

## Pengaruh Media Sosial Terhadap Peningkatan Kejahatan Siber dan Tantangan Penegakan Hukum Pidana

Iswandy Rani Saputra\*, Rachman Rizal A. Sapada, A. Dzuqarnain, Suprpto Suprpto

Fakultas Hukum Institut Ilmu Sosial dan Bisnis Andi Sapada

Corrsponding Email: [iswandys@gmail.com](mailto:iswandys@gmail.com)\*

### Abstract

This study discusses the influence of social media on the increase in cybercrime in Indonesia and the challenges of criminal law enforcement in dealing with it. Using normative legal research methods, this study analyses applicable regulations, technical barriers, and social dynamics that affect the effectiveness of law enforcement against cybercrime, especially those that originate from activities on social media. The study results show that the high penetration of social media, low digital literacy, and the development of increasingly complex crime modes have encouraged an increase in cybercrime cases. On the other hand, law enforcement still faces regulatory limitations, a lack of competent human resources, cross-border jurisdictional challenges, and weak coordination between agencies. This research recommends adaptive regulatory reforms, capacity building of law enforcement officials, strengthening national and international cooperation, and public digital literacy education to create a safer and more equitable digital ecosystem.

**Keywords** : Social Media; Cybercrime; Law Enforcement

**Publish Date** : 18 Mei 2025

### Pendahuluan

Media sosial telah menjadi bagian tak terpisahkan dari kehidupan masyarakat modern di Indonesia, memberikan kemudahan dalam berkomunikasi, berbagi informasi, dan membangun jejaring sosial. Namun, di balik manfaat tersebut, media sosial juga menghadirkan tantangan baru dalam bentuk kejahatan siber yang semakin kompleks dan sulit dikendalikan. Fenomena ini ditandai dengan meningkatnya kasus penipuan daring, pencurian identitas, penyebaran berita bohong (hoaks), ujaran kebencian, hingga cyberbullying yang dapat menimbulkan kerugian material maupun immaterial bagi korban.<sup>1</sup>

Peningkatan penggunaan media sosial secara masif telah membuka peluang bagi pelaku kejahatan siber untuk memanfaatkan celah keamanan dan kerentanan pengguna.<sup>2</sup>

Banyak masyarakat yang belum memiliki literasi digital dan kecakapan berpikir kritis, sehingga mudah terjebak dalam modus-modus kejahatan yang berkembang di dunia maya. Algoritma media sosial yang menampilkan konten berdasarkan preferensi pengguna juga memperparah penyebaran informasi palsu dan manipulatif, sehingga memperbesar risiko terjadinya tindak pidana siber.<sup>3</sup>

Dari sudut pandang hukum pidana, kejahatan siber yang berakar pada aktivitas di media sosial menimbulkan persoalan serius dalam penegakan hukum. Penyebaran berita bohong, misalnya, merupakan perbuatan melawan hukum yang mengandung unsur objektif dan subjektif tindak pidana, namun pelaku seringkali sulit diidentifikasi karena dapat

<sup>1</sup> Ananta, K. D., Ambodo, T., & Tohawi, A. (2024). Pengaruh Media Sosial terhadap Peningkatan Kejahatan Siber di Indonesia. *Islamic Law: Jurnal Siyasah*, 9(2), 118-13.

<sup>2</sup> Syahril, M. A. F. (2023). Cyber Crime in terms of the

Human Rights Perspective. *International Journal of Multicultural and Multireligious Understanding*, 10(5), 119-130.

<sup>3</sup> Ananta, K. D., Ambodo, T., & Tohawi, A. (2024). Pengaruh Media Sosial terhadap Peningkatan Kejahatan Siber di Indonesia. *Islamic Law: Jurnal Siyasah*, 9(2), 118-13.

menyembunyikan identitasnya menggunakan teknologi seperti VPN atau jaringan anonym.<sup>4</sup> <sup>5</sup> Hal ini menyulitkan aparat penegak hukum dalam melakukan penyelidikan dan penuntutan terhadap pelaku kejahatan siber.

Penegakan hukum terhadap kejahatan siber di Indonesia menghadapi tantangan besar, salah satunya adalah keterbatasan regulasi yang mampu mengantisipasi perkembangan teknologi digital. Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) yang ada saat ini dinilai belum sepenuhnya efektif untuk menanggulangi berbagai bentuk kejahatan siber yang semakin beragam dan canggih, seperti pemanfaatan blockchain, cryptocurrency, hingga kecerdasan buatan.<sup>6</sup> Kondisi ini menuntut adanya pembaruan regulasi agar mampu menjawab tantangan kejahatan siber yang terus berkembang.

Selain itu, pengumpulan dan pembuktian alat bukti digital dalam kasus kejahatan siber merupakan tantangan tersendiri. Bukti digital yang tersebar di berbagai perangkat dan server dapat dengan mudah diubah atau dihapus, sehingga proses penyidikan menjadi lebih rumit dan membutuhkan keahlian khusus dari aparat penegak hukum.<sup>7</sup> Hal ini diperparah dengan minimnya sumber daya manusia yang memiliki kompetensi di bidang forensik digital.

Upaya pencegahan dan penindakan kejahatan siber melalui media sosial juga telah dilakukan oleh aparat penegak hukum, salah satunya dengan membentuk satuan tugas khusus seperti Cyber Patrol. Namun,

efektivitas upaya ini masih terbatas karena kendala teknis dan yuridis, termasuk kurangnya regulasi yang mengatur pemanfaatan teknologi informasi secara komprehensif serta keterbatasan alat pendukung penyidikan.<sup>8</sup>

Di sisi lain, kejahatan siber melalui media sosial tidak hanya berdampak pada individu, tetapi juga dapat mengancam stabilitas sosial dan keamanan nasional. Penyebaran hoaks, ujaran kebencian, dan konten provokatif berpotensi memecah belah masyarakat serta menimbulkan konflik horizontal. Oleh sebab itu, penanganan kejahatan siber membutuhkan sinergi antara pemerintah, aparat penegak hukum, sektor swasta, dan masyarakat untuk meningkatkan kesadaran akan pentingnya keamanan digital serta memperkuat regulasi yang ada.<sup>9</sup>

Berdasarkan uraian di atas, penelitian ini menjadi penting untuk menganalisis secara normatif bagaimana pengaruh media sosial terhadap peningkatan kejahatan siber serta tantangan yang dihadapi dalam penegakan hukum pidana di Indonesia. Penelitian ini diharapkan dapat memberikan kontribusi dalam pengembangan hukum pidana nasional, khususnya dalam merespons dinamika kejahatan siber yang terus berkembang seiring kemajuan teknologi informasi dan komunikasi.

## Metode Penelitian

Penelitian ini menggunakan metode penelitian hukum normatif, yaitu penelitian yang menitikberatkan pada kajian terhadap norma-norma hukum yang berlaku, baik berupa peraturan perundang-undangan, doktrin, maupun putusan pengadilan yang relevan dengan kejahatan siber melalui media sosial.<sup>10</sup> Data yang digunakan dalam

<sup>4</sup> Angraeni, N., Bunga, D., Citranu, C., & Aris, A. (2024). *Hukum Pidana: Teori Komprehensif*. PT. Sonpedia Publishing Indonesia.

<sup>5</sup> Syahril, M. A. F. (2023). Cyber Crime in terms of the Human Rights Perspective. *International Journal of Multicultural and Multireligious Understanding*, 10(5), 119-130.

<sup>6</sup> Syahril, M. A. F. (2023). Cyber Crime in terms of the Human Rights Perspective. *International Journal of Multicultural and Multireligious Understanding*, 10(5), 119-130.

<sup>7</sup> Syahril, M. A. F. (2023). Cyber Crime in terms of the Human Rights Perspective. *International Journal of Multicultural and Multireligious Understanding*, 10(5), 119-130.

<sup>8</sup> Syahril, Muh. A. F. *Hukum Informasi dan Transaksi Elektronik*. Eureka Media Aksara, 2023.

<sup>9</sup> Ananta, K. D., Ambodo, T., & Tohawi, A. (2024). Pengaruh Media Sosial terhadap Peningkatan Kejahatan Siber di Indonesia. *Islamic Law: Jurnal Siyasah*, 9(2), 118-13.

<sup>10</sup> Julardi, B., Runtunuwu, Y. B., Musthofa, M. H., TL, A. D., Asriyani, A., Hazmi, R. M., ... & Samara, M. R. (2023). *Metode penelitian hukum*. CV. Gita Lentera.

penelitian ini merupakan data sekunder yang diperoleh melalui studi kepustakaan (*library research*), meliputi Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), Kitab Undang-Undang Hukum Pidana (KUHP), peraturan pelaksana, literatur hukum, jurnal ilmiah, dan sumber-sumber hukum lainnya. Analisis data dilakukan secara kualitatif dengan pendekatan deskriptif-analitis untuk mengidentifikasi, mengkaji, dan menafsirkan ketentuan hukum yang berkaitan dengan kejahatan siber serta tantangan penegakan hukum pidana di Indonesia.<sup>11</sup>

Dalam pelaksanaannya, penelitian ini juga menggunakan pendekatan konseptual (*conceptual approach*) untuk memahami konsep-konsep dasar tentang kejahatan siber, media sosial, serta penegakan hukum pidana. Peneliti akan membandingkan regulasi yang berlaku di Indonesia dengan praktik di beberapa negara lain sebagai bahan analisis kritis dan rekomendasi pembaruan hukum. Dengan demikian, hasil penelitian diharapkan dapat memberikan gambaran komprehensif mengenai efektivitas regulasi dan penegakan hukum pidana terhadap kejahatan siber yang berkembang melalui media sosial, serta menawarkan solusi normatif atas berbagai tantangan yang dihadapi.<sup>12</sup>

### **Analisis dan Diskusi Pengaruh Media Sosial Terhadap Peningkatan Kejahatan Siber di Indonesia**

Pertumbuhan pesat pengguna media sosial di Indonesia telah membawa dampak signifikan terhadap dinamika kejahatan siber di tanah air. Dengan lebih dari 170 juta pengguna internet yang mayoritasnya aktif di media sosial, Indonesia menjadi salah satu negara dengan tingkat penetrasi media sosial tertinggi di dunia.<sup>13</sup> Platform seperti

Facebook, Instagram, dan Twitter tidak hanya memudahkan komunikasi, tetapi juga membuka peluang bagi pelaku kejahatan siber untuk melakukan berbagai tindak kriminal seperti penipuan daring, pencurian identitas, dan penyebaran berita palsu.<sup>14</sup>

Salah satu faktor utama yang mendorong peningkatan kejahatan siber melalui media sosial adalah rendahnya literasi digital di kalangan masyarakat. Banyak pengguna yang belum memahami pentingnya menjaga data pribadi, sehingga kerap membagikan informasi sensitif secara terbuka di akun media sosial mereka. Fenomena oversharing ini memudahkan pelaku kejahatan untuk mengumpulkan data korban dan melakukan serangan seperti phishing dan social engineering.<sup>15</sup>

Data empiris menunjukkan bahwa lebih dari 50% kasus kejahatan siber di Indonesia berawal dari aktivitas di media sosial. Jenis kejahatan yang paling banyak dilaporkan meliputi penipuan online, pencurian identitas, cyberbullying, dan penyebaran konten ilegal. Pada tahun 2023, tercatat lebih dari 97.000 insiden phishing terjadi di Indonesia, dengan 45% di antaranya menargetkan pengguna media sosial sebagai korban utama.

Peningkatan kejahatan siber juga didorong oleh algoritma media sosial yang menampilkan konten berdasarkan preferensi pengguna. Algoritma ini sering kali memperkuat penyebaran informasi palsu dan manipulatif, sehingga memperbesar peluang terjadinya kejahatan seperti penipuan investasi, penjualan barang palsu, hingga penyebaran hoaks yang dapat memicu keresahan sosial.

Remaja menjadi kelompok yang

---

Islamic Jurisprudence, Economic and Legal Theory, 2(1), 139-153.

<sup>14</sup> Ambodo, T., Ananta, K. D., & Tohawi, A. (2024). Pengaruh Media Sosial terhadap Peningkatan Kejahatan Siber di Indonesia. *Islamic Law: Jurnal Siyasah*, 9(2), 118-130. <https://doi.org/10.53429/iljs.v9i2.858>

<sup>15</sup> Ambodo, T., Ananta, K. D., & Tohawi, A. (2024). Pengaruh Media Sosial terhadap Peningkatan Kejahatan Siber di Indonesia. *Islamic Law: Jurnal Siyasah*, 9(2), 118-130. <https://doi.org/10.53429/iljs.v9i2.858>

<sup>11</sup> Syarif, M., Ramadhani, R., Graha, M. A. W., Yanuaria, T., Muhtar, M. H., Asmah, N., ... & Jannah, M. (2024). *PENELITIAN HUKUM*.

<sup>12</sup> Syarif, M., Ramadhani, R., Graha, M. A. W., Yanuaria, T., Muhtar, M. H., Asmah, N., ... & Jannah, M. (2024). *Metode Penelitian Hukum*.

<sup>13</sup> Fairuzzen, M. R., Putra, A. A., Reihan, A., & SH, L. P. (2024). Perkembangan Hukum dan Kejahatan Siber "Cybercrime" di Indonesia. *Indonesian Journal of*

paling rentan terhadap kejahatan siber melalui media sosial. Studi kualitatif menunjukkan bahwa kurangnya pengawasan orang tua, tingginya ketergantungan pada media sosial, dan paparan terhadap konten negatif menjadi faktor utama yang membuat remaja mudah terjerumus dalam perilaku menyimpang atau menjadi korban kejahatan digital. Selain itu, *cyberbullying* dan pornografi daring juga meningkat seiring dengan semakin mudahnya akses dan komunikasi di dunia maya.<sup>16</sup>

Kasus-kasus besar seperti kebocoran data ASN dan pembobolan data NPWP pada tahun 2024 menyoroti lemahnya sistem keamanan siber di Indonesia. Serangan yang dilakukan oleh peretas melalui media sosial atau pemanfaatan data yang tersebar di platform digital menyebabkan kerugian besar, baik secara individu maupun institusional. Hal ini mempertegas pentingnya peningkatan standar keamanan dan perlindungan data pribadi di era digital.<sup>17</sup> Kurangnya kesadaran akan keamanan digital juga menjadi masalah utama. Survei menunjukkan bahwa banyak pengguna media sosial di Indonesia belum memahami risiko kejahatan siber dan langkah-langkah pencegahannya. Akibatnya, mereka sering menjadi korban penipuan, pencurian data, atau bahkan pemerasan daring. Upaya edukasi dan peningkatan kesadaran masyarakat akan pentingnya keamanan digital masih perlu ditingkatkan secara masif.

Regulasi yang ada, seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), dinilai belum mampu memberikan perlindungan maksimal terhadap pengguna media sosial. Implementasi hukum yang masih lemah dan kurangnya penegakan terhadap pelaku kejahatan siber membuat korban sering kali tidak mendapatkan keadilan. Selain itu, perkembangan modus kejahatan yang semakin canggih menuntut pembaruan

regulasi yang lebih responsif terhadap dinamika teknologi.<sup>18</sup>

Kolaborasi antara pemerintah, sektor swasta, dan masyarakat sangat diperlukan untuk menekan angka kejahatan siber melalui media sosial. Pemerintah perlu memperkuat regulasi dan penegakan hukum, sementara sektor swasta—khususnya platform media sosial—harus meningkatkan sistem keamanan dan moderasi konten. Masyarakat juga harus didorong untuk lebih waspada dan meningkatkan literasi digital agar tidak mudah menjadi korban kejahatan siber.<sup>19</sup>

Secara keseluruhan, pengaruh media sosial terhadap peningkatan kejahatan siber di Indonesia sangat nyata dan kompleks. Tanpa upaya kolaboratif yang serius dan berkelanjutan dari seluruh pemangku kepentingan, risiko kejahatan siber akan terus meningkat seiring dengan pertumbuhan pengguna media sosial di Indonesia. Oleh karena itu, perlindungan hukum, edukasi digital, dan penguatan sistem keamanan menjadi kunci utama dalam menciptakan ekosistem digital yang aman dan berdaya tahan.<sup>20</sup>

### **Tantangan Penegakan Hukum Pidana dalam Menghadapi Kejahatan Siber melalui Media Sosial**

Penegakan hukum pidana terhadap kejahatan siber melalui media sosial di Indonesia menghadapi tantangan yang semakin kompleks seiring pesatnya perkembangan teknologi digital. Kejahatan siber bersifat dinamis dan lintas batas, sehingga aparat penegak hukum harus beradaptasi dengan modus operandi yang

<sup>16</sup> Dakota, A. D., & Valensia, V. (2025). Pengaruh Sosial Media terhadap Peningkatan Kejahatan di Kalangan Remaja di Indonesia. *Jurnal Multidisiplin Ilmu Akademik*, 2(2), 311-315.

<sup>17</sup> Netmarks. (2025). Serangan Siber Terbesar yang Pernah Terjadi di Indonesia.

<sup>18</sup> Hadi, M. H. S., & Syahril, M. A. F. (2024). Melindungi Generasi Muda dari Intimidasi Online: Solusi Mengatasi Cyber Bullying di Era Digital. *Amsir Community Service Journal*, 2(2), 75-79.

<sup>19</sup> Ambodo, T., Ananta, K. D., & Tohawi, A. (2024). Pengaruh Media Sosial terhadap Peningkatan Kejahatan Siber di Indonesia. *Islamic Law: Jurnal Siyasah*, 9(2), 118-130. <https://doi.org/10.53429/iljs.v9i2.858>

<sup>20</sup> Ambodo, T., Ananta, K. D., & Tohawi, A. (2024). Pengaruh Media Sosial terhadap Peningkatan Kejahatan Siber di Indonesia. *Islamic Law: Jurnal Siyasah*, 9(2), 118-130. <https://doi.org/10.53429/iljs.v9i2.858>

terus berubah dan sering kali melibatkan pelaku dari berbagai negara. Sifat global ini membuat penegakan hukum tidak hanya terbatas pada yurisdiksi nasional, tetapi juga memerlukan kerja sama lintas negara yang efektif agar pelaku dapat diidentifikasi dan diproses secara hukum.<sup>21</sup>

Salah satu kendala utama adalah keterbatasan regulasi yang mengatur tindak pidana siber. Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) yang menjadi landasan hukum utama dinilai belum sepenuhnya mampu mengantisipasi perkembangan teknologi terbaru seperti blockchain, *cryptocurrency*, dan kecerdasan buatan. Hal ini menyebabkan banyak bentuk kejahatan siber yang tidak terakomodasi secara spesifik dalam regulasi yang ada, sehingga menimbulkan celah hukum yang dapat dimanfaatkan pelaku.<sup>22</sup>

Selain aspek regulasi, tantangan teknis juga menjadi hambatan signifikan dalam proses penyidikan kejahatan siber. Pengumpulan dan analisis bukti digital memerlukan keahlian khusus serta perangkat forensik yang canggih. Banyak aparat penegak hukum di Indonesia belum memiliki kompetensi yang memadai di bidang forensik digital, sehingga penyidikan sering kali terhambat atau bahkan gagal mengungkap pelaku kejahatan. Bukti digital yang tersebar di berbagai platform dan mudah dihapus atau dimodifikasi semakin memperumit proses pembuktian di Pengadilan.<sup>23</sup>

Keterbatasan sumber daya manusia dan infrastruktur juga menjadi faktor penghambat utama. Penyidik sering kali tidak dibekali pelatihan yang cukup dalam menangani bukti digital, seperti analisis log

aktivitas, pelacakan alamat IP, atau penguraian data terenkripsi. Selain itu, alat analisis forensik digital yang mutakhir masih langka atau tidak tersedia di banyak wilayah, sehingga penyidikan menjadi tidak optimal.<sup>24</sup>

Masalah yurisdiksi juga menjadi tantangan besar dalam penegakan hukum pidana kejahatan siber. Banyak kasus kejahatan siber yang melibatkan pelaku dari luar negeri atau menggunakan server di luar wilayah Indonesia, sehingga memerlukan kerja sama internasional yang erat. Namun, perbedaan kebijakan dan standar hukum antarnegara sering kali menghambat proses ekstradisi dan pertukaran bukti, sehingga pelaku sulit dijerat hukum.<sup>25</sup>

Proses peradilan yang rumit dan memakan waktu lama juga menjadi kendala dalam penegakan hukum kejahatan siber. Rumitnya mekanisme pembuktian, kurangnya pemahaman hakim terhadap aspek teknis kejahatan siber, serta minimnya preseden hukum yang relevan membuat proses persidangan berjalan lambat dan sering kali tidak memberikan efek jera kepada pelaku.<sup>26</sup>

Tantangan lain yang dihadapi adalah rendahnya literasi digital masyarakat dan budaya permisif terhadap konten negatif di media sosial. Banyak masyarakat yang belum memahami bahaya dan konsekuensi hukum dari tindak pidana siber, sehingga mudah terlibat atau menjadi korban kejahatan digital. Edukasi dan sosialisasi mengenai penggunaan teknologi informasi yang aman dan etis menjadi sangat penting untuk mengurangi jumlah kasus kejahatan siber.<sup>27</sup>

<sup>21</sup> Wibowo, M. S. I., Munawar, A., & Hidayatullah. (2024). Tindak Pidana Cybercrime: Tantangan Hukum Pidana Dalam Penanggulangan Kejahatan Dunia Maya di Indonesia. *Jurnal Kajian Sosial*, 8(2), 1-15.

<sup>22</sup> Pamungkas, A. T., Mulyono, A., & Lahangatubun, N. (2024). The Crisis of Cybercrime Law Enforcement in Indonesia. *Delictum: Jurnal Hukum Pidana dan Kriminologi*, 2(2), 101-113.

<sup>23</sup> Mansur, D. M. A., & Gultom, E. (2018). *Cyber Law: Aspek Hukum Teknologi Informasi*. Refika Aditama.

<sup>24</sup> Wibowo, M. S. I., Munawar, A., & Hidayatullah. (2024). Tindak Pidana Cybercrime: Tantangan Hukum Pidana Dalam Penanggulangan Kejahatan Dunia Maya di Indonesia. *Jurnal Kajian Sosial*, 8(2), 1-15.

<sup>25</sup> Pamungkas, A. T., Mulyono, A., & Lahangatubun, N. (2024). The Crisis of Cybercrime Law Enforcement in Indonesia. *Delictum: Jurnal Hukum Pidana dan Kriminologi*, 2(2), 101-113.

<sup>26</sup> Pamungkas, A. T., Mulyono, A., & Lahangatubun, N. (2024). The Crisis of Cybercrime Law Enforcement in Indonesia. *Delictum: Jurnal Hukum Pidana dan Kriminologi*, 2(2), 101-113.

<sup>27</sup> Pamungkas, A. T., Mulyono, A., &

Ketidakjelasan aturan hukum dalam menentukan tanggung jawab atas kejahatan siber berbasis teknologi canggih, seperti kecerdasan buatan dan deepfake, juga menjadi masalah baru. Penegakan hukum terhadap kejahatan berbasis AI memerlukan alat forensik digital yang lebih canggih dan keahlian teknis yang tinggi, sementara regulasi yang ada belum secara eksplisit mengatur tanggung jawab hukum dalam kasus-kasus tersebut.<sup>28</sup>

Kurangnya koordinasi antarinstansi penegak hukum di tingkat nasional maupun internasional turut memperburuk efektivitas penanganan kasus kejahatan siber. Penanganan kasus yang melibatkan berbagai instansi sering kali terhambat oleh birokrasi dan kurangnya sistem koordinasi yang terpadu, sehingga mengurangi efisiensi dan kecepatan penanganan Kasus.<sup>29</sup>

Untuk mengatasi tantangan-tantangan tersebut, diperlukan solusi komprehensif seperti pembaruan regulasi yang responsif terhadap perkembangan teknologi, peningkatan kapasitas sumber daya manusia melalui pelatihan intensif di bidang forensik digital, serta penguatan koordinasi antar lembaga penegak hukum baik di tingkat nasional maupun internasional. Selain itu, edukasi masyarakat dan literasi digital harus terus ditingkatkan agar masyarakat lebih waspada dan mampu melindungi diri dari kejahatan siber.<sup>30</sup>

Dengan demikian, penegakan hukum pidana terhadap kejahatan siber melalui media sosial di Indonesia harus dilakukan secara multidimensi, melibatkan pembaruan regulasi, peningkatan kapasitas SDM,

penguatan infrastruktur, serta kolaborasi lintas sektor dan negara. Hanya dengan langkah-langkah strategis dan terintegrasi, upaya pemberantasan kejahatan siber dapat berjalan efektif dan memberikan perlindungan yang optimal bagi masyarakat di era digital<sup>31 32</sup>

## Kesimpulan

Penegakan hukum pidana terhadap kejahatan siber melalui media sosial di Indonesia masih menghadapi berbagai tantangan signifikan, mulai dari keterbatasan regulasi yang belum sepenuhnya mengakomodasi perkembangan teknologi, kurangnya kapasitas sumber daya manusia dan infrastruktur forensik digital, hingga hambatan yurisdiksi lintas negara serta rendahnya literasi digital masyarakat. Oleh karena itu, diperlukan pembaruan regulasi yang adaptif, peningkatan kompetensi aparat penegak hukum, penguatan kerja sama nasional dan internasional, serta edukasi masyarakat secara berkelanjutan agar upaya pemberantasan kejahatan siber di era digital dapat berjalan lebih efektif dan memberikan perlindungan hukum yang optimal bagi seluruh pengguna media sosial.

## Referensi

- Ambodo, T., Ananta, K. D., & Tohawi, A. (2024). Pengaruh Media Sosial terhadap Peningkatan Kejahatan Siber di Indonesia. *Islamic Law: Jurnal Siyasah*, 9(2), 118-130. <https://doi.org/10.53429/iljs.v9i2.858>
- Ananta, K. D., Ambodo, T., & Tohawi, A. (2024). Pengaruh Media Sosial terhadap Peningkatan Kejahatan Siber di Indonesia. *Islamic Law: Jurnal Siyasah*, 9(2), 118-13.

Lahangatubun, N. (2024). The Crisis of Cybercrime Law Enforcement in Indonesia. *Delictum: Jurnal Hukum Pidana dan Kriminologi*, 2(2), 101-113.

<sup>28</sup> Respati, N. (2024). Tantangan Penegakan Hukum terhadap Kejahatan Berbasis Kecerdasan Buatan di Indonesia. *Innovative: Jurnal Ilmiah Hukum*, 6(1), 55-67.

<sup>29</sup> Pamungkas, A. T., Mulyono, A., & Lahangatubun, N. (2024). The Crisis of Cybercrime Law Enforcement in Indonesia. *Delictum: Jurnal Hukum Pidana dan Kriminologi*, 2(2), 101-113.

<sup>30</sup> Pamungkas, A. T., Mulyono, A., & Lahangatubun, N. (2024). The Crisis of Cybercrime Law Enforcement in Indonesia. *Delictum: Jurnal Hukum Pidana dan Kriminologi*, 2(2), 101-113.

<sup>31</sup> Wibowo, M. S. I., Munawar, A., & Hidayatullah. (2024). Tindak Pidana Cybercrime: Tantangan Hukum Pidana Dalam Penanggulangan Kejahatan Dunia Maya di Indonesia. *Jurnal Kajian Sosial*, 8(2), 1-15.

<sup>32</sup> Pamungkas, A. T., Mulyono, A., & Lahangatubun, N. (2024). The Crisis of Cybercrime Law Enforcement in Indonesia. *Delictum: Jurnal Hukum Pidana dan Kriminologi*, 2(2), 101-113.

- Angraeni, N., Bunga, D., Citranu, C., & Aris, A. (2024). *Hukum Pidana: Teori Komprehensif*. PT. Sonpedia Publishing Indonesia.
- Dakota, A. D., & Valensia, V. (2025). Pengaruh Sosial Media terhadap Peningkatan Kejahatan di Kalangan Remaja di Indonesia. *Jurnal Multidisiplin Ilmu Akademik*, 2(2), 311-315.
- Fairuzzen, M. R., Putra, A. A., Reihan, A., & SH, L. P. (2024). Perkembangan Hukum dan Kejahatan Siber "Cybercrime" di Indonesia. *Indonesian Journal of Islamic Jurisprudence, Economic and Legal Theory*, 2(1), 139-153.
- Hadi, M. H. S., & Syahril, M. A. F. (2024). Melindungi Generasi Muda dari Intimidasi Online: Solusi Mengatasi Cyber Bullying di Era Digital. *Amsir Community Service Journal*, 2(2), 75-79.
- Juliardi, B., Runtunuwu, Y. B., Musthofa, M. H., TL, A. D., Asriyani, A., Hazmi, R. M., ... & Samara, M. R. (2023). *Metode penelitian hukum*. CV. Gita Lentera.
- Mansur, D. M. A., & Gultom, E. (2018). *Cyber Law: Aspek Hukum Teknologi Informasi*. Refika Aditama.
- Netmarks. (2025). Serangan Siber Terbesar yang Pernah Terjadi di Indonesia.
- Pamungkas, A. T., Mulyono, A., & Lahangatubun, N. (2024). The Crisis of Cybercrime Law Enforcement in Indonesia. *Delictum: Jurnal Hukum Pidana dan Kriminologi*, 2(2), 101-113.
- Respati, N. (2024). Tantangan Penegakan Hukum terhadap Kejahatan Berbasis Kecerdasan Buatan di Indonesia. *Innovative: Jurnal Ilmiah Hukum*, 6(1), 55-67.
- Syahril, M. A. F. (2023). Cyber Crime in terms of the Human Rights Perspective. *International Journal of Multicultural and Multireligious Understanding*, 10(5), 119-130.
- Syahril, Muh. A. F. *Hukum Informasi dan Transaksi Elektronik*. Eureka Media Aksara, 2023.
- Syarif, M., Ramadhani, R., Graha, M. A. W., Yanuaria, T., Muhtar, M. H., Asmah, N., ... & Jannah, M. (2024). *Metode Penelitian Hukum*.
- Wibowo, M. S. I., Munawar, A., & Hidayatullah. (2024). Tindak Pidana Cybercrime: Tantangan Hukum Pidana Dalam Penanggulangan Kejahatan Dunia Maya di Indonesia. *Jurnal Kajian Sosial*, 8(2), 1-15.

#### Conflict of Interest Statement:

The author declares that the research was conducted without any commercial or financial relationships that could potentially create a conflict of interest.

Copyright © 2025 Litigasi. All rights reserved.