PERTANGGUNGJAWABAN PIDANA HACKER DAN CRACKER DALAM PENCURIAN DATA GAME DI INDONESIA

Oleh
I Putu Edi Rusmana
Universitas Pendidikan Nasional
e-mail: edirusmana@undiknas.ac.id

Abstrak

Penelitian ini membahas penegakan hukum pidana terhadap pelaku kejahatan siber, khususnya hacker dan cracker, yang melakukan pencurian data game di Indonesia. Kasus pencurian data dalam industri game semakin sering terjadi dan mengakibatkan kerugian besar, baik bagi pengguna maupun perusahaan pengembang. Dengan menggunakan metode penelitian normatif, penelitian ini menganalisis dasar hukum dan upaya penegakan yang diatur dalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) serta undang-undang terkait lainnya. Pendekatan perundang-undangan dan konseptual diterapkan untuk memahami pertanggungjawaban pidana bagi pelaku kejahatan siber dalam konteks pencurian data game. Hasil penelitian menunjukkan bahwa penegakan hukum di Indonesia masih menghadapi berbagai kendala, seperti keterbatasan keahlian teknis dalam forensik digital, masalah yurisdiksi lintas negara, serta perlunya peningkatan regulasi perlindungan data pribadi. Rekomendasi penelitian ini menekankan perlunya sinergi antara pemerintah, industri, dan masyarakat, serta peningkatan kapasitas aparat penegak hukum. Dengan regulasi yang lebih kuat dan kolaborasi yang baik, diharapkan kasus pencurian data dapat ditekan dan memberikan keamanan lebih bagi ekosistem digital di Indonesia, khususnya dalam industri game.

Kata Kunci: Kejahatan Siber, Pencurian Data Game, Penegakan Hukum Pidana

PENDAHULUAN

Industri game di Indonesia dan dunia telah berkembang pesat seiring dengan meningkatnya akses masyarakat terhadap teknologi digital. Banyaknya pengguna aktif, terutama anak muda, menjadikan game sebagai salah satu industri digital yang bernilai ekonomi tinggi (Andriyanty, Rafiq, & Rambey, 2023). Data pengguna yang tersimpan dalam aplikasi dan sistem game seperti identitas pemain, data finansial, dan kemajuan permainan menjadi target penting bagi para hacker dan cracker. Di era digital ini, tindakan pencurian data menjadi semakin sering terjadi dan mengakibatkan kerugian besar bagi perusahaan, pemain, dan keamanan data pribadi (Widianingrum, 2024). Hacker, dengan kemampuan mereka dalam mengakses dan meretas sistem, sering kali dimanfaatkan untuk kegiatan ilegal, termasuk pencurian data di game.

Penting untuk memahami perbedaan serta peran hacker dan cracker dalam konteks kejahatan siber, khususnya dalam pencurian data di industri game. Dalam pengertian umum, hacker adalah individu yang memiliki keahlian mendalam dalam mengeksplorasi, menganalisis, dan meretas sistem komputer atau jaringan (Ali, M. & Nurhayati, 2020). Meski kemampuan teknis mereka sering dikaitkan dengan aktivitas ilegal, tidak semua hacker beroperasi di luar batas hukum. Hacker sendiri terbagi menjadi beberapa jenis, di antaranya *white hat hackers* yang bekerja untuk keamanan sistem, *grey hat hackers* yang berada di antara legalitas dan ilegalitas, serta *black hat hackers* yang bertindak untuk merusak dan

mengeksploitasi sistem secara ilegal (Wibowo Noor Fikri et al., 2023). Sementara itu, cracker secara khusus merujuk pada individu yang memiliki motivasi merusak atau mencuri, serta menggunakan keterampilan mereka untuk mengakses data atau sistem dengan tujuan jahat atau merugikan pihak lain (Ramadhanti, Tias, Lestari, & Hosnah, 2024). Dalam konteks pencurian data game, cracker cenderung mencari keuntungan finansial dengan mencuri dan memperjualbelikan data pemain, item dalam game, atau hasil dari sistem keuangan dalam permainan tersebut.

Pencurian data game oleh cracker sering kali melibatkan beberapa tindakan kriminal, seperti *bypassing* proteksi sistem, menembus enkripsi data, dan mengeksploitasi kerentanan pada server game. Data game yang dicuri biasanya mencakup informasi pribadi pengguna seperti nama, alamat email, hingga data pembayaran, yang kemudian bisa dijual di pasar gelap atau dark web. Selain itu, cracker juga kerap mencuri *in game assets* atau item dalam permainan, yang memiliki nilai ekonomi tinggi dalam sistem permainan tertentu. Dalam beberapa kasus, data ini juga digunakan untuk mencuri akun pemain dengan peringkat atau item langka, yang kemudian diperjualbelikan di pasar ilegal (damar chikawati hera, 2021). Fenomena ini menunjukkan bahwa cracker berperan besar dalam kejahatan yang memiliki efek domino, tidak hanya merugikan perusahaan pengembang game dari segi finansial dan reputasi, tetapi juga melanggar privasi dan keamanan data pribadi para pemain.

Sementara itu, para hacker yang memilih untuk berperan sebagai cracker, dalam beberapa kasus, terdorong oleh kesempatan ekonomi yang menggiurkan. Mengingat industri game memiliki komunitas pemain yang besar, terutama di Indonesia, nilai ekonomi dari pencurian data game cukup signifikan. Tidak jarang hacker yang awalnya hanya tertarik pada aspek teknis suatu sistem tergoda untuk melakukan tindakan yang melampaui batas legal, terutama ketika data yang dicuri dapat menghasilkan keuntungan. Sebagai contoh, beberapa hacker memanfaatkan kemampuan mereka untuk meretas server game, lalu melakukan akses ilegal yang memungkinkan mereka mencuri data pemain atau mengeksploitasi sistem reward game. Data yang dicuri tersebut kemudian dijual ke pasar atau pihak ketiga yang berkepentingan, yang semakin menambah risiko pencurian data pribadi di industri ini (Suci, 2016).

Perbedaan peran dan motivasi antara hacker dan cracker menjadi penting untuk dijelaskan dalam konteks hukum, mengingat karakteristik mereka yang berbeda bisa berimplikasi pada pendekatan penanganan hukum yang berbeda pula. Walaupun hacker dan cracker sama-sama memiliki keterampilan teknis yang tinggi dalam bidang siber, pendekatan dan tujuan akhir mereka berbeda, yang mana cracker bertujuan secara langsung untuk melanggar hukum dengan cara merugikan sistem atau pengguna lain. Oleh karena itu, pemahaman yang tepat mengenai karakteristik keduanya dapat membantu pihak penegak hukum dan pembuat kebijakan dalam mengembangkan kebijakan pidana yang lebih relevan dan komprehensif untuk melindungi data game serta hak para pemain.

Indonesia sebenarnya memiliki beberapa regulasi yang mengatur kejahatan siber, salah satunya adalah Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) yang kemudian direvisi sebanyak 2 (dua) kali yaitu melalui Undang-Undang Nomor 19 Tahun 2016 dan Undang-Undang Nomor 1 Tahun 2024 (Putri, Oktaria, Ardinata, Yanuar, & Althafi, 2024). Undang-undang ini menjadi dasar utama dalam penegakan hukum terhadap tindak pidana siber, termasuk pencurian data yang melibatkan hacker dan cracker. Pasal-pasal dalam UU ITE mengatur tentang perlindungan data pribadi, larangan akses ilegal, perusakan sistem, hingga penyebaran informasi tanpa izin, yang semuanya relevan dalam konteks pencurian data game. Namun, meskipun UU ITE telah

mencakup berbagai aspek kriminalitas siber, regulasi ini dianggap masih kurang komprehensif dalam menanggulangi fenomena kejahatan digital yang semakin kompleks dan beragam. Industri game, yang memiliki karakteristik unik dan beroperasi di ranah digital yang cepat berkembang, sering kali menghadapi tantangan hukum yang spesifik, terutama terkait pencurian data pengguna atau transaksi ilegal di dalam game.

Selain UU ITE, terdapat juga Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik yang mengatur tentang kewajiban penyedia sistem elektronik dalam menjaga keamanan data pengguna (Yusuf, 2024). Namun, penerapan regulasi ini dalam konteks industri game masih terbatas, karena banyaknya perusahaan game asing yang beroperasi di Indonesia, yang sering kali menyimpan data pengguna di server luar negeri dan tidak terikat sepenuhnya oleh peraturan Indonesia. Hal ini mengakibatkan adanya celah hukum dalam melindungi data pengguna game, karena perusahaan asing sering kali tunduk pada regulasi negara asalnya, bukan Indonesia. Selain itu, aspek penegakan hukum terhadap hacker dan cracker di Indonesia sering kali menemui kendala karena kurangnya kemampuan teknis dan infrastruktur yang memadai dari lembaga penegak hukum. Hacker dan cracker yang melakukan pencurian data game sering kali menggunakan teknik yang canggih dan sulit dilacak, sehingga memerlukan sumber daya dan kerja sama lintas negara yang lebih kuat.

Kendala dalam penegakan hukum ini juga diperparah oleh keterbatasan pemahaman masyarakat umum tentang pentingnya perlindungan data pribadi di dunia digital, termasuk dalam permainan (ADITYA, n.d.). Banyak pemain game yang tidak menyadari risiko pencurian data dan tidak waspada terhadap tindakan yang dapat mengancam keamanan akun mereka, seperti berbagi informasi pribadi atau login ke aplikasi tidak resmi. Minimnya kesadaran ini sering kali dimanfaatkan oleh cracker yang mencuri data dengan memanfaatkan kelemahan pengguna, misalnya melalui phishing atau malware. Dengan demikian, upaya preventif dan edukatif dari pemerintah juga menjadi penting untuk melengkapi langkah penegakan hukum yang ada.

Selain tantangan teknis dan kurangnya kesadaran masyarakat, lambatnya proses adaptasi hukum terhadap perkembangan teknologi juga menjadi masalah signifikan. Perkembangan teknologi yang begitu cepat sering kali tidak diimbangi dengan perubahan regulasi yang memadai, sehingga membuat aturan yang ada mudah ketinggalan zaman dan kurang relevan dalam menanggapi modus operandi baru yang muncul. Banyak kasus kejahatan siber, termasuk pencurian data dalam industri game, menggunakan teknik-teknik baru yang belum sepenuhnya diatur dalam perundang-undangan yang ada. Hal ini membuat aparat penegak hukum menghadapi tantangan besar dalam menangani kejahatan siber yang melibatkan hacker dan cracker, karena kerangka hukum yang tersedia belum mampu menjangkau segala aspek teknis dan perkembangan modus yang dinamis dalam dunia digital.

Dengan semua keterbatasan ini, pertanggungjawaban pidana bagi hacker dan cracker yang terlibat dalam pencurian data game di Indonesia menjadi hal yang rumit dan penuh tantangan. Banyak kasus kejahatan siber, termasuk pencurian data game, yang akhirnya sulit diusut hingga tuntas karena keterbatasan teknis, hukum, dan kerja sama lintas negara. Dalam menghadapi situasi ini, diperlukan upaya untuk memperbarui kebijakan dan memperkuat infrastruktur penegakan hukum siber di Indonesia agar lebih adaptif dan responsif terhadap kejahatan digital yang semakin berkembang.

Penelitian ini bertujuan untuk memahami lebih lanjut bagaimana sistem hukum Indonesia memandang tindakan

pencurian data oleh hacker dan cracker dalam industri game. Jika dilihat dari penelitian sebelumnya yang berjudul Mengenal Hacking Sebagai Salah Satu Kejahatan Di Dunia Maya yag ditulis oleh Indah Sari pada tahun 2023 hanya penjelasan *hacker* dan *cracker* secara umum dalam hukum pidana di Indonesia (Sari, 2014). Selanjutnya pada penelitian yang dilakukan oleh Adelina Damayanti Anggarini dengan judul penelitian Kajian Hukum Dan Regulasi Terkait Serangan Hacking Pada Platform Digital Di Indonesia pada tahun 2024 menjelaskan tentang kajian hukum terhadap *hacking* (Damayanti & Prastyanti, 2024). Dari 2 (dua) penelitian yang dilakukan bahwa tidak ada yang membahas terkait dengan cracker yang mengkhusus terhadap game, padahal pada masa kini perlu adanya penelitian terhdap hal tersebut untuk melindungi hak-hak dari *developer* dan *user* dari industri game tersebut.

Dengan memahami pertanggungjawaban pidana, diharapkan dapat ditemukan solusi atau rekomendasi bagi peningkatan kebijakan hukum yang lebih jelas, komprehensif, dan sesuai dengan perkembangan teknologi digital saat ini. Dalam jangka panjang, penelitian ini diharapkan dapat memberikan kontribusi terhadap perumusan kebijakan yang melindungi data pribadi pemain game, perusahaan, serta membangun ekosistem game yang aman di Indonesia.

METODE PENELITIAN

Metode penelitian yang digunakan dalam pembahasan ini adalah jenis penelitian hukum normatif yang berfokus pada pendekatan perundang-undangan (statute approach) dan pendekatan konseptual (conceptual approach). Pendekatan perundang-undangan digunakan untuk menganalisis regulasi yang berlaku di Indonesia terkait tindak pidana siber, khususnya UU ITE, serta peraturan tambahan terkait perlindungan data pribadi. Sementara itu, pendekatan konseptual digunakan untuk memahami konsep pertanggungjawaban pidana dalam konteks kejahatan siber, khususnya yang melibatkan peretasan (hacking) dan peretasan destruktif (cracking) dalam kasus pencurian data game. Pengumpulan data dilakukan melalui studi literatur, yang mencakup bahan hukum primer, sekunder, dan tersier. Analisis bahan hukum dilakukan secara kualitatif dengan menginterpretasikan aturan hukum yang berlaku untuk menentukan bagaimana penegakan hukum di Indonesia terhadap kasus pencurian data game dapat ditingkatkan.

HASIL DAN PEMBAHASAN

Pengaturan Hukum Pidana di Indonesia terhadap Tindakan Pencurian Data dalam Industri Game yang Dilakukan oleh Hacker dan Cracker

Perkembangan industri game di era digital mendorong pertumbuhan aktivitas daring, di mana berbagai data pengguna, seperti identitas pribadi, informasi pembayaran, dan preferensi bermain, dikumpulkan oleh pengembang game. Data ini bukan hanya memiliki nilai penting bagi pengguna, tetapi juga sangat berharga bagi para pelaku kejahatan siber seperti hacker dan cracker, yang memanfaatkan data tersebut untuk kepentingan pribadi atau dijual di pasar gelap. Di Indonesia, pencurian data dalam industri game ini menjadi perhatian serius karena kasus-kasus peretasan yang merugikan pengguna maupun perusahaan game semakin sering terjadi (Mudjiyanto & Roring, 2024). Fenomena ini menimbulkan kebutuhan akan peraturan hukum yang tegas, khususnya yang terkait dengan perlindungan data pribadi dan sanksi bagi pelaku kejahatan siber.

Indonesia memiliki berbagai regulasi yang mengatur tindak pidana siber, di antaranya adalah Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) yang kemudian diperbarui dengan Undang-Undang Nomor 19 Tahun 2016 dan diperbaharui kembali dengan Undang-Undang Nomor 1 Tahun 2024 (Mangode, 2023). UU ITE ini merupakan landasan utama untuk

penanganan masalah hukum yang muncul akibat penggunaan teknologi informasi, termasuk di dalamnya pencurian data yang dilakukan oleh hacker dan cracker. Salah satu aspek penting dari UU ITE adalah pengaturan mengenai akses ilegal ke dalam sistem elektronik (Ramadhani, 2023). Pasal 30 UU ITE dengan tegas menyatakan bahwa setiap orang dilarang melakukan akses ke dalam sistem elektronik milik orang lain tanpa izin, serta tindakan manipulasi terhadap data yang ada di dalam sistem tersebut. Dalam hal ini, tindakan hacker dan cracker yang mencuri data pengguna game dan merusak sistem permainan dapat dikenakan sanksi berdasarkan ketentuan tersebut. Pencurian data pribadi yang dilakukan oleh hacker dapat dianggap sebagai pelanggaran terhadap pasal-pasal ini, karena ia mengakses sistem tanpa izin dan mengambil data secara ilegal.

Selain itu, Pasal 32 UU ITE mengatur larangan untuk menyebarkan informasi elektronik yang tidak sah, yang dapat mencakup penyebaran data pribadi pengguna yang telah dicuri. Dalam konteks industri game, ini berarti bahwa hacker yang berhasil mendapatkan data pengguna seperti nama, alamat email, atau bahkan data pembayaran, dan kemudian menjualnya atau menyebarkannya kepada pihak ketiga, dapat dikenakan hukuman sesuai dengan pasal ini. Peraturan ini sudah mencakup beberapa aspek dasar dalam mengatur tindak pidana terkait pencurian data, namun banyak pihak yang menilai bahwa pengaturan ini belum sepenuhnya memadai untuk menanggulangi kejahatan yang lebih kompleks yang terjadi dalam ranah siber, terutama di industri game.

Namun, meskipun UU ITE telah memberikan dasar hukum yang cukup kuat untuk mengatasi tindak pidana seperti pencurian data, pengaturannya dirasa masih bersifat umum dan belum spesifik terhadap sektor tertentu seperti industri game. Misalnya, meskipun ada pengaturan mengenai perlindungan data pribadi, UU ITE tidak mengatur secara rinci tentang kewajiban penyelenggara sistem elektronik, seperti perusahaan game, dalam hal pengelolaan dan perlindungan data pemain (FAUZAN, n.d.). Dengan demikian, banyak pengembang game yang belum sepenuhnya menyadari atau menerapkan prinsip-prinsip keamanan data yang optimal, yang pada akhirnya membuka peluang bagi cracker untuk mengeksploitasi kelemahan sistem mereka.

Dalam hal ini, Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PSTE) menjadi salah satu regulasi pendukung yang cukup relevan. Peraturan ini mengharuskan penyelenggara sistem elektronik, yang juga mencakup penyedia layanan game, untuk memiliki sistem perlindungan data yang memadai agar dapat mencegah terjadinya kebocoran atau pencurian data. Pasal 11 dalam PP 71/2019 mengharuskan para penyelenggara untuk melakukan pengamanan sistem elektronik, yang meliputi langkah-langkah preventif seperti enkripsi data dan penggunaan protokol keamanan lainnya. Di sisi lain, meskipun peraturan ini memberikan pedoman teknis bagi perusahaan game dalam menjaga data pengguna, implementasi peraturan ini masih terbatas pada pihak penyelenggara sistem, dan belum mengatur dengan rinci mengenai sanksi bagi individu atau pihak luar yang berusaha mengakses atau mencuri data secara ilegal.

Selain itu, Peraturan Menteri Komunikasi dan Informatika No. 20 Tahun 2016 yang mengatur tentang Perlindungan Data Pribadi dalam Sistem Elektronik juga menjadi pedoman penting. Peraturan ini lebih mengarah pada pengaturan kewajiban untuk melindungi data pribadi pengguna yang disimpan dalam sistem elektronik, yang termasuk dalam kategori data pengguna game. Namun, tantangan yang dihadapi di Indonesia adalah perbedaan kapasitas dan kesadaran antara perusahaan-perusahaan besar dengan penyedia layanan game kecil dalam hal penerapan

regulasi perlindungan data. Banyak perusahaan game asing yang beroperasi di Indonesia lebih memilih mengikuti regulasi di negara asal mereka, yang seringkali memiliki standar perlindungan data yang lebih longgar dibandingkan dengan yang ditetapkan di Indonesia. Hal ini menambah kompleksitas dalam penegakan hukum, karena ketidaksesuaian antara praktik yang berlaku di Indonesia dengan regulasi internasional yang diterapkan oleh penyelenggara layanan game global.

Dengan demikian, meskipun sudah ada berbagai regulasi yang mengatur terkait perlindungan data pribadi dalam dunia digital, tantangan utama yang dihadapi oleh Indonesia dalam mengatur pencurian data di industri game adalah ketidaklengkapan regulasi yang bersifat spesifik untuk sektor ini. Beberapa pasal dalam UU ITE dan peraturan terkait memberikan dasar yang cukup untuk menangani pencurian data yang dilakukan oleh hacker dan cracker, tetapi regulasi yang ada masih perlu diperbaharui atau diperkuat untuk menghadapi kejahatan siber yang semakin kompleks dan terus berkembang. Upaya untuk memperbaharui hukum pidana di Indonesia agar lebih spesifik dalam menangani kejahatan siber, terutama yang terkait dengan industri game, akan sangat penting agar dapat memberikan perlindungan yang lebih efektif bagi para pemain game serta mengurangi kerugian yang dialami oleh perusahaan penyedia layanan game.

Meski sudah memiliki dasar hukum, penerapan aturan ini dalam konteks industri game tidak selalu mudah. Hacker dan cracker sering kali menggunakan teknik canggih yang menyulitkan pelacakan, dan tidak jarang mereka beroperasi lintas negara, yang menambah kompleksitas penegakan hukum (Habibi & Liviani, 2020). Selain itu, banyak perusahaan game yang beroperasi di Indonesia adalah perusahaan internasional yang tidak sepenuhnya terikat pada peraturan dalam negeri. Keadaan ini menciptakan tantangan tersendiri dalam menegakkan hukum pidana terhadap tindakan pencurian data dalam game. Sebagai contoh, ketika data pengguna game Indonesia dicuri dari server yang berada di luar negeri, diperlukan kerja sama internasional yang solid untuk bisa menangkap pelaku (Lestyaningrum et al., 2022).

Sebagai upaya memahami apakah pengaturan hukum pidana di Indonesia sudah memadai, perlu juga dilakukan perbandingan dengan negara lain yang lebih berpengalaman dalam menangani kejahatan siber di industri game. Beberapa negara, seperti Amerika Serikat dan Uni Eropa, telah mengembangkan undang-undang siber yang lebih spesifik dan ketat, termasuk dalam aspek perlindungan data pribadi. General Data Protection Regulation (GDPR) di Uni Eropa, misalnya, memberikan perlindungan menyeluruh bagi data pribadi pengguna, termasuk sanksi yang ketat bagi pelanggaran data (Wempy, Efendi, & Putra, 2024). Dengan membandingkan kebijakan ini, dapat diperoleh gambaran mengenai langkah-langkah yang perlu diterapkan di Indonesia untuk meningkatkan efektivitas pengaturan hukum dalam menangani kejahatan pencurian data game oleh hacker dan cracker.

Menghadapi tantangan yang terus berkembang di dunia siber, khususnya dalam industri game, pemerintah Indonesia perlu mempertimbangkan penguatan hukum pidana yang lebih spesifik untuk kejahatan siber. Revisi terhadap UU ITE dan peraturan terkait dapat mencakup aspek-aspek khusus seperti kejahatan siber dalam game, perlindungan data pribadi, dan sanksi lebih tegas bagi hacker dan cracker. Selain itu, regulasi yang baru perlu mempertimbangkan aspek keamanan digital yang sesuai dengan perkembangan teknologi modern, serta mencakup perlindungan yang memadai untuk pengguna dari berbagai ancaman siber. Langkah ini diharapkan dapat memberikan kepastian hukum yang lebih kuat bagi pelaku industri game dan masyarakat pengguna.

Pencurian data dalam industri game memiliki dampak yang luas, tidak hanya bagi perusahaan penyedia layanan, tetapi juga bagi masyarakat sebagai pengguna. Data pribadi yang bocor dapat disalahgunakan untuk berbagai kejahatan siber lainnya, seperti penipuan atau bahkan pencurian identitas, yang merugikan pengguna secara signifikan (Hasibuan & Putri, 2024). Selain itu, perusahaan game yang gagal melindungi data pengguna akan kehilangan reputasi dan mengalami kerugian ekonomi yang besar. Dalam konteks ini, pengaturan hukum pidana yang kuat sangat penting untuk memastikan perlindungan yang memadai bagi semua pihak, serta menjaga ekosistem digital yang sehat dan aman bagi industri game di Indonesia.

Berdasarkan analisis yang telah dilakukan, dapat disimpulkan bahwa pengaturan hukum pidana di Indonesia terkait pencurian data dalam industri game oleh hacker dan cracker masih memiliki sejumlah kelemahan, baik dari segi kejelasan maupun implementasi. Meskipun Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) dan Peraturan Pemerintah Nomor 71 Tahun 2019 memberikan dasar hukum yang penting untuk menangani kejahatan siber, peraturan-peraturan tersebut masih terlalu umum dan belum secara spesifik mengatur tentang perlindungan data dalam konteks industri game. Hal ini mengakibatkan kerentanannya terhadap perkembangan teknologi dan teknik yang digunakan oleh para hacker dan cracker. Oleh karena itu, perbaikan regulasi yang ada sangat diperlukan untuk menjamin perlindungan data pengguna game secara lebih efektif dan memadai.

Penulis memberikan beberapa rekomendasi yang dapat diajukan, rekomendasi pertama yang dapat diajukan adalah penguatan regulasi hukum pidana dengan membentuk peraturan khusus mengenai kejahatan siber di sektor industri game. Dalam peraturan ini, diharapkan dapat diatur secara lebih mendetail terkait kewajiban perusahaan game dalam menjaga data pribadi pengguna, serta sanksi yang jelas dan tegas bagi para pelaku kejahatan siber yang terlibat dalam pencurian dan penyebaran data ilegal. Sebagai contoh, peraturan tersebut dapat mencakup kewajiban penyedia layanan game untuk secara rutin melakukan audit keamanan terhadap sistem mereka, serta memberikan pelatihan mengenai pentingnya perlindungan data pribadi kepada karyawan yang terlibat dalam pengelolaan data pengguna. Selain itu, perlu adanya mekanisme pemantauan yang lebih intensif terhadap aktivitas siber dalam platform game, sehingga potensi ancaman dapat dikenali lebih dini dan ditangani sebelum berkembang menjadi serangan besar yang dapat merugikan banyak pihak.

Rekomendasi kedua adalah memperkuat kerja sama antara pemerintah, sektor swasta, dan komunitas internasional dalam rangka menghadapi kejahatan siber lintas negara. Kejahatan seperti pencurian data game sering kali melibatkan pelaku yang beroperasi di luar wilayah Indonesia, yang membuat penegakan hukum menjadi lebih kompleks. Oleh karena itu, Indonesia perlu mengintensifkan kerja sama internasional dalam hal perjanjian ekstradisi dan kerja sama hukum antarnegara dalam menghadapi pelaku cybercrime. Indonesia juga perlu memperkuat peran serta aktif dalam organisasi internasional seperti Interpol atau EUROPOL yang dapat memberikan dukungan dalam investigasi dan penuntutan terhadap hacker dan cracker yang berada di luar yurisdiksi Indonesia. Dengan demikian, tindakan pencurian data yang terjadi dalam industri game dapat diatasi secara lebih efektif, meskipun pelaku beroperasi di luar negeri.

Selanjutnya, perlu ada penambahan pengetahuan dan kesadaran hukum bagi para pengembang game, terutama bagi perusahaan kecil dan menengah yang mungkin belum sepenuhnya memahami dampak dari kebocoran data dan bagaimana cara melindunginya. Pendidikan dan pelatihan tentang perlindungan

ISSN No. 1978-3787
Open Journal Systems

data pribadi bagi penyedia layanan game harus lebih diutamakan. Pemerintah dan asosiasi industri game di Indonesia bisa bekerja sama untuk menyelenggarakan program-program pelatihan terkait keamanan data dan kejahatan siber. Selain itu, perusahaan game harus diberikan insentif, seperti potongan pajak atau pengurangan biaya operasional, jika mereka menerapkan standar keamanan tinggi dalam pengelolaan data pengguna. Pendekatan ini akan mendorong industri game untuk lebih proaktif dalam mencegah kebocoran data, bukan hanya mengandalkan penegakan hukum setelah kejadian pencurian.

Rekomendasi ketiga adalah pembentukan aturan yang lebih tegas terkait sanksi bagi pelaku kejahatan siber, yang meliputi pencurian data dalam industri game. Sanksi pidana yang lebih berat bagi hacker dan cracker yang terlibat dalam pencurian data dapat memberikan efek jera yang lebih kuat. Hal ini tidak hanya penting untuk mengurangi angka kejahatan, tetapi juga untuk menunjukkan keseriusan negara dalam melindungi data pribadi masyarakat. Selain itu, penegakan hukum yang cepat dan tepat dapat meningkatkan kepercayaan publik terhadap sistem hukum Indonesia, serta mendorong perusahaan game untuk lebih berhati-hati dalam mengelola data pengguna mereka.

Rekomendasi terakhir adalah untuk melakukan pendekatan berbasis pencegahan yang melibatkan pengguna game itu sendiri. Mengedukasi masyarakat mengenai pentingnya perlindungan data pribadi melalui kampanye kesadaran keamanan siber bisa membantu mengurangi risiko pencurian data. Pengguna harus diberikan pemahaman tentang pentingnya menjaga kerahasiaan informasi pribadi mereka, seperti menggunakan kata sandi yang kuat dan menghindari berbagi informasi pribadi secara sembarangan di platform game. Dengan pendekatan ini, diharapkan akan tercipta ekosistem yang lebih aman dan terjaga baik dari sisi pengguna, penyedia layanan, dan pemerintah.

Secara keseluruhan, rekomendasi yang penulis buat dirancang untuk memberikan dampak jangka panjang yang positif dalam membangun ekosistem hukum yang lebih efektif untuk menghadapi kejahatan siber, khususnya di industri game. Dengan penerapan peraturan yang lebih komprehensif dan penegakan hukum yang lebih tegas, diharapkan Indonesia dapat menjadi negara yang lebih siap menghadapi tantangan dunia maya yang semakin kompleks dan memastikan perlindungan data pribadi bagi semua pihak yang terlibat. Peningkatan kualitas dan kapasitas hukum di sektor ini tidak hanya akan melindungi individu, tetapi juga mendorong pertumbuhan industri game yang sehat, inovatif, dan aman di masa depan.

Penegakan Hukum Pidana terhadap Hacker dan Cracker dalam Pencurian Data Game di Indonesia

Penegakan hukum pidana terhadap hacker dan cracker dalam pencurian data game di Indonesia menghadapi tantangan yang cukup besar, baik dari sisi regulasi maupun implementasi di lapangan. Pencurian data game adalah salah satu jenis kejahatan siber yang melibatkan pelaku yang menggunakan berbagai teknik peretasan untuk mencuri informasi penting yang ada dalam sistem permainan (Widianingrum, 2024). Data yang dicuri dapat berupa data pribadi pengguna, informasi transaksi, hingga data internal yang sangat penting bagi perusahaan pengembang game. Hacker dan cracker sering kali memanfaatkan celah dalam sistem keamanan untuk meretas dan mengakses data tanpa izin (Sari, 2014). Hal ini membuat industri game, yang sering kali beroperasi secara daring, menjadi sangat rentan terhadap ancaman kejahatan siber. Penegakan hukum pidana yang efektif dalam konteks ini menjadi sangat penting, mengingat dampak yang dapat ditimbulkan, baik bagi individu yang datanya dicuri maupun bagi perusahaan yang mengalami kerugian besar akibat kebocoran data. Oleh karena itu, upaya

penegakan hukum terhadap kejahatan ini harus mengedepankan pendekatan yang komprehensif, melibatkan berbagai pihak, dan mengadaptasi hukum yang ada agar bisa mengimbangi perkembangan teknologi yang begitu cepat (Andriyani et al., 2023).

Salah satu regulasi yang menjadi dasar penegakan hukum terhadap hacker dan cracker dalam pencurian data game di Indonesia adalah Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), yang telah diperbarui dengan Undang-Undang No. 19 Tahun 2016 dan diperbaharui kembali dengan Undang-Undang Nomor 1 Tahun 2024. UU ITE ini memberikan dasar hukum yang jelas untuk mengatasi berbagai bentuk kejahatan siber, termasuk pencurian data melalui akses ilegal ke sistem informasi (Luthiya, Irawan, & Yulia, 2021). Pasal 30 UU ITE mengatur tentang larangan akses ilegal terhadap sistem elektronik atau informasi yang dilindungi, sementara Pasal 32 UU ITE melarang penyebaran informasi elektronik yang merugikan orang lain. Dengan menggunakan dasar hukum ini, aparat penegak hukum, seperti kepolisian, dapat melakukan penyelidikan dan penyidikan terhadap kejahatan yang dilakukan oleh hacker dan cracker. Namun, meskipun UU ITE telah memberikan landasan hukum yang cukup kuat, implementasinya masih menghadapi sejumlah tantangan. Salah satu tantangan terbesar adalah kompleksitas identifikasi hacker dan cracker sering kali beroperasi secara anonim, menggunakan berbagai teknik untuk menyembunyikan jejak digital mereka, dan beroperasi di luar batas wilayah Indonesia (Dr. Muhammad Ridha Albaar, 2021). Dalam banyak kasus, pelaku kejahatan siber dapat bersembunyi di balik jaringan yang terdistribusi di berbagai negara, sehingga membuatnya sulit untuk ditangkap oleh aparat penegak hukum Indonesia. Selain itu, hacker sering kali menggunakan teknologi seperti VPN atau TOR untuk menyamarkan identitas dan lokasi mereka, yang membuat proses identifikasi dan penangkapan menjadi semakin rumit.

Sebagai bagian dari proses penegakan hukum, penyelidikan dan penyidikan terhadap kasus pencurian data game memerlukan kemampuan teknis yang tinggi dari aparat penegak hukum. Bareskrim Polri memiliki kewenangan untuk menangani kasus-kasus kejahatan siber, termasuk pencurian data melalui peretasan internet, khususnya pada sistem game (Azahra, Simanjuntak, Tarigan, & Hosnah, 2024). Namun, proses penyidikan sering kali memerlukan bukti yang bersifat digital, seperti log server, rekaman aktivitas jaringan, dan jejak digital lainnya yang dapat digunakan untuk melacak pelaku. Pengumpulan bukti-bukti digital ini memerlukan keahlian khusus dalam forensik digital (RACHMIE, 2020). Tanpa keahlian yang memadai, aparat penegak hukum akan kesulitan dalam mengidentifikasi dan mengumpulkan bukti yang dapat diterima di pengadilan. Oleh karena itu, peningkatan kapasitas dan kemampuan aparat penegak hukum dalam bidang teknologi informasi dan forensik digital menjadi hal yang sangat penting. Selain itu, pengembangan infrastruktur yang mendukung proses penyidikan, seperti peralatan forensik digital yang canggih dan pusat data yang aman, juga diperlukan agar proses investigasi dapat berjalan dengan lebih cepat dan efektif. Meskipun demikian, tantangan terbesar dalam penegakan hukum terhadap kejahatan siber adalah adanya hambatan geografis dan yurisdiksi. Kejahatan siber sering kali melibatkan pelaku yang berada di luar negeri, dan proses ekstradisi atau kerja sama internasional sering kali menjadi rumit. Negara yang menjadi tempat tinggal pelaku mungkin tidak memiliki peraturan yang sama atau mungkin tidak memiliki kepentingan untuk menyerahkan tersangka kepada Indonesia. Dalam hal ini, kerja sama internasional menjadi kunci utama dalam menangani kejahatan siber yang berskala lintas negara.

Selain hambatan teknis dan yurisdiksi, terdapat pula tantangan dalam hal penegakan hukum yang tepat sasaran. Salah satu masalah yang sering dihadapi dalam kasus pencurian data game adalah penegakan hukum yang tidak konsisten. Dalam beberapa kasus, sanksi yang dijatuhkan terhadap pelaku hacker dan cracker dianggap tidak cukup berat untuk memberikan efek jera (Efendi, 2020). Padahal, pencurian data pribadi dan informasi sensitif yang dilakukan oleh hacker dapat menyebabkan kerugian yang sangat besar bagi individu maupun perusahaan. Kerugian finansial akibat pencurian data bisa mencapai miliaran rupiah, belum lagi kerugian reputasi yang dialami oleh perusahaan game (Idik Saeful Bahri, 2023). Oleh karena itu, perlu ada upaya untuk memperberat sanksi terhadap pelaku kejahatan siber yang terbukti bersalah. Hal ini juga menjadi tantangan bagi sistem peradilan Indonesia yang harus memastikan bahwa kasus kejahatan siber ditangani dengan serius dan proporsional. Peningkatan pelatihan untuk hakim, jaksa, dan pengacara dalam hal keahlian digital dan teknologi juga menjadi langkah penting untuk memastikan bahwa mereka dapat memahami dan memproses kasus kejahatan siber dengan baik. Dalam hal ini, pendidikan dan pelatihan khusus dalam bidang teknologi informasi dan hukum siber harus dimasukkan sebagai bagian dari kurikulum bagi para aparat penegak hukum.

Seiring dengan perkembangan teknologi yang terus berkembang pesat, tantangan penegakan hukum terhadap pencurian data game semakin besar (Hapsari & Pambayun, 2023). Dalam menghadapi tantangan ini, selain peran aktif aparat penegak hukum, pihak swasta dan industri game juga harus berperan aktif dalam melindungi data pengguna mereka. Pengembang game harus memastikan bahwa sistem yang mereka bangun aman dan tahan terhadap serangan hacker (Paryati, 2008). Mereka harus berinvestasi dalam keamanan siber yang lebih baik dan melakukan audit secara berkala terhadap sistem mereka untuk memastikan bahwa tidak ada celah yang dapat dimanfaatkan oleh cracker. Selain itu, perusahaan game harus mengedukasi pengguna mereka tentang pentingnya keamanan data pribadi dan memberikan instruksi yang jelas mengenai cara melindungi informasi pribadi mereka dalam game. Upaya preventif ini menjadi bagian dari langkah untuk meminimalkan potensi terjadinya pencurian data yang merugikan kedua belah pihak, baik pengguna maupun perusahaan.

Dalam rangka meningkatkan efektivitas penegakan hukum terhadap kejahatan siber, Indonesia juga harus terus memperbarui regulasinya. Salah satu langkah yang dapat dilakukan adalah dengan memperkenalkan Undang-Undang Perlindungan Data Pribadi yang lebih komprehensif, yang tidak hanya mengatur tentang hak individu atas data pribadi, tetapi juga memberikan kewajiban kepada penyelenggara layanan digital untuk melindungi data yang mereka kelola (Anggen Suari & Sarjana, 2023). Regulasi ini juga harus mencakup ketentuan yang memperberat sanksi bagi mereka yang terbukti melakukan pencurian data, serta memberikan kejelasan mengenai prosedur penegakan hukum bagi kasus kejahatan siber yang melibatkan data pribadi. Pemerintah harus memastikan bahwa regulasi yang ada tidak hanya sesuai dengan perkembangan teknologi tetapi juga dapat diterapkan secara efektif di lapangan. Penegakan hukum yang jelas dan konsisten akan memberikan dampak positif dalam mengurangi kasus pencurian data dan meningkatkan kepercayaan masyarakat terhadap industri game dan platform digital lainnya (Rauf, Rahman, & Razak, 2024).

Penegakan hukum pidana terhadap hacker dan cracker yang melakukan pencurian data game di Indonesia memerlukan berbagai upaya yang komprehensif, mulai dari perbaikan regulasi, peningkatan kapasitas aparat penegak hukum, hingga peningkatan kerjasama internasional (Maskun, 2022). Diperlukan sinergi antara pemerintah, industri game, dan

masyarakat untuk menciptakan ekosistem digital yang lebih aman, transparan, dan bertanggung jawab (Sudibyo, 2022). Hanya dengan demikian, kejahatan siber yang merugikan banyak pihak, termasuk pencurian data game, dapat ditekan dan diatasi secara efektif di masa depan.

PENUTUP

Kesimpulan

Kesimpulan dari pembahasan mengenai penegakan hukum terhadap hacker dan cracker dalam pencurian data game di Indonesia menekankan bahwa tantangan dalam mengatasi kejahatan siber ini bersifat kompleks, mencakup aspek regulasi, kemampuan teknis, serta hambatan yurisdiksi. UU ITE sebagai landasan hukum sudah memberikan dasar yang cukup untuk menjerat pelaku, tetapi implementasi di lapangan masih membutuhkan peningkatan dalam hal kemampuan forensik digital dan penegakan hukum yang konsisten. Selain itu, keberhasilan penanganan kasus kejahatan siber memerlukan sinergi antara aparat penegak hukum, industri game, dan pengguna. Aparat penegak hukum perlu terus meningkatkan kapasitas dalam penyelidikan kejahatan digital, sementara industri game harus proaktif dalam meningkatkan sistem keamanan dan melindungi data pengguna. Di sisi lain, pengguna juga perlu mendapatkan edukasi tentang keamanan data pribadi. Kolaborasi antara berbagai pihak dan penerapan regulasi yang kuat, seperti perlindungan data pribadi yang komprehensif, sangat penting untuk menciptakan lingkungan digital yang aman dan untuk membangun kepercayaan masyarakat terhadap platform game online. Dengan komitmen bersama dan peningkatan berkelanjutan dalam regulasi dan penegakan hukum, diharapkan bahwa kasus pencurian data game dapat ditekan, sehingga tercipta ekosistem digital yang lebih aman dan terlindungi dari ancaman kejahatan siber di masa depan.

Saran yang tepat berdasarkan pembahasan di atas adalah terkait dengan penanganan kejahatan siber memerlukan pelatihan forensik digital bagi aparat penegak hukum, penguatan regulasi perlindungan data pribadi, serta penerapan teknologi keamanan oleh industri game untuk melindungi data pengguna. Edukasi kepada masyarakat juga penting untuk meningkatkan kesadaran menjaga keamanan data pribadi. Sinergi pemerintah, aparat, industri, dan masyarakat menjadi kunci menciptakan ekosistem digital yang aman. Implikasinya, regulasi yang adaptif, kemampuan teknis aparat, dan kepercayaan pengguna terhadap platform digital akan meningkat, sehingga kejahatan siber, khususnya pencurian data game, dapat diminimalkan.

DAFTAR PUSTAKA

[1] R. Andriyanty, M. N. Rafiq, and T. Rambey, “Analisis strategi ekonomi kreatif KZ Studio berbasis gambar digital menuju niche market,” *Mediastima*, vol. 29, no. 1, pp. 20–37, 2023, [Online]. Available: http://ejournal-ibik57.ac.id/index.php/mediastima/article/view/696%0Ahttps://ejournal-ibik57.ac.id/index.php/mediastima/article/download/696/325

[2] A. R. Widianingrum, “Analisis Implementasi Kebijakan Hukum Terhadap Penanganan Kejahatan Siber Di Era Digital,” *J. Iuris Sci.*, vol. 2, no. 2, pp. 90–102, 2024, doi: 10.62263/jis.v2i2.40.

[3] D. Ali, M. & Nurhayati, “Perlindungan Data Pribadi dalam Era Digital di Indonesia: Tantangan dan Solusi.,” *J. Huk. Pembang.*, vol. 50, no. 1, pp. 25–39, 2020.

[4] A. Wibowo Noor Fikri *et al.*, “Analisis Keamanan Sistem Operasi dalam Menghadapi Ancaman Phishing dalam Layanan Online Banking,” *J. Ilmu Multidisplin*, vol. 2, no. 1, pp. 84–91, 2023, doi: 10.38035/jim.v2i1.228.

[5] A. N. Ramadhanti, T. A. Tias, E. D. Lestari, and A. U. Hosnah, "Cara Operasi Kejahatan Phising di Ranah Siber yang Diatur OlehHukum Positif Indonesia," *J. Pendidik. Tambusai*, vol. 8, no. 1, pp. 1299–1305, 2024.

[6] damar chikawati hera, "Tinjauan Hukum Islam Dan Hukum Positif Transaksi Jasa Dan Jual Beli Game Online Audition Ayodance," *Universitas Islam Negeri Syarif Hidayatullah*. Fakultas Syariah dan Hukum UIN Syarif HIdayatullah Jakarta, pp. 24–27, 2021.

[7] Suci, *Etika Profesi Teknologi Informasi. (Buku Ajar)*. Feri Sulianta, 2016.

[8] I. K. Putri, J. Oktaria, O. Ardinata, A. Yanuar, and F. D. Althafi, "Viralitas Dan Hukum: Dampak Media Sosial Terhadap Penegakan Hukum Dalam Kasus Pembunuhan Vina Dan Eky Di Cirebon," *J. Terekam Jejak*, vol. 2, no. 1, pp. 1–19, 2024.

[9] P. A. Yusuf, "TANGGUNG JAWAB KEAMANAN DATA DIGITAL OLEH PENYELENGGARA SISTEM ELEKTRONIK," *LEX Priv.*, vol. 13, no. 5, 2024.

[10] Y. P. ADITYA, "Perlindungan Hukum Bagi Korban Perdagangan Data Pribadi Sebagai Objek Transaksi Non-Fungible Token pada Platform Opensea".

[11] I. Sari, "Mengenal Hacking Sebagai Salah Satu Kejahatan Di Dunia Maya," *J. Sist. Inf. Univ. Suryadarma*, vol. 10, no. 2, pp. 169–186, 2014, doi: 10.35968/jsi.v10i2.1086.

[12] A. Damayanti and R. A. Prastyanti, "Kajian Hukum Dan Regulasi Terkait Serangan Hacking Pada Platform Digital Di Indonesia," *Multidiscip. Indones. Cent. J.*, vol. 1, no. 2, pp. 1043–1054, 2024, doi: 10.62567/micjo.v1i2.117.

[13] B. Mudjiyanto and F. P. Roring, "Tendensi Politik Kejahatan Dunia Maya," *JIKA (Jurnal Ilmu Komun. Andalan)*, vol. 7, no. 2, pp. 26–51, 2024.

[14] Y. R. Mangode, "Tindak Pidana Pencemaran Nama Baik Melalui Media Sosial Ditinjau Berdasarkan Uu No. 19 Tahun 2016 Tentang Perubahan Atas Uu No. 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik," *J. Lex Adm.*, vol. 12, no. 5, pp. 1–11, 2023.

[15] F. Ramadhani, "Dinamika UU ITE Sebagai Hukum Positif di Indonesia Guna Meminimalisir Kejahatan Siber," *Kult. J. Ilmu Hukum, Sos. dan Hum.*, vol. 1, no. 1, pp. 89–97, 2023.

[16] M. R. FAUZAN, "PERLINDUNGAN HUKUM PELAKU TOP-UP DIAMOND PADA MOBILE LEGEND BANG BANG MELALUI PERORANGAN DI INDONESIA." Fakultas Syariah dan Hukum UIN Syarif Hidayatullah Jakarta.

[17] M. R. Habibi and I. Liviani, "Kejahatan Teknologi Informasi (Cyber Crime) dan Penanggulangannya dalam Sistem Hukum Indonesia," *Al-Qanun J. Pemikir. dan Pembaharuan Huk. Islam*, vol. 23, no. 2, pp. 400–426, 2020, doi: 10.15642/alqanun.2020.23.2.400-426.

[18] I. K. M. Lestyaningrum, A. Trisiana, D. A. Safitri, Supriyanti, A. Y. Pratama, and T. P. Wahana, *Pendidikan Global Berbasis Teknologi Digital di Era Milenial*. Unisri Press, 2022. [Online]. Available: https://www.google.co.id/books/edition/Pendidikan_Global_Berbasis_Teknologi_Dig/xeqbEAAAQBAJ?hl=en&gbpv=1

[19] A. Wempy, Z. Efendi, and M. D. Putra, "Regulation Of Cybersecurity Technology As An Effort To Address Security Threats To Privacy In The Digital Era," *J. Huk. Sehasen*, vol. 10, no. 2, pp. 509–516, 2024.

[20] E. S. Hasibuan and E. A. Putri, "Perlindungan Keamanan Atas Data Pribadi Di Dunia Maya," *J. Huk. Sasana*, vol. 10, no. 1, pp. 70–83, 2024, doi: 10.31599/sasana.v10i1.2134.

[21] W. Andriyani, R. Sacipto, D. Susanto, C. Vidiati, R. Kurniawan, and R. A. G. Nugrahani, *Technology, Law And Society*. Tohar Media, 2023.

[22] A. N. Luthiya, B. Irawan, and R. Yulia, "Kebijakan Hukum Pidana Terhadap Pengaturan Pencurian Data Pribadi Sebagai Penyalahgunaan Teknologi Komunikasi Dan Informasi," *J. Huk. Pidana Dan Kriminologi*, vol. 2, no. 2, pp. 14–29, 2021.

[23] S. K. M. K. Dr. Muhammad Ridha Albaar, *Etika Profesi Informatika*, vol. 1. uwais inspirasi indonesia, 2021.

[24] A. P. Azahra, A. C. A. Simanjuntak, E. S. Tarigan, and A. U. Hosnah, "Analisa Kepada Para Oknum Yang Tidak Bijak Dalam Menggunakan Media Sosial Atau Cyberspace," *Civilia J. Kaji. Huk. dan Pendidik. Kewarganegaraan*, vol. 3, no. 1, pp. 34–47, 2024, [Online]. Available: http://jurnal.anfa.co.id

[25] S. RACHMIE, "Peranan Ilmu Digital Forensik Terhadap Penyidikan Kasus Peretasan Website," *Litigasi*, vol. 21, no. 21, pp. 104–127, 2020, doi: 10.23969/litigasi.v21i1.2388.

[26] F. Y. Efendi, "Analisis Tindak Pidana Cracking Menurut Hukum," *Skripsi, Univ. Islam Negeri Walisongo*, 2020.

[27] Idik Saeful Bahri, *Cyber Crime dalam Sorotan Hukum Pidana (Edisi 2023)*, vol. 159. Bahasa Rakyat, 2023.

[28] R. D. Hapsari and K. G. Pambayun, "ANCAMAN CYBERCRIME DI INDONESIA: Sebuah Tinjauan Pustaka Sistematis," *J. Konstituen*, vol. 5, no. 1, pp. 1–17, 2023, doi: 10.33701/jk.v5i1.3208.

[29] Paryati, "Keamanan Sistem Informasi," *Semin. Nas. Inform. 2008 (semnasIF 2008) UPN "Veteran" Yogyakarta, 24 Mei 2008*, vol. 2008, no. semnasIF, pp. 379–386, 2008.

[30] K. R. Anggen Suari and I. M. Sarjana, "Menjaga Privasi di Era Digital: Perlindungan Data Pribadi di Indonesia," *J. Anal. Huk.*, vol. 6, no. 1, pp. 132–142, 2023, doi: 10.38043/jah.v6i1.4484.

[31] A. Rauf, S. Rahman, and A. Razak, *Penegakan Hukum Terhadap Pelaku Tindak Pidana Penipuan Melalui Media Elektronik*. Penerbit NEM, 2024. [Online]. Available: http://www.pasca-umi.ac.id/index.php/jlp/article/view/1624%0Ahttp://www.pasca-umi.ac.id/index.php/jlp/article/download/1624/1898

[32] Maskun, *Buku Kejahatan Siber (Cyber Crime): Suatu Pengantar*. Prenada Media, 2022. [Online]. Available: https://books.google.com/books?hl=en&lr=&id=b1S6EAAAQBAJ&oi=fnd&pg=PA88&dq=kejahatan+hukum+cyber+crime+cyber+law&ots=qbRtkmJsQA&sig=LGIFu12sry9awdQKXyfwjOnnib4

[33] A. Sudibyo, *Dialektika Digital*. Kepustakaan Populer Gramedia, 2022. [Online]. Available: https://books.google.com/books?hl=en%5C&lr=%5C&id=BcBmEAAAQBAJ%5C&oi=fnd%5C&pg=PP1%5C&dq=kelayakan+penggunaan+sistem+artificial+intelligence+terhadap+efektivitas+sistem+informasi+manajemen%5C&ots=Jmb8njgnGV%5C&sig=GWAhATdGzGeFQta-bz6aYVxaBxI

ISSN No. 1978-3787
Open Journal Systems

HALAMAN INI SENGAJA DIKOSONGKAN