban.[16] UU ITE menyediakan dasar bagi informasi dan dokumen elektronik serta mengatur berbagai perbuatan terhadap sistem elektronik, tetapi tidak dirancang sebagai rezim KDRT yang membaca rangkaian kontrol dalam relasi domestik.[17] UU PDP penting untuk perlindungan data, tetapi Pasal 2 ayat (2) mengecualikan pemrosesan data pribadi oleh orang perseorangan dalam kegiatan pribadi atau rumah tangga, sehingga tidak dapat otomatis dijadikan dasar universal bagi seluruh bentuk pengawasan pasangan.[18]

Pernyataan APH-01 menggambarkan cara aparat mencoba menjembatani fragmentasi tersebut.

> *"Kekerasannya diambil dari UU PKDRT, teknologinya masuk dalam UU ITE, dan untuk keamanan data seseorang ada di dalam UU PDP."* (APH-01)

Pada aspek pemilihan dan pengintegrasian dasar hukum, data empiris terutama berasal dari perspektif APH-01 sebagai aparat yang berhadapan langsung dengan konstruksi hukum perkara. Perspektif tersebut menunjukkan bahwa penanganan KDRT berbasis teknologi dalam praktik membutuhkan pembacaan lintas rezim hukum, karena karakter kekerasan, penggunaan teknologi, dan perlindungan data tidak seluruhnya berada dalam satu instrumen hukum. Temuan ini selanjutnya memperoleh penguatan melalui analisis normatif terhadap UU PKDRT, UU TPKS, UU ITE, dan UU PDP.

Pernyataan tersebut menunjukkan bahwa aparat tidak menghadapi kekosongan absolut, melainkan kebutuhan untuk menghubungkan norma dari beberapa rezim pada satu rangkaian peristiwa. Kondisi ini menghasilkan dua bentuk fragmentasi. Pertama, fragmentasi normatif terjadi karena setiap undang-undang memiliki objek, tujuan, dan unsur yang berbeda. Kedua, fragmentasi interpretatif terjadi karena petugas lini pertama harus menentukan hubungan antarnorma tanpa pedoman yang khusus memetakan pola KDRT berbasis teknologi. Apabila setiap tindakan dipisahkan menjadi satu pesan, satu akses akun, satu pelacakan, atau satu unggahan, fungsi kontrol yang menghubungkan keseluruhan rangkaian dapat hilang.

Pemetaan kapasitas normatif, celah interpretatif, dan implikasinya terhadap deteksi risiko serta penguatan tafsir APH disajikan pada Tabel 2.

Tabel 2. Peta Kesiapan Normatif terhadap KDRT Berbasis Teknologi

Rezim Hukum	Kapasitas yang Tersedia	Celah/Kebutuhan Interpretatif	Implikasi terhadap Deteksi Risiko/Penguatan Tafsir APH
UU PKDRT No. 23/2004	Mengatur kekerasan fisik, psikis, seksual, dan penelantaran; kekerasan psikis dirumuskan berbasis akibat.	Belum menyebut kontrol, pelacakan, pengawasan, atau intimidasi digital secara eksplisit; dibutuhkan indikator pola dan	APH perlu menghubungkan pola digital dengan akibat psikis atau bentuk KDRT yang relevan dan mencatat indikator berulang

[16] Undang-Undang Nomor 12 Tahun 2022 tentang Tindak Pidana Kekerasan Seksual, termasuk pengaturan Kekerasan Seksual Berbasis Elektronik.

[17] Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

[18] Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, Pasal 2 ayat (2).

		dampak.	sebagai dasar skrining risiko.
UU TPKS No. 12/2022	Mengakui kekerasan seksual berbasis elektronik serta kerangka penanganan dan pemulihan.	Cakupan utamanya dimensi seksual; tidak seluruh kontrol digital domestik merupakan kekerasan seksual.	Jika terdapat dimensi seksual berbasis elektronik, skrining perlu mengaktifkan jalur penanganan, perlindungan, dan pemulihan khusus tanpa memperluas rezim TPKS ke seluruh bentuk kontrol digital.
UU ITE jo. UU No. 1/2024	Mengatur informasi/dokumen elektronik dan sejumlah perbuatan melalui sistem elektronik.	Tidak dirancang sebagai kerangka KDRT; perlu integrasi dengan relasi domestik, pola kontrol, dan dampak korban.	Modus elektronik perlu dipetakan bersama konteks relasi domestik, pola kontrol, dan bukti agar perbuatan tidak dibaca sebagai insiden digital yang terpisah.
UU PDP No. 27/2022	Memberikan kerangka perlindungan data pribadi secara umum.	Pengecualian kegiatan pribadi/rumah tangga membatasi penerapan otomatis terhadap hubungan pasangan.	Penggunaan data korban untuk skrining harus dibatasi menurut dasar hukum, tujuan, akses, dan keamanan; pengecualian kegiatan pribadi atau rumah tangga perlu diuji sebelum UU PDP diterapkan.
KUHAP No. 20/2025	Mengakui bukti elektronik secara eksplisit dan menyediakan basis bantuan teknis penyidikan.	Tantangan bergeser ke preservasi, autentikasi, atribusi, legalitas perolehan, dan kapasitas forensik digital.	Deteksi awal harus segera diikuti preservasi, autentikasi, atribusi, dan chain of custody agar indikator risiko dapat diterjemahkan menjadi bukti elektronik yang sah.

Sumber: Analisis peneliti terhadap peraturan perundang-undangan, 2026.

Temuan ketiga berhubungan dengan bukti elektronik. APH-01 menyatakan bahwa korban sering terlambat melapor karena takut, malu, bergantung secara ekonomi, atau berada di bawah ancaman. Akibatnya, pesan, rekaman, foto, atau data lain dapat terhapus sebelum diamankan. Informan juga menekankan kebutuhan untuk memastikan autentisitas dan integritas bukti. Perubahan KUHAP melalui Undang-Undang Nomor 20 Tahun 2025 memperkuat posisi bukti elektronik sebagai alat bukti dan memberikan landasan yang lebih

jelas bagi penggunaan bantuan teknis digital forensik.[19] Oleh karena itu, problem pada 2026 bukan lagi sekadar legal admissibility, melainkan evidentiary readiness: kemampuan faktual untuk menemukan, mengamankan, menjaga integritas, mengautentikasi, mengatribusikan, dan menyajikan bukti secara sah.

Pada temuan ini, data empiris mengenai keterlambatan pelaporan, risiko hilangnya bukti, serta kebutuhan autentikasi berasal terutama dari APH-01; temuan tersebut ditriangulasi dengan literatur digital evidence dan tidak diklaim sebagai pengalaman langsung ADV-01 atau KOR-01.

Stoykova menunjukkan bahwa proses digital evidence dapat menimbulkan ancaman terhadap fairness ketika teknologi digunakan secara tidak konsisten, jaminan prosedural tidak menyesuaikan proses digital, dan reliabilitas digital forensics tidak diuji secara memadai.[20] Dalam perkara IPV, Cho dan kolega menekankan bahwa korban menghadapi risiko khusus ketika bukti disimpan pada perangkat yang dapat diakses pelaku; karena itu, mekanisme pengumpulan dan penyimpanan bukti perlu berorientasi pada keselamatan korban.[21] Temuan tersebut menguatkan kebutuhan akan digital evidence preservation protocol yang sederhana pada lini pertama, dengan prinsip legalitas, chain of custody, keamanan data, dan trauma-informed practice.

Temuan keempat adalah kesenjangan kapasitas kelembagaan. APH-01 menyatakan bahwa keterampilan digital forensik, analisis bukti digital, dan pemahaman kejahatan siber masih dimiliki oleh personel tertentu yang telah mengikuti pelatihan. Penanganan perkara juga membutuhkan dukungan laboratorium, ahli, dan koordinasi dengan penyedia layanan. Kondisi daerah memperbesar tantangan karena sumber daya digital tidak selalu tersedia di unit terdekat. Penelitian Harris dan Woodlock menunjukkan bahwa lokasi geografis dan kapasitas lembaga memengaruhi respons terhadap digital coercive control, sehingga pelatihan dan sumber daya perlu tersedia di luar pusat kota.[22]

Temuan kapasitas kelembagaan juga terutama bersumber dari APH-01 dan diperlakukan sebagai informasi institusional dari satu informan kunci, kemudian diuji konsistensinya melalui literatur mengenai keterbatasan pelatihan dan sumber daya pada penanganan technology-facilitated abuse.

Temuan kelima berasal dari pengalaman korban. KOR-01 menjelaskan tekanan sehari-hari akibat merasa diikuti dan dibuntuti. Ia juga menyatakan bahwa proses hukum yang panjang berjalan bersamaan dengan konflik batin dan beban mental. Pada akhirnya, korban memilih berdamai setelah merasa lelah, meskipun tekanan tidak otomatis hilang.

Sebaliknya, temuan mengenai pengalaman korban dan kelelahan prosedural bersumber khusus dari KOR-01 dan digunakan untuk menangkap pengalaman korban secara mendalam, bukan untuk digeneralisasi sebagai pola seluruh korban KDRT.

> *"Saya sudah matang untuk mau berpisah, tapi karena proses cukup lama, pada akhirnya saya capek dan memilih untuk damai saja dengan beberapa kesepakatan."* (KOR-01)

Penelitian ini menyebut mekanisme tersebut sebagai procedural fatigue atau kelelahan prosedural: menurunnya daya tahan korban untuk mempertahankan proses hukum ketika tekanan relasional berlangsung bersamaan dengan proses formal yang lama dan emosional. Kategori ini tidak berarti setiap perdamaian merupakan hasil tekanan, tetapi menunjukkan

[19] Undang-Undang Nomor 20 Tahun 2025 tentang Kitab Undang-Undang Hukum Acara Pidana.
[20] Stoykova, "Digital Evidence: Unaddressed Threats to Fairness and the Presumption of Innocence."
[21] Cho et al., "DEF-IPV: A Digital Evidence Framework for Intimate Partner Violence Victims."
[22] Harris and Woodlock, "'You Can't Actually Escape It': Policing the Use of Technology in Domestic Violence in Rural Australia."

bahwa durasi dan kualitas proses hukum dapat memengaruhi agensi korban. O'Brien dan Maras mengingatkan bahwa respons hukum terhadap technology-facilitated coercive control harus menghindari victim blaming, systems abuse, dan reformasi reaktif yang justru mengurangi otonomi korban.[23] Dari perspektif akses keadilan, kecepatan respons bukan sekadar efisiensi administrasi, melainkan bagian dari perlindungan substantif.

3.2 Kesiapan Hukum Penggunaan AI untuk Deteksi Dini Risiko KDRT yang Akuntabel dan Menjaga Due Process

Proposal penelitian menempatkan AI sebagai bagian dari agenda deteksi dini. Namun, integritas analisis mengharuskan pembedaan antara apa yang terkonfirmasi dalam data primer dan apa yang masih merupakan emerging risk. Wawancara terverifikasi menunjukkan penggunaan atau dugaan penggunaan teknologi berupa pelacakan, penyadapan komunikasi, CCTV, GPS, media sosial, dan kontrol digital. Data tersebut belum cukup untuk menyatakan bahwa deepfake, chatbot generatif, atau sistem AI otonom telah menjadi modus dominan dalam perkara yang ditangani informan. Karena itu, penelitian ini tidak memaksakan AI sebagai temuan empiris, melainkan menilai kesiapan hukumnya sebagai horizon perkembangan teknologi dan sebagai kemungkinan alat bantu penilaian risiko.

Pembedaan ini penting karena AI memiliki dua posisi yang berbeda. Pada sisi pertama, AI dapat menjadi sarana kekerasan melalui pembuatan konten sintetis, impersonasi, manipulasi citra atau suara, otomatisasi pelecehan, analisis lokasi, dan pemrosesan data yang memperbesar skala kontrol. Pada sisi kedua, AI dapat digunakan oleh institusi untuk membantu skrining risiko, mengorganisasi informasi, atau mendukung prioritisasi penanganan. Kedua posisi tersebut menimbulkan persoalan hukum yang berbeda: penyalahgunaan AI oleh pelaku berkaitan dengan kriminalisasi, privasi, bukti, dan perlindungan korban; penggunaan AI oleh negara berkaitan dengan akuntabilitas algoritmik, due process, non-diskriminasi, transparansi, dan batas diskresi manusia.

Penelitian Turner, Brown, dan Medina-Ariza menunjukkan potensi machine learning untuk membantu penilaian risiko domestic abuse, tetapi juga menegaskan pentingnya fairness dan kualitas data.[24] Bukti yang lebih kritis datang dari Valdivia, Hyde-Vaamonde, dan García Marcos dalam analisis terhadap alat penilaian risiko IPV di Basque Country. Mereka menemukan risiko salah klasifikasi pada kasus berisiko tinggi dan kekurangan pedoman hukum bagi hakim yang menggunakan keluaran algoritmik.[25] Pelajaran pentingnya adalah bahwa peningkatan kemampuan prediktif tidak otomatis meningkatkan keadilan. Kesalahan pada kasus high-risk dapat berakibat serius, sementara opasitas sistem dapat membuat APH terlalu percaya pada skor yang mekanismenya tidak dipahami.

Atas dasar itu, kesiapan hukum penggunaan AI untuk deteksi dini harus berangkat dari lima batas. Pertama, AI tidak boleh menjadi dasar tunggal untuk menentukan ada atau tidaknya tindak pidana, penetapan tersangka, atau pengurangan hak prosedural. Kedua, setiap keluaran AI harus dapat ditinjau oleh manusia yang memiliki kompetensi hukum dan pemahaman KDRT. Ketiga, data yang digunakan harus relevan, proporsional, dan diperoleh secara sah, terutama karena informasi korban dapat memuat data sensitif. Keempat, sistem

[23] O'Brien and Maras, "Technology-Facilitated Coercive Control: Response, Redress, Risk, and Reform."
[24] Turner, Brown, and Medina-Ariza, "Predicting Domestic Abuse (Fairly) and Police Risk Assessment."
[25] Valdivia, Hyde-Vaamonde, and Marcos, "Judging the Algorithm: Algorithmic Accountability on the Risk Assessment Tool for Intimate Partner Violence in the Basque Country.".

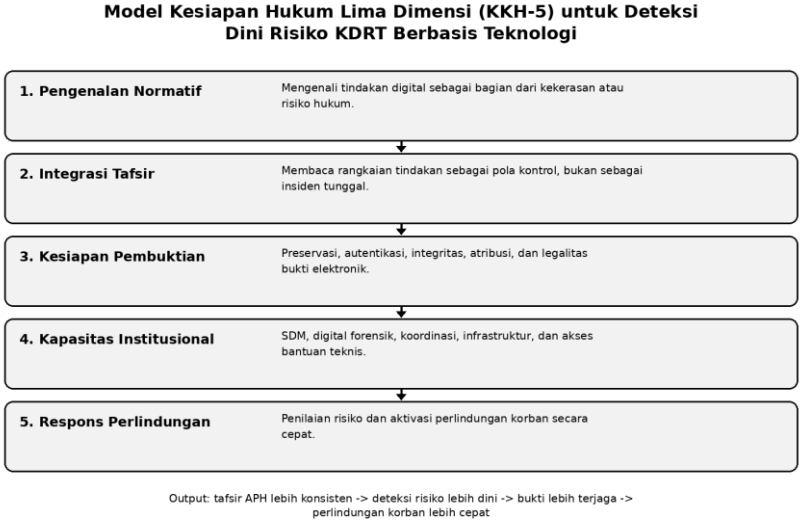
harus menyimpan jejak audit yang memungkinkan rekonstruksi bagaimana suatu rekomendasi atau skor dihasilkan. Kelima, tersedia mekanisme koreksi dan keberatan ketika keluaran sistem tidak sesuai dengan fakta atau merugikan korban maupun pihak yang diperiksa.

Prinsip tersebut sejalan dengan diskursus governance yang menempatkan transparansi, akuntabilitas, fairness, privasi, dan human oversight sebagai unsur utama penggunaan AI dalam pengambilan keputusan sosial dan hukum.[26] Dalam perkara KDRT, prinsip ini harus diperketat karena data berhubungan dengan relasi intim, kondisi psikologis, informasi kesehatan, komunikasi pribadi, dan potensi risiko keselamatan. Dengan demikian, istilah "deteksi dini berbasis AI" tidak boleh dipahami sebagai penggantian diskresi hukum oleh mesin. Posisi yang lebih aman adalah AI-assisted decision support, yaitu teknologi yang membantu mengidentifikasi indikator yang perlu diperiksa lebih lanjut, sedangkan kualifikasi hukum, penilaian kredibilitas, tindakan perlindungan, dan keputusan koersif tetap berada di bawah tanggung jawab manusia.

Kesiapan hukum juga harus bersifat technology-neutral. Regulasi atau pedoman yang terlalu terikat pada satu jenis aplikasi akan cepat usang. Fokus normatif sebaiknya diarahkan pada fungsi perbuatan: pengawasan tanpa persetujuan, pembatasan akses, ancaman, impersonasi, manipulasi informasi, penyebaran konten, pemaksaan akses data, dan penggunaan sistem untuk menciptakan ketakutan atau ketidakberdayaan. Kerangka berbasis fungsi mampu menjangkau teknologi yang ada saat ini sekaligus mengantisipasi perkembangan AI yang belum muncul dalam data lapangan.

3.3 Perangkat Penguatan Tafsir Operasional bagi APH: Model Kesiapan Hukum Lima Dimensi (KKH-5)

Sintesis antara data empiris dan analisis normatif menghasilkan Model Kesiapan Hukum Lima Dimensi (KKH-5). Model ini tidak menciptakan unsur tindak pidana baru dan tidak menggantikan kewenangan penyidik, penuntut umum, atau hakim. Fungsinya adalah menyediakan kerangka skrining dan organisasi informasi pada tahap awal agar dimensi digital, pola kontrol, bukti, kapasitas institusional, dan kebutuhan perlindungan tidak ditangani secara terpisah.



Gambar 1. Model Kesiapan Hukum Lima Dimensi (KKH-5)
Sumber: Hasil sintesis data primer dan analisis normatif, 2026.

[26] Qian, Siau, and Nah, "Societal Impacts of Artificial Intelligence: Ethical, Legal, and Governance Issues."

Gambar 1 menunjukkan hubungan antara lima dimensi KKH-5 sebagai alur yang saling terkait, pengenalan normatif dan integrasi tafsir menjadi dasar kesiapan pembuktian. Ketiganya memerlukan kapasitas institusional dan bermuara pada respons perlindungan yang cepat. Dengan demikian, model tidak membaca tiap dimensi secara terpisah, melainkan sebagai rangkaian kesiapan operasional sejak penerimaan laporan hingga aktivasi perlindungan korban.

Dimensi pertama adalah pengenalan normatif. APH perlu mengenali bahwa tindakan digital dapat mempunyai relevansi hukum meskipun perangkat yang digunakan bersifat umum dan legal. Pertanyaan awal bukan "apakah aplikasi ini ilegal", melainkan "fungsi apa yang dijalankan tindakan tersebut dalam relasi, akibat apa yang muncul, dan norma mana yang menyediakan titik masuk". Dimensi ini mendorong APH untuk menghubungkan fakta dengan UU PKDRT, UU TPKS, UU ITE, KUHP apabila relevan, dan ketentuan lain berdasarkan unsur konkret, bukan berdasarkan label teknologi.

Dimensi kedua adalah integrasi tafsir. Rangkaian tindakan dibaca sebagai pola sebelum dipisahkan untuk pembuktian unsur masing-masing delik. Pattern-based interpretation penting karena risiko KDRT sering berasal dari akumulasi tindakan yang secara individual tampak kecil. Permintaan lokasi, akses kata sandi, pemeriksaan pesan, ancaman melalui media sosial, dan pembatasan pergaulan dapat mempunyai makna berbeda jika muncul dalam rangkaian kontrol yang disertai rasa takut dan ketidakberdayaan. Pendekatan pola tidak mengurangi asas legalitas; ia bekerja pada tahap konstruksi fakta agar konteks relasi tidak hilang sebelum norma diterapkan.

Dimensi ketiga adalah kesiapan pembuktian. Pada tahap penerimaan laporan, APH perlu segera memetakan sumber bukti elektronik, status perangkat, risiko penghapusan data, kebutuhan tangkapan layar atau ekspor data, kemungkinan metadata, akun yang terhubung, serta kebutuhan rujukan forensik digital. Dokumentasi awal harus dilakukan tanpa mengubah data asli dan tetap memperhatikan keselamatan korban. Model DEF-IPV menunjukkan pentingnya desain pengumpulan bukti yang mempertimbangkan fakta bahwa pelaku mungkin memiliki akses terhadap perangkat korban.[27] Karena itu, preservasi bukti dan keselamatan korban harus berjalan bersamaan.

Dimensi keempat adalah kapasitas institusional. Tidak semua unit harus memiliki laboratorium digital forensik, tetapi setiap unit yang menerima laporan KDRT perlu mengetahui kapan dan bagaimana meminta bantuan teknis, kepada siapa perangkat dirujuk, bagaimana chain of custody dijaga, dan bagaimana komunikasi dengan lembaga layanan korban dilakukan. Temuan Douglas et al. dan Flynn et al. memperlihatkan bahwa pelatihan, sumber daya, dan pengenalan hukum merupakan faktor penting dalam meningkatkan respons kepolisian terhadap technology-facilitated abuse.[28] Oleh sebab itu, pedoman harus membagi tugas antara petugas penerima laporan, penyidik PPA, unit siber/forensik, pendamping korban, dan ahli.

Dimensi kelima adalah respons perlindungan. Screening teknologi tidak boleh berhenti pada klasifikasi hukum. Ketika pola menunjukkan peningkatan pengawasan, ancaman, kehilangan otonomi, atau kombinasi dengan kekerasan fisik, seksual, dan ekonomi, hasil skrining harus memicu penilaian risiko serta kebutuhan perlindungan. Hal ini menjawab pengalaman KOR-01 bahwa proses yang terlalu lama dapat berinteraksi dengan tekanan

[27] Cho et al., "DEF-IPV: A Digital Evidence Framework for Intimate Partner Violence Victims."
[28] Douglas et al., "Policing Technology-Facilitated Domestic Abuse (TFDA): Views of Service Providers in Australia and the United Kingdom."

psikologis dan mengubah keputusan korban. Protective responsiveness menempatkan kecepatan respons, informasi perkembangan perkara, keamanan data, akses pendampingan, dan rujukan sebagai bagian dari kualitas penegakan hukum.

Secara operasional, KKH-5 dapat diterjemahkan ke dalam lima pertanyaan screening bagi APH: (1) apakah teknologi digunakan secara berulang untuk memantau, membatasi, mengancam, mempermalukan, mengisolasi, atau mengendalikan korban; (2) apakah rangkaian tindakan menimbulkan ketakutan, ketidakberdayaan, hilangnya kebebasan bertindak, atau penderitaan yang relevan secara hukum; (3) norma apa yang menyediakan titik masuk dan bagaimana hubungan antarnorma tersebut; (4) bukti elektronik apa yang harus segera dipreservasi dan bagaimana menjaga legalitas, integritas, serta atribusinya; dan (5) apakah pola menunjukkan risiko eskalasi yang memerlukan perlindungan segera.

Sintesis hubungan antara temuan penelitian, risiko sistem hukum, dan perangkat penguatan tafsir APH disajikan pada Tabel 3.

Tabel 3. Sintesis Temuan dan Perangkat Penguatan Tafsir APH

Temuan	Risiko Sistem Hukum	Perangkat Penguatan
Under-recognition dimensi digital	Unsur teknologi tidak tercatat; pola kekerasan terbaca sebagai insiden fisik semata.	Pertanyaan intake wajib mengenai kontrol, pengawasan, ancaman, akses akun, pelacakan, dan penyebaran konten.
Fragmented legal readiness	APH berhenti pada kebingungan memilih satu pasal atau satu undang-undang.	Matriks norma–modus–akibat–bukti untuk menghubungkan UU PKDRT, UU TPKS, UU ITE, dan aturan terkait.
Evidentiary gap	Bukti terhapus, tidak autentik, sulit diatribusikan, atau diperoleh secara tidak sah.	Protokol preservasi bukti elektronik, chain of custody, dan mekanisme rujukan digital forensik.
Kapasitas institusional tidak merata	Penanganan lambat dan bergantung pada personel tertentu.	Pelatihan berjenjang, focal point digital, jejaring ahli, dan SOP koordinasi PPA–siber–layanan korban.
Procedural fatigue	Korban kehilangan daya tahan untuk mengikuti proses meskipun risiko belum berhenti.	Standar waktu respons, pembaruan informasi perkara, pendampingan, risk review berkala, dan perlindungan cepat.
Penggunaan AI tanpa safeguards	Automation bias, diskriminasi, opasitas, dan pelanggaran due process.	Human oversight, audit trail, pembatasan tujuan, data minimization, validasi berkala, dan hak koreksi.

Sumber: Data primer dan analisis peneliti, 2026.

Model tersebut menawarkan kebaruan pada tiga tingkat. Pertama, penelitian menggeser diagnosis dari legal vacuum menuju fragmented legal readiness, sehingga pembaruan hukum tidak otomatis diarahkan pada penambahan delik, tetapi pada integrasi norma dan kapasitas implementasi. Kedua, penelitian membedakan legal admissibility dari evidentiary readiness, yang penting setelah bukti elektronik memperoleh dasar lebih tegas dalam KUHAP baru. Ketiga, penelitian mengidentifikasi procedural fatigue sebagai mekanisme yang dapat memengaruhi keberlanjutan akses korban terhadap keadilan. Ketiganya memperluas diskusi

dari pertanyaan "apakah hukum tersedia?" menuju "apakah hukum dapat bekerja secara cepat, terpadu, dapat dibuktikan, dan tetap menjaga agensi korban?".

Dalam jangka pendek, implikasi kebijakan penelitian bukan pembentukan sistem AI yang langsung digunakan untuk menilai korban atau pelaku. Prioritas pertama adalah membangun kualitas data, pedoman interpretasi, protokol bukti, dan koordinasi kelembagaan. Hanya setelah fondasi tersebut stabil, decision-support berbasis AI dapat diuji secara terbatas dengan data yang sah, indikator yang teruji, audit independen, dan human oversight. Pendekatan bertahap ini mengurangi risiko techno-solutionism, yaitu asumsi bahwa teknologi dapat menyelesaikan masalah yang sebenarnya berakar pada fragmentasi norma, kapasitas institusi, dan relasi kuasa.

Implikasi pertama dari model tersebut adalah perlunya membedakan kebutuhan reformasi legislasi dari kebutuhan reformasi interpretasi. Dorongan informan untuk menghadirkan regulasi khusus mencerminkan pengalaman praktis ketika petugas sulit menemukan jalur hukum yang jelas. Namun, pembentukan norma baru sebaiknya didahului evaluasi atas kapasitas norma yang telah ada. Apabila penderitaan psikis, ancaman elektronik, akses tanpa hak, kekerasan seksual berbasis elektronik, atau tindakan lain sebenarnya dapat dijangkau oleh norma yang tersedia, maka persoalan mendesaknya adalah konsistensi tafsir dan prosedur. Sebaliknya, apabila ditemukan pola kontrol yang nyata merugikan tetapi tidak dapat dikualifikasi secara adil tanpa perluasan unsur pidana, barulah kebutuhan reformulasi undang-undang memperoleh dasar empiris yang lebih kuat. Pendekatan ini mencegah over-criminalisation sekaligus menghindari under-protection terhadap korban.

Implikasi kedua berkaitan dengan tahap penerimaan laporan. Intake KDRT pada era digital perlu memuat pertanyaan yang mampu mengidentifikasi konteks teknologi tanpa mengubah petugas menjadi pemeriksa forensik. Pertanyaan dapat diarahkan pada apakah korban merasa dipantau, apakah lokasi diketahui tanpa penjelasan, apakah akun atau perangkat diakses tanpa persetujuan, apakah terdapat ancaman penyebaran informasi atau konten, apakah akses keuangan digital dikendalikan, serta apakah perilaku tersebut berubah menjadi lebih intens setelah konflik atau upaya berpisah. Informasi ini tidak otomatis membuktikan tindak pidana, tetapi membantu membangun chronology of control dan menentukan bukti apa yang rawan hilang. Pendekatan demikian juga mengurangi ketergantungan pada kemampuan korban untuk memberi label hukum terhadap pengalaman yang dialaminya.

Implikasi ketiga adalah perlunya tata kelola data korban yang lebih ketat. Bukti digital dapat mengandung percakapan pribadi, lokasi, foto, informasi kesehatan, data anak, data keuangan, dan identitas pihak ketiga. Semakin banyak data yang dikumpulkan untuk kepentingan deteksi dini, semakin besar pula kewajiban institusi untuk membatasi akses, tujuan penggunaan, masa penyimpanan, dan pihak yang dapat memproses data tersebut. Prinsip data minimization menjadi penting agar perlindungan korban tidak berubah menjadi bentuk pengawasan baru oleh institusi. Pada titik ini, keamanan informasi harus dipandang sebagai bagian dari due process dan victim protection, bukan sekadar kebutuhan teknis. Setiap integrasi data lintas unit juga memerlukan dasar kewenangan, pencatatan akses, dan mekanisme akuntabilitas yang jelas.

Implikasi keempat berhubungan dengan desain masa depan sistem AI. Sebelum model prediktif digunakan, institusi perlu memiliki baseline non-algoritmik yang jelas: indikator apa yang dinilai, siapa yang menilai, bagaimana keputusan dicatat, dan bagaimana kesalahan diperbaiki. AI seharusnya masuk setelah prosedur manusia dapat diaudit, bukan digunakan

untuk menutupi kelemahan prosedur tersebut. Uji coba juga perlu membandingkan hasil AI dengan penilaian ahli dan outcome nyata, termasuk mengukur false negative pada kasus berisiko tinggi, false positive yang dapat membebani pihak tertentu, serta kemungkinan bias terhadap kelompok dengan pola penggunaan teknologi berbeda. Dengan cara ini, inovasi ditempatkan sebagai proses pembelajaran institusional yang tunduk pada hukum, bukan sebagai teknologi yang memperoleh otoritas hanya karena dianggap lebih cepat atau objektif.

4. Kesimpulan

Penelitian menunjukkan bahwa kesiapan hukum Indonesia dalam menghadapi KDRT berbasis teknologi tidak berada dalam kondisi kekosongan hukum absolut. Norma relevan telah tersedia secara parsial melalui UU PKDRT, UU TPKS, UU ITE, UU PDP, dan KUHAP baru. Persoalan yang lebih nyata adalah fragmented legal readiness: norma berada pada rezim berbeda, sementara APH belum selalu memiliki kerangka integratif untuk mengenali pola kontrol digital, menghubungkan tindakan dengan dampak hukum, mempreservasi bukti elektronik, dan mengaktifkan perlindungan korban secara cepat. Data empiris juga memperlihatkan under-recognition terhadap dimensi digital, keterbatasan kapasitas digital forensik, serta kelelahan prosedural yang dapat memengaruhi keputusan korban untuk melanjutkan proses hukum.

Penelitian juga menegaskan bahwa AI perlu ditempatkan secara hati-hati. Data primer yang tersedia lebih kuat membuktikan technology-facilitated abuse daripada penggunaan AI spesifik seperti deepfake atau chatbot otonom. Karena itu, AI diposisikan sebagai emerging risk dan sebagai kemungkinan decision-support, bukan sebagai pengganti penilaian hukum. Setiap penggunaan AI untuk deteksi dini harus tunduk pada human oversight, due process, pembatasan tujuan, legalitas data, audit trail, validasi, non-diskriminasi, dan hak koreksi. Kesiapan hukum harus dibangun sebelum otomatisasi diperluas.

Kontribusi utama penelitian adalah Model Kesiapan Hukum Lima Dimensi (KKH-5) yang mengintegrasikan pengenalan normatif, integrasi tafsir, kesiapan pembuktian, kapasitas institusional, dan respons perlindungan. Model ini mendorong pergeseran dari incident-based interpretation menuju pattern-based interpretation dan menghubungkan deteksi risiko dengan preservasi bukti serta perlindungan korban. Secara praktis, model dapat dikembangkan menjadi matriks norma–modus–bukti, formulir skrining risiko digital, dan SOP rujukan digital forensik bagi Unit PPA.

Keterbatasan penelitian terletak pada jumlah informan empiris yang masih terbatas pada tiga kategori informan kunci di Gorontalo dan pada belum selesainya validasi FGD terhadap KKH-5 pada saat manuskrip ini disusun. Temuan mengenai procedural fatigue juga berasal dari pengalaman korban yang bersifat eksploratif dan tidak dapat digeneralisasi tanpa penelitian tambahan. Penelitian berikutnya perlu melibatkan lebih banyak penyidik, jaksa, hakim, pendamping, ahli teknologi, dan penyintas dari beberapa wilayah; menguji reliabilitas indikator skrining; serta menilai safeguards apabila AI digunakan sebagai alat bantu penilaian risiko. Dengan penguatan tersebut, deteksi dini dapat berkembang sebagai fungsi hukum yang adaptif tanpa mengorbankan asas legalitas, due process, perlindungan data, dan agensi korban.

Acknowledgements

The authors thank the Directorate of Research and Community Service (DPPM) for research support under the 2026 Penelitian Dosen Pemula (PDP) scheme. The authors also acknowledge the law-enforcement officer, legal counsel, and survivor who contributed

information to this study. All empirical identities are anonymised in accordance with the research protocol.

Funding
This research was funded through the 2026 Penelitian Dosen Pemula (PDP) research grant administered by the Directorate of Research and Community Service (DPPM). Grant/contract number: 295/C3/DT.05.00/PL-BARU/2026; 031/M/DST/LL16/AL.04/2026.

Conflicts of Interest
The authors declare no financial, professional, personal, or other conflicts of interest that could have influenced the conduct, analysis, interpretation, or publication of this research.

Author Contributions
Endah Rizki Ekwanto: Conceptualization, Methodology, Funding Acquisition, Investigation, Formal Analysis, Project Administration, Supervision, Validation, Writing – Original Draft, Writing – Review & Editing.
Vicky Ibrahim: Investigation, Data Curation, Formal Analysis, Resources, Validation, Project Administration, Writing – Review & Editing.
Yeti S. Hasan: Formal Analysis, Methodology, Validation, Resources, Writing – Review & Editing.
Parmin Ishak: Formal Analysis, Validation, Visualization, Writing – Review & Editing.
Syalfadilah Kahar: Investigation, Data Curation, Resources, Project Administration, Writing – Review & Editing.
Putry Rahayu Pakaya: Investigation, Data Curation, Resources, Project Administration, Writing – Review & Editing.
All authors contributed to the intellectual development of the manuscript according to their respective roles, reviewed the relevant sections, approved the final version for publication, and agreed to be accountable for their contributions.

Declaration of the Use of AI
The authors used generative AI-assisted tools during the manuscript preparation process solely to support the organization of ideas, language refinement, readability improvement, and preliminary synthesis of the manuscript. Generative AI was not used to generate, alter, fabricate, or manipulate empirical data; conduct interviews; determine research findings; or make autonomous legal interpretations or conclusions.
All empirical findings were derived from the research data collected by the research team, while all legal analyses and interpretations were critically reviewed and validated by the authors. All factual statements, legal interpretations, citations, references, analytical arguments, and final wording were reviewed, verified, corrected where necessary, and approved by the authors. The authors remain fully responsible for the accuracy, integrity, originality, and academic content of the manuscript.

Referensi
Bailey, Louis, Joanne Hulley, Tim Gomersall, Gillian Kirkman, Graham R. Gibbs, and Adele D. Jones. "The Networking of Abuse: Intimate Partner Violence and the Use of Social Technologies." Criminal Justice and Behavior 51, no. 2 (2024): 266–85. https://doi.org/10.1177/00938548231206827.

Bakue, R., S. R. L. Pade, K. Z. Mamu, and Endah Rizki Ekwanto. "Criminological Review of Domestic Violence Against Wife: Case Study of Boalemo Police Station." International Journal of Business, Law, and Education 5, no. 2 (2024): 2732–39. https://doi.org/10.56442/ijble.v5i2.954.

Brown, Andi, Diarmaid Harkin, and Leonie Maria Tanczer. "Safeguarding the 'Internet of Things' for Victim-Survivors of Domestic and Family Violence: Anticipating Exploitative Use and Encouraging Safety-by-Design." Violence Against Women 31, no. 5 (2025): 1039–62. https://doi.org/10.1177/10778012231222486.

Cho, Kyungsuk, Kyuyeon Choi, Yunji Park, Minsoo Kim, Seoyoung Kim, and Doowon Jeong. "DEF-IPV: A Digital Evidence Framework for Intimate Partner Violence Victims." Forensic Science International: Digital Investigation 54 (2025): 301979. https://doi.org/10.1016/j.fsidi.2025.301979.

Cuomo, Dana, and Natalie Dolci. "New Tools, Old Abuse: Technology-Enabled Coercive Control (TECC)." Geoforum 126 (2021): 224–32. https://doi.org/10.1016/j.geoforum.2021.08.002.

Dizon, Michael Anthony C. "Socio-Legal Study of Technology: A Norms and Values Approach to Hacking and Encryption Law and Policy." Computer Law & Security Review 52 (2024): 105958. https://doi.org/10.1016/j.clsr.2024.105958.

Douglas, Heather, Leonie Tanczer, Freya McLachlan, and Bridget A. Harris. "Policing Technology-Facilitated Domestic Abuse (TFDA): Views of Service Providers in Australia and the United Kingdom." Journal of Family Violence 40 (2025): 341–52. https://doi.org/10.1007/s10896-023-00619-2.

Ekwanto, Endah Rizki, and Vicky Ibrahim. "Pendekatan Kriminologi dalam Penanggulangan Tindak Pidana Kekerasan terhadap Perempuan di Kota Gorontalo." At-Tanwir Law Review 5, no. 1 (2025): 302–16. https://doi.org/10.31314/atlarev.v5i1.4317.

Ekwanto, Endah Rizki, Vicky Ibrahim, and Parmin Ishak. "Penguatan Sistem Hukum atas Penyalahgunaan Artificial Intelligence dalam Kekerasan Rumah Tangga melalui Perspektif Kriminologi." Unes Journal of Swara Justisia 9, no. 4 (2026): 673–88. https://doi.org/10.31933/f8341626.

Flynn, Asher, Anastasia Powell, and Sophie Hindes. "Policing Technology-Facilitated Abuse." Policing and Society 33, no. 5 (2023): 575–92. https://doi.org/10.1080/10439463.2022.2159400.

Harris, Bridget A., and Delanie Woodlock. "'You Can't Actually Escape It': Policing the Use of Technology in Domestic Violence in Rural Australia." International Journal for Crime, Justice and Social Democracy 11, no. 1 (2022): 135–48. https://doi.org/10.5204/ijcjsd.2190.

Kim, Chunrye, and Riccardo Ferraresso. "Examining Technology-Facilitated Intimate Partner Violence: A Systematic Review of Journal Articles." Trauma, Violence, & Abuse 24, no. 3 (2023): 1325–43. https://doi.org/10.1177/15248380211061402.

Komisi Nasional Anti Kekerasan terhadap Perempuan. "Siaran Pers Memperingati Hari Kebangkitan Teknologi Nasional 2025: Membangun Ruang Aman Dunia Digital." August 12, 2025. https://komnasperempuan.go.id/siaran-pers-detail/siaran-pers-komnas-perempuan-memperingati-hari-kebangkitan-teknologi-nasional-2025.

Kuo, Shih-Ya, Luyue Zhang, and Kuang-Ming Chang. "Technology-Facilitated Abuse in the Context of Intimate Partner Violence: A Qualitative Study of Women Survivors in Taiwan." Violence Against Women 29, nos. 12–13 (2023): 2464–85. https://doi.org/10.1177/10778012231188093.

Marzuki, Peter Mahmud. Penelitian Hukum: Edisi Revisi. Jakarta: Kencana, 2017.

O'Brien, Wendy, and Marie-Helen Maras. "Technology-Facilitated Coercive Control: Response, Redress, Risk, and Reform." International Review of Law, Computers & Technology 38, no. 2 (2024): 174–94. https://doi.org/10.1080/13600869.2023.2295097.

Polyzoidou, Vagia. "Digital Violence Against Women: Is There a Real Need for Special Criminalization?" International Journal for the Semiotics of Law 37, no. 6 (2024): 1777–97. https://doi.org/10.1007/s11196-024-10179-3.

Qian, Yuzhou, Keng L. Siau, and Fiona F. Nah. "Societal Impacts of Artificial Intelligence: Ethical, Legal, and Governance Issues." Societal Impacts 3 (2024): 100040. https://doi.org/10.1016/j.socimp.2024.100040.

Rogers, Michaela M., Colleen Fisher, Parveen Ali, Peter Allmark, and Lisa Fontes. "Technology-Facilitated Abuse in Intimate Relationships: A Scoping Review." Trauma, Violence, & Abuse 24, no. 4 (2023): 2210–26. https://doi.org/10.1177/15248380221090218.

Stoykova, Adi. "Digital Evidence: Unaddressed Threats to Fairness and the Presumption of Innocence." Computer Law & Security Review 42 (2021): 105575. https://doi.org/10.1016/j.clsr.2021.105575.

Sumarna, Dadang, and Ayyub Kadriah. "Penelitian Kualitatif terhadap Hukum Empiris." Jurnal Penelitian Serambi Hukum 16, no. 2 (2023): 101–13. https://doi.org/10.59582/sh.v16i02.730.

Turner, Emily, Gavin Brown, and Juanjo Medina-Ariza. "Predicting Domestic Abuse (Fairly) and Police Risk Assessment." Psychosocial Intervention 31, no. 3 (2022): 145–57. https://doi.org/10.5093/pi2022a11.

Valdivia, Ana, Cari Hyde-Vaamonde, and Julián García Marcos. "Judging the Algorithm: Algorithmic Accountability on the Risk Assessment Tool for Intimate Partner Violence in the Basque Country." AI & Society 40 (2025): 2633–50. https://doi.org/10.1007/s00146-024-02016-9.

Woodlock, Delanie, Mandy McKenzie, Deborah Western, and Bridget Harris. "Technology as a Weapon in Domestic Violence: Responding to Digital Coercive Control." Australian Social Work 73, no. 3 (2020): 368–80. https://doi.org/10.1080/0312407X.2019.1607510.

Undang-Undang Nomor 23 Tahun 2004 tentang Penghapusan Kekerasan dalam Rumah Tangga.

Undang-Undang Nomor 12 Tahun 2022 tentang Tindak Pidana Kekerasan Seksual.

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.

Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Undang-Undang Nomor 20 Tahun 2025 tentang Kitab Undang-Undang Hukum Acara Pidana.