JULIA Jurnal Litigasi Amsir

Volume 12
Nomor 2
Februari 2025

Kejahatan Berbasis Identitas Digital: Menggagas Kebijakan Kriminal untuk Dunia Metaverse

Zul Khaidir Kadir[1]
[1]Fakultas Hukum Universitas Muslim Indonesia
Email: zulkhaidirkadir@gmail.com[1]

Abstract
This study examines the challenges of criminal policies related to digital identity in the metaverse using a qualitative method with a conceptual approach. Digital identity, which includes personal information, digital assets, and user interaction patterns, is the main foundation of an individual's existence in the metaverse however, the lack of specific regulations indicates weaknesses in current criminal policies. The results of the study show that the metaverse presents new crime risks that have not been fully accommodated by the existing legal system, such as identity theft, avatar counterfeiting, and digital asset fraud. To overcome this, fundamental reforms of criminal policy are needed that include a cross-border collaborative approach, strengthening the regulation of technology platforms, and developing appropriate legal standards. The success of these policies relies heavily on collaboration between governments, technology companies, and civil society.

Keywords : Digital Identity; Criminal Policy; Metaverse
Publish Date : 30 Januari 2025

Pendahuluan

Kemunculan metaverse sebagai lingkungan virtual yang terintegrasi dengan teknologi augmented reality (AR) dan virtual reality (VR) telah memicu perubahan besar dalam berbagai aspek kehidupan manusia, termasuk dinamika sosial, ekonomi, dan hukum.[1] Metaverse menawarkan pengalaman interaktif yang menggabungkan dunia nyata dengan ruang digital, memungkinkan individu untuk berinteraksi, bekerja, belajar, dan melakukan transaksi ekonomi melalui representasi virtual yang disebut identitas digital. Identitas digital tersebut diwujudkan dalam bentuk avatar atau profil personal yang tidak hanya mencerminkan identitas pribadi pengguna tetapi juga memiliki kapasitas untuk menjadi alat ekspresi, kreativitas, dan produktivitas di dunia maya. Namun, kompleksitas teknologi ini juga melahirkan tantangan serius, terutama dalam aspek kriminalitas yang berbasis identitas digital. Perubahan paradigma interaksi yang dihadirkan metaverse telah menciptakan celah baru yang dapat dieksploitasi oleh pelaku kriminal, menimbulkan kebutuhan mendesak untuk merancang kebijakan kriminal yang relevan dan adaptif.

Identitas digital menjadi fondasi utama keberadaan individu di metaverse.[2] Sebagai representasi diri, identitas digital tidak hanya mencakup informasi dasar seperti nama atau data pribadi, tetapi juga melibatkan aset digital, jejak transaksi, serta pola interaksi pengguna di dunia maya. Hal ini membuat identitas digital tidak hanya bernilai secara sosial, tetapi juga memiliki nilai ekonomi yang tinggi. Misalnya dalam transaksi berbasis mata uang kripto atau penjualan aset non-fungible token (NFT), identitas digital menjadi elemen kunci yang memungkinkan pengguna untuk mengklaim kepemilikan dan melakukan transaksi. Namun, sifat digital dari identitas juga

[1]Filipova, I. (2023). Creating the Metaverse: Consequences for Economy, Society, and Law. Journal of Digital Technologies and Law, 1(1): 7-32.

[2]Mitrushchenkova. (2022). Personal Identity in the Metaverse: Challenges and Risks. Kutafin Law Review, 9(4): 793-817.

membuatnya rentan terhadap berbagai bentuk kejahatan, seperti pencurian data, pemalsuan identitas, dan manipulasi avatar. Pelaku kriminal dapat menggunakan teknologi seperti *deepfake* untuk menciptakan representasi virtual yang menyerupai individu tertentu, yang kemudian dimanfaatkan untuk melakukan penipuan, pencemaran nama baik, atau bahkan eksploitasi seksual dalam bentuk digital.

Metaverse juga memperkenalkan dinamika baru dalam pola kejahatan lintas negara. Karena sifatnya yang virtual dan global, tindakan kriminal yang terjadi di metaverse sering kali melibatkan pelaku, korban, dan platform yang berada di berbagai jurisdiksi hukum yang berbeda. Hal ini menciptakan tantangan besar bagi penegakan hukum tradisional, yang umumnya didasarkan pada batasan teritorial dan yurisdiksi yang jelas. Misalnya kasus pencurian aset digital di sebuah platform metaverse mungkin melibatkan pelaku yang berdomisili di satu negara, korban di negara lain, dan server platform yang berada di wilayah hukum yang berbeda lagi. Ketidaksesuaian antara jurisdiksi hukum dimanfaatkan oleh pelaku untuk menghindari penuntutan, menciptakan rasa impunitas yang mendorong meningkatnya kejahatan berbasis identitas digital. Akibatnya penegakan hukum tidak hanya memerlukan reformasi kebijakan yang berbasis pada kebutuhan lokal, tetapi juga kolaborasi internasional untuk menciptakan penanganan yang harmonis dalam menangani kejahatan lintas negara.

Di sisi lain, pengaturan hukum terhadap metaverse juga menimbulkan dilema etis dan normatif yang kompleks. Identitas digital sering dianggap sebagai perpanjangan dari identitas pribadi seseorang, yang berarti bahwa perlindungan terhadap identitas digital harus selaras dengan prinsip hak asasi manusia, termasuk privasi dan kebebasan berekspresi.[3] Namun, banyak platform metaverse saat ini memiliki kontrol yang besar atas data pengguna, termasuk informasi pribadi, kebiasaan online, dan preferensi konsumen. Data ini tidak hanya digunakan untuk mengoptimalkan pengalaman pengguna tetapi juga dapat dimanfaatkan untuk tujuan komersial, seperti iklan berbasis data atau analitik perilaku. Dalam beberapa kasus, eksploitasi data menciptakan risiko yang sangat besar bagi pengguna, terutama jika data tersebut jatuh ke tangan yang salah. Selain itu, banyak platform metaverse yang belum memiliki mekanisme yang memadai untuk melindungi pengguna dari pelecehan, eksploitasi, atau penipuan, menimbulkan pertanyaan tentang tanggung jawab platform dalam memastikan keamanan lingkungan digital.

Ketiadaan regulasi yang spesifik untuk metaverse juga mencerminkan kelemahan dalam kebijakan kriminal yang ada saat ini. Sebagian besar sistem hukum yang berlaku masih didasarkan pada paradigma yang mengutamakan interaksi fisik, dengan sedikit perhatian pada implikasi dunia maya. Sebagai contoh, banyak undang-undang tentang pencurian atau penipuan yang mendefinisikan kejahatan tersebut dalam konteks pengambilalihan aset fisik, sehingga sulit untuk diterapkan dalam kasus yang melibatkan aset digital seperti NFT atau mata uang kripto. Selain itu, banyak sistem hukum yang belum mengakui avatar atau identitas digital sebagai entitas hukum yang dapat dilindungi, yang berarti bahwa pelaku kejahatan yang menyerang avatar seseorang mungkin tidak dapat dituntut dengan undang-undang yang ada.

Selain tantangan hukum, metaverse juga menghadirkan tantangan sosial yang memerlukan perhatian khusus dalam perumusan kebijakan kriminal. Masalah pelecehan seksual berbasis avatar, yang meskipun tidak melibatkan kontak fisik, dapat memiliki dampak psikologis yang serius bagi korban. Dalam banyak kasus, pelaku menggunakan fitur-fitur di metaverse untuk melakukan tindakan seperti manipulasi avatar, penggunaan bahasa yang merendahkan, atau bahkan pemaksaan visual yang tidak diinginkan. Sayangnya, banyak platform metaverse yang belum

[3]Beduschi, A. (2019). Digital Identity: Contemporary Challenges For Data Protection, Privacy and Non-Discrimination Rights. Big Data & Society, 6(2): 1-6.

memiliki mekanisme yang efektif untuk pencegahan sehingga meninggalkan korban tanpa perlindungan atau upaya pemulihan.

Lebih ironisnya lagi karena metaverse terus berkembang menjadi bagian integral dari kehidupan manusia. Banyak perusahaan besar teknologi, termasuk Meta, Microsoft, dan Google, telah berinvestasi miliaran dolar untuk menciptakan ekosistem metaverse yang lebih canggih dan inklusif. Dengan populasi pengguna yang terus meningkat, potensi dampak sosial, ekonomi, dan kriminal dari metaverse juga menjadi semakin besar. Kebijakan kriminal harus menghadapi tantangan yang tidak hanya harus bersifat adaptif terhadap perkembangan teknologi tetapi juga harus mencerminkan nilai-nilai keadilan, inklusivitas, dan perlindungan hak asasi manusia.

Penelitian ini bertujuan untuk menjelaskan secara analitis berbagai tantangan dan peluang yang dihadirkan oleh metaverse dalam kaitannya dengan kebijakan kriminal berbasis identitas digital. Melalui pendekatan yang terstruktur akan menguraikan definisi dan karakteristik identitas digital, menganalisis pola kejahatan berbasis identitas di metaverse, mengevaluasi kesenjangan dalam kebijakan kriminal yang ada, serta menawarkan rekomendasi strategis untuk menciptakan solusi yang adaptif dan efektif. Dengan demikian, diharapkan dapat menjadi kontribusi yang relevan dalam diskursus akademik maupun praktis tentang reformasi kebijakan kriminal di era digital.

Metode Penelitian

Penelitian ini menggunakan metode penelitian kualitatif. Penelitian kualitatif adalah penelitian untuk memahami fenomena sosial dan perilaku manusia dengan mengolah data yang sifatnya deskriptif.[4] Penelitian ini dilakukan dengan pendekatan konseptual (*conceptual approach*).[5] Konseptual berfokus pada analisis konsep atau teori yang relevan dengan penelitian yang diangkat. Metode pengumpulan data dikumpulkan dengan menggunakan studi kepustakaan, lalu dianalisis menggunakan metode kualitatif dan disajikan secara deskriptif.

Analsis dan Pembahasan

Definisi dan Karakteristik Identitas Digital dalam Metaverse

Identitas digital merupakan representasi unik individu dalam dunia virtual yang memungkinkan pengguna berpartisipasi, berinteraksi, dan menjalankan berbagai aktivitas secara imersif di ruang digital.[6] Dalam metaverse, identitas digital tidak sekadar refleksi dari atribut personal seperti nama atau profil dasar, melainkan wujud kompleks dari eksistensi virtual yang mencakup dimensi personal, sosial, dan bahkan ekonomi. Identitas digital terintegrasi dengan berbagai teknologi seperti kecerdasan buatan, blockchain, dan data biometrik, menciptakan entitas yang tidak hanya dapat dikenali secara unik, tetapi juga memfasilitasi pengakuan dan transaksi dalam ekosistem digital yang sepenuhnya terdesentralisasi.

Komponen dasar identitas digital di metaverse melibatkan tiga elemen utama. Pertama, identitas personal mencakup data pribadi pengguna, termasuk informasi yang bersifat unik seperti nama, lokasi, atau biometrik. Elemen ini sering digunakan untuk otentikasi dan personalisasi layanan dalam platform metaverse. Kedua, identitas relasional yang terbentuk dari interaksi pengguna dengan individu lain, komunitas, atau entitas digital lainnya. Relasi ini menciptakan jaringan sosial yang tidak hanya memperkuat dimensi personal dari identitas digital, tetapi juga memungkinkan pengguna membangun reputasi atau kepercayaan

[4]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.

[5]Syarif, M., Ramadhani, R., Graha, M. A. W., Yanuaria, T., Muhtar, M. H., Asmah, N., ... & Jannah, M. (2024). Metode Penelitian Hukum.

[6]Majeed, M. M. F., Adisaputera, A., & Ridwan, M. (2020). Digital Identity. Konfrontasi: Jurnal Kultural, Ekonomi, dan Perubahan Sosial, 7(4): 246-252.

dalam komunitas virtual. Ketiga, identitas performatif yang mencerminkan cara pengguna mengekspresikan dirinya melalui avatar, aset virtual, atau interaksi berbasis kreatif di metaverse. Identitas performatif dapat menjadi sarana bagi pengguna untuk mengeksplorasi identitas baru atau memperluas batasan yang ada dalam dunia nyata.

Ciri khas identitas digital dalam metaverse adalah fluiditasnya, di mana pengguna memiliki kebebasan untuk menciptakan dan mengubah representasi digital mereka sesuai dengan preferensi atau kebutuhan. Berbeda dari identitas fisik yang cenderung statis, identitas digital memberikan fleksibilitas yang hampir tak terbatas dalam mengekspresikan diri. Misalnya, seorang pengguna dapat memilih untuk tampil sebagai avatar yang sepenuhnya berbeda dari wujud fisiknya, baik dalam hal jenis kelamin, usia, ras, maupun atribut lainnya. Kebebasan tersebut membuka peluang bagi individu untuk membangun identitas yang lebih inklusif atau imajinatif, tetapi sekaligus menciptakan tantangan baru terkait otentisitas dan integritas identitas tersebut. Dalam konteks kriminalitas, pelaku dapat menyamarkan identitasnya sehingga mempersulit upaya penegakan hukum dalam melacak atau mengidentifikasi pelaku kejahatan.

Identitas digital dalam metaverse juga erat kaitannya dengan konsep hak digital, yang mencakup hak atas privasi, keamanan, dan kepemilikan data.[7] Dalam ekosistem metaverse, data pribadi menjadi komoditas yang sangat berharga, baik untuk pengguna maupun penyedia layanan. Pengguna mengandalkan data ini untuk mengakses dan menikmati layanan, sementara platform menggunakan data tersebut untuk mengembangkan fitur, menganalisis perilaku pengguna, atau menjalankan model bisnis berbasis data. Namun, ketergantungan terhadap data juga menciptakan risiko besar, terutama jika data tersebut disalahgunakan atau dicuri. Kejadian seperti pelanggaran data, manipulasi identitas, atau penggunaan data untuk tujuan kriminal menunjukkan bahwa identitas digital bukan hanya aset, tetapi juga titik kerentanan yang dapat dieksploitasi oleh pihak yang tidak bertanggung jawab.

Selain aspek personal, identitas digital juga memiliki nilai ekonomi yang tidak dapat diabaikan. Dalam banyak platform metaverse, identitas digital terkait langsung dengan aset virtual seperti mata uang kripto, token NFT, atau barang-barang digital lainnya. Aset-aset tersebut dapat diperdagangkan, dimiliki, atau dipertukarkan menggunakan identitas digital sebagai penghubung utama. Nilai ekonomi yang melekat pada identitas digital menjadikannya target empuk bagi pelaku kriminal yang bertujuan untuk mendapatkan keuntungan finansial. Modus operandi seperti pencurian kredensial, eksploitasi kelemahan keamanan platform, atau manipulasi data transaksi menjadi tantangan yang memerlukan perhatian khusus dari pembuat kebijakan.

Penting untuk dicatat bahwa identitas digital bukan sekadar refleksi dari diri individu, tetapi juga alat untuk membangun kepercayaan dalam ekosistem metaverse. Dalam banyak interaksi digital, kepercayaan menjadi elemen kunci yang memungkinkan kolaborasi, transaksi, atau kerja sama lintas platform. Identitas digital yang kuat dan terpercaya dapat meningkatkan partisipasi pengguna dalam berbagai aktivitas di metaverse, sementara identitas yang lemah atau rentan dapat mengurangi kredibilitas individu maupun komunitas yang terlibat. Oleh karena itu, membangun sistem identitas digital yang aman, terpercaya, dan inklusif menjadi prioritas utama dalam mengembangkan ekosistem metaverse yang berkelanjutan.

Namun, pengembangan identitas digital yang ideal memerlukan keseimbangan antara fleksibilitas dan keamanan. Di satu sisi, pengguna membutuhkan kebebasan untuk mengekspresikan diri mereka secara penuh di metaverse.[8] Di sisi lain, platform

[7]Wu, H., & Zhang, W. (2023). Digital Identity, Privacy Security, and Their Legal Safeguard in the Metaverse. Security and Safety, 2(1): 1-14.

[8]Fornasier, M. O. (2023). Freedom of Expression and the Metaverse: On the Importance of Content

dan pembuat kebijakan harus memastikan bahwa kebebasan tersebut tidak disalahgunakan untuk tujuan yang merugikan individu lain atau komunitas secara keseluruhan. Misalnya, fleksibilitas dalam menciptakan avatar tidak boleh mengorbankan perlindungan terhadap pelecehan atau eksploitasi berbasis identitas digital. Demikian pula, kebijakan yang terlalu membatasi atau mengontrol identitas digital dapat berdampak pada hak-hak pengguna, termasuk hak privasi atau kebebasan berekspresi.

Sebagai bagian dari ekosistem digital yang semakin kompleks, identitas digital memerlukan kerangka kerja hukum dan teknis yang mampu menjawab berbagai tantangan yang muncul. Dalam perspektif kebijakan kriminal, identitas digital memerlukan perlindungan hukum yang setara dengan identitas fisik, termasuk pengakuan terhadap kejahatan yang menargetkan identitas digital sebagai bentuk pelanggaran hukum yang serius. Selain itu, teknologi seperti blockchain dapat digunakan untuk meningkatkan keamanan identitas digital dengan menciptakan sistem otentikasi yang lebih andal dan transparan. Dengan pendekatan yang holistik dan terintegrasi, identitas digital dapat menjadi fondasi yang kokoh untuk menciptakan metaverse yang aman, inklusif, dan adil bagi semua penggunanya.

Ditinjau dari segi kerentanannya, identitas digital dalam metaverse menghadirkan berbagai peluang untuk eksplorasi dan ekspresi diri, tetapi di balik potensi tersebut terdapat sejumlah kerentanan yang memengaruhi keamanan, privasi, dan integritas individu. Kerentanan berasal dari sifat dasar teknologi yang menjadi fondasi metaverse, termasuk ketergantungan pada data, kurangnya regulasi yang jelas, dan kompleksitas interaksi antara pengguna, platform, serta pihak ketiga. Identitas digital tidak hanya menjadi cerminan virtual dari pengguna, tetapi juga berfungsi sebagai pintu gerbang untuk mengakses layanan, bertransaksi, dan membangun jaringan sosial. Oleh karena itu, setiap celah dalam sistem yang melindungi identitas digital memiliki konsekuensi yang jauh melampaui ranah virtual, dengan dampak nyata terhadap keamanan, reputasi, dan hak individu.

Kerentanan utama identitas digital terletak pada eksposur data pribadi yang berlebihan.[9] Untuk dapat beroperasi di metaverse, pengguna diharuskan memberikan sejumlah informasi pribadi yang mencakup nama, lokasi, preferensi, hingga data biometrik seperti pengenalan wajah atau suara. Data-data ini dikumpulkan, disimpan, dan dikelola oleh platform, yang sering kali tidak memiliki mekanisme perlindungan data yang memadai. Ketika data tersebut disalahgunakan, baik melalui pelanggaran keamanan siber, kebocoran informasi, atau penyalahgunaan oleh pihak internal platform, pengguna dapat menghadapi risiko yang sangat besar, termasuk pencurian identitas, eksploitasi finansial, dan manipulasi reputasi. Selain itu, banyak platform yang mengintegrasikan teknologi pelacakan seperti cookies atau perangkat lunak analitik untuk memantau aktivitas pengguna. Praktik ini tidak hanya meningkatkan potensi pelanggaran privasi, tetapi juga menciptakan basis data yang sangat besar yang rentan terhadap serangan siber.

Kerentanan identitas digital juga diperburuk oleh munculnya teknologi manipulasi canggih seperti *deepfake*.[10] Teknologi ini memungkinkan pembuatan representasi visual atau suara yang hampir tidak dapat dibedakan dari aslinya, menciptakan peluang bagi pelaku kriminal untuk melakukan berbagai modus operandi. Dalam metaverse, pelaku dapat menggunakan teknologi *deepfake* untuk

Creation for the Emerge of a Complex Environment. Revista de Investigaes Constitucionais, 10(1): 1-30.

[9]Permana, F. A., & Jamaluddin, A. (2023). Personal Data Vulnerability in the Digital Era: Study of Modus Operandi and Mechanisms to Prevent Phising Crimes. Jurnal Al-Hakim: Jurnal Ilmiah Mahasiswa, Studi Syariah, Hukum dan Filantropi, 5(2): 201-216.

[10]Kirchengast, T. (2020). Deepfakes and Image Manipulation: Criminalisation and Control. Information & Communication Technology Law, 29(3): 308-323.

menciptakan avatar atau suara digital yang menyerupai pengguna tertentu, yang kemudian digunakan untuk tujuan penipuan, pencemaran nama baik, atau pelecehan. Misalnya saja pelaku dapat meniru identitas digital seseorang untuk mendapatkan akses ke aset virtual atau data sensitif, sementara korban menghadapi kesulitan besar dalam membuktikan bahwa tindakan tersebut dilakukan oleh pihak ketiga. Kompleksitas teknologi tentu menantang otoritas hukum yang masih berjuang untuk memahami dan mengidentifikasi cara kerja *deepfake* dalam kejahatan berbasis identitas digital.

Dimensi lain dari kerentanan identitas digital adalah kelemahan dalam otentikasi dan pengelolaan kredensial. Sebagian besar sistem metaverse mengandalkan mekanisme otentikasi tradisional seperti kombinasi nama pengguna dan kata sandi untuk memberikan akses kepada pengguna. Namun, metode ini telah lama dianggap tidak aman karena rentan terhadap serangan seperti *phishing, brute force*,[11] atau pencurian kredensial. Ketika kredensial pengguna dicuri, pelaku dapat dengan mudah mengakses akun metaverse korban, mengambil alih identitas digitalnya, dan melakukan tindakan kriminal atas nama korban. Di sisi lain, beberapa platform telah beralih ke mekanisme otentikasi yang lebih canggih seperti pengenalan biometrik atau autentikasi multi-faktor (MFA). Meskipun lebih aman, metode ini tidak sepenuhnya bebas dari risiko. Data biometrik, misalnya, tidak dapat diubah seperti kata sandi jika terjadi kebocoran, sehingga menciptakan dampak jangka panjang yang sulit diperbaiki.

Kerentanan lain yang tidak kalah penting adalah kurangnya transparansi dalam pengelolaan identitas digital oleh platform. Sebagian besar pengguna metaverse tidak memiliki kendali penuh atas data,[12] termasuk bagaimana data tersebut digunakan, disimpan, atau dibagikan kepada pihak ketiga. Ketika platform mengontrol seluruh proses pengelolaan identitas digital, pengguna menjadi rentan terhadap eksploitasi komersial yang tidak etis, seperti penjualan data ke perusahaan pihak ketiga tanpa persetujuan pengguna. Selain itu, beberapa platform menggunakan algoritma untuk menganalisis perilaku pengguna, yang kemudian dapat dimanfaatkan untuk menciptakan profil digital yang sangat detail. Profil tersebut tidak hanya digunakan untuk menargetkan iklan, tetapi juga dapat digunakan untuk manipulasi perilaku atau bahkan pengambilan keputusan otomatis yang berdampak pada kehidupan pengguna.

Keberadaan pelaku kriminal yang memanfaatkan celah keamanan di metaverse juga menjadi faktor yang memperburuk kerentanan identitas digital. Modus kejahatan seperti phishing berbasis avatar, serangan malware, dan penipuan dalam transaksi ekonomi virtual semakin meningkat seiring dengan bertambahnya jumlah pengguna metaverse. Misalnya pelaku dapat menciptakan avatar palsu yang menyerupai figur otoritatif untuk menipu pengguna lain agar memberikan data pribadi atau aset virtual. Dalam beberapa kasus, pelaku bahkan memanfaatkan kerentanan dalam sistem keamanan platform untuk melakukan serangan terhadap banyak akun secara bersamaan, yang dikenal sebagai serangan massal berbasis bot. Akibatnya, korban tidak hanya kehilangan aset virtual tetapi juga menghadapi kesulitan dalam memulihkan reputasi digital mereka.

Ketimpangan regulasi antara berbagai negara juga memperbesar risiko kerentanan identitas digital.[13] Karena metaverse bersifat lintas batas, banyak pelaku kejahatan memanfaatkan jurisdiksi yang lemah atau tidak memiliki regulasi yang memadai untuk melindungi identitas digital. Misalnya serangan yang dilakukan oleh pelaku di satu negara terhadap pengguna di negara lain

[11]Mappaselleng, N. F., & Kadir, Z. K. (2018). Rethinking Cyber Crime. Yogyakarta: Arti Bumi Intaran.

[12]Jaber, T. A. (2022). Security Risks of the Metaverse World. International Journal of Interactive Mobile Technologies, 16(13): 4-14.

[13]Selvam, D., & Khanna, A. (2024). Enhancing Utility Sector Efficiency and Security: Integrating Digital Identity System Amidst Privacy and Ransomware Challenges. International Journal of Advanced Research in Science, Communication and Technology, 4(1): 759-772

sering kali tidak dapat ditangani secara efektif karena tidak adanya kerangka kerja hukum internasional yang harmonis. Kondisi ini menciptakan tantangan besar bagi penegak hukum yang harus bekerja sama dengan otoritas di berbagai negara untuk mengidentifikasi pelaku dan menegakkan hukum.

Kerentanan identitas digital dalam metaverse tidak hanya berdampak pada individu tetapi juga pada stabilitas dan kepercayaan terhadap ekosistem metaverse secara keseluruhan. Ketika pengguna merasa bahwa identitas digital mereka tidak aman, kepercayaan terhadap platform metaverse akan menurun, yang pada akhirnya menghambat adopsi teknologi ini secara luas. Oleh karena itu, mitigasi kerentanan identitas digital memerlukan pendekatan yang komprehensif, termasuk penguatan regulasi, peningkatan literasi digital, dan pengembangan teknologi keamanan yang lebih canggih. Pendekatan ini tidak hanya bertujuan untuk melindungi pengguna, tetapi juga untuk menciptakan lingkungan metaverse yang aman, inklusif, dan berkelanjutan.

Kejahatan Berbasis Identitas Digital di Metaverse

Metaverse telah menciptakan paradigma baru dalam dunia digital yang memungkinkan manusia untuk berinteraksi secara virtual melalui avatar dan identitas digital.[14] Namun, lingkungan ini juga membuka ruang bagi beragam bentuk kejahatan yang mengeksploitasi identitas digital, menciptakan tantangan yang kompleks bagi sistem hukum dan penegakan hukum di seluruh dunia. Kejahatan berbasis identitas digital di metaverse bukan sekadar lanjutan dari kejahatan siber tradisional, tetapi sering kali berbentuk fenomena baru yang mengintegrasikan aspek sosial, ekonomi, dan teknologi. Sifat unik metaverse sebagai ruang yang tidak memiliki batas geografis dan hukum konvensional memperumit penanganan kejahatan tersebut, menuntut analisis mendalam untuk memahami pola-pola kejahatan yang terjadi serta langkah-langkah mitigasi yang diperlukan.

Bentuk kejahatan yang paling umum di metaverse adalah pencurian identitas digital. Pencurian identitas digital melibatkan pengambilalihan atau penggunaan tanpa izin identitas digital seseorang untuk tujuan yang merugikan, seperti penipuan, pencurian aset, atau pelecehan. Dalam metaverse, identitas digital tidak hanya mencerminkan data pribadi seperti nama atau alamat email, tetapi juga mencakup elemen yang lebih kompleks, seperti avatar, aset virtual, dan jejak transaksi pengguna. Pencurian identitas digital dapat dilakukan melalui berbagai metode, termasuk serangan phishing, rekayasa sosial, atau eksploitasi celah keamanan dalam platform metaverse.[15] Ketika pelaku berhasil menguasai identitas digital korban, mereka dapat dengan mudah menyamar sebagai korban, mengakses aset virtual yang dimiliki, atau bahkan menciptakan kerugian reputasi yang sulit diperbaiki. Tantangan utama yang timbul yaitu sulitnya melacak pelaku yang sering kali berada di jurisdiksi hukum yang berbeda dari korban, sehingga memerlukan kerja sama internasional untuk penyelidikan dan penegakan hukum.

Pemalsuan identitas juga menjadi ancaman serius dalam metaverse, terutama dengan berkembangnya teknologi avatar canggih. Pemalsuan identitas di dunia maya melibatkan pembuatan representasi digital yang menyerupai individu tertentu untuk menipu pihak lain. Dalam metaverse, pelaku dapat menciptakan avatar yang terlihat identik dengan individu tertentu, kemudian menggunakannya untuk melakukan penipuan, manipulasi, atau bahkan pelecehan. Teknologi *deepfake* juga memungkinkan pelaku untuk mereplikasi wajah, suara, atau gerakan individu tertentu dengan akurasi yang sangat tinggi, sehingga korban atau pihak ketiga sulit membedakan

[14]Zare, A., & Jalali, A. (2024). A Perspective Metaverse Paradigm Based on the Reality-Virtuality Continuum and Digital Twins. Recent Advances in Computer Science and Communications, 18(1): 1-19.

[15]Huang, Y, Li, Y., & Cai, Z. (2023). Security and Privacy in Metaverse: A Comprehensive Survey. Big Data Mining and Analytics, 6(2): 234-247.

antara representasi asli dan palsu.[16] Dalam banyak kasus, pemalsuan identitas ini digunakan untuk menipu pengguna lain agar memberikan informasi sensitif, seperti kata sandi atau data pribadi, yang kemudian digunakan untuk tujuan kriminal lainnya.

Selain itu, penipuan berbasis metaverse menjadi salah satu modus kejahatan yang semakin marak, terutama dalam transaksi ekonomi yang melibatkan aset virtual seperti mata uang kripto, token NFT, atau barang-barang digital lainnya. Penipuan ini biasanya dilakukan melalui skema yang dirancang untuk memanfaatkan kepercayaan pengguna terhadap sistem atau platform metaverse. Salah satu contoh adalah skema investasi palsu, di mana pelaku menawarkan peluang investasi yang menggiurkan dalam bentuk aset digital tetapi sebenarnya tidak memiliki nilai. Modus lainnya adalah manipulasi pasar, di mana pelaku menciptakan permintaan palsu terhadap aset tertentu untuk meningkatkan harganya sebelum menjualnya dengan keuntungan besar. Penipuan semacam ini tidak hanya merugikan individu tetapi juga mengganggu stabilitas ekonomi digital di metaverse, menciptakan ketidakpercayaan yang dapat berdampak jangka panjang pada adopsi teknologi tersebut.

Kejahatan lain yang tidak kalah mengkhawatirkan adalah pelecehan dan eksploitasi berbasis avatar. Dalam metaverse, avatar menjadi perpanjangan identitas digital pengguna, memungkinkan mereka untuk berinteraksi secara visual dan fisik di ruang virtual. Namun, interaksi ini juga dapat disalahgunakan oleh pelaku untuk melakukan pelecehan verbal, visual, atau bahkan tindakan seksual berbasis avatar. Misalnya, pelaku dapat menggunakan avatar mereka untuk mendekati korban secara tidak diinginkan, mengirimkan konten visual yang ofensif, atau bahkan memaksa korban untuk terlibat dalam aktivitas tertentu. Meskipun tindakan semacam ini terjadi di dunia maya, dampaknya terhadap korban sering kali nyata, mencakup trauma psikologis, rasa malu, atau hilangnya kepercayaan terhadap lingkungan metaverse. Salah satu tantangan utama dalam menangani kasus ini adalah kurangnya mekanisme yang efektif untuk melaporkan dan menangani pelecehan berbasis avatar, terutama di platform yang belum memiliki kebijakan keamanan yang memadai.

Eksploitasi data pribadi juga menjadi bentuk kejahatan yang menonjol dalam metaverse. Platform metaverse sering kali mengumpulkan data pribadi pengguna untuk meningkatkan pengalaman mereka, tetapi data ini juga menjadi target bagi pelaku kriminal. Eksploitasi data pribadi dapat mencakup pencurian informasi pengguna melalui serangan siber, penjualan data tanpa izin, atau penggunaan data untuk tujuan yang tidak sah. Misalnya, pelaku dapat mencuri data biometrik pengguna yang digunakan untuk otentikasi di metaverse, seperti sidik jari atau pengenalan wajah, yang kemudian digunakan untuk membobol akun atau menciptakan avatar palsu. Risiko lain adalah penggunaan data oleh pihak ketiga tanpa persetujuan pengguna, yang sering kali sulit diidentifikasi karena kurangnya transparansi dalam pengelolaan data oleh platform. Eksploitasi data semacam ini tidak hanya melanggar hak privasi pengguna tetapi juga menciptakan ketidakamanan sistemik yang dapat merusak kepercayaan terhadap metaverse secara keseluruhan.

Keberadaan kejahatan berbasis identitas digital di metaverse juga diperparah oleh tantangan dalam penegakan hukum. Sifat lintas batas metaverse membuat banyak kasus kejahatan melibatkan pelaku, korban, dan platform yang berada di jurisdiksi hukum yang berbeda, menciptakan hambatan besar dalam investigasi dan penuntutan. Selain itu, kurangnya regulasi yang harmonis di tingkat internasional memperumit upaya untuk menangani kejahatan semacam ini. Sebagai contoh, banyak negara belum memiliki undang-undang yang spesifik mengenai identitas digital, sehingga sulit untuk menetapkan pelanggaran dan sanksi yang relevan. Hal ini memberikan celah bagi pelaku untuk

[16]Poulsen, S. V. (2021). Face Off: A Semiotic Technology Study of Software for Making Deepfakes. Sign Systems Studies, 49(3): 489-508.

memanfaatkan jurisdiksi dengan regulasi yang lemah untuk menjalankan aktivitas kriminal mereka tanpa takut akan konsekuensi hukum.

Metaverse juga memperkenalkan tantangan baru dalam hal bukti digital. Kejahatan berbasis identitas digital sering kali meninggalkan jejak yang sangat minim, membuat proses pengumpulan bukti menjadi sangat sulit. Dalam banyak kasus, pelaku menggunakan teknologi enkripsi atau metode anonimitas lainnya untuk menyembunyikan aktivitas mereka, sehingga menyulitkan otoritas hukum untuk melacak dan mengidentifikasi pelaku. Selain itu, bukti yang dikumpulkan dari metaverse sering kali tidak diterima di pengadilan karena kurangnya standar yang jelas mengenai validitas bukti digital. Kondisi ini menunjukkan perlunya reformasi dalam sistem hukum untuk mengakomodasi realitas baru yang dihadirkan oleh metaverse, termasuk pengembangan standar bukti digital yang dapat diterima secara universal.

Kesenjangan Kebijakan Kriminal dalam Menghadapi Metaverse

Metaverse menghadirkan realitas baru yang melampaui batasan fisik dan temporal dalam kehidupan manusia, namun perkembangan teknologi ini tidak diiringi dengan kesiapan kebijakan kriminal yang memadai. Sebagai lingkungan digital yang sepenuhnya terintegrasi dengan kecerdasan buatan, realitas virtual, dan blockchain, metaverse menciptakan ruang interaksi baru yang penuh dengan kompleksitas hukum. Meskipun berbagai bentuk kejahatan berbasis identitas digital telah muncul di dalam metaverse, sebagian besar sistem hukum tradisional belum mampu menyesuaikan diri dengan tantangan yang ditimbulkan oleh fenomena tersebut. Kesenjangan kebijakan kriminal yang terjadi tidak hanya memperbesar risiko terhadap pengguna, tetapi juga menghambat upaya penegakan hukum, menciptakan ruang bagi pelaku kejahatan untuk memanfaatkan celah hukum yang ada.

Kesenjangan dalam kebijakan kriminal terkait metaverse adalah kurangnya harmonisasi regulasi internasional.[17] Metaverse bersifat lintas batas, di mana aktivitas yang terjadi dalam platform digital yang melibatkan individu, entitas, atau aset yang tersebar di berbagai negara.[18] Sayangnya, regulasi hukum yang ada masih didasarkan pada prinsip yurisdiksi teritorial yang membatasi otoritas hukum dalam wilayah geografis tertentu. Misalnya, kasus pencurian aset digital di metaverse mungkin melibatkan pelaku di satu negara, korban di negara lain, dan server platform di yurisdiksi yang berbeda lagi. Ketidakharmonisan regulasi di antara negara-negara tersebut menciptakan celah yang sering dimanfaatkan oleh pelaku kejahatan untuk menghindari penuntutan. Lebih jauh lagi, tidak adanya mekanisme kerja sama internasional yang efektif untuk menangani kejahatan berbasis metaverse memperburuk situasi ini, membuat banyak kasus tidak terselesaikan.

Ketiadaan definisi yang jelas mengenai identitas digital dalam sistem hukum juga menjadi salah satu penyebab utama kesenjangan kebijakan kriminal.[19] Identitas digital di metaverse tidak hanya mencakup data pribadi pengguna, tetapi juga mencakup aspek-aspek lain seperti avatar, jejak transaksi, dan aset virtual. Namun, banyak sistem hukum belum mengakui identitas digital sebagai entitas hukum yang memiliki perlindungan setara dengan identitas fisik. Akibatnya, kejahatan yang menargetkan identitas digital, seperti pencurian avatar atau eksploitasi data pribadi, sering kali tidak dapat dituntut di bawah hukum yang ada. Sebagai contoh, dalam beberapa jurisdiksi, pencurian identitas digital belum diakui sebagai kejahatan yang berdampak pada hak

[17]Lee, W. S. (2022). A Study on the Role of Criminal Law in Metaverse. Institute for Legal Studies Chonnam National University, 42(3): 177-202.
[18]Oleksii, K., Oleksii, D., & Dmytro, Z. (2024). Metaverse: Ensuring Legal Recognition of Avatars and Electronic Personalities Through a Cross-Border Personalized ID-Code. International Jounal of Innovative Technologies in Social Science, 2(42): 1-5.
[19]Tantimin, Febriyani, E., Agustianto, Hutauruk, R. H. (2024). Defining Legal Contours of Digital Identity Theft. Jurnal Akta, 11(3): 1044-1059.

individu, sehingga pelaku tidak dapat dikenakan sanksi yang setara dengan dampak yang ditimbulkan.

Kerentanan lain yang mencolok dalam kebijakan kriminal terkait metaverse adalah lemahnya regulasi terhadap platform teknologi yang menjadi pengelola ekosistem tersebut. Sebagian besar platform metaverse memiliki kekuasaan yang besar dalam mengelola data, aset, dan interaksi pengguna. Namun, regulasi yang mengatur tanggung jawab platform dalam melindungi pengguna masih sangat terbatas. Banyak platform yang gagal menyediakan mekanisme pengamanan yang memadai untuk mencegah kejahatan berbasis identitas digital, seperti pencurian data atau pelecehan berbasis avatar. Selain itu, ketidaktransparanan dalam pengelolaan data oleh platform membuat pengguna tidak menyadari bagaimana data tersebut digunakan, disimpan, atau dibagikan. Hal ini menciptakan ketidakpastian hukum yang tidak hanya merugikan pengguna tetapi juga menghambat upaya penegakan hukum untuk mengidentifikasi pelaku kejahatan.

Kesenjangan kebijakan juga terlihat dalam hal kurangnya standar internasional untuk pengumpulan dan penggunaan bukti digital di metaverse. Kejahatan berbasis identitas digital sering kali meninggalkan jejak digital yang sangat minim, sehingga proses pengumpulan bukti menjadi tantangan besar bagi penegak hukum. Selain itu, banyak bukti digital yang dikumpulkan dari metaverse tidak diterima di pengadilan karena tidak memenuhi standar yang berlaku dalam sistem hukum tradisional. Sebagai contoh, bukti berupa log aktivitas pengguna atau rekaman avatar sering kali dianggap tidak valid karena kurangnya mekanisme otentikasi yang dapat menjamin keasliannya. Ketiadaan standar yang jelas mengenai validitas bukti digital di tingkat internasional tidak hanya menghambat proses penuntutan tetapi juga memberikan ruang bagi pelaku kejahatan untuk memanfaatkan celah tersebut.

Selain masalah teknis, kesenjangan kebijakan kriminal juga mencakup aspek etis yang terkait dengan perlindungan hak digital pengguna di metaverse. Identitas digital sering kali dianggap sebagai perpanjangan dari identitas personal, sehingga pelanggaran terhadap identitas digital dapat berdampak langsung pada hak asasi manusia, termasuk privasi, keamanan, dan kebebasan berekspresi. Namun, banyak kebijakan yang dirancang untuk mengatasi kejahatan digital justru berbenturan dengan prinsip-prinsip tersebut. Sebagai contoh penggunaan teknologi pengawasan oleh platform atau pemerintah untuk mencegah kejahatan menimbulkan kekhawatiran mengenai pelanggaran privasi. Pada tingkat tertentu, kebijakan yang terlalu represif dalam mengatur aktivitas di metaverse dapat berdampak negatif pada kebebasan berekspresi pengguna, menciptakan ketakutan untuk berinteraksi secara bebas di ruang digital.[20] Sebab secara teoretis, kebebasan berekspresi masih dianggap suatu perbuatan yang dibolehkan selama itu memenuhi standar rasio kewajaran.[21]

Kesenjangan kebijakan kriminal dalam menghadapi metaverse juga terlihat dalam kurangnya edukasi dan literasi digital di kalangan masyarakat dan penegak hukum. Banyak pengguna metaverse yang tidak sepenuhnya memahami risiko yang terkait dengan identitas digital mereka, sehingga mudah menjadi target bagi pelaku kejahatan. Di sisi lain, penegak hukum sering kali tidak memiliki keahlian teknis yang diperlukan untuk menangani kasus-kasus kejahatan berbasis metaverse. Ketidaksiapan memicu hambatan dalam proses penyelidikan dan penuntutan, serta menurunkan efektivitas penegakan hukum secara keseluruhan. Tanpa adanya upaya untuk meningkatkan literasi digital di kalangan pengguna dan kapasitas teknis di kalangan penegak hukum, kesenjangan ini akan terus melebar, memberikan keuntungan bagi pelaku kejahatan yang semakin canggih.

[20]Hine, E. (2023). Content Moderation in the Metaverse Could Be a New Frontier to Attack Freedom of Expression. Philosophy & Technology, 36(43): 1-10.

[21]Mappaselleng, N. F., & Kadir, Z. K. (2023). Ilmu Hukum Pidana 101. Yogyakarta: Arti Bumi Intaran.

Tantangan terakhir yang perlu disoroti adalah kurangnya kolaborasi antara pemerintah, perusahaan teknologi, dan masyarakat sipil dalam menangani kejahatan berbasis identitas digital di metaverse. Banyak kebijakan kriminal yang dirancang tanpa melibatkan pemangku kepentingan utama, seperti platform teknologi yang memiliki akses langsung ke data dan aktivitas pengguna. Hal ini mengakibatkan kebijakan yang dirancang sering kali tidak relevan atau sulit diimplementasikan. Sebaliknya, keterlibatan platform teknologi dalam proses perumusan kebijakan dapat membantu menciptakan solusi yang lebih efektif dan praktis, seperti pengembangan mekanisme pelaporan kejahatan yang lebih mudah diakses oleh pengguna. Selain itu, masyarakat sipil juga perlu dilibatkan untuk memastikan bahwa kebijakan yang dirancang tidak hanya berfokus pada aspek keamanan tetapi juga memperhatikan prinsip-prinsip keadilan dan inklusivitas.

Gagasan Kebijakan Kriminal untuk Metaverse

Metaverse menawarkan lanskap digital yang inovatif, namun tantangan kriminalitas yang muncul menuntut pendekatan kebijakan kriminal yang tidak hanya adaptif tetapi juga progresif. Keberhasilan metaverse sebagai ruang digital yang aman, adil, dan inklusif bergantung pada kemampuan pembuat kebijakan untuk merancang kerangka regulasi yang efektif dalam menghadapi risiko yang unik. Gagasan kebijakan kriminal untuk metaverse harus mencakup langkah-langkah yang mencerminkan keadilan, perlindungan hak, dan kolaborasi lintas sektor, sambil mengakomodasi perubahan teknologi yang cepat. Pendekatan yang komprehensif diperlukan untuk menciptakan kebijakan yang mampu mengatasi kerentanan identitas digital, kejahatan siber berbasis metaverse, dan tantangan penegakan hukum lintas yurisdiksi.

Gagasan dalam merancang kebijakan kriminal untuk metaverse adalah perlunya harmonisasi hukum internasional. Sebagai ruang digital tanpa batas geografis, metaverse melibatkan interaksi antara pengguna, platform, dan aset digital yang tersebar di berbagai negara. Namun, sistem hukum tradisional cenderung terfragmentasi dan berbasis teritorial, sehingga menciptakan celah dalam penanganan kejahatan lintas negara. Untuk itu, diperlukan kerangka kerja global yang memungkinkan koordinasi antara pemerintah, organisasi internasional, dan perusahaan teknologi. Kerangka ini dapat mencakup standar internasional untuk definisi kejahatan berbasis metaverse, prosedur pengumpulan bukti digital, dan mekanisme ekstradisi yang lebih efektif. Harmonisasi semacam ini akan mempermudah investigasi, penuntutan, dan pemberian sanksi terhadap pelaku kejahatan, sekaligus memastikan bahwa hak-hak korban terlindungi di semua yurisdiksi yang terlibat.

Penguatan regulasi terhadap platform teknologi juga menjadi elemen kunci dalam kebijakan kriminal untuk metaverse. Platform metaverse memainkan peran dalam mengelola identitas digital, aset, dan interaksi pengguna, sehingga mereka harus memikul tanggung jawab yang lebih besar dalam mencegah kejahatan. Regulasi perlu menetapkan standar keamanan minimum yang wajib diterapkan oleh semua platform, termasuk enkripsi data, sistem autentikasi multi-faktor, dan mekanisme pelaporan insiden. Selain itu, platform harus diwajibkan untuk memberikan transparansi dalam pengelolaan data pengguna, termasuk informasi tentang bagaimana data dikumpulkan, digunakan, dan dilindungi. Regulasi juga dapat mengharuskan platform untuk mengembangkan alat pendeteksian kejahatan berbasis kecerdasan buatan yang mampu mengidentifikasi aktivitas mencurigakan secara real-time.[22] Dengan melibatkan platform sebagai mitra dalam penegakan hukum, kebijakan ini tidak hanya akan meningkatkan keamanan metaverse tetapi juga menciptakan ekosistem yang lebih terpercaya bagi pengguna.

[22]Yeoh, P. (2019). Artificial Intelligence: Accelerator or Panaceo for Financial Crime? Journal of Financial Crime, 26(2): 634-646.

Pengembangan standar bukti digital yang diakui secara internasional juga merupakan langkah yang sangat diperlukan. Kejahatan berbasis metaverse sering kali meninggalkan jejak digital yang menjadi satu-satunya bukti dalam kasus tersebut. Namun, banyak sistem hukum yang belum memiliki pedoman yang jelas mengenai validitas dan otentisitas bukti digital. Untuk itu, kebijakan kriminal perlu mencakup protokol yang memastikan bahwa bukti digital dapat dikumpulkan, disimpan, dan diverifikasi dengan cara yang memenuhi standar hukum. Penggunaan teknologi blockchain dapat menjadi solusi untuk menciptakan rantai bukti yang transparan dan tidak dapat dimanipulasi. Dengan memastikan bahwa bukti digital dapat diterima di pengadilan, kebijakan yang diterapkan akan memperkuat kapasitas penegak hukum dalam menangani kejahatan berbasis metaverse dan memberikan keadilan bagi korban.

Di sisi lain, kebijakan kriminal untuk metaverse juga harus mencakup perlindungan terhadap hak-hak digital pengguna. Identitas digital dianggap sebagai perpanjangan dari identitas personal, sehingga pelanggaran terhadap identitas digital dapat berdampak langsung pada privasi, reputasi, dan keamanan individu. Untuk itu, kebijakan harus menetapkan batasan yang jelas tentang bagaimana data pengguna dapat digunakan oleh platform atau pihak ketiga. Regulasi perlindungan data seperti General Data Protection Regulation (GDPR) di Uni Eropa dapat menjadi model yang relevan untuk diterapkan di metaverse.[23] Selain itu, pengguna harus memiliki hak untuk mengontrol data mereka, termasuk hak untuk mengakses, mengubah, atau menghapus informasi pribadi yang tersimpan di platform. Dengan memastikan bahwa hak-hak digital terlindungi, kebijakan ini akan menciptakan keseimbangan antara keamanan dan privasi di metaverse.

Kolaborasi antara pemerintah, perusahaan teknologi, dan masyarakat sipil juga menjadi elemen kunci dalam merancang kebijakan kriminal untuk metaverse. Pemerintah memiliki peran dalam menetapkan regulasi yang adil dan efektif, sementara perusahaan teknologi memiliki tanggung jawab untuk mengimplementasikan langkah-langkah keamanan yang sesuai. Di sisi lain, masyarakat sipil dapat berkontribusi melalui advokasi, penelitian, atau pemberian umpan balik mengenai kebijakan yang diterapkan. Kolaborasi semacam ini tidak hanya akan menghasilkan kebijakan yang lebih inklusif tetapi juga memastikan bahwa kebijakan tersebut mencerminkan kebutuhan dan perspektif semua pemangku kepentingan. Selain itu, platform teknologi perlu didorong untuk berbagi informasi tentang ancaman atau kejahatan yang terjadi di metaverse, sehingga penegak hukum dapat merespons dengan lebih cepat dan efektif.

Sebagai bagian dari kebijakan kriminal yang holistik, pengembangan teknologi keamanan yang canggih juga harus menjadi prioritas. Teknologi seperti kecerdasan buatan, blockchain, dan analitik data dapat digunakan untuk mendeteksi, mencegah, dan menangani kejahatan berbasis metaverse. Misalnya, algoritma kecerdasan buatan dapat digunakan untuk mengidentifikasi pola aktivitas yang mencurigakan, sementara blockchain dapat digunakan untuk menciptakan sistem yang transparan dan tidak dapat dimanipulasi. Selain itu, teknologi enkripsi yang lebih kuat dapat digunakan untuk melindungi data pribadi pengguna dari ancaman siber. Namun, pengembangan teknologi ini harus dilakukan dengan memperhatikan prinsip-prinsip etika, sehingga tidak digunakan untuk tujuan yang melanggar hak-hak digital pengguna.

Kesimpulan

Metaverse menghadirkan tantangan kompleks dalam kebijakan kriminal, terutama terkait kejahatan berbasis identitas

[23]Gonzalez, N. M., & Bozkir, E. (2024). Eye-Tracking for Virtual and Augmented Reality Metaverse Environments and Their Compatibility With the European Union General Data Protection Regulation. Digital Society, 3(39): 1-28.

digital. Meskipun membuka peluang luas untuk interaksi sosial, transaksi ekonomi, dan inovasi kreatif, metaverse juga memunculkan risiko kejahatan canggih dan lintas batas yang belum terakomodasi oleh sistem hukum yang ada. Tantangan ini diperparah oleh ketidakharmonisan regulasi internasional, lemahnya perlindungan hukum terhadap identitas digital, dan kurangnya transparansi serta tanggung jawab platform metaverse. Oleh karena itu, diperlukan reformasi mendasar kebijakan kriminal yang mencakup pendekatan kolaboratif lintas negara, penguatan regulasi platform teknologi, dan pengembangan standar hukum yang mampu menjawab kompleksitas kejahatan berbasis metaverse.

Keberhasilan kebijakan kriminal dalam menghadapi tantangan di metaverse bergantung pada kolaborasi antara pemerintah, perusahaan teknologi, dan masyarakat sipil. Kerangka hukum yang dirancang harus melindungi hak-hak digital pengguna seperti privasi, keamanan data, dan kebebasan berekspresi. Integrasi teknologi seperti blockchain, kecerdasan buatan, dan sistem keamanan berbasis analitik diperlukan untuk menciptakan mekanisme yang lebih kuat dalam mendeteksi dan mencegah kejahatan. Peningkatan literasi digital di kalangan pengguna dan penegak hukum juga penting untuk mengurangi risiko kejahatan dan memperkuat kapasitas penegakan hukum. Dengan pendekatan komprehensif dan progresif ini, metaverse diharapkan dapat berkembang menjadi ruang digital yang inklusif, berkelanjutan, aman, dan adil, seiring dengan inovasi teknologi.

Referensi

Beduschi, A. (2019). Digital Identity: Contemporary Challenges For Data Protection, Privacy and Non-Discrimination Rights. Big Data & Society, 6(2): 1-6.

Filipova, I. (2023). Creating the Metaverse: Consequences for Economy, Society, and Law. Journal of Digital Technologies and Law, 1(1): 7-32.

Fornasier, M. O. (2023). Freedom of Expression and the Metaverse: On the Importance of Content Creation for the Emerge of a Complex Environment. Revista de Investigaes Constitucionais, 10(1): 1-30.

Gonzalez, N. M., & Bozkir, E. (2024). Eye-Tracking for Virtual and Augmented Reality Metaverse Environments and Their Compatibility With the European Union General Data Protection Regulation. Digital Society, 3(39): 1-28.

Hine, E. (2023). Content Moderation in the Metaverse Could Be a New Frontier to Attack Freedom of Expression. Philosophy & Technology, 36(43): 1-10.

Huang, Y, Li, Y., & Cai, Z. (2023). Security and Privacy in Metaverse: A Comprehensive Survey. Big Data Mining and Analytics, 6(2): 234-247.

Jaber, T. A. (2022). Security Risks of the Metaverse World. International Journal of Interactive Mobile Technologies, 16(13): 4-14.

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.

Kirchengast, T. (2020). Deepfakes and Image Manipulation: Criminalisation and Control. Information & Communication Technology Law, 29(3): 308-323.

Lee, W. S. (2022). A Study on the Role of Criminal Law in Metaverse. Institute for Legal Studies Chonnam National University, 42(3): 177-202.

Majeed, M. M. F., Adisaputera, A., & Ridwan, M. (2020). Digital Identity. Konfrontasi: Jurnal Kultural, Ekonomi, dan Perubahan Sosial, 7(4): 246-252.

Mappaselleng, N. F., & Kadir, Z. K. (2018). Rethinking Cyber Crime. Yogyakarta: Arti Bumi Intaran.

Mappaselleng, N. F., & Kadir, Z. K. (2023). Ilmu Hukum Pidana 101. Yogyakarta: Arti Bumi Intaran.

Mitrushchenkova. (2022). Personal Identity in the Metaverse: Challenges and Risks. Kutafin Law Review, 9(4): 793-817.

Oleksii, K., Oleksii, D., & Dmytro, Z. (2024). Metaverse: Ensuring Legal Recognition of Avatars and Electronic Personalities Through a Cross-Border Personalized ID-Code. International Jounal of Innovative Technologies in Social Science, 2(42): 1-5.

Permana, F. A., & Jamaluddin, A. (2023). Personal Data Vulnerability in the Digital Era: Study of Modus Operandi and Mechanisms to Prevent Phising Crimes. Jurnal Al-Hakim: Jurnal Ilmiah Mahasiswa, Studi Syariah, Hukum dan Filantropi, 5(2): 201-216.

Poulsen, S. V. (2021). Face Off: A Semiotic Technology Study of Software for Making Deepfakes. Sign Systems Studies, 49(3): 489-508.

Selvam, D., & Khanna, A. (2024). Enhancing Utility Sector Efficiency and Security: Integrating Digital Identity System Amidst Privacy and Ransomware Challenges. International Journal of Advanced Research in Science, Communication and Technology, 4(1): 759-772

Syarif, M., Ramadhani, R., Graha, M. A. W., Yanuaria, T., Muhtar, M. H., Asmah, N., ... & Jannah, M. (2024). Metode Penelitian Hukum.

Tantimin, Febriyani, E., Agustianto, Hutauruk, R. H. (2024). Defining Legal Contours of Digital Identity Theft. Jurnal Akta, 11(3): 1044-1059.

Wu, H., & Zhang, W. (2023). Digital Identity, Privacy Security, and Their Legal Safeguard in the Metaverse. Security and Safety, 2(1): 1-14.

Yeoh, P. (2019). Artificial Intelligence: Accelerator or Panaceo for Financial Crime? Journal of Financial Crime, 26(2): 634-646.

Zare, A., & Jalali, A. (2024). A Perspective Metaverse Paradigm Based on the Reality-Virtuality Continuum and Digital Twins. Recent Advances in Computer Science and Communications, 18(1): 1-19.

Conflict of Interest Statement:

The author declares that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.