LEXARA
Journal of Law and Legal Studies
Lexara: Journal of Law and Legal Studies
Vol. 1 No. 3 2026
E-ISSN: 3164-5763
punggawajournal.com/lexara

Analisis Yuridis Pertanggungjawaban Pidana Atas Dugaan Penyadapan Komunikasi Elektronik Presiden Republik Indonesia, Pejabat Negara, Dan Tokoh Publik: Perspektif Hukum Pidana, Keamanan Negara, Dan Fikih Siyasah Jinayah

Muhammad Febri Eka Saputra[1]
[1] Universitas Islam Negeri Sjech M.Djamil Djambek Bukittinggi, Indonesia
Korespondensi: febri75saputra@gmail.com

Informasi Artikel
Riwayat artikel:
Received Sept 17th, 2026
Revised Oct 26th, 2026
Accepted Nov 3th, 2026

Keyword:
Penyadapan; Pertanggungjawaban Pidana; Keamanan Negara; Tajassus; Siyasah Jinayah.

ABSTRAK
Penelitian ini menganalisis konstruksi pertanggungjawaban pidana atas dugaan penyadapan komunikasi elektronik terhadap Presiden Republik Indonesia, pejabat negara, dan tokoh publik melalui perspektif hukum pidana, keamanan negara, serta fikih siyasah jinayah. Kajian ini berangkat dari dugaan penggunaan sistem intersepsi tanpa verifikasi dan dasar penegakan hukum yang memadai, termasuk dugaan penghapusan data hasil intersepsi, dengan rentang peristiwa yang diberitakan melintasi perubahan rezim hukum pada 2 Januari 2026. Penelitian dilakukan sebagai penelitian hukum normatif dengan pendekatan perundang-undangan, konseptual, kasus, dan hukum Islam. Analisis menunjukkan bahwa penentuan pertanggungjawaban harus membedakan legalitas kewenangan, unsur tindak pidana, bentuk kesalahan, peran setiap pihak, serta keabsahan bukti elektronik. Status sasaran sebagai pejabat negara tidak dengan sendirinya membentuk tindak pidana terhadap keamanan negara. Dalam perspektif fikih siyasah jinayah, intersepsi tanpa alasan syar'i dan otorisasi yang sah dapat beririsan dengan larangan tajassus, pelanggaran amanah, dan tindakan yang merugikan kehormatan serta kemaslahatan umum. Penelitian ini merumuskan parameter evaluasi yang mengintegrasikan asas legalitas, proporsionalitas, akuntabilitas, dan perlindungan hak.

© 2026 The Authors. Published by Punggawa Legacy Center. This is an open access article under the CC BY license (https://creativecommons.org/licenses/by/4.0/)

PENDAHULUAN

Perkembangan teknologi komunikasi elektronik telah mengubah cara kekuasaan negara memperoleh, mengolah, menyimpan, dan menggunakan informasi. Komunikasi pejabat publik, lembaga pemerintahan, pelaku politik, organisasi masyarakat, media, dan warga kini berlangsung melalui infrastruktur digital yang meninggalkan jejak elektronik serta memungkinkan pengawasan secara real time. Kapasitas tersebut memiliki nilai strategis bagi penegakan hukum, pencegahan kejahatan, dan perlindungan keamanan nasional. Namun, kapasitas yang sama juga menghadirkan risiko penyalahgunaan ketika akses terhadap komunikasi privat dilakukan tanpa dasar kewenangan, tanpa tujuan yang dibenarkan hukum, atau tanpa pengawasan yang memadai. Oleh karena itu, penyadapan tidak dapat dipahami semata-mata sebagai tindakan teknis memperoleh informasi, melainkan sebagai bentuk intervensi serius terhadap hak atas privasi, kerahasiaan komunikasi, kebebasan berekspresi, serta integritas penyelenggaraan kekuasaan negara(Anggraeniko et al., 2026).

Persoalan tersebut memperoleh relevansi aktual setelah aparat penegak hukum pada 3 November 2026 mengumumkan perkembangan penyidikan mengenai dugaan penyadapan komunikasi elektronik terhadap Presiden Republik Indonesia dan sejumlah kategori sasaran lain, termasuk pejabat negara, tokoh politik, media, organisasi masyarakat, lembaga swadaya masyarakat, dan pelaku usaha. Menurut keterangan yang diberitakan, dugaan tindakan berlangsung pada periode 2025–2026, dengan

sejumlah nomor dimasukkan ke dalam sistem pengelolaan intersepsi tanpa proses verifikasi dan tanpa keterkaitan dengan proses penegakan hukum. Pemberitaan yang sama menyebut adanya dugaan penghapusan berkas hasil penyadapan pada Oktober 2026 serta penetapan tiga orang sebagai tersangka. Seluruh informasi tersebut harus ditempatkan secara tepat sebagai keterangan penyidikan yang diberitakan kepada publik, bukan sebagai fakta kesalahan yang telah diputus pengadilan. Artikel ini tidak menetapkan siapa yang bersalah dan tidak mengasumsikan motif tertentu; penilaian pidana tetap mensyaratkan pembuktian yang sah, independen, dan tunduk pada asas praduga tidak bersalah(Rahmani, 2026).

Konteks tersebut mengandung sekurang-kurangnya tiga persoalan hukum yang saling berkaitan. Pertama, apakah tindakan memperoleh atau memantau komunikasi elektronik dilakukan berdasarkan atribusi kewenangan yang sah, tujuan yang dibenarkan, dan prosedur yang berlaku. Kedua, bagaimana pertanggungjawaban pidana dibangun apabila suatu rangkaian tindakan melibatkan pihak yang meminta, memerintahkan, menyetujui, mengoperasikan sistem, mengakses hasil, atau menghapus data. Ketiga, apakah dan dalam batas apa tindakan demikian dapat menimbulkan implikasi terhadap keamanan negara, khususnya ketika sasaran intersepsi merupakan Presiden atau pejabat yang menjalankan fungsi konstitusional. Ketiga persoalan itu tidak dapat diselesaikan hanya melalui identitas sasaran atau status jabatan orang yang diduga terlibat. Pemeriksaan harus diarahkan pada perbuatan konkret, kewenangan, unsur delik, kesalahan, hubungan kausal, dan kualitas pembuktian.

Kompleksitas analisis meningkat karena periode dugaan tindakan disebut melintasi 2 Januari 2026, yaitu tanggal mulai berlakunya Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana dan Undang-Undang Nomor 20 Tahun 2025 tentang Kitab Undang-Undang Hukum Acara Pidana. Sejak tanggal tersebut, ketentuan pidana mengenai intersepsi dalam Pasal 31 ayat (1) dan ayat (2) Undang-Undang Informasi dan Transaksi Elektronik yang lama telah dicabut berdasarkan ketentuan peralihan KUHP, sedangkan larangan penyadapan tanpa hak dirumuskan dalam Pasal 258 KUHP Nasional. Akses tanpa hak terhadap sistem elektronik memperoleh pengaturan dalam Pasal 332 KUHP, sementara perbuatan terhadap integritas informasi elektronik harus dinilai berdasarkan ketentuan yang masih berlaku, termasuk ketentuan relevan dalam Undang-Undang ITE. Konsekuensinya, tidak tepat menerapkan satu rezim hukum secara seragam terhadap seluruh rangkaian peristiwa. Setiap tindakan harus dipetakan berdasarkan waktu, bentuk, objek, dan norma yang berlaku pada saat perbuatan dilakukan.

Dari sudut hukum pidana, penyadapan yang dilakukan oleh aparat atau melalui sistem milik institusi negara tidak otomatis menjadi sah hanya karena terdapat fasilitas teknis atau jabatan yang melekat pada pelaksana. Legalitas bergantung pada sumber kewenangan, cakupan atribusi, tujuan tindakan, pemenuhan syarat prosedural, serta batas penggunaan hasil intersepsi. Sebaliknya, pelanggaran prosedur tidak selalu secara otomatis memenuhi seluruh unsur tindak pidana. Pembedaan ini penting agar penegakan hukum tidak melakukan kriminalisasi berlebihan sekaligus tidak memberikan kekebalan terhadap penyalahgunaan kewenangan. Pertanggungjawaban pidana harus dibangun secara individual, dengan menguji apakah pelaku melakukan tindakan yang dirumuskan sebagai tindak pidana, apakah tindakan tersebut melawan hukum, dan apakah terdapat kesalahan yang dapat dicelakan kepadanya.

Dimensi keamanan negara juga memerlukan batas konseptual yang tegas. Penyadapan terhadap komunikasi Presiden atau pejabat negara dapat menimbulkan risiko bagi kerahasiaan deliberasi pemerintahan, keamanan informasi strategis, dan keberlangsungan fungsi konstitusional. Akan tetapi, status korban atau sasaran tidak serta-merta mengubah setiap tindakan penyadapan menjadi kejahatan terhadap keamanan negara, makar, atau pengkhianatan. Kualifikasi demikian hanya dapat digunakan apabila fakta memenuhi unsur delik khusus yang dirumuskan undang-undang. Keamanan negara harus dipahami sebagai perlindungan terhadap keselamatan masyarakat, kedaulatan, integritas institusi, dan tatanan konstitusional; ia bukan dalih abstrak untuk memperluas kewenangan pengawasan atau membungkam kritik yang sah.

Perspektif fikih siyasah jinayah memberikan dimensi normatif tambahan terhadap persoalan ini. Larangan tajassus dalam Al-Qur'an, khususnya QS Al-Hujurat [49]:12, dan etika meminta izin untuk memasuki ruang privat sebagaimana QS An-Nur [24]:27, menunjukkan bahwa kehormatan serta ruang pribadi memiliki perlindungan moral-hukum. Prinsip amanah membatasi penggunaan kewenangan yang dipercayakan kepada pejabat, sedangkan konsep maslahah menuntut agar tindakan penguasa diarahkan pada kemaslahatan yang dapat dipertanggungjawabkan. Namun, fikih siyasah tidak

dapat disederhanakan menjadi larangan absolut terhadap seluruh bentuk pengumpulan informasi. Pengawasan atau intelijen yang benar-benar diperlukan untuk mencegah bahaya serius dapat dinilai berbeda sepanjang memiliki otorisasi yang sah, tujuan yang jelas, kebutuhan yang terukur, dan tidak berubah menjadi pengintaian atas urusan privat tanpa alasan yang dibenarkan.

Kajian terdahulu mengenai penyadapan di Indonesia telah membahas legalitas intersepsi, kewenangan aparat penegak hukum, perlindungan privasi, kedudukan bukti elektronik, dan pertanggungjawaban atas akses tanpa hak. Literatur hukum Islam kontemporer juga mulai menghubungkan perlindungan data pribadi, larangan tajassus, maqashid al-syari'ah, dan kejahatan siber. Meskipun demikian, masih terdapat ruang untuk mengintegrasikan dimensi hukum pidana materiil, keamanan negara, dan fikih siyasah jinayah dalam satu kerangka analisis atas dugaan penyadapan yang berlangsung melintasi perubahan hukum nasional pada 2026. Secara khusus, kebutuhan analisis tidak hanya terletak pada apakah penyadapan dilarang, tetapi juga pada konstruksi atribusi peran, hukum antarwaktu, integritas bukti digital, serta batas pembenaran tindakan pengawasan atas nama kepentingan negara.

Kebaruan penelitian ini terletak pada pengembangan analisis berlapis yang menghubungkan empat simpul argumentasi: legalitas kewenangan intersepsi, pertanggungjawaban pidana individual, perlindungan keamanan negara yang dibatasi prinsip konstitusional, dan evaluasi etis-yuridis melalui fikih siyasah jinayah. Artikel ini mengajukan tesis bahwa penyadapan hanya memperoleh legitimasi ketika seluruh mata rantai tindakannya permintaan, otorisasi, aktivasi, pemantauan, akses hasil, penyimpanan, penggunaan, dan pemusnahan dapat ditelusuri pada dasar hukum serta tujuan yang sah. Pada saat yang sama, pelanggaran pada satu mata rantai harus dinilai menurut konsekuensi hukumnya secara proporsional dan tidak boleh secara otomatis disamakan dengan tindak pidana tanpa pembuktian unsur serta kesalahan.

Berdasarkan persoalan tersebut, penelitian ini bertujuan menganalisis konstruksi pertanggungjawaban pidana atas dugaan penyadapan komunikasi elektronik terhadap Presiden Republik Indonesia, pejabat negara, dan tokoh publik; menguji kaitannya dengan perlindungan keamanan negara dan fungsi konstitusional; serta menilai perbuatan tersebut berdasarkan prinsip-prinsip fikih siyasah jinayah. Kontribusi penelitian diharapkan bersifat teoretis melalui perumusan hubungan antara legalitas intersepsi, asas pertanggungjawaban individual, dan larangan tajassus, serta bersifat praktis melalui penyusunan parameter untuk menilai otorisasi, proporsionalitas, pembuktian digital, dan pengawasan atas penggunaan sistem intersepsi.

METODE PENELITIAN

Penelitian ini merupakan penelitian hukum normatif atau doktrinal dengan karakter deskriptif-analitis dan preskriptif. Penelitian diarahkan untuk menguji norma hukum positif, asas konstitusional, doktrin pertanggungjawaban pidana, dan prinsip fikih siyasah jinayah yang berkaitan dengan penyadapan komunikasi elektronik. Karena objek kajian utamanya berupa norma, putusan, dan doktrin, penelitian ini tidak menggunakan populasi dan sampel dalam pengertian penelitian empiris. Unit analisisnya adalah peraturan perundang-undangan, putusan pengadilan, sumber hukum Islam, dan literatur ilmiah yang relevan dengan isu intersepsi, privasi, keamanan negara, serta tindak pidana siber(Marzuki, 2021).

Bahan hukum primer meliputi Undang-Undang Dasar Negara Republik Indonesia Tahun 1945; Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah, khususnya norma yang tetap berlaku setelah pencabutan sebagian ketentuan pidananya; Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana; Undang-Undang Nomor 20 Tahun 2025 tentang Kitab Undang-Undang Hukum Acara Pidana; Undang-Undang Nomor 1 Tahun 2026 tentang Penyesuaian Pidana; Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi; serta Kovenan Internasional tentang Hak-Hak Sipil dan Politik (ICCPR) yang disahkan melalui Undang-Undang Nomor 12 Tahun 2005, dan Putusan Mahkamah Konstitusi Nomor 5/PUU-VIII/2010 serta Nomor 20/PUU-XIV/2016. Analisis fikih menggunakan Al-Qur'an, Sunnah, kaidah fikih, prinsip maqashid al-syari'ah, dan doktrin fikih jinayah serta siyasah yang relevan. Bahan hukum sekunder mencakup artikel jurnal, buku, dan pendapat ahli mengenai penyadapan, privasi, hukum pidana, keamanan negara, bukti elektronik, dan hukum Islam.

Pendekatan perundang-undangan digunakan untuk menelaah dasar kewenangan intersepsi, rumusan tindak pidana, ketentuan peralihan, dan hubungan antara KUHP, KUHAP, Undang-Undang

ITE, serta Undang-Undang Pelindungan Data Pribadi. Pendekatan konseptual digunakan untuk mengurai pengertian penyadapan, intersepsi, sifat melawan hukum, kesalahan, penyertaan, keamanan negara, tajassus, amanah, maslahah, dan ta'zir. Pendekatan kasus digunakan untuk menganalisis prinsip hukum dalam putusan Mahkamah Konstitusi yang relevan serta menempatkan perkembangan perkara yang diberitakan pada 3 November 2026 sebagai konteks faktual terbatas. Pemberitaan media dan keterangan aparat pada tahap penyidikan tidak diperlakukan sebagai pengganti berkas perkara, alat bukti, atau putusan pengadilan(Efendi & Ibrahim, 2022).

Analisis dilakukan secara kualitatif melalui penafsiran gramatikal, sistematis, teleologis, dan konstitusional. Setiap tindakan yang diduga terjadi dipilah berdasarkan tempus delicti, subjek, objek, modus, tujuan, dasar kewenangan, dan akibat. Selanjutnya dilakukan pengujian unsur delik dan kesalahan secara terpisah, termasuk pembedaan antara intersepsi transmisi, akses tanpa hak terhadap sistem, perubahan atau penghapusan informasi elektronik, serta penyertaan dalam tindak pidana. Prinsip hukum antarwaktu diperiksa dengan memperhatikan tanggal mulai berlakunya KUHP dan KUHAP baru serta perubahan ketentuan umum melalui Undang-Undang Nomor 1 Tahun 2026. Prinsip fikih dianalisis secara normatif dengan menimbang larangan tajassus, perlindungan kehormatan, amanah, kemaslahatan, dan batas kewenangan penguasa(Diantha, 2019). Hasilnya disintesiskan untuk merumuskan parameter pertanggungjawaban yang koheren dan tidak melampaui fakta yang tersedia.

HASIL DAN PEMBAHASAN

Konstruksi Konseptual Penyadapan dan Batas Legalitas Intersepsi

Istilah penyadapan dalam praktik hukum Indonesia kerap digunakan untuk menunjuk tindakan memperoleh isi atau informasi komunikasi yang tidak ditujukan kepada pihak yang melakukan pengawasan. Dalam terminologi teknologi dan regulasi, istilah intersepsi lebih spesifik merujuk pada tindakan mendengarkan, merekam, membelokkan, mengubah, menghambat, atau mencatat transmisi informasi elektronik dan/atau dokumen elektronik yang tidak bersifat publik. Penyadapan dapat dilakukan melalui jaringan kabel maupun nirkabel, dan dalam konteks digital dapat melibatkan pengambilan metadata, akses terhadap sistem, perekaman isi komunikasi, maupun pemantauan lalu lintas data. Akan tetapi, tindakan-tindakan tersebut tidak selalu identik secara yuridis. Intersepsi atas transmisi, akses terhadap sistem, pengumpulan data yang telah tersimpan, dan penghapusan data merupakan perbuatan yang harus dianalisis berdasarkan objek serta unsur delik masing-masing(Christianto, 2020).

Pembedaan konseptual tersebut penting karena istilah "penyadapan ilegal" dalam pemberitaan belum dengan sendirinya menjelaskan konstruksi pidana yang tepat. Perlu ditentukan apakah dugaan perbuatan berupa intersepsi atas transmisi nonpublik, akses tanpa hak terhadap sistem elektronik, penggunaan kredensial di luar lingkup kewenangan, pengambilan atau pemindahan data, penyebarluasan hasil komunikasi, atau penghapusan informasi elektronik. Satu rangkaian fakta dapat memuat beberapa tindakan, tetapi penegak hukum tetap wajib menguraikan hubungan faktual dan normatif setiap tindakan. Penggunaan beberapa pasal secara kumulatif harus memiliki dasar yang jelas agar tidak terjadi tumpang tindih kualifikasi, perluasan makna delik, atau penghukuman ganda atas perbuatan yang sama(Hikmawati, 2022).

Legalitas intersepsi harus dinilai berdasarkan sekurang-kurangnya empat dimensi. Pertama, kompetensi kewenangan, yaitu apakah institusi dan pejabat yang melakukan atau memerintahkan intersepsi memperoleh kewenangan secara tegas dari undang-undang. Kedua, legitimasi tujuan, yaitu apakah intersepsi dilakukan untuk penegakan hukum atau tujuan publik lain yang secara limitatif dibenarkan hukum. Ketiga, legitimasi prosedural, yakni apakah permintaan, persetujuan, aktivasi, jangka waktu, pembatasan sasaran, dan pengelolaan hasil telah mengikuti prosedur yang sah. Keempat, proporsionalitas, yakni apakah intrusi terhadap hak komunikasi merupakan tindakan yang benar-benar diperlukan, memiliki hubungan rasional dengan tujuan, serta dibatasi pada lingkup yang tidak berlebihan. Kewenangan teknis untuk mengoperasikan suatu sistem tidak dapat menggantikan dasar hukum substantif untuk melakukan intersepsi.

Standar internasional memperkuat kerangka tersebut. Pasal 17 ICCPR melindungi setiap orang dari intervensi yang melawan hukum atau sewenang-wenang terhadap kehidupan privat, keluarga, rumah, dan korespondensinya. Komite Hak Asasi Manusia PBB melalui Komentar Umum Nomor 16 menegaskan bahwa perlindungan tersebut berlaku terhadap tindakan aparat negara maupun aktor

nonnegara, sehingga negara wajib membangun perlindungan legislatif, administratif, dan yudisial. Resolusi Majelis Umum PBB 68/167 mengenai hak atas privasi pada era digital juga menegaskan bahwa perlindungan privasi berlaku dalam komunikasi digital dan meminta negara meninjau prosedur, praktik, serta peraturan mengenai pengawasan dan intersepsi komunikasi. Dalam kerangka ini, legalitas formal saja belum memadai apabila tindakan tetap bersifat arbitrer; pembatasan harus dapat dibenarkan berdasarkan tujuan yang sah, kebutuhan konkret, dan proporsionalitas. Standar tersebut relevan untuk menilai tindakan pengawasan yang melibatkan pejabat publik tanpa menjadikan status pejabat sebagai satu-satunya dasar perlindungan.

Putusan Mahkamah Konstitusi Nomor 5/PUU-VIII/2010 memberikan pijakan penting mengenai sifat intrusif penyadapan. Mahkamah menegaskan bahwa penyadapan merupakan pembatasan terhadap hak privasi dan bahwa tata cara serta batas kewenangannya perlu diatur pada tingkat undang-undang agar tidak terjadi penyalahgunaan. Putusan tersebut juga menyatakan Pasal 31 ayat (4) Undang-Undang ITE 2008 tidak mempunyai kekuatan hukum mengikat, karena pembatasan hak asasi tidak dapat diserahkan kepada pengaturan yang tidak memadai pada tingkat peraturan pelaksana. Putusan ini tidak berarti bahwa seluruh penyadapan dilarang secara absolut. Makna konstitusionalnya adalah kewenangan tersebut hanya dapat dijalankan berdasarkan dasar hukum yang jelas, dengan batasan serta mekanisme pengawasan yang dapat diuji(M. K. R. Indonesia, 2011).

Putusan Mahkamah Konstitusi Nomor 20/PUU-XIV/2016 juga relevan dalam konteks pembuktian. Putusan tersebut memberikan penegasan mengenai penggunaan informasi atau dokumen elektronik sebagai alat bukti dalam rangka penegakan hukum atas permintaan institusi penegak hukum yang ditentukan undang-undang. Putusan ini tidak tepat dibaca sebagai pengesahan umum terhadap setiap bentuk pengumpulan informasi digital, dan tidak pula menggantikan kewajiban untuk membuktikan autentisitas, integritas, serta legalitas cara perolehan bukti. Dengan demikian, legalitas tindakan memperoleh informasi dan admissibilitas bukti merupakan dua persoalan yang berhubungan, tetapi tidak identik. Bukti dapat autentik secara teknis, namun perolehannya tetap dapat dipersoalkan secara hukum; sebaliknya, dasar kewenangan yang sah tidak meniadakan kewajiban menjaga integritas bukti(M. K. R. Indonesia, 2016).

Rezim Hukum Pidana Antarwaktu: Perbuatan Sebelum dan Sesudah 2 Januari 2026

Perubahan rezim hukum pada 2 Januari 2026 menjadi variabel sentral dalam menentukan hukum yang berlaku terhadap dugaan penyadapan yang diberitakan berlangsung pada 2025–2026. Undang-Undang Nomor 1 Tahun 2023 tentang KUHP mulai berlaku pada 2 Januari 2026(R. Indonesia, 2023). Pada tanggal yang sama, Undang-Undang Nomor 20 Tahun 2025 tentang KUHAP mulai berlaku dan mencabut Undang-Undang Nomor 8 Tahun 1981(R. Indonesia, 2025). Oleh karena itu, penentuan hukum pidana materiil harus berangkat dari waktu terjadinya setiap perbuatan, sedangkan penentuan hukum acara harus memperhatikan waktu tindakan prosedural dilakukan dan ketentuan peralihan yang relevan.

Untuk tindakan intersepsi yang diduga dilakukan sebelum 2 Januari 2026, norma yang harus diperiksa adalah Pasal 31 ayat (1) dan ayat (2) Undang-Undang ITE sebagaimana berlaku pada saat itu, beserta ketentuan pidana yang terkait. Kedua ayat tersebut mengatur larangan intersepsi atau penyadapan tanpa hak atau melawan hukum terhadap informasi elektronik pada sistem tertentu dan transmisi informasi elektronik atau dokumen elektronik yang tidak bersifat publik. Ketentuan tersebut tidak boleh diterapkan terhadap perbuatan yang dilakukan setelah dicabut, kecuali terdapat dasar hukum antarwaktu yang sah dan relevan. Dalam konteks ini, kronologi setiap tindakan harus disusun secara individual, bukan hanya diberi label sebagai satu rangkaian peristiwa 2025–2026(R. Indonesia, 2024).

Untuk tindakan sejak 2 Januari 2026, Pasal 258 KUHP Nasional menjadi ketentuan utama yang harus diuji terhadap dugaan penyadapan komunikasi elektronik. Pasal tersebut pada pokoknya mengatur perbuatan melawan hukum berupa mendengarkan, merekam, membelokkan, mengubah, menghambat, dan/atau mencatat transmisi informasi elektronik atau dokumen elektronik yang tidak bersifat publik, termasuk penyebarluasan hasil pembicaraan atau perekaman. Ketentuan pengecualian dalam ayat berikutnya mengakui pelaksanaan tindakan berdasarkan peraturan perundang-undangan atau perintah jabatan yang sah sebagaimana dirujuk dalam KUHP. Pengecualian ini tidak dapat ditafsirkan sebagai kekebalan bagi setiap orang yang mengaku bertindak atas perintah atasan. Perintah jabatan harus berada dalam lingkup kewenangan, memiliki tujuan yang sah, dan tidak bertentangan dengan syarat hukum yang mengatur tindakan tersebut(Winriadirahman et al., 2026).

Perubahan melalui Undang-Undang Nomor 1 Tahun 2026 tentang Penyesuaian Pidana juga perlu dibaca sebagai bagian dari rezim hukum yang berlaku. Undang-undang tersebut mengubah sejumlah ketentuan umum KUHP, termasuk pengaturan mengenai perubahan peraturan perundang-undangan setelah perbuatan dilakukan. Karena itu, penilaian mengenai hukum yang lebih menguntungkan tidak boleh dilakukan hanya berdasarkan rumusan asas yang dipahami secara umum tanpa memeriksa bunyi ketentuan Pasal 3 KUHP setelah penyesuaian. Penegak hukum harus membandingkan norma yang berlaku pada saat perbuatan dilakukan dengan ketentuan yang berlaku kemudian, memperhatikan apakah perbuatan masih dikualifikasikan sebagai tindak pidana, dan menerapkan ketentuan peralihan secara konsisten. Hal ini menjadi semakin penting apabila satu rangkaian kejadian mencakup tindakan intersepsi, akses sistem, penyebaran informasi, dan penghapusan data pada tanggal yang berbeda(R. Indonesia, 2026).

Pembedaan rezim hukum acara harus dilakukan secara terpisah dari hukum pidana materiil. KUHAP baru berlaku sejak 2 Januari 2026 dan mengatur kembali kewenangan penyidik, upaya paksa, hak tersangka dan korban, bukti, koordinasi penegak hukum, serta mekanisme pengujian prosedur. Tindakan penyidikan yang dilakukan setelah tanggal tersebut harus diuji menurut KUHAP baru, dengan memperhatikan ketentuan peralihan bagi tindakan yang telah dimulai sebelumnya. Dengan demikian, tempus delicti menentukan kerangka hukum pidana materiil, sedangkan tempus tindakan prosedural menentukan kerangka hukum acara. Pemisahan ini menghindari penerapan retroaktif dan menjaga kepastian hukum bagi semua pihak.

Unsur Tindak Pidana dan Konstruksi Pertanggungjawaban Individual

Pertanggungjawaban pidana atas intersepsi tidak dapat dibentuk hanya dari fakta bahwa seseorang memiliki jabatan, mengendalikan akses sistem, atau berada dalam struktur organisasi yang terkait dengan fasilitas penyadapan. Asas pertanggungjawaban individual menuntut pembuktian perbuatan dan kesalahan setiap orang. Dalam analisis Pasal 258 KUHP, unsur perbuatan harus diidentifikasi secara spesifik, termasuk apakah tindakan yang dilakukan berupa mendengarkan, merekam, membelokkan, mengubah, menghambat, atau mencatat transmisi nonpublik. Unsur melawan hukum selanjutnya menuntut pengujian terhadap ada tidaknya kewenangan dan terpenuhi tidaknya syarat penggunaan kewenangan. Unsur kesalahan harus dibuktikan melalui keadaan batin yang relevan menurut rumusan delik, bukan disimpulkan semata-mata dari akibat atau kontroversi tindakan(Febriansyah et al., 2026).

Apabila dugaan tindakan melibatkan akses terhadap sistem elektronik, Pasal 332 KUHP perlu dipertimbangkan sepanjang fakta memenuhi unsur kesengajaan, ketiadaan hak atau sifat melawan hukum, dan akses terhadap komputer atau sistem elektronik milik orang lain. Namun, akses oleh pegawai atau pejabat yang secara formal memiliki kredensial tidak otomatis dapat disamakan dengan akses yang sah untuk semua tujuan. Pemeriksaan harus menentukan apakah akses berada dalam batas tugas, apakah penggunaan kredensial melampaui kewenangan, dan apakah pelaku secara sadar mengetahui bahwa tindakan tersebut tidak diperbolehkan. Pembedaan ini penting dalam lingkungan organisasi, ketika seseorang dapat memiliki akses teknis tetapi tidak memiliki otorisasi substantif untuk tujuan tertentu(Kusuma et al., 2025).

Dugaan penghapusan data hasil intersepsi harus dikualifikasikan secara terpisah dari intersepsi itu sendiri. Penghapusan data dapat menjadi bagian dari tata kelola yang sah apabila dilakukan berdasarkan kewenangan, jadwal retensi, serta prosedur pemusnahan yang terdokumentasi. Sebaliknya, penghapusan tanpa hak yang menyentuh informasi elektronik milik orang lain atau informasi elektronik yang bersifat publik di dalam sistem elektronik dapat menimbulkan persoalan berdasarkan ketentuan Pasal 32 Undang-Undang ITE yang tetap berlaku, sepanjang unsur mengenai perubahan, pemindahan, perusakan, penghilangan, atau penyembunyian informasi elektronik terpenuhi. Kualifikasi pidana tetap mensyaratkan pembuktian terhadap objek, bentuk perbuatan, keadaan tanpa hak, kesengajaan, serta unsur lain yang ditentukan undang-undang. Fakta bahwa suatu file tidak ditemukan tidak dengan sendirinya membuktikan adanya tindakan pidana penghapusan atau motif menghilangkan jejak(Samudra et al., 2026).

Rangkaian peran dalam dugaan tindak pidana perlu dibedakan antara pihak yang menginisiasi permintaan, pihak yang memberi persetujuan, pihak yang memasukkan sasaran ke sistem, operator yang melakukan aktivasi, pihak yang mengakses atau menggunakan hasil, dan pihak yang menghapus data. Kategori peran tersebut merupakan peta investigasi, bukan kesimpulan mengenai pelaku. Untuk menentukan pertanggungjawaban, harus diuji ketentuan penyertaan dalam KUHP, termasuk apakah

seseorang bertindak sebagai pelaku, orang yang menyuruh melakukan, turut serta, penganjur, atau pembantu. Penilaian harus berdasarkan kontribusi konkret, kesengajaan atau bentuk kesalahan yang disyaratkan, hubungan perbuatan dengan tindak pidana, serta bukti yang mendukung atribusi tersebut.

Perintah atasan tidak dapat diperlakukan sebagai alasan pembenar secara otomatis. Hukum membedakan perintah jabatan yang sah dari perintah yang diberikan tanpa kewenangan atau melampaui batas kewenangan. Bagi pelaksana teknis, pertanyaan yang harus dijawab mencakup apakah ia mengetahui ketiadaan dasar hukum, apakah terdapat kewajiban untuk melakukan verifikasi, apakah ia memiliki kesempatan untuk menolak, dan apakah ia secara sadar tetap melaksanakan tindakan yang terlarang. Bagi pemberi perintah, perlu dibuktikan isi perintah, kewenangan faktual untuk mengarahkan pelaksanaan, pengetahuan mengenai sifat melawan hukum, serta kontribusi terhadap terjadinya tindak pidana. Dengan demikian, struktur hierarkis tidak boleh dijadikan jalan pintas untuk menentukan kesalahan bawahan maupun atasan.

Pemisahan antara pelanggaran administrasi, pelanggaran disiplin, pelanggaran etik, dan tindak pidana juga merupakan keharusan. Tidak setiap ketidaktertiban dokumentasi atau ketidakpatuhan prosedural memenuhi unsur delik. Namun, pelanggaran prosedural dapat menjadi bukti penting apabila menunjukkan bahwa tindakan dilakukan tanpa dasar kewenangan, dengan pengetahuan atas ketiadaan izin, atau untuk tujuan yang dilarang. Sebaliknya, penegak hukum tidak boleh mengubah setiap kesalahan administratif menjadi tindak pidana tanpa pembuktian unsur. Pengujian yang cermat menjaga keseimbangan antara efektivitas penegakan hukum, kepastian hukum, dan perlindungan dari kriminalisasi yang tidak proporsional.

Keamanan Negara, Fungsi Konstitusional, dan Batas Kriminalisasi

Penyadapan terhadap komunikasi Presiden dan pejabat negara memiliki dimensi institusional yang patut diperhatikan karena komunikasi tertentu dapat berhubungan dengan penyelenggaraan fungsi konstitusional, keamanan informasi strategis, koordinasi kebijakan, dan perlindungan kepentingan nasional. Namun, perlindungan tersebut bukan privilese personal yang membebaskan pejabat dari pengawasan hukum. Presiden, pejabat negara, dan tokoh publik tetap berada dalam lingkup prinsip persamaan di hadapan hukum. Keistimewaan analitis terletak pada kemungkinan dampak institusional dari intersepsi, bukan pada penghapusan akuntabilitas pejabat atau pemberian imunitas terhadap proses penegakan hukum(Prasetyo et al., 2024).

Keamanan negara perlu dibedakan dari keamanan rezim, kepentingan politik pejabat, atau perlindungan reputasi individu yang sedang menjalankan jabatan. Keamanan negara berhubungan dengan kedaulatan, keutuhan wilayah, keselamatan masyarakat, ketahanan institusi, dan keberlangsungan tatanan konstitusional. Karena itu, penggunaan frasa “kepentingan keamanan negara” harus disertai identifikasi ancaman, objek yang dilindungi, dasar hukum, kebutuhan tindakan, serta mekanisme pengawasan. Pengumpulan informasi oleh institusi negara dapat dibenarkan dalam kondisi tertentu jika diotorisasi undang-undang dan dilakukan secara proporsional. Akan tetapi, tujuan keamanan tidak dapat menjadi alasan yang berdiri sendiri untuk mengakses komunikasi privat secara tidak terbatas(E. A. Putri et al., 2025).

Dugaan penyadapan terhadap seorang Presiden tidak otomatis merupakan tindak pidana makar, pengkhianatan, atau kejahatan terhadap keamanan negara. Kualifikasi tersebut hanya dapat dipertimbangkan apabila terdapat norma pidana khusus yang relevan dan seluruh unsur objektif maupun subjektifnya terbukti. Tindakan penyadapan tanpa hak dapat lebih tepat dianalisis terlebih dahulu sebagai tindak pidana terhadap kerahasiaan komunikasi, akses sistem, atau integritas data, bergantung pada perbuatan konkret. Apabila terdapat bukti tambahan mengenai pengumpulan atau pembocoran informasi pertahanan, gangguan terhadap sistem strategis, atau tindakan lain yang memenuhi rumusan delik keamanan negara, barulah konstruksi pidana khusus dapat diuji. Tanpa pembuktian unsur tersebut, penggunaan label kejahatan terhadap negara berisiko memperluas kriminalisasi dan mengaburkan asas legalitas.

Aspek keamanan negara juga memuat kewajiban positif untuk menjaga sistem intersepsi itu sendiri. Sistem yang dapat mengakses komunikasi privat harus memiliki kontrol keamanan yang ketat, pembagian hak akses, autentikasi berlapis, pencatatan yang tidak mudah diubah, dan audit berkala. Penyalahgunaan oleh orang dalam menunjukkan bahwa ancaman tidak selalu berasal dari aktor eksternal, tetapi dapat muncul dari penyimpangan akses yang sah secara teknis namun tidak sah secara hukum. Karena itu, perlindungan keamanan nasional harus mencakup pencegahan penyalahgunaan

internal, keamanan data, pengawasan institusional, dan penegakan pertanggungjawaban yang transparan.

Bukti Elektronik, Integritas Data, dan Hukum Acara Pidana

Dalam perkara intersepsi, bukti elektronik berpotensi menjadi sumber utama untuk merekonstruksi kronologi, identitas pengguna, alur instruksi, sasaran komunikasi, perubahan konfigurasi, akses terhadap hasil, serta penghapusan data. Jenis bukti dapat meliputi log sistem, metadata, catatan autentikasi, daftar akun, rekaman perintah, konfigurasi perangkat, cadangan data, artefak aplikasi, dan hasil pemeriksaan forensik. Namun, keberadaan data digital tidak dengan sendirinya menjamin kebenaran peristiwa. Bukti harus diuji dari aspek autentisitas, integritas, relevansi, reliabilitas metode perolehan, serta hubungan antara data dan subjek yang diduga melakukan tindakan(Paripurna et al., 2025).

Rantai penguasaan barang bukti digital harus didokumentasikan sejak tahap identifikasi, pengamanan, akuisisi, penyalinan, pemeriksaan, penyimpanan, hingga penyajian di persidangan. Pemeriksa perlu mencatat sumber perangkat, kondisi awal, waktu dan zona waktu, metode akuisisi, alat serta versi perangkat lunak yang digunakan, nilai hash, identitas petugas, dan setiap perpindahan penguasaan. Nilai hash membantu memastikan bahwa salinan tidak berubah setelah proses akuisisi, tetapi tidak dengan sendirinya membuktikan bahwa data sumber tidak pernah dimanipulasi sebelumnya atau bahwa data yang diperoleh lengkap. Karena itu, pemeriksaan harus menggunakan metode yang dapat diaudit dan, sepanjang mungkin, dapat direplikasi oleh ahli lain(N. A. F. S. B. Putri & Rusdiana, 2026).

Apabila terdapat dugaan penghapusan hasil intersepsi, pemeriksaan forensik perlu menguji log penghapusan, riwayat akses, snapshot, cadangan data, artefak sistem, dan kemungkinan pemulihan informasi. Pemeriksaan juga harus membedakan penghapusan log audit, penghapusan berkas hasil intersepsi, pengubahan metadata, dan penghapusan data pada perangkat pengguna. Masing-masing tindakan dapat menimbulkan konsekuensi yang berbeda. Penegak hukum tidak boleh menyimpulkan adanya penghilangan barang bukti hanya berdasarkan ketidaktersediaan berkas, tanpa menguji kemungkinan kerusakan teknis, rotasi log otomatis, kebijakan retensi, atau tindakan pemusnahan yang sah.

Legalitas perolehan bukti merupakan isu yang berbeda dari autentisitas teknis. Bukti digital yang secara teknis utuh tetap dapat dipersoalkan apabila diperoleh melalui intersepsi yang tidak memiliki dasar kewenangan atau dilakukan di luar prosedur. Sebaliknya, bukti yang diperoleh berdasarkan kewenangan sah tetap harus memenuhi persyaratan integritas dan keandalan. Putusan Mahkamah Konstitusi Nomor 20/PUU-XIV/2016 mempertegas pentingnya keterkaitan penggunaan informasi elektronik sebagai alat bukti dengan proses penegakan hukum dan permintaan institusi yang memiliki kewenangan berdasarkan undang-undang. Dalam proses peradilan, ruang bagi pihak yang berperkara untuk menguji cara perolehan dan keutuhan bukti merupakan bagian dari fair trial.

KUHAP berdasarkan Undang-Undang Nomor 20 Tahun 2025 menjadi kerangka prosedural yang harus diperhatikan untuk tindakan penyidikan dan pembuktian setelah tanggal berlakunya. Penguatan hak tersangka, korban, saksi, advokat, serta mekanisme pengujian tindakan penyidik merupakan bagian penting untuk memastikan bahwa penggunaan teknologi investigatif tidak menghapus perlindungan prosedural. Pengawasan terhadap intersepsi harus dapat diperiksa melalui mekanisme hukum acara yang tersedia, sedangkan tindakan penyitaan, pemeriksaan perangkat, dan akuisisi data harus mengikuti syarat kewenangan dan dokumentasi. Dengan demikian, efektivitas investigasi digital tidak dapat dipisahkan dari jaminan proses yang adil.

Analisis Fikih Siyasah Jinayah: Tajassus, Amanah, Maslahah, dan Ta‘zir

Dalam perspektif fikih siyasah jinayah, penyadapan komunikasi elektronik dapat dianalisis melalui relasi antara larangan tajassus, perlindungan kehormatan, kewajiban amanah, kemaslahatan umum, dan kewenangan penguasa dalam mencegah kejahatan. Tajassus secara umum menunjuk tindakan mencari atau mengungkap hal-hal tersembunyi dari orang lain, terutama urusan privat yang tidak diperuntukkan bagi pengetahuan publik. QS Al-Hujurat [49]:12 memuat larangan tajassus dalam rangka menjaga kehormatan dan hubungan sosial, sedangkan QS An-Nur [24]:27 mengatur etika memasuki ruang privat dengan izin. Kedua prinsip tersebut memberi landasan bahwa ruang pribadi dan kerahasiaan tidak boleh ditembus semata-mata karena seseorang memiliki kemampuan teknis untuk melakukannya(Nisa’, 2021).

Larangan tajassus tidak dapat ditafsirkan secara sederhana sebagai larangan terhadap seluruh kegiatan intelijen atau pengumpulan informasi oleh negara. Dalam tradisi siyasah, penguasa memiliki tanggung jawab menjaga keamanan dan mencegah bahaya terhadap masyarakat. Namun, kewenangan itu merupakan amanah, bukan hak tanpa batas. Pengumpulan informasi hanya dapat dipertimbangkan apabila terdapat dasar kepentingan publik yang nyata, ancaman atau dugaan tindak pidana yang cukup spesifik, otorisasi dari pihak yang berwenang, kebutuhan yang dapat dijelaskan, dan pembatasan terhadap objek maupun durasi. Pengawasan atas kehidupan privat tanpa alasan yang sah, terutama untuk kepentingan pribadi atau politik, bertentangan dengan perlindungan kehormatan dan prinsip amanah(Putra et al., 2024).

Prinsip amanah menuntut pejabat menggunakan kewenangan sesuai tujuan pemberiannya dan tidak mengalihkan sarana negara untuk kepentingan yang tidak sah. Dalam konteks sistem intersepsi, akses teknis merupakan tanggung jawab yang harus dilaksanakan berdasarkan batas mandat. Penggunaan sistem untuk memantau komunikasi tanpa hubungan dengan proses penegakan hukum atau tujuan publik yang diakui hukum dapat dinilai sebagai penyimpangan amanah. Apabila tindakan itu disertai pengambilan, pemanfaatan, atau penghapusan data secara merugikan, penilaian fikih dapat mencakup unsur ta‘addi (melampaui batas), khiyanah (pengkhianatan terhadap amanah), dan dharar (menimbulkan kerugian), dengan tetap menilai fakta serta konteksnya secara hati-hati.

Prinsip maslahah menghendaki agar kebijakan penguasa diarahkan pada perlindungan kepentingan umum, bukan kepentingan individual pemegang kekuasaan. Kemaslahatan tidak cukup dinyatakan secara abstrak; ia harus diuji berdasarkan manfaat yang nyata, risiko kerugian, proporsionalitas sarana, dan kemungkinan penggunaan cara lain yang lebih ringan. Kaidah bahwa tindakan darurat harus diukur sesuai kadar kedaruratannya (al-darurat tuqaddaru bi qadariha) dapat menjadi parameter pembatas: alasan keamanan hanya membenarkan tindakan sejauh benar-benar diperlukan. Demikian pula, prinsip pencegahan kerusakan harus dipertimbangkan bersama kewajiban mencegah kezaliman dan pelanggaran hak. Dengan pendekatan tersebut, kebutuhan keamanan nasional tidak meniadakan privasi, tetapi harus diharmonisasikan dengan batas etis dan yuridis.

Dari sudut fikih jinayah, perbuatan intersepsi tanpa hak tidak secara otomatis masuk ke dalam kategori hudud atau qisas. Dalam banyak keadaan, tindakan tersebut lebih dekat kepada jarimah ta‘zir karena bentuk dan sanksinya tidak ditentukan secara spesifik sebagai hudud atau qisas, sedangkan otoritas yang sah dapat menetapkan konsekuensi yang proporsional untuk melindungi masyarakat. Penilaian ta‘zir harus memperhatikan unsur perbuatan, kesengajaan, tingkat bahaya, kerugian korban, penyalahgunaan amanah, serta dampaknya terhadap ketertiban umum. Konstruksi ini tidak berarti hukum positif Indonesia dapat digantikan oleh kategori fikih; analisis fikih berfungsi sebagai perspektif normatif dan etis untuk menilai sifat tercela, tujuan perlindungan, dan prinsip keadilan dalam kebijakan pidana(Ubaidillah, 2025).

Pertanggungjawaban dalam fikih jinayah juga menuntut hubungan antara perbuatan dan pelaku. Unsur syar‘i berkaitan dengan dasar larangan dan legitimasi penetapan hukuman; unsur maddi berhubungan dengan tindakan nyata seperti memantau, merekam, mengambil, menyebarkan, atau menghapus data; sedangkan unsur adabi berkaitan dengan kemampuan bertanggung jawab dan sikap batin pelaku. Pemetaan ini dapat memperkaya analisis hukum positif karena menegaskan bahwa penilaian tidak cukup hanya berdasarkan akibat atau jabatan. Pelaku yang bertindak tanpa pengetahuan atau tanpa kehendak tertentu harus dinilai berbeda dari pihak yang dengan sadar memerintahkan atau melaksanakan tindakan yang dilarang. Prinsip keadilan mengharuskan pertanggungjawaban disesuaikan dengan peran dan kadar kesalahan masing-masing.

Dengan demikian, fikih siyasah jinayah memberikan dua arah penilaian. Pada sisi perlindungan individu, tajassus, pelanggaran kehormatan, dan penyalahgunaan amanah merupakan dasar kritik terhadap intersepsi yang tidak memiliki alasan sah. Pada sisi kewenangan negara, pengumpulan informasi yang diperlukan untuk mencegah ancaman serius dapat dipertimbangkan sebagai tindakan siyasah sepanjang terikat pada otorisasi, kebutuhan, proporsionalitas, dan akuntabilitas. Sintesis tersebut menghindari dua ekstrem: menganggap semua pengawasan negara sebagai tindakan terlarang atau menganggap seluruh tindakan pengawasan dapat dibenarkan atas nama kemaslahatan.

Sintesis dan Parameter Penilaian Pertanggungjawaban Pidana

Analisis hukum pidana, keamanan negara, dan fikih siyasah jinayah menunjukkan adanya titik temu pada prinsip pembatasan kewenangan. Hukum pidana menuntut dasar delik, sifat melawan

hukum, dan kesalahan; hukum tata negara membatasi tindakan negara melalui legalitas, perlindungan hak, serta pengawasan; sedangkan fikih siyasah menempatkan kewenangan sebagai amanah yang harus diarahkan pada maslahah dan tidak boleh berubah menjadi tajassus tanpa dasar yang sah. Ketiga perspektif tersebut tidak identik dan tidak boleh dicampuradukkan. Hukum positif menentukan dasar pemidanaan, sedangkan perspektif konstitusional dan fikih membantu menjelaskan legitimasi, tujuan, serta batas moral-yuridis dari penggunaan kewenangan intersepsi(Nababan et al., 2023).

Berdasarkan sintesis tersebut, penilaian terhadap dugaan penyadapan perlu dilakukan melalui urutan pengujian yang konsisten. Pertama, identifikasi perbuatan dan waktunya secara rinci. Kedua, tentukan norma pidana yang berlaku pada tempus delicti, termasuk ketentuan peralihan. Ketiga, periksa sumber kewenangan dan keabsahan otorisasi. Keempat, uji unsur objektif dan subjektif delik, termasuk bentuk kesalahan serta peran setiap orang. Kelima, periksa legalitas perolehan, autentisitas, integritas, dan rantai penguasaan bukti elektronik. Keenam, nilai apakah terdapat dimensi keamanan negara yang memenuhi rumusan delik khusus, bukan semata-mata didasarkan pada jabatan sasaran. Ketujuh, evaluasi tindakan berdasarkan prinsip tajassus, amanah, maslahah, dan proporsionalitas sebagai kerangka etis-yuridis tambahan(Natamiharja et al., 2022).

Parameter tersebut juga mengarah pada kebutuhan perbaikan tata kelola sistem intersepsi. Pengawasan tidak cukup berhenti pada persetujuan awal, tetapi harus mencakup keseluruhan siklus data. Sistem perlu menerapkan pemisahan kewenangan antara pemohon, pemberi persetujuan, operator, penyimpan, dan auditor; pencatatan elektronik yang tidak mudah dimodifikasi; autentikasi berlapis; pembatasan akses berbasis kebutuhan; penetapan batas waktu; audit independen; dan prosedur pemusnahan yang terdokumentasi. Hasil intersepsi harus dibatasi pada tujuan yang telah disahkan, sedangkan data yang tidak relevan harus dikelola menurut ketentuan retensi dan perlindungan data. Mekanisme pengaduan dan pemulihan harus tersedia bagi pihak yang dirugikan, tanpa mengabaikan kepentingan sah penyidikan(Roselin & Putra, 2025).

Kebutuhan pengawasan independen menjadi semakin penting ketika sistem intersepsi berada dalam kendali institusi yang juga memiliki fungsi penyelidikan dan penyidikan. Tanpa pemisahan fungsi, pencatatan yang dapat diaudit, dan pengawasan eksternal, proses verifikasi dapat berubah menjadi pemeriksaan internal yang tidak cukup independen. Pembentuk undang-undang perlu memastikan bahwa dasar intersepsi, pejabat yang berwenang, jenis tindak pidana yang dapat menjadi alasan, standar permulaan bukti, prosedur persetujuan, batas waktu, penanganan materi hasil, serta mekanisme pengawasan dan pemulihan diatur secara jelas. Penguatan tersebut bukan untuk melemahkan penegakan hukum, melainkan untuk memastikan bahwa penggunaan kewenangan intrusif dapat dipertanggungjawabkan secara hukum dan memperoleh legitimasi publik.

Perkara yang menjadi konteks penelitian masih harus dibuktikan melalui pemeriksaan alat bukti dan proses peradilan. Karena itu, kesimpulan yuridis mengenai siapa yang melakukan, siapa yang memerintahkan, apa motifnya, dan pasal apa yang terbukti tidak dapat ditetapkan hanya berdasarkan pemberitaan atau pengumuman penyidikan. Penelitian normatif ini menawarkan kerangka untuk membaca fakta ketika kelak tersedia dokumen resmi, dakwaan, keterangan ahli, dan putusan pengadilan. Pengujian faktual lanjutan tetap diperlukan untuk memastikan apakah tindakan yang diduga terjadi memenuhi unsur Pasal 31 UU ITE yang berlaku sebelum 2 Januari 2026, Pasal 258 KUHP setelah tanggal tersebut, ketentuan akses tanpa hak, atau norma lain yang relevan.

KESIMPULAN

Dugaan penyadapan komunikasi elektronik terhadap Presiden Republik Indonesia, pejabat negara, dan tokoh publik harus dianalisis melalui pemisahan yang cermat antara legalitas kewenangan, unsur tindak pidana, kesalahan individual, dampak terhadap keamanan negara, dan prinsip fikih siyasah jinayah. Penyadapan tidak otomatis menjadi sah hanya karena dilakukan melalui sistem milik institusi negara atau oleh personel yang memiliki akses teknis; keabsahannya bergantung pada dasar kewenangan, tujuan yang sah, otorisasi, kebutuhan, proporsionalitas, pembatasan waktu, serta pengawasan terhadap hasil intersepsi. Pertanggungjawaban pidana harus ditentukan berdasarkan perbuatan konkret dan kontribusi setiap orang, dengan membedakan intersepsi, akses tanpa hak, penggunaan atau penyebarluasan hasil, serta perubahan atau penghapusan data. Pelanggaran prosedural tidak serta-merta identik dengan tindak pidana, tetapi dapat menjadi fakta penting apabila berkaitan dengan unsur melawan hukum dan kesalahan yang dirumuskan undang-undang. Karena dugaan peristiwa diberitakan melintasi 2 Januari 2026, penentuan hukum materiil harus didasarkan pada tempus

delicti dan perubahan rezim KUHP, sedangkan tindakan prosedural harus dinilai menurut KUHAP serta ketentuan peralihannya. Dari perspektif keamanan negara, penyadapan terhadap pejabat publik dapat menimbulkan risiko institusional, tetapi tidak otomatis merupakan makar atau kejahatan terhadap keamanan negara tanpa pembuktian unsur delik khusus. Dalam fikih siyasah jinayah, intersepsi tanpa dasar yang sah dapat beririsan dengan larangan tajassus, pelanggaran amanah, dan timbulnya dharar, sedangkan tindakan pengumpulan informasi untuk mencegah ancaman serius hanya dapat dipertimbangkan sepanjang memenuhi maslahah, kebutuhan, dan pembatasan yang ketat. Penelitian ini menegaskan perlunya tata kelola intersepsi yang akuntabel melalui pemisahan fungsi, audit independen, integritas bukti digital, perlindungan data, dan mekanisme pemulihan. Kesimpulan mengenai pertanggungjawaban pihak tertentu tetap harus menunggu pembuktian yang sah dan putusan pengadilan.

DAFTAR PUSTAKA

Anggraeniko, L. S., Ambarwati, A., & Utami, F. R. (2026). Admissibility of digital evidence in Indonesia: Criminal–civil implications for the chain of custody and evidentiary validity. *Priviet Social Sciences Journal*, *6*(4), 483–494. https://doi.org/10.55942/pssj.v6i4.1566

Christianto, H. (2020). From crime control model to due process model: A critical study of wiretapping arrangement by the Corruption Eradication Commission of Indonesia. *Padjadjaran Jurnal Ilmu Hukum (Journal of Law)*, *7*(3), 421–442. https://doi.org/10.22304/pjih.v7n3.a7

Diantha, I. M. P. (2019). *Metodologi penelitian hukum normatif dalam justifikasi teori hukum (Cetakan ke-3)*. Prenadamedia Group.

Efendi, J., & Ibrahim, J. (2022). *Metode penelitian hukum normatif dan empiris (Edisi ke-2)*. Kencana.

Febriansyah, A., Flambonita, S., Banjarani, D. R., & Novianti, V. (2026). The dilemma of wiretapping in corruption crimes in Indonesia: A legal reform perspective based on human rights. *Jurnal Bina Mulia Hukum*, *10*(2), 327–344. https://doi.org/10.24198/jbmh.v10i2.2525

Hikmawati, P. (2022). Pengaturan izin penyadapan oleh KPK pasca Putusan Mahkamah Konstitusi Nomor 70/PUU-XVII/2019. *Negara Hukum: Membangun Hukum Untuk Keadilan Dan Kesejahteraan*, *13*(1), 83–102. https://doi.org/10.22212/jnh.v13i1.2969

Indonesia, M. K. R. (2011). *Putusan Nomor 5/PUU-VIII/2010, diucapkan pada 24 Februari 2011, tentang pengujian Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*. https://mkri.id/public/content/persidangan/putusan/Putusan 5_PUU_VIII_2010 _edit panitera_.pdf

Indonesia, M. K. R. (2016). *Putusan Nomor 20/PUU-XIV/2016 tentang pengujian ketentuan alat bukti elektronik dalam perkara pidana*. https://jdih.mkri.id/produk-hukum/putusan?frase=20%2FPUU-XIV%2F2016

Indonesia, R. (2023). *Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana*. https://peraturan.bpk.go.id/Details/234935/uu-no-1-tahun-2023

Indonesia, R. (2024). *Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*. https://peraturan.bpk.go.id/Details/274494/uu-no-1-tahun-2024

Indonesia, R. (2025). *Undang-Undang Nomor 20 Tahun 2025 tentang Kitab Undang-Undang Hukum Acara Pidana*. https://peraturan.bpk.go.id/Details/337302/uu-no-20-tahun-2025

Indonesia, R. (2026). *Undang-Undang Nomor 1 Tahun 2026 tentang Penyesuaian Pidana*. https://peraturan.bpk.go.id/Details/337869

Kusuma, D. P., Sihotang, E., & Saputra, K. E. D. (2025). Juridical review of wiretapping based on Law Number 1 of 2024 amending Law Number 11 of 2008 on Electronic Information and Transactions related to criminal acts at Bali Regional Police. *Journal of Social Science*, *4*(1), 12–19. https://doi.org/10.57185/joss.v4i1.413

Marzuki, P. M. (2021). *Penelitian hukum (Edisi revisi, cetakan ke-15)*. Kencana.

Nababan, D. M. B., Lasmadi, S., & Erwin. (2023). Pertanggungjawaban pidana terhadap penyalahgunaan data pribadi pada tindak pidana dunia maya. *PAMPAS: Journal of Criminal Law*, *4*(2), 232–251. https://doi.org/10.22437/pampas.v4i2.26981

Natamiharja, R., Sabatira, F., Banjarani, D. R., Davey, O. M., & Setiawan, I. (2022). Balancing two conflicting perspectives on wiretapping act: Rights to privacy and law enforcement. *Al-Risalah: Forum Kajian Hukum Dan Sosial Kemasyarakatan*, *22*(1), 18–30.

https://doi.org/10.30631/alrisalah.v22i1.1226

Nisa', I. S. (2021). Penyadapan telepon dalam pandangan Ahlussunah Wal Jemaah. *Jurnal Sosial Teknologi*, *1*(9), 987–994. https://doi.org/10.59188/jurnalsostech.v1i9.194

Paripurna, A., Lafrance, S., & Indriani, M. (2025). Intelligence surveillance, counterterrorism, and the right to privacy in Indonesia and Canada. *Journal of Southeast Asian Human Rights*, *9*(2), 304–338. https://doi.org/10.19184/jseahr.v9i2.41171

Prasetyo, E. A., Lasmadi, S., & Erwin. (2024). Criminal liability and the application of mens rea in the criminal offence of interception in Indonesia. *Hukum Responsif*, *15*(2), 295–307. https://doi.org/10.33603/responsif.v15i2.9467

Putra, T. I., Islam, A. J., & Rahman, A. M. A. (2024). Integrating Islamic laws into Indonesian data protection laws: An analysis of regulatory landscape and ethical considerations. *Contemporary Issues on Interfaith Law and Society*, *3*(1), 85–118. https://doi.org/10.15294/ciils.v3i1.78690

Putri, E. A., Rahayu, S., & Lasmadi, S. (2025). Tindakan lawful interception oleh penyidik dalam penegakan hukum. *PAMPAS: Journal of Criminal Law*, *6*(3), 324–341. https://doi.org/10.22437/pampas.v6i3.48453

Putri, N. A. F. S. B., & Rusdiana, E. (2026). Addressing the regulatory gap: A legal analysis of wiretapping procedures in the 2025 Criminal Procedure Code. *Lex Journal: Kajian Hukum Dan Keadilan*, *10*(3), 467–483. https://doi.org/10.25139/lex.v10i3.12334

Rahmani, N. P. (2026). Polri: Tiga tersangka penyadapan ilegal sadap Presiden hingga ormas. In *ANTARA News*. https://www.antaranews.com/berita/5829847/polri-tiga-tersangka-penyadapan-ilegal-sadap-presiden-hingga-ormas

Roselin, S., & Putra, M. R. S. (2025). Personal data subject rights protection: A comparative study between Indonesian PDP Law and the UK Data Protection Act. *Jurnal USM Law Review*, *8*(2), 825–835. https://doi.org/10.26623/julr.v8i2.12076

Samudra, A. H., Basu, S., & Perez, C. S. (2026). Digital challenge, analogue mind-set: Assessing Indonesia's electronic criminal evidence framework. *Journal of Indonesian Legal Studies*, *11*(1), 257–298. https://doi.org/10.15294/jils.v11i1.35378

Ubaidillah, M. H. (2025). Electronic information interception from the perspectives of positive law and Islamic criminal law. *Kawanua International Journal of Multicultural Studies*, *6*(1), 51–66. https://doi.org/10.30984/kijms.v6i1.1347

Winriadirahman, P., Faizin, M., & Ramadha, B. S. (2026). Authentication, chain of custody, and the exclusionary rule for electronic evidence under Indonesia's 2025 Criminal Procedure Code. *De Juncto Delicti: Journal of Law*, *6*(2), 195–228. https://doi.org/10.35706/djd.v6i2.13858