JIHHP: Jurnal Ilmu Hukum, Humaniora dan Politik
E-ISSN: 2747-1993
P-ISSN: 2747-2000
https://dinastirev.org/JIHHP dinasti.info@gmail.com +62 811 7404 455
DOI: https://doi.org/10.38035/jihhp.v6i6
https://creativecommons.org/licenses/by/4.0/
Received: 31 Juli 2026 | **Revised**: 28 Agustus 2026 | **Accepted**: 7 September 2026

Implikasi Yuridis Berlakunya KUHP Nasional Terhadap Penyidikan Tindak Pidana *Cyber*

Laurenzo Ivander Taolin[1], Finsensius Samara[2], Elisabet Nanda Pantur[3]
[1]Program Studi Hukum, Universitas Katolik Widya Mandira Kupang, Indonesia, ivantaolin271@gmail.com.
[2]Program Studi Hukum, Universitas Katolik Widya Mandira Kupang, Indonesia, finsensamara16@gmail.com.
[3] Program Studi Hukum, Universitas Katolik Widya Mandira Kupang, Indonesia.

Corresponding Author: finsensamara16@gmail.com

Abstract: *The enactment of the National Criminal code (KUHP NASIONAL) under law Number 1 of 2023 brings fundamnenal changes to Indonesia's criminal law system. The National Code replaces the colonial-era Dutch criminal code and serves as the foundation for reforming substantive criminal law in Indonesia. Meanwhile, rapid developments in information technology have given rise to various new forms of crime known as cyber crime, which have been regulated under the Elektronic Information And Transctions Law (UU ITE). This research aims to analyze the juridical implications of the National Criminal code's enforcement on the investigation cyber criminal offenses, considering aspects of investigator authority, electronic evidence, an the relationship between the National Criminal Code and UU ITE. Rhe research employs a normative legal research method with a statute approach and conceptual approach. The results indicate that the enactment of the National Criminal Code brings significant juridical implications, including the expansion of law enforcement jurisdiction, updates to the concept of criminal liability in the cyber domain,an harmonization of criminal provisions between the Nationsl Criminal Code and UU ITE. Furthemore, the investigation of cyber crime requires adjustmenst in infestigator compentence, electronic evidence seizure procedures, and interagency coordination. This research recommends the establishment of comprehensive technical regulations as guidelines for investigating cybe crimes under the National Criminal Code regime.*

Keywords: *national criminal code, cyber crime, investigigation, electronic evidence, legal implications*

Abstrak: Berlakunya Kitab Undang-Undang Tindak Pidana (KUHP) Nasional berdasarkan Undang -Undang Nomor 1 Tahun 2023 membawa perubahan mendasar dalam sistem hukum pidana Indonesia (Indonesia, Undang-Undang Nomor 1 Tahun 2023 tentang KUHP Nasional, Lembaran Negara Tahun 2023 Nomor 1). KUHP Nasional menggantikan KUHP peninggalan kolonial Belanda yang telah berusia lebih dari satu abad dan menjadi landasan pembaruan

hukum pidana materiil di Indonesia. Disisi lain, perkembangan teknologi informasi yang pesat telah melahirkan berbagai bentuk tindak pidana baru yang dikenal sebagai *cyber crime*, yang penangananannya selama ini merujuk pada Undang -Undang Informasi dan Transaksi Elektronik (UU ITE). penelitian ini bertujuan untuk menganalisis implikasi yuridis berlakunya KUHP Nasional terhadap penyidikan tindak pidana *cyber*, yang memperhatikan aspek kewenangan penyidik, alat bukti elektronik, dan hubungan antara KUHP Nasional dengan UU ITE. Metode penelitian yang di gunakan adalah penelitian hukum normatif dengan pendekatan perundang-undangan (*statute approach*) dan pendekatan konseptual (*conceptual approach*). Hasil penelitian menunjukkan bahwa berlakunya KUHP Nasional membawa implikasi yuridis yang signifikan, antara lain perluasan yurisdiksi penegakan hukum, pembaruan konsep pertanggung jawaban pidana dalam lingkup siber, serta harmonisasi ketentuan pidana antara KUHP Nasional dan UU ITE selain itu, penyidikan tindak pidana *cyber* memerlukan penyesuaian dalam hal kompetensi penyidik, prosedur penyitaan alat bukti elektronik, dan koordinasi lintas lembaga. Penelitian ini merekomendasikan perlu adanya regulasi teknis yang komprehensif sebagai pedoman penyidikan tindak pidana *cyber* dibawah rezim KUHP Nasional.

Kata Kunci: KUHP Nasional, tindak pidana *cyber*, penyidikan, alat bukti elektronik, implikasi yuridis

PENDAHULUAN

Pembaruan hukum pidana merupakan kebutuhan yang tidak terhindarkan dalam suatu negara yang terus berkembang. Indonesia, sebagai negara hukum yang berdasarkan Pancasila dan Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, telah lama merasakan kebutuhan mendesak untuk memperbarui Kitab Undang–Undang Hukum Pidana (KUHP) yang merupakan warisan kolonial Belanda yang diberlakukan sejak tahun 1918 (Moeljatno, 2015: 3). Setelah melalui proses pembahasan yang panjang dan berliku selama lebih dari enam dekade, pada tanggal 2 Januari 2023, pemerintah Indonesia akhirnya mengesahkan Undang-Undang nomor 1 tahun 2023 tentang Kitab Undang-Undang Hukum Pidana yang sering disebut sebagai KUHP Nasional.

Sementara itu, perkembangan teknologi informasi dan komunikasi yang luar biasa pesat dalam dua dekade terakhir telah melahirkan berbagai fenomena baru dalam kehidupan masyarakat, termasuk dalamnya munculnya berbagai bentuk tindak pidana yang memanfaatkan teknologi digital sebagai sarana maupun sasarannya. Tindak pidana yang dilakukan melalui media siber atau yang lebih dikenal dengan istilah tindak pidana *cyber* (*cyber crime*) telah menjadi ancaman nyata bagi keamanan nasional, perekonomian, dan kehidupan masyarakat Indonesia (Indonesia, UU Nomor 11 Tahun 2008 jo. UU Nomor 19 Tahun 2016 dan UU Nomor 1 Tahun 2024 tentang ITE).

Regulasi mengenai tindak pidana *cyber* di Indonesia selama ini bersumber dari Undang-Undang Nomor 11 Tahun 2008 tentang informasi dan Transaksi Elektronik (UU ITE) beserta perubahannya, yang memuat ketentuan pidana materiil maupun formil terkait tindak pidana di bidang teknologi informasi (Barda Nawawi Arief, 2006: 7). Undang-undang ini (KUHP Nasional) mulai berlaku setelah 3 (tiga) tahun terhitung sejak tanggal diundangkan (pada tanggal 2 Januari 2026) (Pasal 624 UU Nomor 1 Tahun 2023), munculnya pertanyaan mendasar mengenai bagaimana hubungan antara KUHP Nasional dengan UU ITE, serta apa implikasinya terhadap proses penyidikan tindak pidana *cyber* di Indonesia.

Pertanyaan ini menjadi semakin relevan mengingat KUHP Nasional memuat ketentuan-ketentuan baru yang berbeda dari KUHP lama, terutama dalam hal asas legalitas (Pasal 1 ayat (1) KUHP Nasional), sistim pemidanaan, pertanggungjawaban pidana, serta pengaturan

mengenai tindak pidana yang di lakukan melalui media elektronik. Di sisilain, penyidikan tindak pidana *cyber* memiliki karakter khusus yang membedakannya dari penyidik tindak pidana konvensional, terutama dalam hal penangananan alat bukti elektronik, yurisdiksi lintas batas, dan kebutuhan keahlian teknis yang tinggi.

Bertolak dari latar belakang tersebut, penelitian ini berupa menjawab dua permasalahan utama: pertama, bagaimana implikasi yuridis berlakunya KUHP Nasional terhadap ketentuan tindak pidana *cyber* yang di atur dalam UU ITE; dan kedua, bagaimana pengaruh berlakunya KUHP Nasional terhadap mekanisme penyidikan tindak pidana *cyber* di Indonesia. Penelitian ini diharapkan dapat memberikan kontribusi pemikiran yang bermanfaat bagi pengembangan ilmu hukum pidana, khususnya dalam bidang hukum pidana teknologi informasi, serta menjadi acuan bagi para praktisi hukum dalam memahami dan menerapkan ketentuan-ketentuan baru dalam KUHP Nasional terkait tindak pidana *cyber*.

Konsep Pembaruan Hukum Pidana Dalam KUHP Nasional

Pembaruan hukum pidana (penal reform) merupakan upaya untuk melakukan penataan ulang terhadap sistem hukum pidana yang berlaku agar lebih sesuai dengan nilai-nilai, kebutuhan, dan perkembangan masyarakat (Soerjono Soekanto, 1986: 51). KUHP Nasional sebagai produk pembaruan hukum pidana Indonesia mengandung perubahan paradigmatik yang fundamental di bandingkan dengan KUHP lama, antara lain dalam hal orientasi pemidanaan yang tidak hanya bersifat pembalasan (Retributf) melainkan juga restoratif dan rehabiltatif.

Beberapa prinsip dasar yang menjadi landasan KUHP Nasional antara lai: (1) asas legalitas yang di perluas mencakup hukum yang hidup dalam masyarakat (*Living law*); (2) pengakuan terhadap pertanggung jawaban korporasi secara lebih komprehensif; (3) penguatan sanksi alternatif dan pidana pengawasan; serta (4) pengakuan terhadap pengakuan nilai-nilai moral dan agama dalam pemidanaan. Perubahan-perubahan ini membawa konsekuensi yuridis yang signifikan terhadap berbagai bidang hukum pidana, termasuk hukum pidana siber.

Tindak Pidana *Cyber*: Konsep dan Pengaturannya

Tindak pidana *cyber* atau *cyber crime* merupakan tindak pidana yang menggunakan komputer dan jaringan internet sebagai sarana, alat, atau objeknya (Abdul Wahid dan Mohammad Labib, 2005: 40). Definisi ini mencakup berbagai bentuk kejahatan mulai dari penipuan elektronik, pembobolan sistem komputer (*hacking*), penyebaran konten ilegal, pencurian data, hingga serangan terhadap infrastruktur kritis negara yang di lakukan melalui media siber.

Di Indonesia pengaturan tindak pidana *cyber* secara khusus di atur dalam UU ITE. Undang-Undang ini mengatur berbagai bentuk tindak pidana yang berkaitan dengan teknologi informasi, pemalsuan data elektronik, penipuan elektronik, serta konten yang dilarang (Dikdik M. Arief Mansur dan Elisatris Gultom, 2005: 9). Dengan berlakunya KUHP Nasional, muncul pertanyaan mengenai bagaimana hubungan antara ketentuan UU ITE dengan ketentuan-ketentuan baru dalam KUHP Nasional yang juga mengatur beberapa perbuatan yang berkaitan dengan teknologi informasi.

KUHP Nasional memuat beberapa ketentuan yang secara langsung berkaitan dengan tindak pidana siber, antara lain dalam bab tentang tindak pidana yang berkaitan dengan teknologi informasi (Pasal 98 KUHP Nasional). Selain itu sebagai tindak pidana konvensional dalam KUHP Nasional yang dapat dilakukan melalui media elektronik, seperti pencemaran nama baik, penipuan, pemerasan, dan ancaman, juga memiliki relevansi langsung dengan pengaturan *cyber crime*.

Penyidikan Tindak Pidana *Cyber*

Penyidikan merupakan serangkaian tindak penyidik dalam hal dan menurut cara yang diatur dalam Undang-Undang untuk mencari serta mengumpulkan bukti yang terjadi mengenai tindak pidana guna menemukan tersangkanya (Andi Hamzah, 2020: 118). Dalam konteks

tindak pidana *cyber*, penyidikan memiliki karakteristik khusus yang membedakan dari penyidik tindak pidana konvensional .

Pertama, penyidikan tindak pidana *cyber* sangat bergantung pada alat bukti elektronik (*digital evidence*) yang memiliki sifat muda berubah, rentan terhadap manipulasi dan cepat hilang jika tidak segera diamankan. Kedua, tindak pidana *cyber* sering kali bersifat transnasional, sehingga penyidikan memerlukan kerja sama lintas yurisdiksi yang kompleks. Ketiga, penyidikan tindak pidana *cyber* membutuhkan keahlian teknis khusus yang tidak selalu dimiliki oleh penyidik konvensional (Agus Raharjo, 2002: 22).

METODE PENELITIAN

Penelitian ini menggunakan metode penelitian normatif (*normative legal research*), yaitu penelitian yang dilakukan terhadap bahan hukum sekunder dengan menganalisis norma-norma, kaidah-kaidah, dan prinsip-prinsip hukum yang berlaku (Peter Mahmud Marzuki, 2017: 93). Metode ini dipilih karena objek penelitian ini adalah norma hukum positif yang terkandung dalam KUHP Nasional, UU ITE, dan peraturan perundang-undangan yang terkait lainya.

Pendekatan yang digunakan dalam penelitian ini adalah : (1) Pendekatan Perundang-undangan (*stute apptoach*), yaitu dengan menelaah semua regulasi dan perundang-undangan yang bersangkut paut dengan isu hukum yang sedang di tangani ; dan (2) pendekatan konseptual (*Conceptual approach*), yaitu dengan mengacuh kepada prinsip-prinsip hukum yang dapat di temukan dalam pandangan- pandangan sarjana hukum ataupun doktrin-doktrin hukum (Peter Mahmud Marzuki, 2017: 141).

Bahan hukum yang digunakan dalam penelitian ini terdiri dari tiga lapisan. Bahan hukum primer meliput KUHP Nasional (UU No 1 Tahun 2023), KUHP (UU No 8 Tahun 1981),UU ITE (UU No 11 Tahun 2008 jo. UU No 19 Tahun 2016 jo. UU No 1 Tahun 2024) , serta peraturan pelaksana terkait penyidik tindak pidana *cyber*. Bahan hukum sekunder terdiri dari teks hukum pidana, jurnal ilmiah hukum, hasil penelitian, dan pendapat para ahli hukum. Bahan hukum tersier meliputi kamus hukum, ensiklopedia, dan artikel ilmiah populer. Teknik pengumpulan bahan hukum dilakukan melalui studi kepustakaan (*library research*),sedangkan teknik analisisnya menggunakan metode deskriptif-perspektif, yakni mendeskripsikan norma-norma hukum yang berlaku dan memberikan preskripsi atas permasalahan yang diteliti.

HASIL DAN PEMBAHASAN

Implikasi Yuridis KUHP Nasional Terhadap Ketentuan Tindak Pidana *Cyber*

1) Harmonisasi Hukum Pidana Materiil

Berlakunya KUHP Nasional membawa implikasi yuridis yang signifikan terhadap ketentuan tindak pidana *cyber* yang selam ini di atur dalam UU ITE. Salah satu implikasi paling mendasar adalah keharusan untuk melakukan harmonisasi antara ketentuan KUHP Nasional dengan ketentuan-kententuan dalam UU ITE (Teguh Prasetyo, 2014: 27).

KUHP Nasional sebagai kodifikasi hukum pidana nasional secara hirarki berkedudukan sebagai *lex generalis* (hukum umum) yang berlaku secara umum, sementara UU ITE berkedudukan sebagai *lex specialis* (hukum khusus) yang berlaku secara khusus dalam bidang teknologi informasi dan transaksi elektronik. Berdasarkan asas *lex specialis derogat legi generali*, maka dalam hal terjadi pertentangan antara ketentuan UU ITE dengan ketentuan KUHP Nasional, ketentuan UU ITE sebagai *lex specialis* harus didahulukan penerapannya.

Namun demikian, perlu diperhatikan bahwa asas tersebut hanya berlaku ketika terdapat pertentangan antara dua norma yang mengatur materi yang sama. Dalam hal KUHP Nasional mengatur materi yang belum di atur dalam UU ITE, maka ketentuan KUHP Nasional tersebut tetap berlaku dan dapat di terapkan. Selain itu, terdapat beberapa

ketentuan dalam KUHP Nasional yang secara eksplisit mengatur tindak pidana yang berkaitan dengan teknologi informasi (Penjelasan Umum UU Nomor 1 Tahun 2023 angka 4), yang dapat berfungsi sebagai pelengkap atau bahkan sebagai dasar hukum alternatif bagi penuntutan tindak pidana *cyber*.

2) Perluasan Yurisdiksi Penegakan Hukum

Salah satu implikasi yuridis yang paling signifikan dari berlakunya KUHP Nasional adalah peluasan yurisdiksi penegakan hukum pidana Indonesia.KUHP Nasional memperluas jangkauan hukum pidana Indonesia tidak hanya berdasarkan asas teritorial, melainkan juga berdasarkan asas personalitas aktif, asas personalitas pasif, asas perlindungan, dan asas universalitas (Pasal 4 KUHP Nasional).

Perluasan yurisdiksi ini memiliki relevansi yang sangat besar dalam konteks penegakan hukum terhadap tindak pidana *cyber*, mengingat karakteristik tindak pidana *cyber* yang seringkali bersifat transnasional. Pelaku tindak pidana *cyber* dapat berada dinegara lain dan menyerang korban yang berada di Indonesia, atau sebaliknya pelaku di Indonesia menyerang korban diluar negeri. Dengan adanya perluasan yurisdiksi dalam KUHP Nasional, penegak hukum di Indonesia memiliki landasan yuridis yang lebih kuat untuk menangani berbagai kasus tindak pidana *cyber* yang bersifat lintas batas yurisdiksi.

3) Pembaruan Konsep Pertanggungjawaban Pidana

KUHP Nasional membawa pembaruan penting dalam konsep pertanggungjawaban pidana yang berdampak pada penangananan tindak pidana *cyber* (Chairul Huda, 2006: 68). Salah satu pembaruan yang signifikan adalah pengakuan pertanggungjawabn pidana korporasi secara lebih komprehensif. Dalam konteks tindak pidana *cyber*, hal ini sangat relevan mengingat banyak kasus *cyber crime* yang dilakukan secara terorganisir oleh korporasi yang melibatkan atau melibatkan korporasi sebagai korban.

KUHP Nasional juga memperjelas syarat-syarat pertanggungjawaban pidana, termasuk dalam hal kesalahan (*schuld)* dan kemampuan bertanggung jawab (Pasal 29 s.d. Pasal 49 KUHP Nasional). Dalam konteks tindak pidana *cyber*, pembaruan ini penting kerena banyak tindak pidana *cyber* yng memerlukan analisis mendalam mengenai unsur kesengajaan atau kealpaan pelaku, yang seringkali dibuktikan dalam lingkup siber yang anonim dan kompleks.

Pengaruh KUHP Nasional Terhadap Mekanisme Tindak Pidana *Cyber*

1) Kewenangan Penyidik

Penyidikan tindak pidana *cyber* di Indonesia secara formal dilaksanakan berdasarkan ketentuan KUHAP yang berlaku sebagai hukum acara pidana umum, serta ketentuan khusus yang diatur dalam pasal 43 UU ITE (Pasal 43 UU ITE). Dengan berlakunya KUHP Nasional, muncul kebutuhan untuk mengevaluasi kembali kewenangan penyidik dalam menangani tindak pidana *cyber*, terutama terkait dengan penyesuaian antara ketentuan-ketentuan baru dalam KUHP Nasional dengan prosedur penyidikan yang telah ada.

UU ITE memberikan kewenangan penyidikan kepada dua jenis penyidik: pertama, penyidik pejabat polisi Negara Republik Indonesia; dan kedua, penyidik Pegawai Negeri Sipil (PPNS) dilingkungan pemerintah yang lingkup tugas dan tanggungjawabnya dibidang Teknologi Informasi dan Transaksi Elektronik (Pasal 43 ayat (5) UU ITE). Dualisme penyidik ini sering menimbulkan pertanyaan mengenai koordinasi dan pembagian kewenangan, yang perlu diatasi melalui regulasi yang lebih komprehensif dibawah rezim KUHP Nasional.

Selain itu, berlakunya KUHP Nasional juga berimplikasi pada kebutuhan untuk meningkatkan kompetensi penyidik dalam memahami dan menerapkan ketentuan-

ketentuan baru. Penyidik tindak pidana *cyber* tidak hanya dituntut untuk memahami aspek teknis forensik digital, tetapi juga harus mampu memahami konstruksi norma-norma baru dalam KUHP Nasional yang relevan dengan tindak pidana *cyber* (Peraturan Kepala Kepolisian Negara Republik Indonesia Nomor 6 Tahun 2019).

2) Penangananan Alat Bukti Elektronik

Salah satu aspek yang paling krusial dalam penyidikan tindak pidana *cyber* adalah penangananan alat bukti elektronik (*digital evidence*). UU ITE telah memberikan pengakuan terhadap alat bukti elektronik sebagai alat bukti yang sah dalam proses peradilan pidana (Pasal 5 ayat (1) UU ITE). Namun demikian, prosedur pengumpulan, pengaman, pemeriksaan, dan penyajian alat bukti elektronik dalam penyidikan masih memerlukan pedoman teknis yang lebih rinci dan komprehensif.

KUHP Nasional tidak secara eksplisit mengatur mengenai alat bukti elektronik, sehingga ketentuan UU ITE beserta KUHAP tetap menjadi landasan utama dalam hal penangananan alat bukti elektronik (Pasal 175 KUHAP jo. Pasal 43 UU ITE). Namun demikian, berlakunya KUHP Nasional dapat memberikan dampak tidak langsung terhadap penanganan alat bukti elektronik, terutama terkait dengan pembuktian unsur-unsur tindak pidana yang didakwakan berdasarkan norma-norma baru dalam KUHP Nasional.

Tantangan utama dalam penanganan alat bukti elektronik dalam penyidikan tindak pidana *cyber* meliputi: (1) volatilitas data digital yang dapat berubah atau hilang dalam waktu sangat singkat; (2) kebutuhan untuk mempertahankan *chain of custody* yang ketat agar alat bukti tidak dianggap terkontaminasi; (3) kompleksitas teknik dalam melakukan forensik digital terhadap berbagai jenis perangkat dan sistem; (4) perbedaan standar teknis forensik digital yang mungkin berlaku diberbagai yurisdiksi dalam kasus tindak pidana *cyber* transnasional (Edmon Makarim, 2005: 413).

3) Harmonisasi Prosedur Penyidikan

Berlakunya KUHP Nasional juga berimplikasi pada kebutuhan untuk menyelaraskan prosedur penyidikan tindak pidana *cyber* dengan ketentuan-ketentuan baru dalam KUHP Nasional. Hal ini mencakup penyesuaian dalam hal: (1) kualifikasi tindak pidana dalam surat perintah penyidikan; (2) penerapan konstruksi pertanggungjawaban pidana yang baru dalam proses penyidikan; dan (3) koordinasi dengan negara lain dalam penanganan kasus tindak pidana *cyber* transnasional berdasarkan ketentuan yurisdiksi yang baru dalam KUHP Nasional (Yudi Kristiana, 2016: 55).

Salah satu isu penting yang perlu mendapat perhatian adalah kemungkinan adanya tumpang tindih (*overlapping*) antara ketentuan tindak pidana dalam KUHP Nasional dengan konstruksi dalam UU ITE. Tumpang tindih ini dapat menimbulkan ketidakpastian hukum dalam penentuan dasar hukum yang digunakan dalam penyidikan, yang pada gilirannya dapat mempengaruhi keabsahan proses penyidikan dan penuntutan (Widodo, 2013: 77).

Untuk mengatasi permasalahan tersebut, di perlukan pedoman teknis yang jelas mengenai penerapan KUHP Nasional dalam penyidikan tindak pidana *cyber*. Pedoman ini idealnya mencakup pemetaan tindak pidana *cyber* berdasarkan ketentuan KUHP Nasional dan UU ITE, prosedur penyidikan yang disesuaikan dengan karakteristik tindak pidana *cyber*, serta mekanisme koordinasi antara penegak hukum dan antara lembaga dalam penanganan kasus tindak pidana *cyber* (Pasal 112 dan Pasal 113 KUHP Nasional).

KESIMPULAN

Berdasarkan pembahasan yang telah dilakukan, dapat ditarik beberapa kesimpulan sebagai berikut:

1) Berlakunya KUHP Nasional membawa implikasi yuridis yang signifikan terhadap tindak pidana *cyber*, terutama dalam hal harmonisasi hukum pidana materiil antar

KUHP Nasional dan UU ITE, perluasan yurisdksi penegakan hukum yang memperkuat kemampuan Indonesia dalam menangani tindak pidana *cyber* transnasional, serta pembaruan konsep pertanggungjawaban pidana termasuk pertanggungjawaban korporasi yang relevan dengan kejahatan siber terorganisir.

2) Mekanisme penyidikan tindak pidana *cyber* memerlukan penyesuaian dengan berlakunya KUHP Nasional, khususnya dalam hal kewenangan penyidik, prosedur penanganan alat bukti elektronik, dan harmonisasi prosedur penyidikan. Hal ini menuntut peningkatan kompetensi penyidik serta tersedianya pedoman teknis yang komprehensif dan jelas mengenai penyidikan tidak pidana *cyber* dibawah rezim KUHP Nasional.
3) Prinsip *lex specialis derogat legi gerelari* tetap menjadi pedoman dalam menentukan ketentuan mana yang berlaku ketika terdapat potensi konflik norma antara KUHP Nasional dan UU ITE, namun penegasan ini memerlukan dukungan regulasi teknik yang lebih rinci untuk memberikan kepastian hukum dalam praktik penyidikan.

REFERENSI

Abdul Wahid dan Mohammad Labil, Kejahatan Mayantra (*Cyber Crime*), bandung: Rafika Aditama, 2025

Agus Raharjo, *Cybercrime*: Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi, Bandung: Citra Adyta Bakti, 2002

Andi Hazma, Hukum Acara Pidana Indonesia, Edisi Ketiga, Jakarta: Sinar Grafika 2020

Barda Nawawi Arief, Tindak Pidana Mayantra: Perkembangan Kajian *Cyber Crime* di Indonesia, Jakarta: Raja Grafindo Persada 2006.

Chairul Huda, Dari Tiada Pidana Tanpa Kesalahan Menuju Kepada Tiada Pertanggungjawaban Pidana Tanpa Kesalahan, Jakarata: kencana,2006

Dikdik M. Arief Mansur dan Elisatris Gultom, *Cyber* Law: Aspek Hukum Teknologi Informasi, Bandung:Refika Aditama, 2005.

Edmon Makarim, Pengaturan Hukum Telematika: Suatu Komplikasi Kajian, Jakarta: Raja Grafindo Persada, 2025

Moeljatno, Asas- Asas Hukum Pidana, Jakarta: Rineka Cipta,2015

Peraturan Kepala Kepolisian Negara Republik Indonesia Nomor 6 Tahun 2019 tentang Penyidikan Tindak Pidana.

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

Soerjono Soekanto, Pengantar Penelitian Hukum, Jakarta: UI Press, 1986.

Teguh Prasetyo, Hukum Pidana, E disi Revisi, Jakarta: Raja Grafindo Persada, 2014

Undang-Undang Dasar Republik Tahun 1945

Undang-Undang Nomor 1 Tahun 2023 Tentang Kitab Undang-Undang Hukum Pidana (KUPH Nasional).

Undang-Undang Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang Nomor 11 Tahun 2008.

Undang-Undang Nomor 11 Tahu 2008 Informasi dan Transaksi Elektronik.

Undang-Undang Nomor 11 Tahun 2006 Tentang Perubahan atas Undang-undang Nomor 11 Tahun 2008.

Undang-Undang Nomor 8 Tahun 1981 Tentang Hukum Acara Pidana (KUHAP).

Widodo, Hukum Pidana di Bidang Teknologi Informasi: *Cybercrime* Law, Yogyakarta: Aswaja Pressindo, 2013.

Yudi Kristiana, Pemberantasan Tindak Pidana Korupsi: Perspektif Hukum Progresif, Yogyakarta: Thafa Media, 2016