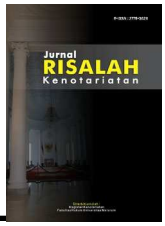
Jurnal Risalah Kenotariatan
Volume 7, Issue 1, January-June 2026
open access at : http://risalah.unram.ac.id
Magister Kenotariatan Fakultas Hukum Universitas Mataram



KEAMANAN SIBER SEBAGAI BAGIAN DARI *DUE PROCESS OF LAW* DALAM PENEGAKAN HUKUM PIDANA

CYBERSECURITY AS PART OF DUE PROCESS OF LAW IN CRIMINAL LAW ENFORCEMENT

Ufran
Fakultas Hukum Universitas Mataram
E-mail: ufran@unram.ac.id

Ahwan
Fakultas Hukum Universitas Mataram
E-mail: ahwan@staff.unram.a.c.id

Abstrak

Digitalisasi penegakan hukum pidana telah menjadikan data pribadi dan bukti digital sebagai fondasi utama dalam proses penyidikan, penuntutan, dan pemeriksaan di pengadilan. Ponsel, metadata komunikasi, rekaman elektronik, serta basis data perkara kini berfungsi sebagai "bahan bakar" proses pidana modern. Namun, kerangka hukum acara dan praktik penegakan hukum masih kerap memposisikan keamanan siber sebagai urusan administratif atau teknis, bukan sebagai bagian dari jaminan prosedural. Akibatnya, kebocoran, manipulasi, dan penyalahgunaan data berpotensi menggerus hak privasi, merusak integritas pembuktian, melemahkan prinsip *fair trial*, serta memicu reviktimisasi korban. Artikel ini menggunakan metode penelitian hukum normatif dengan pendekatan perundang-undangan dan konseptual, serta ditopang kajian perbandingan dan kebijakan internasional. Artikel ini berargumen bahwa keamanan siber merupakan prasyarat esensial *due process of law* dalam penegakan hukum pidana berbasis data. Pemenuhan *due process* tidak cukup dinilai dari legalitas pengumpulan data, tetapi harus mencakup tata kelola keamanan sepanjang siklus hidup data dan bukti digital. Oleh karena itu, artikel ini menawarkan parameter operasional *due process digital* yang menekankan akuntabilitas, auditabilitas, pembatasan akses, perlindungan korban dan saksi, serta mekanisme pemulihan yang efektif.

Kata Kunci: Keamanan Siber; Due Process Of Law; Penegakan Hukum Pidana; Pelindungan Data Pribadi; Bukti Digital.

Abstract

The digitalization of criminal law enforcement has transformed personal data and digital evidence into the core foundation of modern criminal proceedings. Mobile devices, communication metadata, electronic records, and case databases now function as the primary "fuel" of investigation, prosecution, and adjudication. Nevertheless, legal frameworks and law enforcement practices often treat cybersecurity as a merely administrative or technical matter rather than as an integral component of procedural guarantees. This approach exposes criminal justice processes to data breaches, manipulation, and misuse, which may undermine privacy rights, compromise evidentiary integrity, weaken the right to a fair trial, and lead to the re-victimization of victims. This article employs normative legal research through statutory and conceptual approaches, supported by comparative and international policy analysis. It argues that cybersecurity constitutes an essential prerequisite of due process of law in data-driven criminal law enforcement. Compliance with due process cannot be assessed solely by the legality of data collection but must encompass secure and accountable governance throughout the entire lifecycle of digital data and evidence. Accordingly, the article proposes operational parameters of

DOI : https://doi.org/10.29303/risalahkenotariatan.v7i1.432

"digital due process" that emphasize accountability, auditability, access limitation, victim and witness protection, and effective remedial mechanisms.

Keywords: Cybersecurity; Due Process Of Law; Criminal Law Enforcement; Personal Data Protection; Digital Evidence.

A. PENDAHULUAN

Digitalisasi membuat penegakan hukum pidana masuk ke sebuah fase baru: data menjadi infrastruktur utama untuk memahami peristiwa, menelusuri relasi, dan membangun pembuktian. Dalam ekonomi informasi global, arus data pribadi bukan lagi periferal; ia menjadi "nadi" aktivitas sehari-hari dan juga menjadi objek yang diperebutkan dalam konflik regulasi lintas yurisdiksi. Di level internasional, perdebatan mengenai arus data lintas negara kerap disebut sebagai "perang data" karena menyangkut pertaruhan besar antara kepentingan ekonomi, kedaulatan, dan perlindungan hak warga.[1] Pada titik ini, proses pidana yang berbasis data tidak berdiri di ruang hampa: ia selalu berada dalam tarikan kepentingan yang saling mendesak—keamanan publik di satu sisi, dan hak serta kebebasan sipil di sisi lain.

Tegangan itu menjadi semakin tajam karena teknologi komunikasi modern meningkatkan kapasitas negara (dan juga aktor non-negara) untuk melakukan intersepsi, pengumpulan, dan pengawasan data dalam skala yang sebelumnya sulit dibayangkan. Laporan PBB tentang privasi di era digital menggarisbawahi bahwa kemampuan pengawasan kini tidak lagi terbatas oleh skala atau durasi; turunnya biaya teknologi dan penyimpanan data menghapus "penghambat alamiah" yang dulu menahan ekspansi *surveillance*.[2] Akibatnya, praktik pengawasan massal dapat bergeser dari tindakan luar biasa menjadi kebiasaan birokratis—dan ini berimplikasi bukan hanya pada privasi, tetapi juga pada hak-hak lain yang terkait erat dengan kehidupan demokratis.[3] Dalam kacamata negara hukum demokratis, persoalannya bukan semata "apakah negara boleh mengumpulkan data", melainkan bagaimana kekuasaan itu diorganisasi dan dikendalikan agar tidak berubah menjadi dominasi sewenang-wenang. Gutwirth dan De Hert, misalnya, menempatkan privasi sebagai "alat opasitas" untuk melindungi kondisi otonomi individu, sementara kekuasaan publik justru perlu "alat transparansi" agar dapat dipertanggungjawabkan—logika dua arah ini penting untuk membaca ulang desain kebijakan data dalam keamanan publik.[4]

Di ranah *policing*, literatur sejak awal 2000-an sudah memetakan bagaimana peningkatan *computing power*, penyimpanan, akses daring yang dapat di *logging*, dan kemampuan analitik data membentuk "lingkungan operasional" baru bagi aparat.[5] Ketika penegakan hukum menjadi makin bertumpu pada basis data, interoperabilitas sistem, dan kemampuan analitik, muncul persoalan klasik tetapi dalam skala yang berbeda: fragmentasi basis data, duplikasi input, kolasi manual, dan lemahnya

1 Paul M. Schwartz and Karl-Nikolaus Peifer, "Transatlantic Data Privacy Law," *Georgetown Law Journal, UC Berkeley Public Law Research Paper* 106, no. 115 (2017).

2 United Nations High Commissioner for Human Right, "The Right to Privacy in The Digital Age" 12799, no. August (2018).

3 United Nations High Commissioner for Human Right.

4 Serge Gutwirth and Paul De Hert, "Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power," *Direito Público* 18, no. 100 (2022), https://doi.org/https://doi.org/10.11117/rdp.v18i100.6200.

5 Ian Brwon and Douwe Korff, "Technology Development and Its Effect on Privacy & Law Enforcement," *UK Information Commissioner Study Project*, 2004.

kemampuan menautkan informasi antar-sistem.[6] Riset kebijakan tentang *big data policing* menegaskan dua sisi sekaligus: potensi pemanfaatan data "hampir tak terbatas" bila infrastruktur memadai, tetapi justru karena itu dibutuhkan kerangka keputusan etis yang jelas agar pemanfaatan data tidak menabrak hak privasi.[7] Dengan kata lain, "kebutuhan operasional" dan "perlindungan hak" berkembang secara simultan—bukan saling meniadakan, melainkan saling menguji.

Ketegangan makin kompleks ketika analitik data tidak lagi hanya dipakai untuk menjelaskan masa lalu, tetapi untuk memprediksi masa depan. Pada titik ini, problemnya bukan hanya privasi, tetapi juga profiling, bias, dan diskriminasi tidak langsung. Lynskey menunjukkan bahwa perlindungan data dalam konteks *predictive policing* bisa "*precarious*": bahkan apakah sistem itu masuk cakupan hukum perlindungan data dapat tidak pasti dan sangat kontekstual; sementara larangan keputusan otomatis dapat disiasati lewat berbagai pengecualian dan "*statutory footing*".[8] Dari sisi teori tata kelola, Yeung menjelaskan bagaimana big data dapat beroperasi sebagai *regulation by design* melalui "*hypernudge*": pengaturan perilaku yang bersifat sangat personal, dinamis, dan opak, yang problem legitimasi dan akuntabilitasnya tidak selesai hanya dengan "*notice and consent*".[9] Ini penting bagi proses pidana modern karena ekosistem data (platform, broker data, algoritma scoring, perangkat analitik) dapat membentuk keputusan-keputusan penegakan hukum secara halus namun signifikan—sering kali tanpa jejak alasan yang mudah dipahami publik.

Pada fase berikutnya, tegangan beralih ke ruang peradilan. Ketika pengadilan mulai berhadapan dengan alat bantu AI, otomasi, atau sistem digital yang kompleks, ada risiko bahwa "alasan putusan" dan "pemahaman para pihak" tergerus oleh opasitas teknologi. Panduan AI untuk pengadilan menegaskan bahwa *open justice* dapat melemah bila sistem tidak dapat menjelaskan operasi kepada publik atau bahkan kepada hakim; ini berimbas pada akuntabilitas dan efektivitas kontrol melalui mekanisme banding.[10] Di sisi lain, prinsip *open justice* juga berkembang ke arah kewajiban memberi alasan yang *benar-benar dapat diakses publik*, bukan sekadar formalitas—sehingga pembatasan publikasi alasan putusan harus dipahami sebagai pengecualian yang menuntut pembenaran kuat.[11] Dengan demikian, problem *due process* dalam era digital bukan hanya "ada tidaknya kewenangan", tetapi juga bagaimana keputusan dapat ditelusuri, diuji, dan dipertanggungjawabkan di hadapan publik.

Akhirnya, isu data dalam penegakan hukum tidak selalu berhenti pada privasi dan keamanan negara: ia juga menyentuh risiko eksklusi dan kerentanan kelompok tertentu. Literatur tentang identitas digital mengingatkan bahwa teknologi identifikasi sering dipromosikan sebagai solusi netral untuk inklusi, padahal dalam praktiknya dapat melahirkan eksklusi baru ketika bertemu dengan realitas politik-ekonomi

---

6 Alexander Babuta, "Big Data and Policing An Assessment of Law Enforcement Requirements, Expectations and Priorities" (London, 2017).

7 Babuta."title":"Big Data and Policing An Assessment of Law Enforcement Requirements, Expectations and Priorities"

8 Orla Lynskey, "Criminal Justice Profiling and EU Data Protection Law : Precarious Protection from Predictive Policing," *International Journal of Law in Context* 15, no. 2 (2019): 162–76, https://doi.org/10.1017/S1744552319000090.

9 Karen Yeung, "'Hypernudge': Big Data as a Mode of Regulation by Design," *Information, Communication & Society* 20, no. 1 (2017): 118–36, https://doi.org/10.1080/1369118X.2016.1186713.

10 Jake Silove and Monika Zalnieriute Felicity Bell, Lyria Bennett Moses, Michael Legg, "AI Decision-Making and the Courts A Guide for Judges, Tribunal Members and Court Administrators" (New South Wales, 2022).

11 Jason Bosland and Jonathan Gill, "The Principle of Open Justice and The Judicial Duty to Give Public Reasons," *Melbourne University Law Review* 38, no. 482 (2014): 482–524.

identitas, kapasitas institusi, dan praktik diskriminatif.[12]Bahkan gagasan "identifikasi demi pelayanan" bisa berubah menjadi "identifikasi demi kontrol" bila tata kelola data lemah. Dalam konteks penegakan hukum pidana, ini relevan karena akses terhadap mekanisme pengaduan, pemulihan, atau pembelaan dapat ikut dipengaruhi oleh akses digital, literasi, dan status identitas—yang pada akhirnya berkaitan dengan kualitas perlindungan prosedural yang diterima warga.

Dari sintesis persoalan tersebut, terlihat bahwa problem utama bukan memilih salah satu kubu (privasi vs penegakan hukum), melainkan merumuskan cara pandang yang lebih matang: perlindungan data pribadi dan keamanan siber perlu dipahami sebagai prasyarat prosedural untuk menjaga integritas proses pidana, sekaligus mencegah kekuasaan berbasis data berkembang tanpa kontrol demokratis. Di tingkat global, perdebatan arus data lintas batas dan *cloud* menunjukkan bahwa desain akses data penegakan hukum harus mempertimbangkan insentif dan dampak samping: rezim akses yang tidak adaptif dapat mendorong fragmentasi internet (*splinternet*), memperkuat dorongan lokalisasi data, dan pada akhirnya membuat data "kurang aman".[13] Sederhananya, konseptualisasi "keamanan siber sebagai bagian dari *due process*" dibangun dari realitas bahwa proses pidana modern beroperasi dalam ekosistem data yang rentan: rentan terhadap *abuse*, rentan terhadap opasitas, rentan terhadap bias, dan rentan terhadap kegagalan tata kelola.

Sintesis persoalan pada bagian sebelumnya menunjukkan bahwa ketegangan antara pelindungan data pribadi dan kebutuhan penegakan hukum bukan sekadar soal "boleh atau tidak boleh" mengakses data, melainkan soal bagaimana kekuasaan berbasis data diorganisasi, dibatasi, dan dipertanggungjawabkan. Dari sini, terdapat beberapa *gap* yang perlu dijelaskan lebih tajam.

Pertama, masih terdapat *gap* konseptual dalam cara keamanan siber diposisikan dalam hukum pidana. Banyak diskursus menempatkan keamanan siber sebagai isu administratif dan teknis organisasi, sementara literatur hukum menunjukkan bahwa pemrosesan data oleh aparat merupakan bentuk *interference* terhadap hak privat yang menuntut dasar hukum yang jelas, tujuan sah, serta pembatasan berbasis *necessity–proportionality dan purpose limitation*.[14] Ketika konsep-konsep ini tidak diterjemahkan ke dalam tata kelola keamanan data (kerahasiaan, integritas, ketersediaan, dan akuntabilitas), "kebenaran prosedural" menjadi rapuh: tindakan pengambilan data bisa sah, tetapi pemrosesan dan penyimpanan yang tidak aman dapat mencederai keadilan prosedural dan hak pihak-pihak yang berperkara. Dalam konteks ini, kritik klasik Stuntz tentang risiko menjadikan privasi sebagai retorika tunggal tanpa desain kontrol yang konsisten tetap relevan: doktrin sering "menyelamatkan diri" melalui pengecualian, sehingga perlindungan yang seharusnya substantif berpotensi menjadi formalitas.[15]

Kedua, terdapat *gap* operasional berupa ketiadaan indikator yang dapat diaudit untuk menjembatani prinsip-prinsip perlindungan data dengan kebutuhan pembuktian pidana. Studi kebijakan menunjukkan bahwa keterbatasan bukan hanya pada norma, tetapi juga pada infrastruktur dan tata kelola: fragmentasi basis data, interoperabilitas yang lemah, serta ketergantungan pada kolasi manual membuat penggunaan data

12 Christoph Sperfeldt, "Digital Exclusions: Legal Identity, Identification, and the Sustainable Development Goals in Southeast Asia," 2023.

13 Reema Shah, "Law Enforcement and Data Privacy : A Forward-Looking Approach," *The Yale Law Journal* 125, no. 543 (2015): 543–58.

14 Council of Europe, *Practical Guide on the Use of Personal Data in the Police Sector* (Strasbourg: Directorate General of Human Rights and Rule of Law, 2018).

15 William J. Stuntz, "Privacy's Problem and the Law of Criminal Procedure," *Michigan Law Review* 93, no. 5 (1995).

rawan salah sasaran dan menyulitkan akuntabilitas.[16] Pada saat yang sama, literatur keamanan siber menegaskan bahwa perlindungan informasi minimal harus menjamin *confidentiality, integrity,* dan *availability* (CIA triad).[17] Namun, "bahasa CIA" ini belum secara memadai dipakai sebagai indikator *due process* digital yang dapat diukur melalui kontrol akses berbasis peran, *audit trail*, *chain of custody* digital, retensi/penghapusan terukur, dan mekanisme redaksi/anonimisasi untuk melindungi korban dan saksi.

Ketiga, terdapat *gap* akuntabilitas dan transparansi dalam penggunaan teknologi kompleks (termasuk AI dan analitik big data) pada ekosistem peradilan pidana. Literatur tentang AI di pengadilan menekankan bahwa *open justice* dan akuntabilitas dapat melemah ketika proses pengambilan keputusan tidak dapat dipahami oleh publik, para pihak, bahkan hakim; "*black box*" melemahkan efektivitas mekanisme tradisional seperti banding dan kewajiban memberi alasan.[18] Di level kebijakan, Yeung menunjukkan bahwa *big data analytics* dapat berfungsi sebagai *hyper nudge*—regulasi berbasis desain yang opak dan sangat kuat—yang problem legitimasi dan akuntabilitasnya tidak cukup dijawab oleh model *notice-and-consent*.[19] Gap ini penting karena penegakan hukum pidana yang semakin "*data-driven*" berpotensi bergeser dari pola pembuktian yang dapat diuji, menuju pola manajemen risiko yang sulit diawasi.

Keempat, terdapat *gap* perlindungan terhadap kelompok rentan yang muncul dari digitalisasi. Diskursus identitas digital mengingatkan bahwa proyek identifikasi yang dianggap netral dapat menghasilkan eksklusi baru ketika bertemu dengan realitas diskriminasi birokrasi, status kewarganegaraan, atau kapasitas institusi; sehingga digitalisasi bisa memperdalam kerentanan bagi kelompok tertentu.[20] Dalam konteks pidana, persoalan ini berkait langsung dengan kualitas *due process*: siapa yang mampu mengakses mekanisme pembelaan, pemulihan, dan perlindungan, serta siapa yang justru menjadi lebih mudah "ditangkap" oleh sistem berbasis data.

Kelima, terdapat *gap* transnasional yang makin menonjol akibat *cloud computing*, enkripsi, dan arus data lintas negara. Literatur menunjukkan bahwa akses bukti digital lintas batas memicu konflik yurisdiksi dan mendorong dua risiko ekstrem: negara memaksakan akses ekstrateritorial (mengganggu comity dan kedaulatan) atau sebaliknya mendorong lokalisasi data dan fragmentasi internet.[21] Dalam situasi ini, *due process* digital memerlukan desain yang lebih matang: prosedur akses data yang sah, standar *safeguards* yang dapat ditegakkan, dan kerangka kerja sama lintas yurisdiksi—bukan sekadar perluasan kewenangan.

Bertolak dari *gap-gap* tersebut, artikel ini menempatkan keamanan siber bukan sebagai isu teknis terpisah, melainkan sebagai komponen jaminan prosedural yang menghubungkan pelindungan data pribadi, reliabilitas bukti digital, akuntabilitas aparatur, dan perlindungan korban/saksi dalam penegakan hukum pidana berbasis data.

Berdasarkan latar belakang dan *gap* tersebut, konstruksi bahasan dalam artikel ini didasarkan pada rumusan masalah:

1. Bagaimana konstruksi konseptual keamanan siber sebagai bagian dari *due process of law* dalam penegakan hukum pidana berbasis data digital?

16 Babuta, "Big Data and Policing An Assessment of Law Enforcement Requirements, Expectations and Priorities.

17 Jeff Kosseff, "Defining Cybersecurity Law," *Iowa Law Review* 103, no. 985 (2018): 985–1031.

18 Felicity Bell, Lyria Bennett Moses, Michael Legg, "AI Decision-Making and the Courts A Guide for Judges, Tribunal Members and Court Administrators."

19 Yeung, "'Hypernudge': Big Data as a Mode of Regulation by Design."

20 Sperfeldt, "Digital Exclusions: Legal Identity, Identification, and the Sustainable Development Goals in Southeast Asia."

21 Shah, "Law Enforcement and Data Privacy : A Forward-Looking Approach."

2. Parameter/indikator apa yang dapat dipakai untuk menilai pemenuhan *due process* pada pengumpulan, penyimpanan, dan penggunaan data/bukti digital?
3. Apa implikasi normatif dan kebijakan (perlindungan data pribadi, akuntabilitas aparat, dan perlindungan korban) bagi pembaruan hukum serta praktik penegakan hukum pidana?

Secara teoretik, artikel ini bertujuan memperluas pemahaman *due process of law* agar mencakup domain keamanan siber—bukan semata urusan teknis, melainkan jaminan prosedural yang menentukan reliabilitas pembuktian, perlindungan privasi, dan akuntabilitas kekuasaan. Secara praktis, artikel ini bertujuan merumuskan indikator operasional "due process digital" untuk SOP penanganan data dan bukti digital (misalnya kontrol akses, audit trail, chain of custody digital, retensi/penghapusan, dan perlindungan data korban/saksi), sehingga standar minimal keamanan siber benar-benar menjadi bagian dari tata kelola penegakan hukum pidana.

B. METODE

Penelitian ini merupakan penelitian hukum normatif (*doctrinal legal research*) yang berfokus pada kajian norma, asas, dan doktrin hukum untuk menilai bagaimana keamanan siber dapat diposisikan sebagai bagian integral dari *due process of law* dalam penegakan hukum pidana berbasis data digital. Pendekatan ini relevan karena perluasan kewenangan pengumpulan dan pengolahan data oleh aparat penegak hukum menuntut penilaian atas batas-batas kekuasaan negara serta jaminan perlindungan terhadap individu—isu yang secara klasik berada dalam wilayah kajian *due process of law*.[22] Penelitian ini menggunakan pendekatan perundang-undangan (*statute approach*) dan pendekatan konseptual (*conceptual approach*). Pendekatan perundang-undangan digunakan untuk mengkaji pengaturan mengenai data pribadi, bukti elektronik, dan kewenangan penegakan hukum, terutama yang berkaitan dengan perlindungan data dan keamanan pemrosesannya. Pendekatan konseptual digunakan untuk membangun argumentasi bahwa keamanan siber tidak dapat direduksi menjadi persoalan teknis, melainkan merupakan jaminan prosedural yang menentukan sah atau tidaknya proses pidana secara substansial.[23]

Analisis dilakukan dalam tiga tahap. ***Pertama***, dilakukan analisis konseptual terhadap due process of law untuk mengidentifikasi unsur-unsur jaminan prosedural yang relevan dalam konteks digital, termasuk privasi, fair trial, akuntabilitas, dan perlindungan korban.[24] ***Kedua***, dilakukan analisis normatif terhadap pengaturan perlindungan data dan keamanan informasi untuk menilai sejauh mana prinsip-prinsip tersebut telah atau belum terintegrasi sebagai standar prosedural dalam penegakan hukum pidana.[25] ***Ketiga***, dilakukan analisis preskriptif untuk merumuskan indikator operasional keamanan siber yang dapat digunakan sebagai alat uji pemenuhan *due process of law* dalam pengelolaan data dan bukti digital. Penelitian ini dibatasi pada kajian normatif mengenai keamanan siber dalam penegakan hukum pidana, khususnya pada tahap pengumpulan, penyimpanan, dan penggunaan data atau bukti digital oleh aparat penegak hukum. Penelitian tidak dimaksudkan untuk menilai efektivitas teknis sistem keamanan tertentu atau melakukan evaluasi empiris terhadap institusi tertentu.

22 Herbert L. Packer, *The Limits of the Criminal Sanction*, *Stanford University Press* (Stanford, California, 1969).

23 Satjipto Rahardjo, *Ilmu Hukum* (Bandung: Citra Aditya Bakti, 2014).

24 Felicity Bell, Lyria Bennett Moses, Michael Legg, "AI Decision-Making and the Courts A Guide for Judges, Tribunal Members and Court Administrators."

25 Kosseff, "Defining Cybersecurity Law."

Fokus utama adalah pada konstruksi hukum dan implikasi normatif dari penempatan keamanan siber sebagai bagian dari *due process of law*, sehingga hasil penelitian diharapkan dapat diterapkan secara umum dalam kerangka pembaruan hukum dan tata kelola penegakan hukum pidana di Indonesia.

C. ANALISIS DAN PEMBAHASAN

1. Konstruksi Keamanan Siber Sebagai Bagian Dari *Due Process of Law*

Evolusi *due process of law* dalam penegakan hukum pidana pada mulanya bertumpu pada pengendalian tindakan-tindakan fisik negara—penangkapan, penggeledahan, penyitaan, penahanan—agar tidak sewenang-wenang dan tetap dapat diuji melalui mekanisme pengawasan serta upaya hukum. Namun, digitalisasi proses pidana mengubah "lokasi" utama risiko: bukan lagi semata pada tindakan fisik aparat, melainkan pada akses, pemrosesan, dan penyimpanan data yang menjadi fondasi pembuktian. Di sinilah *due process* perlu "bermigrasi" ke domain digital: karena tindakan koersif modern dapat berbentuk penguasaan data (ekstraksi, korelasi, penyimpanan, dan distribusi akses), yang dampaknya terhadap privasi dan *fairness* bisa sama atau bahkan lebih berat dibanding tindakan fisik.

Kondisi tersebut terlihat dari praktik kepolisian modern yang semakin ditopang oleh infrastruktur data: basis data besar, integrasi lintas sistem, dan analitik. Di Inggris misalnya, Babuta menggambarkan bagaimana data penegakan hukum tersebar pada banyak basis data yang terfragmentasi sehingga petugas harus memasukkan dan mengkolasi data berulang-ulang; ini menciptakan dorongan kuat pada integrasi dan sistem yang memungkinkan pencarian lintas-basis data.[26] Pada titik tertentu, problemnya bukan lagi "boleh mengumpulkan atau tidak", melainkan "bagaimana data itu dikelola" agar tidak memproduksi kekuasaan yang tak terlihat, tak terkendali, dan sulit diuji. Dalam bahasa Yeung, analitik Big Data dapat bekerja sebagai "mode regulasi berbasis desain" (*design-based regulation*) yang mampu mengarahkan perilaku/keputusan secara halus namun sangat kuat; kritik *rights-based* menjadi relevan ketika transparansi dan akuntabilitas desain tidak memadai.[27] Maka, ketika penegakan hukum mulai mengandalkan ekosistem data dan analitik, *due process* tidak cukup hanya "legalitas kewenangan awal", tetapi harus mencakup tata kelola terhadap siklus hidup data.

Berdasarkan hal ini, konstruksi argumen dalam artikel ini tetap sama dan mempertegas: keamanan siber adalah prasyarat legalitas prosedural dalam penegakan hukum pidana berbasis data. Legalitas pengambilan data (misalnya penyitaan perangkat atau perintah pemblokiran) tidak otomatis menjamin *due process* apabila data yang sudah berada dalam penguasaan negara kemudian dikelola secara tidak aman: bocor, diakses pihak tak berwenang, dimodifikasi, atau tidak dapat dipertanggungjawabkan riwayatnya. Literatur *legal aspects of cybersecurity* mengingatkan bahwa bukti elektronik bersifat volatil dan mudah terkontaminasi; karena itu praktik forensik menuntut pembuatan salinan *bit-for-bit* untuk mencegah perubahan pada data asli, serta penggunaan *Hash Kriptografis* sebagai "tanda tangan digital" guna mendeteksi perubahan.[28] Jika *due process* menuntut pembuktian yang dapat diuji (*contestable*), maka standar teknis seperti

26 Babuta, "Big Data and Policing An Assessment of Law Enforcement Requirements, Expectations and Priorities."
27 Yeung, "'Hypernudge': Big Data as a Mode of Regulation by Design."
28 Artur Appazov, "Legal Aspects of Cybersecurity" (Copenhagen, 2014).

hashing dan *audit trail* bukan "urusan lab semata", melainkan bagian dari jaminan prosedural atas integritas bukti.

Pada level prinsip HAM dan *data protection*, pengalaman Eropa memberi formulasi yang sangat membantu untuk membumikan *due process digital*. Bignami menunjukkan bahwa penyimpanan dan pemrosesan data pribadi untuk tujuan penanggulangan kejahatan merupakan *interference* terhadap hak privat dan karenanya harus memenuhi syarat: dasar hukum yang aksesibel dan cukup presisi untuk mencegah kesewenang-wenangan, tujuan yang sah, dan proporsionalitas.[29] Dalam rezim retensi data, Bignami juga menekankan pentingnya pembatasan: jumlah data dan lamanya penyimpanan tidak boleh melebihi kebutuhan tujuan; harus ada *security precautions* agar data digunakan hanya oleh entitas dan untuk tujuan semula; dan individu perlu memiliki hak untuk memeriksa akurasi dan kepatuhan pemrosesan.[30]

Penguatan yang sangat penting datang dari doktrin *necessity* yang ketat dalam hukum pelindungan data modern. Dalam *Handbook on the Language of Data Protection* (yang mengutip putusan CJEU terkait retensi data), ditegaskan bahwa meski tujuan pemberantasan kejahatan serius sangat penting, hal itu tidak otomatis membuat retensi data berskala luas menjadi "perlu"; pembatasan/derogasi atas perlindungan data hanya boleh sejauh "*strictly necessary*", dan retensi yang menyapu semua orang/semua sarana komunikasi tanpa diferensiasi menimbulkan interferensi yang sangat luas.[31] Dokumen yang sama menyoroti cacat kebijakan retensi ketika tidak ada kriteria objektif mengenai batas akses otoritas dan syarat prosedural-substantif atas akses serta penggunaan data.[32] Hal ini kompatibel dengan proposisi awal: *due process* menuntut batasan akses yang terukur, syarat prosedural yang jelas, dan jejak akuntabilitas—bukan sekadar kewenangan umum.

Dimensi lain yang sering luput dalam diskusi domestik adalah fakta bahwa penegakan hukum berbasis data semakin terkait dengan arus data lintas batas (*cloud*, layanan global, dan penyimpanan di yurisdiksi berbeda). Schwartz dan Peifer menyebut bahwa transfer data internasional merupakan "urat nadi ekonomi digital" dan perbedaan rezim perlindungan data dapat mengancam aliran data penting ini—bahkan memicu "perang data" transatlantik.[33] Dalam konteks penegakan hukum, problem serupa muncul: bagaimana negara mengakses data yang disimpan di luar wilayahnya tanpa merusak kedaulatan, hak privat, dan kepercayaan publik.

McQuinn dan Castro menggunakan contoh perkara Microsoft Ireland untuk menunjukkan "retakan" dalam kerangka akses data lintas batas; jika dibiarkan, ia bisa menghambat penegakan hukum atau mendistorsi pasar layanan digital global.[34] OECD, jauh lebih awal, juga menekankan bahwa meningkatnya arus data lintas batas mengangkat risiko privasi dan membuat pelanggaran keamanan data (*security breaches*) semakin mungkin terjadi dengan dimensi lintas negara; perlindungan privasi bergantung pada kerja sama lintas batas yang lebih sistematis.[35]

---

29 Francesca Bignami, "Privacy and Law Enforcement in the European Union : The Data Retention Directive Privacy and Law Enforcement in the European Union : The Data Retention Directive," *Chicago Journal of International Law* 8, no. 1 (2007).

30 Bignami.

31 Isabel Alice Walbaum Robinson, ed., *Handbook on the Language of Data Protection* (Brussel: European Judicial Training Network (EJTN), 2019).

32 Isabel Alice Walbaum Robinson, hlm. 72.

33 Peifer, "Transatlantic Data Privacy Law."

34 Alan Mcquinn and Daniel Castro, "How Law Enforcement Should Access Data Across Borders" (Washington DC, 2017).

35 OECD, "Report on the Cross-Border Enforcement of Privacy Law" (Paris, 2006), https://doi.org/http://dx.doi.org/10.1787/231304814207.

Pada akhirnya, mengapa semua ini harus dibaca sebagai isu *abuse of power* dan akuntabilitas, bukan sekadar IT? Karena infrastruktur data yang makin terintegrasi dan opak memperlebar peluang "kekuasaan tanpa jejak." Brown dan Korff sudah mengingatkan sejak awal 2000-an bahwa ada ledakan data pribadi yang dihasilkan/ditahan/tersedia, persoalan praktis membatasi koleksi dan retensi, menipisnya pemisahan fungsional antar-entitas publik, serta absennya transparansi dalam koleksi-retensi data—dan bahkan problem "consent" yang tidak *workable* dalam konteks tersebut.[36] Dalam konteks penegakan hukum, ketertutupan dan "kolaborasi rahasia" juga dapat menggerus legitimasi. Shah menegaskan perlunya rezim yang lebih terbuka: *disclosure* harus produk *court orders* dengan ruang lingkup yang ditentukan undang-undang, sehingga menutup era "*secret cooperation*"; ia juga menekankan kebutuhan *minimization requirements* untuk membatasi koleksi/retensi/diseminasi informasi privat.[37]

Dengan demikian, konstruksi yang ditawarkan artikel ini tetap konsisten: keamanan siber adalah bagian inheren dari *due process of law* dalam penegakan hukum pidana berbasis data karena ia menjalankan tiga fungsi prosedural sekaligus—(i) membatasi dan mengarahkan penggunaan kekuasaan negara atas data (*legal basis, necessity–proportionality, minimization/retention*), (ii) menjaga reliabilitas pembuktian (integritas bukti melalui *forensic soundness, hashing*, dan jejak audit), dan (iii) memastikan akuntabilitas serta *fairness* (transparansi penggunaan, kontrol akses, dan pencegahan penyalahgunaan kewenangan).

2. Parameter Pemenuhan Due Process of Law Pada Siklus Data/ Bukti Digital

Jika *due process of law* dipahami sebagai jaminan bahwa kekuasaan negara bekerja secara sah, terukur, dan dapat diuji, maka pada penegakan hukum pidana berbasis data, "uji *due process*" harus dibaca sepanjang siklus hidup data/bukti digital: dari pengumpulan, pemrosesan, penyimpanan, penggunaan, berbagi, hingga retensi dan penghapusan. Di titik ini, ukuran *due process* tidak cukup berhenti pada ada/tidaknya kewenangan mengambil data, tetapi pada kualitas tata kelola yang menjaga kerahasiaan, integritas, ketersediaan, serta akuntabilitas penggunaan data.[38]

Panduan Dewan Eropa untuk sektor kepolisian menegaskan bahwa pemrosesan data pribadi untuk penegakan hukum adalah bentuk *interference* terhadap hak privat; karenanya harus berbasis hukum yang jelas dan dibatasi oleh *necessity* serta *proportionality*, sekaligus terikat pada *purpose limitation* dan *accountability* (kepatuhan yang dapat dibuktikan).[39] Prinsip yang sama muncul dalam praktik "*good governance*" pemrosesan data sensitif untuk penegakan hukum: uji "*strict necessity and proportionality*" dilakukan sebelum memproses data sensitif dan hasilnya harus terdokumentasi; bila tujuan dapat dicapai melalui cara lain (misalnya minimisasi, anonimisasi, atau memakai data non-sensitif), pemrosesan sensitif seharusnya tidak dilakukan.[40] Dengan kerangka itu, indikator *due process digital* dapat dirumuskan secara operasional sebagai berikut.

a. Indikator Pada Tahap Pengumpulan (*Collection*)

1. Legal basis & purpose limitation

36 Korff, "Technology Development and Its Effect on Privacy & Law Enforcement."
37 Shah, "Law Enforcement and Data Privacy : A Forward-Looking Approach."
38 Jeff Kosseff, "Hacking Cybersecurity Law," *University of Illinois Law Review* 2020 (2019): 811–50.
39 Council of Europe, *Practical Guide on the Use of Personal Data in the Police Sector*.
40 Home Office, "Data Protection Legislation Policy on Sensitive Processing for Law Enforcement Purposes, under Part 3 DPA (2018)" (UK, 2021).

Pengumpulan data harus memiliki dasar hukum yang jelas dan tujuan yang spesifik serta sah; tujuan tersebut harus menjadi "pagar" bagi pemrosesan berikutnya. Panduan CoE menekankan bahwa investigator perlu menguji "mengapa data perlu dikumpulkan" dan "untuk tujuan apa"; contoh praktisnya, telephone billing semestinya dibatasi pada nomor dan rentang waktu yang relevan, bukan dikumpulkan secara menyeluruh.[41] Pada titik ini, due process menuntut pemrosesan yang "tidak melebar" menjadi pengumpulan data untuk kepentingan umum yang tidak terkait perkara.

2. Necessity–proportionality & minimization

   Indikator berikutnya adalah apakah pengumpulan dilakukan secukupnya, tidak berlebihan. CoE menegaskan data harus "*adequate*, *relevant*, *non-excessive*"; dan jika tujuan bisa dicapai tanpa memproses data tertentu, maka data itu tidak seharusnya diproses.[42] Logika "*strict necessity*" ini juga menjadi inti dokumen APD (UK) untuk *law enforcement*: bila tujuan dapat dicapai dengan cara lain yang kurang intrusif, pemrosesan data sensitif harus dihindari dan keputusan itu harus dicatat.[43]

3. Kategorisasi subjek & perlindungan pihak rentan (victim/witness safeguards).

   Pengumpulan data yang menyangkut korban/saksi dan pihak ketiga membutuhkan kehati-hatian tambahan. CoE menganjurkan pembedaan kategori subjek data (suspect, convicted, victim, witness/third parties) agar perlakuan dan pembatasan aksesnya jelas.[44] Literatur perlindungan saksi juga menunjukkan bahwa perlindungan identitas (misalnya distorsi wajah/suara, videoconferencing, atau withholding identity) adalah bagian dari perlindungan proses pidana; artinya, data identitas saksi harus diperlakukan sebagai **data berisiko tinggi** yang memerlukan kontrol ekstra.[45]

b. Indikator Pada Tahap Preservasi & Forensik (*Preservation/Forensics*)

1. Forensic *soundness: bit-for-bit copy & hashing*

   Due process pada bukti digital sangat bergantung pada integritas. Appazov menekankan bahwa forensik digital bertujuan memulihkan bukti yang mudah terkontaminasi; praktik yang lazim adalah membuat salinan *bit-for-bit* agar data asli tidak berubah, dan menggunakan *cryptographic hashes* untuk mendeteksi perubahan.[46] Ini bukan sekadar "standar lab", melainkan indikator prosedural: jika bukti digital tidak dipreservasi secara forensik, reliabilitas pembuktian dapat dipersoalkan dan fairness terancam.

2. Digital chain of custody & audit trail (riwayat penguasaan & akses).

   Selain integritas file, *due process* menuntut jejak siapa yang mengakses, kapan, untuk apa. Dalam konteks forensik cloud, *chain of custody* dipahami sebagai dokumentasi kronologis cara bukti dikumpulkan, dipreservasi, dan dianalisis—dan tantangan cloud membuat pengaturan ini makin penting.[47] APD *law enforcement* juga menekankan tata kelola keamanan: sistem harus mencegah data korup dan

41 Council of Europe, *Practical Guide on the Use of Personal Data in the Police Sector*.
42 Council of Europe.
43 Home Office, "Data Protection Legislation Policy on Sensitive Processing for Law Enforcement Purposes, under Part 3 DPA (2018)."
44 Council of Europe, *Practical Guide on the Use of Personal Data in the Police Sector*.
45 UNODC, *Good Practices for the Protection of Witnesses in Criminal Proceedings Involving Organized Crime* (New York: UNODC, 2008).
46 Appazov, "Legal Aspects of Cybersecurity."
47 Alex Akinbi James Baldwin, Omar M. K. Alhawi, Simone Shaughnessy and and Ali Dehghantanha, "Emerging from the Cloud: A Bibliometric Analysis of Cloud Forensics Studies," in *Cyber Threat Intelligence*, ed. Mauro Conti, Ali Dehghantanha and Tooska Dargahi (Cham: Springer, 2018).

memiliki monitoring/standar keamanan, termasuk pelatihan dan kontrol otorisasi.[48] Kombinasi *chain of custody* dan *audit trail* menjawab isu klasik *abuse of power*: tanpa jejak, kekuasaan atas data cenderung tidak teruji.

c. Indikator Pada Tahap Penyimpanan & Pengamanan (*Storage/Security Controls*)

1. CIA triad sebagai "***minimum procedural guarantees***".

   Kosseff mengingatkan bahwa hukum keamanan siber tidak boleh hanya fokus pada kerahasiaan, tetapi juga integritas dan ketersediaan.[49] Dalam konteks bukti digital, CIA triad dapat menjadi indikator minimum: kerahasiaan mencegah kebocoran data perkara (terutama korban/saksi), integritas menjaga bukti bebas manipulasi, dan ketersediaan memastikan akses terotorisasi berjalan reliabel untuk proses pembuktian dan pembelaan.
2. Access control berbasis peran (role-based access) & "need to know".

   Kerangka *governance policing* menekankan pembatasan akses berbasis kebutuhan tugas—semakin sensitif data, semakin ketat aksesnya.[50] Ini indikator penting karena banyak pelanggaran data bukan berasal dari "ketiadaan norma", melainkan lemahnya pembatasan akses dan disiplin internal.
3. Enkripsi & keamanan transmisi.

   Literatur keamanan siber menempatkan enkripsi sebagai kontrol fundamental untuk menjaga kerahasiaan data saat disimpan dan dikirim. Dalam perangkat kebijakan penegakan hukum, keamanan sistem diposisikan untuk mencegah akses tidak sah dan menjaga integritas data.[51] Ketika data bukti bergerak lintas perangkat, jaringan, atau cloud, enkripsi dan pengamanan transmisi menjadi indikator *due process*: tanpa itu, negara gagal menjaga standar kehati-hatian terhadap data yang ia paksa ambil dari warga.

d. Indikator pada Tahap Penggunaan & Pengambilan Keputusan (*Use/Decision-Making*)

1. Purpose-limited use & larangan "function creep"

   Salah satu risiko terbesar penegakan hukum berbasis data adalah *function creep*—data yang dikumpulkan untuk satu tujuan dipakai ulang untuk tujuan lain. Artikel tentang perbedaan rezim GDPR dan LED dalam *security research* menunjukkan "garis batas" antara pemrosesan untuk investigasi/prosecution dan pemrosesan untuk riset/pengembangan teknologi sering kabur; ketidakjelasan ini berisiko menimbulkan salah penerapan safeguards atau pengabaian *safeguards* sama sekali.[52] Sebagai indikator *due process*, setiap penggunaan ulang harus diuji kompatibilitas tujuannya, dasar hukum, serta mekanisme akuntabilitasnya.
2. Kejelasan alasan (reasons-giving) & auditabilitas, terutama saat memakai otomasi/AI.

   Dalam lingkungan digital, fairness menuntut bukan hanya hasil yang adil, tetapi proses yang bisa dipahami dan diuji. Laporan *AI Decision-Making and the*

48 Home Office, "Data Protection Legislation Policy on Sensitive Processing for Law Enforcement Purposes, under Part 3 DPA (2018)."

49 Kosseff, "Defining Cybersecurity Law."

50 Northern Ireland Policing Board, "Human Rights Review of Privacy and Policing," 2023.

51 Richard D. Alexander and Srinivas Panguluri, "Cybersecurity Terminology and Frameworks," in *Cyber-Physical Security Protecting Critical Infrastructure at the State and Local Level*, ed. Simon Hakim, Robert M. Clark (Switzerland: Springer Nature, 2017), 19–48.

52 Stergios Aidinlis et al., "Between GDPR and Law Enforcement Directive in Security Research : The Use of Personal Data by Law Enforcement Authorities," *European Journal of Law and Technology* 15, no. 3 (2024).

Courts menekankan bahwa ketika sistem terlalu opak (*black box*), *open justice* dan akuntabilitas melemah karena hakim/para pihak sulit memahami dasar output.[53] Prinsip "*public reasons*" juga mengingatkan bahwa legitimasi putusan berhubungan dengan alasan yang dapat diakses dan diuji; penahanan atau penutupan alasan harus tunduk pada uji *necessity* yang ketat.[54] Meski konteksnya peradilan, logika ini paralel untuk penegakan hukum: bila analitik atau sistem digital dipakai untuk menetapkan prioritas, risiko, atau tindakan, prosesnya harus *auditable* dan dapat dijelaskan—minimal pada tingkat yang memungkinkan pengujian hukum.

e. Indikator pada Tahap Berbagi Data & Akses Lintas Batas (*Sharing/Cross-Border Access*)

1. Legal ***instrument*** & "***appropriate safeguards***" untuk transfer lintas yurisdiksi.

Dalam praktik internasional, akses data lintas batas menjadi kebutuhan hampir tak terhindarkan. OECD menekankan arus data lintas negara meningkatkan risiko privasi dan *data security breaches*, sehingga perlindungan efektif membutuhkan kerja sama lintas batas.[55] EDPB menegaskan untuk transfer data *law enforcement*, *safeguards* harus memastikan tingkat perlindungan yang "*essentially equivalent*"; perjanjian mengikat secara hukum dipandang memberi kepastian, transparansi, dan konsistensi.[56] Indikator *due process* pada tahap ini: ada/tiada perjanjian yang *enforceable*, mekanisme *redress*, batas tujuan, serta audit atas transfer dan penerimaan data.

***2. Cloud* & lokasi data tidak lagi memadai sebagai basis tunggal akses**

Shah menunjukkan bahwa *cloud computing* dan *encryption* mengubah medan akses data; bergantung pada lokasi fisik server makin tidak masuk akal, dan rezim *warrant* perlu reformasi agar tetap efektif tanpa merusak privasi dan trust.[57] Ini relevan sebagai indikator *due process*: prosedur akses harus menyesuaikan realitas teknis (*cloud/e2ee*) namun tetap mengunci kontrol legal dan keamanan.

f. Indikator pada Tahap Retensi, Penghapusan, dan Pemulihan (*Retention/Erasure/Remedy*)

1. Retention **&** *deletion* terukur **(***storage limitation***).**

CoE menegaskan data yang tidak lagi diperlukan setelah analisis **tidak boleh terus diproses**.[58] Dalam kerangka *due process*, retensi data perkara harus ditetapkan secara proporsional, berbasis kebutuhan, dan disertai prosedur penghapusan aman—karena retensi tanpa batas memperbesar risiko kebocoran dan penyalahgunaan.

2. Incident response, enforcement, dan akuntabilitas nyata**.**

Penguatan *due process* digital membutuhkan konsekuensi ketika standar keamanan dilanggar. Studi tentang enforcement perlindungan data menunjukkan desain penegakan (sanksi, koordinasi kewenangan, dan proporsionalitas) menjadi isu penting, khususnya ketika ada yurisdiksi yang tumpang tindih.[59] Catatan praktik otoritas perlindungan data juga menunjukkan contoh pelanggaran keamanan (misalnya email tidak terenkripsi menyebar akibat virus) yang berujung

53 Felicity Bell, Lyria Bennett Moses, Michael Legg, "AI Decision-Making and the Courts A Guide for Judges, Tribunal Members and Court Administrators."

54 Gill, "The Principle of Open Justice and The Judicial Duty to Give Public Reasons."

55 OECD, "Report on the Cross-Border Enforcement of Privacy Law."

56 European Data Protection Board, "Guidelines 01/2023 on Article 37 Law Enforcement Directive" (Brussels, 2023).

57 Shah, "Law Enforcement and Data Privacy : A Forward-Looking Approach."

58 Council of Europe, *Practical Guide on the Use of Personal Data in the Police Sector*.

59 Guilda Rostama and Teresa Scassa, "The Future of Data Protection Enforcement in Canada : Lessons from the GDPR The Future of Data Protection Enforcement in Canada : Lessons from the GDPR," *Canadian Journal of Law and Technology* 21, no. 1 (2023).

penindakan—ini menegaskan bahwa "keamanan data" bukan norma abstrak, melainkan dapat ditegakkan dan diukur.[60]

Dengan indikator di atas, *due process digital* dapat dipahami sebagai paket jaminan prosedural yang berjalan sepanjang siklus data/bukti digital: (i) dasar hukum dan tujuan yang tegas; (ii) *necessity–proportionality* dan *minimization*; (iii) perlindungan khusus korban/saksi; (iv) preservasi forensik (*bit-copy, hashing, chain of custody*); (v) kontrol akses, enkripsi, dan audit trail; (vi) pembatasan penggunaan ulang dan auditabilitas alasan, terutama saat memakai otomasi; (vii) *safeguards* untuk berbagi data lintas batas; serta (viii) retensi/penghapusan terukur dan mekanisme respons insiden yang akuntabel. Dengan demikian, keamanan siber bukan tambahan administratif, melainkan infrastruktur keadilan prosedural dalam penegakan hukum pidana berbasis data.

3. Implikasi Normatif dan Kebijakan: Perlindungan Data, Akuntabilitas Aparat dan Perlindungan Korban

Menempatkan keamanan siber sebagai bagian dari *due process of law* tidak berhenti pada perumusan indikator teknis (akses berbasis peran, audit trail, *hashing*, retensi/penghapusan). Konsekuensi logis nya adalah reposisi kebijakan: (i) bagaimana hukum acara pidana mengatur tindakan koersif digital, (ii) bagaimana rezim perlindungan data memberi pagar atas pemrosesan untuk penegakan hukum, (iii) bagaimana desain akses data—termasuk *lawful interception* dan *cloud evidence*—diatur agar tidak merusak keamanan sistem dan hak privat, serta (iv) bagaimana mekanisme akuntabilitas dan pemulihan (remedies) dibuat nyata, bukan simbolik.

a. Implikasi Normatif: Menutup Celah antara "Upaya Paksa Digital" dan "Keamanan Pemrosesan"

Secara normatif, pembaruan KUHAP memperlihatkan pengakuan eksplisit bahwa tindakan koersif negara kini mencakup ranah digital. Definisi "upaya paksa" dalam KUHAP baru memasukkan penyadapan dan pemblokiran, menempatkannya setara dengan penangkapan, penggeledahan, dan penyitaan.[61] Bahkan pemblokiran dikonstruksi sebagai tindakan yang dilakukan oleh penyidik/penuntut umum/hakim dan mensyaratkan izin ketua pengadilan negeri.[62] Implikasinya jelas: tindakan digital dipahami sebagai intrusif dan membutuhkan kontrol prosedural. Namun, pengakuan ini belum otomatis menjamin *due process* apabila tidak diikuti standar keamanan pemrosesan setelah data diperoleh.

Di titik inilah rezim UU ITE dan UU PDP saling melengkapi. UU ITE sejak awal menekankan bahwa pembuktian elektronik rentan diubah, disadap, dipalsukan, dan disebarkan sangat cepat, sehingga menimbulkan persoalan kepastian hukum dan keamanan penyelenggaraan sistem elektronik.[63] UU PDP menguatkan basis normatif bahwa pelindungan data pribadi terkait langsung dengan hak asasi; data mudah dikumpulkan dan dipindahkan tanpa sepengetahuan subjek data dan dapat mengancam hak konstitusional.[64] Pada level kewajiban, UU PDP mewajibkan

60 EU Advisory Body on Data Protection and Privacy, "Article 29 - Data Protection Working Party Recent Examples of Enforcement Actions Carried out by Data Protection Authorities" (Brussels, Belgium, 2005).

61 "Undang-Undang Tentang Kitab Undang-Undang Hukum Acara Pidana. UU Nomor 20 Tahun 2025. LN Tahun 2025 No.258 TLN No.7000," n.d.

62 "Undang-Undang Tentang Kitab Undang-Undang Hukum Acara Pidana. UU Nomor 20 Tahun 2025. LN Tahun 2025 No.258 TLN No.7000."

63 "Undang-Undang Tentang Informasi Dan Transaksi Elektronik. UU Nomor 11 Tahun 2008. LN Tahun 2008 No. 58 TLN No. 4843" (n.d.).

64 "Undang-Undang Tentang Pelindungan Data Pribadi. UU Nomor 27 Tahun 2022. LN Tahun 2022 No 196 TLN No. 6820" (n.d.).

pengendali data menjaga keamanan data dari akses/pengungkapan/pengubahan yang tidak sah dan menuntut pertanggungjawaban yang dapat dibuktikan.[65] Namun UU PDP juga memberi pengecualian hak subjek data untuk kepentingan proses penegakan hukum.[66]

Implikasi normatifnya: pengecualian bukan "zona bebas kewajiban". Justru karena penegakan hukum diberi ruang yang lebih besar, standar *due process digital* harus diperkuat melalui kewajiban keamanan, dokumentasi, dan auditabilitas. Dengan kata lain, KUHAP baru mengatur "boleh/tidak" tindakan koersif digital; UU PDP dan UU ITE menyediakan dasar untuk menuntut bagaimana data itu diproses secara aman dan bertanggung jawab. Ini mendukung agenda pembaruan hukum acara: bukan hanya memperluas kewenangan, melainkan menguatkan *procedural safeguards*.

b. Kebijakan Akses Data: Lawful Interception, E2EE/5G, dan Risiko "Mengorbankan Keamanan demi Akses"

Implikasi kebijakan paling sensitif muncul pada isu akses komunikasi: *lawful interception* dan tantangan enkripsi. Laporan kebijakan UE tentang *lawful interception* menjelaskan bahwa akses rahasia *real-time* dapat menyasar konten dan metadata komunikasi, dan dapat dilakukan pada level perangkat, jaringan, atau tujuan (misalnya *cloud storage*). Namun, inovasi teknologi—khususnya layanan OTT, *end-to-end encryption* (E2EE), dan desain 5G yang makin menekankan privasi (*privacy by design*)—membuat akses data oleh aparat semakin sulit, sehingga pembuat kebijakan menghadapi *trade-off*: kebutuhan penegakan hukum versus privasi komunikasi dan keamanan siber.[67]

Jika "solusi kebijakan" dipahami semata sebagai memperluas akses (misalnya mewajibkan *backdoor*), risikonya justru kontraproduktif: melemahkan ekosistem keamanan siber secara keseluruhan, memperbesar permukaan serangan, dan pada akhirnya mengancam integritas bukti digital serta keamanan data korban/tersangka. Karena itu, menempatkan *cybersecurity* sebagai *due process* menuntut prinsip kebijakan: akses yang sah harus kompatibel dengan keamanan sistem. Akses data harus dirancang dengan pagar: pembatasan tujuan, pengawasan independen, dokumentasi, serta standar pengamanan (kontrol akses, audit trail, dan retensi yang terukur). Di sini, "ketersediaan bukti" tidak boleh dibayar dengan mengorbankan keamanan sistem dan hak privat.

c. Cross-Border Evidence: Model "Take/Block", Kedaulatan Data, dan Safeguards

Ekosistem bukti digital semakin lintas batas. Hong Yanqing menggambarkan bahwa digitalisasi membuat akses data lintas yurisdiksi "hampir tak terhindarkan," dan negara-negara membangun pola model yang dapat disederhanakan sebagai "*take*" (mengambil data yang disimpan di luar negeri) versus "*block*" (mencegah akses otoritas asing terhadap data domestik).[68] Dinamika ini penting karena menunjukkan bahwa *due process* kini dipengaruhi bukan hanya oleh hukum acara domestik, tetapi juga oleh konflik yurisdiksi, kedaulatan, dan desain kerja sama.

---

65 Undang-Undang Tentang Pelindungan Data Pribadi. UU Nomor 27 Tahun 2022. LN Tahun 2022 No 196 TLN No. 6820.

66 Undang-Undang Tentang Pelindungan Data Pribadi. UU Nomor 27 Tahun 2022. LN Tahun 2022 No 196 TLN No. 6820.

67 Piotr Bąkowski, "Access to Data for Law Enforcement: Lawful Interception," *European Parliamentary Research Service*, 2025.

68 Hong Yanqing, "' Game of Laws ': Cross-Border Data Access for Law Enforcement Purposes," *Paul Tsai China Center, Yale Law School*, 2018.

OECD lebih awal menekankan bahwa arus data lintas batas meningkatkan risiko privasi dan *data security breaches* yang berdimensi lintas negara; perlindungan privasi efektif membutuhkan kerja sama lintas batas yang lebih sistematis.[69] EDPB menegaskan bahwa untuk transfer data *law enforcement*, *safeguards* harus memastikan tingkat perlindungan yang "*essentially equivalent*," dan perjanjian mengikat diprioritaskan karena memberi kepastian hukum, transparansi, dan konsistensi.[70]

Implikasi kebijakan bagi Indonesia: proses akses bukti digital lintas batas (MLA, permintaan data ke penyedia global, kerja sama intelijen/penegakan) harus dilengkapi perangkat *safeguards* yang dapat diuji: instrumen hukum yang *enforceable*, pembatasan tujuan, audit atas transfer, mekanisme koreksi/keberatan yang realistis, dan standar keamanan penyimpanan serta akses. Dengan begitu, kebutuhan "efisiensi penegakan hukum" tidak menabrak perlindungan hak privat dan integritas bukti.

1. Perlindungan Korban dan Saksi: ***Data Leakage*** sebagai Reviktimisasi Struktural

Menempatkan *cybersecurity* sebagai *due process* menguatkan kewajiban negara terhadap perlindungan korban dan saksi. UNODC menegaskan bahwa perlindungan saksi merupakan kontinum tindakan, termasuk "*procedural measures*" seperti *videoconferencing*, distorsi suara/wajah, dan *withholding* identitas.[71] Dalam praktik program perlindungan saksi, bahkan jejak digital pada perangkat/nomor seri dapat menimbulkan risiko identifikasi—menunjukkan bahwa pengelolaan data dan identitas bukan isu pinggiran.[72]

Implikasinya: SOP data perkara wajib memuat *privacy by design* untuk korban/saksi—pembatasan akses, redaksi identitas, pengaturan retensi, dan kontrol distribusi dokumen perkara. Kegagalan menjaga kerahasiaan data korban bukan sekadar "insiden IT", tetapi dapat menjadi bentuk reviktimisasi struktural: negara yang seharusnya melindungi justru memperluas penderitaan melalui kebocoran data. Dengan demikian, indikator *due process* digital tidak netral; ia harus memberi perlindungan tambahan pada data yang berisiko tinggi.

2. Akuntabilitas dan Remedies: Dari "Kepatuhan Administratif" ke "Penegakan dan Pemulihan yang Nyata"

Due process digital memerlukan desain akuntabilitas dan pemulihan yang konkret. Pengalaman *reform enforcement* menunjukkan bahwa peningkatan kewenangan sanksi administratif menimbulkan isu koordinasi yurisdiksi dan proporsionalitas penalti; desain penegakan harus menghindari *multiple penalties* yang tidak proporsional dan memastikan mekanisme koordinasi lembaga berjalan.[73] Di sisi lain, contoh penindakan otoritas perlindungan data menunjukkan bahwa pelanggaran keamanan (misalnya pengiriman data tanpa enkripsi yang menyebar akibat virus) bukan sesuatu yang abstrak; ia dapat diproses sebagai pelanggaran yang memerlukan konsekuensi nyata.[74]

---

69 OECD, "Report on the Cross-Border Enforcement of Privacy Law."
70 European Data Protection Board, "Guidelines 01/2023 on Article 37 Law Enforcement Directive."
71 UNODC, *Good Practices for the Protection of Witnesses in Criminal Proceedings Involving Organized Crime*.
72 UNODC.
73 Rostama and Scassa, "The Future of Data Protection Enforcement in Canada : Lessons from the GDPR The Future of Data Protection Enforcement in Canada : Lessons from the GDPR."
74 EU Advisory Body on Data Protection and Privacy, "Article 29 - Data Protection Working Party Recent Examples of Enforcement Actions Carried out by Data Protection Authorities."

Dalam kerangka nasional, UU PDP memberi fondasi kewajiban keamanan dan akuntabilitas yang dapat dibuktikan.[75] Agar fondasi ini berfungsi sebagai jaminan *due process*, kebijakan penegakan harus menetapkan: (i) standar minimal keamanan untuk lembaga penegak hukum dan PSE yang memproses data perkara, (ii) kewajiban audit trail dan pelaporan insiden, (iii) mekanisme koreksi dan pemulihan bagi pihak yang dirugikan (terutama korban), dan (iv) pengawasan yang efektif—tidak hanya internal, tetapi juga eksternal (misalnya pengawas independen) untuk mencegah *abuse of power*.

Dengan demikian, implikasi normatif dan kebijakan dari konstruksi "*cybersecurity* sebagai bagian dari *due process*" dapat dirangkum: (1) pembaruan hukum acara pidana harus dibaca bersama kewajiban keamanan pemrosesan data (UU ITE–UU PDP) agar tindakan koersif digital tidak berhenti pada legalitas formal; (2) desain akses data (*lawful interception*, E2EE/5G) harus kompatibel dengan keamanan sistem agar tidak menciptakan kerentanan baru yang merusak integritas bukti dan privasi; (3) akses lintas batas harus ditopang *safeguards* dan instrumen *enforceable* agar *due process* tetap terjaga dalam konflik yurisdiksi; (4) perlindungan korban/saksi menuntut kontrol data yang ketat untuk mencegah reviktimisasi; dan (5) akuntabilitas serta remedies harus dibuat nyata melalui enforcement, audit, dan pemulihan, bukan sekadar kepatuhan administratif.

D. KESIMPULAN

Pertama, artikel ini menunjukkan bahwa digitalisasi penegakan hukum pidana telah menggeser locus risiko *due process of law* dari semata tindakan fisik aparat menuju domain digital—yakni akses, pemrosesan, penyimpanan, dan distribusi data/bukti digital. Karena data pribadi menjadi "bahan bakar" proses pidana, kegagalan keamanan siber bukan sekadar gangguan teknis, melainkan dapat menggerus legalitas prosedural, merusak integritas pembuktian, mengancam privasi, serta memicu reviktimisasi korban. Dengan demikian, keamanan siber harus dipahami sebagai bagian inheren dari *due process of law*: ia berfungsi sebagai arsitektur pengendalian kekuasaan negara agar penggunaan data tetap sah, terbatas, dapat diaudit, dan dapat dipertanggungjawabkan.

Kedua, parameter *due process digital* yang relevan harus dirumuskan sepanjang siklus hidup data/bukti digital. Indikator utama mencakup: dasar hukum dan pembatasan tujuan (*purpose limitation*); uji kebutuhan dan proporsionalitas yang ketat (*strict necessity–proportionality*) serta minimisasi data; perlindungan khusus untuk korban dan saksi; preservasi forensik yang menjaga integritas (*bit-for-bit copy, hashing, chain of custody digital*); kontrol akses berbasis peran dan audit trail; keamanan transmisi/ penyimpanan (termasuk enkripsi); pembatasan penggunaan ulang (*function creep*); *safeguards* untuk berbagi data lintas batas; serta retensi/penghapusan terukur dan mekanisme respons insiden. Indikator-indikator ini menutup *gap* antara "legalitas tindakan" dan "keamanan pemrosesan", sehingga jaminan *fair trial* dan akuntabilitas benar-benar operasional.

Ketiga, implikasi normatif dan kebijakan dari penempatan keamanan siber sebagai jaminan prosedural menuntut integrasi rezim KUHAP baru, UU ITE, dan UU PDP. Pengaturan upaya paksa digital (penyadapan, pemblokiran) perlu dibaca bersama kewajiban keamanan dan pertanggungjawaban pemrosesan data. Tantangan *lawful interception* di era E2EE/5G menuntut desain akses yang sah tetapi tidak mengorbankan

75 Undang-Undang Tentang Pelindungan Data Pribadi. UU Nomor 27 Tahun 2022. LN Tahun 2022 No 196 TLN No. 6820.

keamanan sistem. Pada konteks *cross-border evidence*, diperlukan instrumen kerja sama dan *safeguards* yang *enforceable* agar akses data lintas yurisdiksi tetap sejalan dengan perlindungan hak dan integritas bukti. Dengan demikian, keamanan siber bukan tambahan administratif, melainkan infrastruktur *due process* bagi penegakan hukum pidana berbasis data.

DAFTAR PUSTAKA

Aidinlis, Stergios, David Barnard-wills, Leanne Cochrane, Agata Gurzawska, and Joshua Hughes. "Between GDPR and Law Enforcement Directive in Security Research : The Use of Personal Data by Law Enforcement Authorities." *European Journal of Law and Technology* 15, no. 3 (2024).

Appazov, Artur. "Legal Aspects of Cybersecurity." Copenhagen, 2014.

Babuta, Alexander. "Big Data and Policing An Assessment of Law Enforcement Requirements, Expectations and Priorities." London, 2017.

Bąkowski, Piotr. "Access to Data for Law Enforcement: Lawful Interception." *European Parliamentary Research Service*, 2025.

Bignami, Francesca. "Privacy and Law Enforcement in the European Union : The Data Retention Directive Privacy and Law Enforcement in the European Union : The Data Retention Directive." *Chicago Journal of International Law* 8, no. 1 (2007).

Castro, Alan Mcquinn and Daniel. "How Law Enforcement Should Access Data Across Borders." Washington DC, 2017.

Council of Europe. *Practical Guide on the Use of Personal Data in the Police Sector*. Strasbourg: Directorate General of Human Rights and Rule of Law, 2018.

EU Advisory Body on Data Protection and Privacy. "Article 29 - Data Protection Working Party Recent Examples of Enforcement Actions Carried out by Data Protection Authorities." Brussels, Belgium, 2005.

European Data Protection Board. "Guidelines 01/2023 on Article 37 Law Enforcement Directive." Brussels, 2023.

Felicity Bell, Lyria Bennett Moses, Michael Legg, Jake Silove and Monika Zalnieriute. "AI Decision-Making and the Courts A Guide for Judges, Tribunal Members and Court Administrators." New South Wales, 2022.

Gill, Jason Bosland and Jonathan. "The Principle of Open Justice and The Judicial Duty to Give Public Reasons." *Melbourne University Law Review* 38, no. 482 (2014): 482–524.

Hert, Serge Gutwirth and Paul De. "Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power." *Direito Público* 18, no. 100 (2022). https://doi.org/https://doi.org/10.11117/rdp.v18i100.6200.

Home Office. "Data Protection Legislation Policy on Sensitive Processing for Law Enforcement Purposes, under Part 3 DPA (2018)." UK, 2021.

James Baldwin, Omar M. K. Alhawi, Simone Shaughnessy, Alex Akinbi, and and Ali Dehghantanha. "Emerging from the Cloud: A Bibliometric Analysis of Cloud

Forensics Studies." In *Cyber Threat Intelligence*, edited by Mauro Conti, Ali Dehghantanha and Tooska Dargahi. Cham: Springer, 2018.

Korff, Ian Brwon and Douwe. "Technology Development and Its Effect on Privacy & Law Enforcement." *UK Information Commissioner Study Project*, 2004.

Kosseff, Jeff. "Defining Cybersecurity Law." *Iowa Law Review* 103, no. 985 (2018): 985–1031.

———. "Hacking Cybersecurity Law." *University of Illinois Law Review* 2020 (2019): 811–50.

Lynskey, Orla. "Criminal Justice Profiling and EU Data Protection Law : Precarious Protection from Predictive Policing." *International Journal of Law in Context* 15, no. 2 (2019): 162–76. https://doi.org/10.1017/S1744552319000090.

Northern Ireland Policing Board. "Human Rights Review of Privacy and Policing," 2023.

OECD. "Report on the Cross-Border Enforcement of Privacy Law." Paris, 2006. https://doi.org/http://dx.doi.org/10.1787/231304814207.

Packer, Herbert L. *The Limits of the Criminal Sanction*. *Stanford University Press*. Stanford, California, 1969.

Panguluri, Richard D. Alexander and Srinivas. "Cybersecurity Terminology and Frameworks." In *Cyber-Physical Security Protecting Critical Infrastructure at the State and Local Level*, edited by Simon Hakim, Robert M. Clark, 19–48. Switzerland: Springer Nature, 2017.

Peifer, Paul M. Schwartz and Karl-Nikolaus. "Transatlantic Data Privacy Law." *Georgetown Law Journal, UC Berkeley Public Law Research Paper* 106, no. 115 (2017).

Rahardjo, Satjipto. *Ilmu Hukum*. Bandung: Citra Aditya Bakti, 2014.

Robinson, Isabel Alice Walbaum, ed. *Handbook on the Language of Data Protection*. Brussel: European Judicial Training Network (EJTN), 2019.

Rostama, Guilda, and Teresa Scassa. "The Future of Data Protection Enforcement in Canada : Lessons from the GDPR The Future of Data Protection Enforcement in Canada : Lessons from the GDPR." *Canadian Journal of Law and Technology* 21, no. 1 (2023).

Shah, Reema. "Law Enforcement and Data Privacy : A Forward-Looking Approach." *The Yale Law Journal* 125, no. 543 (2015): 543–58.

Sperfeldt, Christoph. "Digital Exclusions: Legal Identity, Identification, and the Sustainable Development Goals in Southeast Asia," 2023.

Stuntz, William J. "Privacy's Problem and the Law of Criminal Procedure." *Michigan Law Review* 93, no. 5 (1995).

Undang-Undang Tentang Informasi dan Transaksi Elektronik. UU Nomor 11 Tahun 2008. LN Tahun 2008 No. 58 TLN No. 4843 (n.d.).

"Undang-Undang Tentang Kitab Undang-Undang Hukum Acara Pidana. UU Nomor 20 Tahun 2025. LN Tahun 2025 No.258 TLN No.7000," n.d.

Undang-Undang Tentang Pelindungan Data Pribadi. UU Nomor 27 Tahun 2022. LN

Tahun 2022 No 196 TLN No. 6820 (n.d.).

United Nations High Commissioner for Human Right. "The Right to Privacy in The Digital Age" 12799, no. August (2018).

UNODC. *Good Practices for the Protection of Witnesses in Criminal Proceedings Involving Organized Crime*. New York: UNODC, 2008.

Yanqing, Hong. "' Game of Laws ': Cross-Border Data Access for Law Enforcement Purposes." *Paul Tsai China Center, Yale Law School*, 2018.

Yeung, Karen. "'Hypernudge': Big Data as a Mode of Regulation by Design." *Information, Communication & Society* 20, no. 1 (2017): 118–36. https://doi.org/10.1080/1369118X.2016.1186713.