JURNAL ILMU MULTIDISIPLIN

Jurnal Ilmu Multidisiplin
Volume 3 No 1 (2025)
E-ISSN 2541-2332

Hak asasi manusia di era digital: Tantangan dan peluang dalam mengatasi kejahatan siber

Elvan Maulana Rif'at[1], Timbul Dompak[2]
[1,2]*Universitas Putera Batam Indonesia*

Abstrak
Penelitian ini bertujuan untuk menganalisis tantangan dan peluang terkait dengan hak asasi manusia dalam menghadapi kejahatan siber di era digital. Perkembangan pesat teknologi digital memberikan manfaat besar, namun juga menimbulkan ancaman serius terhadap privasi, kebebasan berekspresi, dan perlindungan data pribadi. Penelitian ini menggunakan pendekatan deskriptif kualitatif dengan metode pengumpulan data melalui wawancara mendalam, observasi, dan telaah dokumen. Hasil penelitian menunjukkan bahwa kesenjangan regulasi, rentannya kelompok perempuan, anak-anak, dan minoritas terhadap kejahatan siber, serta perlindungan data pribadi yang masih lemah, menjadi tantangan utama dalam melindungi hak asasi manusia di dunia maya. Di sisi lain, teknologi juga menawarkan peluang untuk mitigasi kejahatan siber melalui solusi keamanan yang canggih, meskipun implementasinya terbatas oleh akses dan biaya. Penelitian ini menyarankan pembaruan regulasi, perluasan edukasi digital, pengembangan teknologi keamanan yang lebih terjangkau, dan pendekatan lintas sektor untuk mengatasi permasalahan tersebut. Kerjasama internasional dan kebijakan yang lebih responsif terhadap perkembangan teknologi digital diharapkan dapat memperkuat perlindungan hak asasi manusia di dunia maya.

Kata Kunci
Hak Asasi Manusia, Kejahatan Siber, Perlindungan Data, Teknologi, Pendekatan Lintas Sektor

PENDAHULUAN

Di era digital yang terus berkembang pesat ini, kemajuan teknologi memberikan dampak yang signifikan terhadap berbagai aspek kehidupan manusia, termasuk dalam hal hak asasi manusia (HAM). Kemudahan akses informasi, komunikasi, dan layanan digital telah membuka berbagai peluang baru bagi individu, organisasi, dan negara. Namun, seiring dengan manfaat tersebut, muncul pula ancaman baru yang tidak bisa diabaikan, yaitu kejahatan siber. Kejahatan siber, yang mencakup berbagai bentuk aktivitas ilegal yang dilakukan melalui teknologi informasi, telah menjadi tantangan besar bagi masyarakat global dalam melindungi hak-hak dasar manusia.

Perubahan besar dalam kehidupan sosial akibat digitalisasi telah mengarah pada pelanggaran hak privasi, kebebasan berekspresi, dan hak untuk mendapatkan perlindungan dari ancaman dunia maya. Kemajuan teknologi dapat menyebabkan penyebaran data pribadi, membahayakan keselamatan dan privasi korban, dan memerlukan peraturan pemerintah khusus untuk melindungi hak asasi manusia (Qotrunnada, 2023). Menurut laporan Cybersecurity Ventures, kejahatan siber diperkirakan akan merugikan dunia lebih dari 10,5 triliun dolar AS setiap tahunnya pada tahun 2025, yang menunjukkan betapa besar ancaman

yang dihadapi oleh masyarakat global dalam menjaga keamanan dan hak asasi individu. Menurut laporan CISA, kejahatan semacam ini tidak hanya mengakibatkan kerugian finansial bagi individu, tetapi juga berpotensi menimbulkan dampak negatif jangka panjang terhadap reputasi serta trauma psikologis bagi para korban (Supriandi et al., 2023).Selain itu, kerugian ini juga mencakup kerusakan terhadap integritas data pribadi dan privasi individu yang seharusnya dilindungi oleh negara dan hukum internasional.

Hak Asasi Manusia (HAM) merupakan hak yang melekat pada setiap individu hanya karena ia adalah manusia. Hak ini meliputi hak-hak sipil, politik, ekonomi, sosial, dan budaya yang mendukung terciptanya kehidupan yang layak dan bermartabat (Maruf & Islam, 2023). Dalam konteks era digital, HAM mengalami pergeseran dan tantangan baru akibat perkembangan teknologi. Salah satu ancaman yang paling signifikan adalah kejahatan siber, yang dapat melanggar hak atas privasi, kebebasan berekspresi, dan perlindungan data pribadi. Kejahatan siber, seperti peretasan, pencurian identitas, dan penyalahgunaan data, berpotensi melanggar hak privasi, membatasi kebebasan berekspresi, serta membahayakan keamanan data pribadi (Supriandi et al., 2023). Oleh karena itu, perlindungan HAM di dunia digital menjadi isu penting dalam diskusi global. Beberapa teori mendukung pemahaman mengenai hubungan antara HAM dan kejahatan siber. Pertama, teori privasi digital menekankan pentingnya melindungi data pribadi sebagai bagian dari hak privasi individu. Privasi digital dipandang sebagai hak fundamental yang esensial untuk menjaga kebebasan individu dan kemandirian di era teknologi digital (Sembiring et al., 2024). Kedua, teori keadilan sosial yang diperkenalkan oleh Rawls menyoroti pentingnya kesetaraan akses terhadap teknologi serta perlindungan bagi kelompok rentan agar terhindar dari eksploitasi di ranah digital (Bukit & Ayunda, 2022). Ketiga, teori keamanan siber menyoroti pentingnya infrastruktur teknologi yang aman untuk mencegah pelanggaran HAM.

Salah satu dampak langsung dari kejahatan siber adalah pelanggaran terhadap hak privasi, yang secara langsung berhubungan dengan hak asasi manusia. Kejahatan seperti pencurian identitas digital, peretasan akun pribadi, dan penyebaran data pribadi tanpa izin menjadi isu besar yang dihadapi oleh masyarakat digital saat ini. Menurut laporan dari Cybersecurity and Infrastructure Security Agency (CISA), lebih dari 60% pengguna internet global mengalami ancaman terhadap data pribadi mereka pada tahun 2022. Kasus-kasus seperti ini menunjukkan betapa mudahnya hak privasi individu dilanggar di dunia maya. Selain itu, kejahatan siber seperti peretasan, doxing, dan perundungan daring tidak hanya mengancam kebebasan berekspresi dan berpendapat, tetapi juga melanggar hak asasi

manusia dan nilai-nilai demokrasi (Muhammad et al., 2024). Tindakan tersebut menciptakan rasa takut di masyarakat dan merusak hak-hak fundamental yang dijamin oleh Deklarasi Universal Hak Asasi Manusia (UDHR). Penyebaran informasi palsu (hoax), kampanye disinformasi, dan penyensoran online yang dilakukan oleh individu atau negara tertentu seringkali bertentangan dengan prinsip kebebasan berbicara. Dalam laporan yang dikeluarkan oleh Freedom House pada 2023, diperkirakan lebih dari 50 negara menerapkan kebijakan pembatasan terhadap kebebasan berekspresi di internet, yang menunjukkan besarnya tantangan untuk mempertahankan hak asasi dalam ruang digital.

Pelanggaran HAM di dunia maya juga berwujud dalam bentuk kejahatan terhadap perempuan dan anak-anak, seperti kekerasan berbasis gender, pelecehan seksual, dan perundungan online (cyberbullying). Kejahatan dunia maya deepfake secara signifikan berdampak pada martabat, perempuan dan melanggar hak privasi mereka, khususnya di platform media sosial (Sharma, 2024). Menurut UN Women, sekitar 73% perempuan di dunia melaporkan mengalami kekerasan online dalam bentuk pelecehan verbal atau ancaman fisik melalui platform digital. Fenomena ini menggarisbawahi perlunya langkah-langkah perlindungan yang lebih efektif dalam menangani kejahatan siber yang menyasar kelompok rentan.

Kejahatan siber tidak hanya berdampak pada individu, tetapi juga berpotensi merusak tatanan sosial dan ekonomi. Kejahatan dunia maya memiliki dampak negatif yang signifikan terhadap pembangunan sosial (Zhang & Zhang, 2024). Serangan terhadap infrastruktur kritis, seperti sistem perbankan dan layanan kesehatan, dapat mengganggu hak masyarakat untuk mendapatkan layanan dasar yang seharusnya dilindungi oleh negara. Pada tahun 2020, serangan siber terhadap sektor kesehatan di Amerika Serikat menyebabkan penundaan dalam penyediaan layanan medis yang krusial bagi jutaan orang, yang berpotensi mengancam hak atas kesehatan masyarakat. Banyak rumah sakit AS tidak siap menghadapi serangan siber, dengan strategi yang lemah dan upaya yang sebagian besar salah arah, sehingga membahayakan pasien secara fisik dan digital saat perangkat medis atau perawatan disusupi (Wasserman & Wasserman, 2022).

Tantangan utama dalam menghadapi kejahatan siber adalah kurangnya regulasi dan kerangka hukum yang jelas. Meskipun banyak negara telah membuat kebijakan dan peraturan mengenai keamanan dunia maya, implementasi dan penegakan hukum sering kali tertinggal. Ketidaksesuaian antara hukum yang ada dengan perkembangan teknologi baru membuat penegakan keadilan dalam kasus kejahatan siber menjadi semakin sulit. Selain itu, hukum

internasional mengenai kejahatan siber masih dalam tahap pengembangan, dan belum ada kesepakatan global mengenai mekanisme penanggulangan yang efektif.

Di sisi lain, teknologi itu sendiri dapat menjadi alat untuk memperkuat perlindungan terhadap hak asasi manusia. Sistem keamanan berbasis teknologi, seperti enkripsi data dan kecerdasan buatan (AI) dalam deteksi ancaman siber, memiliki potensi besar untuk melindungi individu dan masyarakat dari kejahatan dunia maya. Namun, hal ini juga menimbulkan tantangan baru, yaitu ketergantungan pada teknologi yang dapat disalahgunakan oleh pihak-pihak yang tidak bertanggung jawab, termasuk untuk kepentingan pengawasan massal atau pelanggaran privasi.

Mengingat kenyataan bahwa banyak negara dan organisasi yang belum sepenuhnya siap menghadapi dampak buruk dari kejahatan siber terhadap HAM, maka penelitian ini menjadi sangat penting untuk dilakukan. Dalam konteks ini, penting untuk mengeksplorasi berbagai tantangan yang ada, serta mengidentifikasi peluang yang dapat digunakan untuk memperkuat perlindungan hak asasi manusia di era digital. Salah satunya adalah melalui kolaborasi internasional dalam menciptakan kebijakan dan peraturan yang harmonis serta memperkuat kapasitas teknis untuk mendeteksi dan mengatasi kejahatan siber.

Selain itu, perlu adanya peningkatan kesadaran di kalangan masyarakat global mengenai pentingnya perlindungan hak asasi di ruang digital. Pendidikan dan literasi digital harus menjadi prioritas dalam upaya mengurangi kerentanan terhadap kejahatan siber. Organisasi non-pemerintah, pemerintah, dan sektor swasta harus bekerja sama untuk menciptakan ekosistem digital yang aman dan inklusif, yang menghormati dan melindungi hak asasi manusia.

Penelitian ini bertujuan untuk memberikan wawasan yang lebih dalam mengenai hubungan antara kejahatan siber dan hak asasi manusia di era digital. Dengan menggali lebih dalam tantangan-tantangan yang ada, serta peluang-peluang yang dapat dimanfaatkan untuk mengatasi masalah tersebut, diharapkan penelitian ini dapat memberikan rekomendasi praktis bagi kebijakan dan regulasi yang dapat diterapkan oleh berbagai pihak yang terlibat dalam melindungi HAM di dunia maya.

METODE

Penelitian ini menggunakan pendekatan deskriptif kualitatif untuk mendeskripsikan dan menggambarkan situasi, kondisi, serta hubungan yang ada antara hak asasi manusia dan kejahatan siber di era digital. Pendekatan ini dipilih karena bertujuan untuk menginterpretasikan fenomena sosial yang kompleks terkait dengan dampak kejahatan siber terhadap HAM, serta

untuk memberikan gambaran yang jelas mengenai tantangan yang dihadapi dalam melindungi hak asasi manusia di dunia maya.

Teknik pengumpulan data dilakukan melalui beberapa metode, antara lain observasi, telaah data sekunder, serta pengumpulan informasi dari jurnal, buku, dan bahan bacaan lainnya yang relevan dengan topik penelitian ini. Observasi akan difokuskan pada studi kasus kejahatan siber yang telah terjadi, serta penelaahan terhadap kebijakan dan regulasi yang ada mengenai perlindungan hak asasi manusia di dunia maya. Selain itu, penelitian ini juga akan menelaah berbagai laporan dan dokumen yang diterbitkan oleh lembaga internasional dan nasional yang berfokus pada keamanan siber dan perlindungan privasi individu. Analisis data akan dilakukan secara kualitatif, yang melibatkan interpretasi data dan informasi yang diperoleh melalui wawancara, observasi, dan telaah dokumen. Peneliti akan melakukan penafsiran intelektual dan empiris terhadap data yang telah terkumpul untuk mengidentifikasi pola, tantangan, dan peluang dalam mengatasi kejahatan siber yang mengancam hak asasi manusia

HASIL DAN PEMBAHASAN

A. Tantangan Utama: Kesenjangan Regulasi dan Perlindungan Hak Asasi Manusia

Salah satu temuan utama dalam penelitian ini adalah adanya kesenjangan yang besar antara perkembangan teknologi digital dan regulasi yang mengatur hak asasi manusia di dunia maya. Banyak negara, terutama negara berkembang, belum memiliki kebijakan yang memadai untuk melindungi individu dari kejahatan siber, meskipun ada peningkatan kesadaran global akan pentingnya perlindungan privasi dan data pribadi. Sebagai contoh, meskipun Uni Eropa telah mengimplementasikan General Data Protection Regulation (GDPR), banyak negara lainnya masih tertinggal dalam hal pengaturan data pribadi dan perlindungan hak digital (AllahRakha, 2024).

Di era digital, perkembangan teknologi jauh lebih cepat dibandingkan dengan kemampuan regulasi untuk mengikutinya. Kejahatan siber, seperti peretasan, penipuan daring, dan pencurian identitas, semakin mengancam privasi individu. Sementara itu, hukum yang ada sering kali tidak mencakup cakupan global atau menanggapi ancaman baru dengan cepat. Ini menciptakan tantangan bagi pemerintah dan lembaga internasional untuk merumuskan kebijakan yang lebih responsif dan berbasis teknologi untuk melindungi hak asasi manusia.

Diperlukan upaya global untuk memperbarui hukum internasional terkait hak asasi manusia dalam konteks digital. Kerjasama internasional antara negara-negara maju dan berkembang sangat penting untuk menciptakan regulasi yang dapat mengatasi kejahatan siber

lintas batas. Kebijakan perlindungan hak asasi manusia di dunia maya perlu lebih fokus pada perlindungan data pribadi, hak atas privasi, dan kebebasan berekspresi.

B. Kejahatan siber yang terkait dengan Hak Asasi Manusia: Perempuan, Anak-Anak, Kelompok Rentan

Hasil penelitian menunjukkan bahwa kelompok rentan seperti perempuan, anak-anak, dan minoritas sering menjadi target utama dari kejahatan siber yang melanggar hak asasi manusia. Cyberbullying, pelecehan seksual online, serta eksploitasi dan perdagangan manusia melalui platform digital adalah beberapa bentuk kejahatan siber yang paling sering menimpa kelompok ini. Selain itu, banyak dari mereka yang tidak memiliki keterampilan digital yang memadai untuk melindungi diri mereka dari ancaman di dunia maya.

Penelitian ini mengidentifikasi bahwa meskipun teknologi dapat memberdayakan individu, termasuk kelompok rentan, kenyataannya banyak dari mereka yang menjadi sasaran empuk kejahatan siber. Perempuan dan anak-anak, misalnya, sering terjebak dalam perundungan daring dan eksploitasi seksual yang memanfaatkan kerentanannya di dunia maya. Kurangnya edukasi tentang keamanan digital, serta kesulitan dalam melaporkan atau mencari bantuan dalam kasus-kasus ini, memperburuk situasi.

Untuk mengatasi masalah ini, penting untuk merancang kebijakan dan program yang lebih inklusif yang memberikan perhatian khusus kepada kelompok rentan. Pendidikan digital yang mengajarkan cara melindungi diri di dunia maya harus menjadi bagian dari kurikulum pendidikan di seluruh dunia. Selain itu, platform digital juga harus bertanggung jawab untuk memperkenalkan sistem keamanan yang lebih ketat, serta mekanisme pelaporan yang lebih mudah diakses oleh korban.

C. Keamanan Data dan Privasi dalam Era Digital: Perlindungan yang Masih Lemah

Salah satu isu besar yang ditemukan dalam penelitian ini adalah pentingnya perlindungan data pribadi di dunia maya. Kejahatan siber sering kali melibatkan pencurian informasi pribadi seperti nomor identitas, data keuangan, dan rincian pribadi lainnya yang dapat digunakan untuk melakukan penipuan atau kejahatan lainnya (Setiawan et al, 2020). Meskipun beberapa negara telah mengadopsi kebijakan untuk melindungi data pribadi, masih banyak individu yang tidak sadar akan pentingnya perlindungan data pribadi mereka.

Masalah perlindungan data pribadi semakin mendesak di tengah maraknya peretasan dan penyalahgunaan informasi pribadi. Misalnya, peretasan data besar yang melibatkan

perusahaan besar dan pemerintah sering kali mengungkapkan informasi pribadi yang sangat sensitif. Selain itu, munculnya platform media sosial dan aplikasi digital yang mengumpulkan data pengguna tanpa kontrol yang jelas telah meningkatkan kerentanannya terhadap penyalahgunaan.

Penguatan kebijakan privasi dan regulasi perlindungan data pribadi harus menjadi prioritas utama. Negara-negara perlu memperkenalkan regulasi yang lebih ketat mengenai pengumpulan, penyimpanan, dan penggunaan data pribadi. Selain itu, edukasi kepada masyarakat tentang pentingnya perlindungan data pribadi dan cara-cara melindunginya perlu diperluas.

D. Peran Teknologi dalam Menanggulangi Kejahatan Siber: Solusi dan Tantangan

Salah satu isu besar yang ditemukan dalam penelitian ini adalah pentingnya perlindungan data pribadi di dunia maya. Kejahatan siber sering kali melibatkan pencurian informasi pribadi seperti nomor identitas, data keuangan, dan rincian pribadi lainnya yang dapat digunakan untuk melakukan penipuan atau kejahatan lainnya. Meskipun beberapa negara telah mengadopsi kebijakan untuk melindungi data pribadi, masih banyak individu yang tidak sadar akan pentingnya perlindungan data pribadi mereka.

Penelitian ini juga menunjukkan bahwa teknologi tidak hanya menjadi penyebab meningkatnya kejahatan siber, tetapi juga dapat digunakan sebagai alat untuk mendeteksi, mengatasi, dan mencegahnya. Teknologi keamanan canggih, seperti enkripsi, pemantauan jaringan, dan deteksi ancaman berbasis AI, telah banyak dikembangkan untuk melindungi individu dari ancaman digital. Namun, tantangannya adalah bagaimana memastikan bahwa teknologi ini dapat diakses oleh semua orang dan tidak hanya oleh perusahaan atau individu yang memiliki sumber daya besar.

Meskipun teknologi memiliki potensi besar dalam memerangi kejahatan siber, implementasinya seringkali terbatas oleh faktor biaya, aksesibilitas, dan kesadaran. Negara-negara dengan infrastruktur digital yang terbatas sering kali kesulitan untuk mengadopsi teknologi keamanan terbaru (Kusumoningtyas, 2023), yang berpotensi meningkatkan kerentanannya terhadap kejahatan siber. Selain itu, ada masalah etika yang terkait dengan penggunaan teknologi pemantauan dan pengawasan untuk mendeteksi ancaman.

Pemerintah dan lembaga internasional perlu memfasilitasi akses ke teknologi keamanan siber yang lebih terjangkau, terutama bagi negara-negara berkembang. Kerjasama antara sektor publik dan swasta sangat penting dalam mengembangkan dan menerapkan solusi

teknologi yang dapat membantu individu melindungi diri mereka di dunia maya. Selain itu, penting untuk memastikan bahwa penggunaan teknologi ini tetap mematuhi prinsip-prinsip hak asasi manusia, seperti privasi dan kebebasan berekspresi.

Strategi Mitigasi: Pendekatan Lintas Sektor untuk Perlindungan HAM

Hasil penelitian menunjukkan bahwa untuk mengatasi tantangan yang ditimbulkan oleh kejahatan siber terhadap hak asasi manusia, dibutuhkan pendekatan lintas sektor yang melibatkan berbagai pihak. Tidak hanya pemerintah, tetapi juga sektor swasta, organisasi masyarakat sipil, dan lembaga internasional perlu bekerja sama dalam menciptakan ekosistem digital yang aman. Selain itu, penerapan prinsip-prinsip tata kelola yang baik, seperti transparansi, akuntabilitas, dan partisipasi, sangat penting untuk memperkuat keamanan siber (Marwana et al, 2022).

Kejahatan siber yang melanggar hak asasi manusia bukan hanya masalah hukum atau teknologi semata. Masalah ini memerlukan solusi yang melibatkan semua sektor terkait-termasuk regulasi yang kuat, edukasi masyarakat, pengembangan teknologi yang lebih aman, dan kolaborasi internasional. Misalnya, perusahaan teknologi dapat memainkan peran besar dalam mengembangkan perangkat lunak yang lebih aman dan memberikan pelatihan kepada penggunanya tentang cara menghindari risiko di dunia maya.

Dengan menerapkan pendekatan lintas sektor, kita dapat menciptakan strategi mitigasi yang lebih efektif untuk mengatasi kejahatan siber. Kebijakan dan inisiatif yang melibatkan pemerintah, sektor swasta, akademisi, dan masyarakat sipil harus dirancang untuk bekerja bersama dalam menghadapi masalah ini.

KESIMPULAN

Penelitian ini mengidentifikasi tantangan besar terkait hak asasi manusia dalam menghadapi kejahatan siber di era digital. Meskipun teknologi menawarkan manfaat besar, risiko terhadap privasi, kebebasan berekspresi, dan perlindungan data pribadi semakin meningkat. Temuan utama dari penelitian ini adalah:

1. Kesenjangan Regulasi: Banyak negara, terutama negara berkembang, masih tertinggal dalam merumuskan kebijakan yang memadai untuk melindungi hak digital dan data pribadi.
2. Kelompok Rentan: Perempuan, anak-anak, dan kelompok minoritas lebih rentan menjadi korban kejahatan siber, seperti perundungan daring dan eksploitasi seksual online.

3. Perlindungan Data yang Lemah: Pencurian data pribadi masih menjadi ancaman utama, dan banyak individu kurang sadar tentang pentingnya perlindungan data pribadi di dunia maya.
4. Teknologi untuk Mitigasi: Teknologi dapat membantu dalam mendeteksi dan mencegah kejahatan siber, namun akses terbatas di negara-negara dengan infrastruktur yang kurang memadai.

Pendekatan Lintas Sektor: Penyelesaian masalah ini membutuhkan kerjasama antara pemerintah, sektor swasta, lembaga internasional, dan masyarakat sipil

1. Pembaruan Regulasi: Negara-negara harus memperbarui dan menegakkan regulasi untuk melindungi hak digital dan data pribadi, serta menanggapi cepat perubahan teknologi.
2. Edukasi Digital: Perlu diperluas pendidikan digital dan kesadaran masyarakat mengenai pentingnya perlindungan data pribadi dan keamanan dunia maya.
3. Perlindungan untuk Kelompok Rentan: Kebijakan khusus untuk melindungi kelompok rentan, seperti perempuan dan anak-anak, harus diperkuat.
4. Pengembangan Teknologi Keamanan: Akses terhadap teknologi keamanan yang terjangkau dan efektif harus diperluas, terutama bagi negara-negara berkembang.
5. Kolaborasi Global: Pendekatan lintas sektor dan kerjasama internasional sangat penting untuk menciptakan kebijakan yang komprehensif dan efektif dalam menangani kejahatan siber dan melindungi hak asasi manusia.

DAFTAR PUSTAKA

AllahRakha. (2024). International Journal of Law and Policy | Volume: 2 Issue: 4 2024. *International Journal of Law and Policy*, *2*(4), 31–43.

Awaluddin, F., Amsori, & Mulyana, M. (2024). Tantangan dan Peran Digital Forensik dalam Penegakan Hukum terhadap Kejahatan di Ranah Digital. *Humaniorum*, *2*(1), 14–19.

Bukit & Ayunda. (2022). Urgensi Pengesahan RUU Perlindungan Data Pribadi Terhadap Perlindungan Kebocoran Data Penerimaan SMS Dana Cepat. *Reformasi Hukum*, *26*(1), 1–20.

Kusumoningtyas. (2023). Nexus Pengawasan Siber Sebagai Instrumen Keamanan Nasional Dan Relevansinya Dengan Demokrasi: Perbandingan Beberapa Negara. *Jurnal Adhikari*, *2*(3), 416–433.

Madinah Mokobombang, Zulfikri Darwis, & Sabil Mokodenseho. (2023). Pemberantasan Tindak Pidana Cyber di Provinsi Jawa Barat: Peran Hukum dan Tantangan dalam

Penegakan Hukum Terhadap Kejahatan Digital. *Jurnal Hukum Dan HAM Wara Sains*, *2*(6), 517–525.

Maruf & Islam. (2023). *Human Rights and Fundamental Rights in Bangladesh Constitution: A Study Based on Case Law*. *6*(1), 42–54.

Marwana, A., Odier-Contreras Garduñob, D., & Bonfigli, F. (2022). *Detection of Digital Law Issues and Implication for Good Governance Policy in Indonesia Awaludin*. *10*(1), 22–32.

Muhammad, H., Liyorba Indra, G., & Rizka Virnanda, O. (2024). Undermining People's Freedoms and Opinions in the Digital Era. *KnE Social Sciences*, *2024*, 282–293.

Qotrunnada, S. D. (2023). Perlindungan Ham Terhadap Kebocoran Data Pribadi Pasien Akibat Cyber Crime. *Global Education Journal*, *1*(2), 327–332.

Sembiring, T. B., Marshinta, F. U., Mangkunegara, R. A., Utami, I. S., & Haipon, H. (2024). Digital Privacy Rights in the Age of Big Data: Balancing Security and Civil Liberties. *Global International Journal of Innovative Research*, *2*(3), 712–720.

Setiawan, Ghufron, & M. (2020). Perlindungan Hukum Terhadap Data Pribadi Konsumen Dalam AllahRakha. (2024). International Journal of Law and Policy | Volume: 2 Issue: 4 2024. *International Journal of Law and Policy*, *2*(4), 31–43.

Awaluddin, F., Amsori, & Mulyana, M. (2024). Tantangan dan Peran Digital Forensik dalam Penegakan Hukum terhadap Kejahatan di Ranah Digital. *Humaniorum*, *2*(1), 14–19.

Bukit & Ayunda. (2022). Urgensi Pengesahan RUU Perlindungan Data Pribadi Terhadap Perlindungan Kebocoran Data Penerimaan SMS Dana Cepat. *Reformasi Hukum*, *26*(1), 1–20.

Kusumoningtyas. (2023). Nexus Pengawasan Siber Sebagai Instrumen Keamanan Nasional Dan Relevansinya Dengan Demokrasi: Perbandingan Beberapa Negara. *Jurnal Adhikari*, *2*(3), 416–433.

Madinah Mokobombang, Zulfikri Darwis, & Sabil Mokodenseho. (2023). Pemberantasan Tindak Pidana Cyber di Provinsi Jawa Barat: Peran Hukum dan Tantangan dalam Penegakan Hukum Terhadap Kejahatan Digital. *Jurnal Hukum Dan HAM Wara Sains*, *2*(6), 517–525.

Maruf & Islam. (2023). *Human Rights and Fundamental Rights in Bangladesh Constitution: A Study Based on Case Law*. *6*(1), 42–54.

Marwana, A., Odier-Contreras Garduñob, D., & Bonfigli, F. (2022). *Detection of Digital Law Issues and Implication for Good Governance Policy in Indonesia Awaludin*. *10*(1), 22–32.

Muhammad, H., Liyorba Indra, G., & Rizka Virnanda, O. (2024). Undermining People's

Freedoms and Opinions in the Digital Era. *KnE Social Sciences*, *2024*, 282–293.

Qotrunnada, S. D. (2023). Perlindungan Ham Terhadap Kebocoran Data Pribadi Pasien Akibat Cyber Crime. *Global Education Journal*, *1*(2), 327–332.

Sembiring, T. B., Marshinta, F. U., Mangkunegara, R. A., Utami, I. S., & Haipon, H. (2024). Digital Privacy Rights in the Age of Big Data: Balancing Security and Civil Liberties. *Global International Journal of Innovative Research*, *2*(3), 712–720.

Setiawan, Ghufron, & M. (2020). Perlindungan Hukum Terhadap Data Pribadi Konsumen Dalam Transaksi e-Commerce. *MLJ Merdeka Law Journal*, *1*(2), 102–111.

Sharma. (2024). Deepfake Pornography: Examining the Impact on Women's Digital Privacy and Consent. *International Journal For Multidisciplinary Research*, *6*(4), 1–10.

Supriandi, Khairunnisa, & Putra, W. U. (2023). Hak Asasi Manusia di Ranah Digital: Analisis Hukum Siber dan Kebebasan Online. *Jurnal Hukum Dan HAM Wara Sains*, *2*(08), 690–703.

Wasserman, L., & Wasserman, Y. (2022). Hospital cybersecurity risks and gaps: Review (for the non-cyber professional). *Frontiers in Digital Health*, *4*.

Zhang, S., & Zhang, S. (2024). Analysis of the Impact of Transnational Cybercrime in Southeast Asian Countries on Global Social Development. *Highlights in Business, Economics and Management*, *24*, 1049–1053