MASALAH-MASALAH HUKUM
p-ISSN : 2086-2695 e-ISSN : 2527-4716
Diterbitkan oleh Fakultas Hukum Universitas Diponegoro Semarang

JURNAL MASALAH-MASALAH HUKUM
Tersedia online di https://ejournal.undip.ac.id/index.php/mmh/
Volume 53, Nomor 1, Maret 2024

STRATEGI PENANGGULANGAN KEJAHATAN EKONOMI BERBASIS TEKNOLOGI: STUDI KOMPARATIF ANTARA INDONESIA, AMERIKA, DAN EROPA

Dian Alan Setiawan
Fakultas Hukum, Universitas Islam Bandung
Jalan Taman Sari No. 24-26, Kota Bandung, Jawa Barat 40116, Indonesia
dian.alan@unisba.ac.id

Abstract

Technology-based economic crime is a significant threat in the era of digital transformation and global trade. This research aims to develop the concept of overcoming technology-based crime with a multi-faceted macro strategy. This research uses a normative juridical research method with a comparative approach; the results of the study show the importance of a systemic approach involving social, cultural, economic, technological, political, and legal aspects. Comparisons between the approaches applied in America, Europe, and Indonesia show significant differences in regulation, collaboration, and technology implementation. In Indonesia, the main challenges include adaptive regulation, digital security infrastructure, and people's digital literacy. This research emphasizes the need for an integrated, multi-faceted strategy to deal with the complexities of technology-based crime in a global context.

Keywords: *Technology-Based Economic Crime; Digital Transformation; Systemic Approach; Global Comparison.*

Abstrak

Kejahatan ekonomi berbasis teknologi merupakan ancaman signifikan di era transformasi digital dan perdagangan global. Penelitian ini bertujuan untuk mengembangkan konsep penanggulangan kejahatan berbasis teknologi dengan strategi makro yang bersifat multiaspek. Penelitian ini menggunakan metode penelitian yuridis normatif dengan pendekatan komparatif, hasil studi menunjukkan pentingnya pendekatan sistemik yang melibatkan aspek sosial, budaya, ekonomi, teknologi, politik, dan hukum. Komparasi antara pendekatan yang diterapkan di Amerika, Eropa, dan Indonesia menunjukkan perbedaan signifikan dalam regulasi, kolaborasi, dan implementasi teknologi. Di Indonesia, tantangan utama meliputi regulasi yang adaptif, infrastruktur keamanan digital, dan literasi digital masyarakat. Penelitian ini menekankan perlunya strategi multiaspek yang terintegrasi untuk menghadapi kompleksitas kejahatan berbasis teknologi dalam konteks global.

Kata kunci: Kejahatan Ekonomi Berbasis Teknologi; Transformasi Digital; Pendekatan Sistemik; Perbandingan Hukum.

A. Pendahuluan

Transformasi global merupakan arus perubahan terbesar dalam abad modern yang tidak bisa dihindari. Perubahan-perubahan yang dibawa oleh arus globalisasi membawa dampak yang dapat bersifat positif maupun negatif (Sudjito et al., 2016). Pada konteks ini, jaringan telekomunikasi

dan komputer memungkinkan konektivitas global, sehingga suara dan data digital dapat ditransfer melintasi perbatasan negara (Colarik, 2006) Oleh karena itu, perkembangan pesat dalam teknologi informasi dan komunikasi, khususnya internet, telah memberikan dampak positif yang besar dalam berbagai bidang kehidupan manusia. Namun, di balik manfaat tersebut, terdapat pula dampak negatif (*dark side*) yang muncul seiring dengan penggunaan internet yang semakin luas (Wisnusubroto, 2010). Salah satu dampak negatif yang ditimbulkan oleh proses globalisasi adalah munculnya kejahatan-kejahatan yang berdimensi global, seperti penyelundupan, pembajakan (*piracy*/h*ijacking*), pencucian uang (*money laundering*), perdagangan orang (*human trafficking*), terorisme, dan kejahatan siber (*cybercrime*).

Menurut Sutherland dalam upaya pencegahan kejahatan yang paling efektif adalah memberikan perlindungan kepada masyarakat dari bahaya kejahatan. Perlindungan ini dapat dilakukan dengan beberapa cara, antara lain mengubah perilaku pelaku kejahatan melalui metode yang bermanfaat, serta mengisolasi mereka yang tidak dapat diperbaiki. Selain itu, penting untuk menjauhkan individu yang terbukti memiliki kecenderungan tinggi untuk melakukan kejahatan atau bersikap agresif, serta menghilangkan lingkungan sosial yang mendorong terjadinya tindak kriminal. Sutherland menekankan bahwa reformasi ini tidak hanya ditujukan kepada residivis, tetapi juga kepada narapidana lainnya, dengan harapan mereka tidak mengulangi kejahatan di masa depan (Sambas & Andriasari, 2019).

Bernes dan Teeters menyatakan bahwa salah satu cara terbaik untuk mengantisipasi kejahatan adalah dengan memperhatikan kebutuhan sosial dan ekonomi yang dapat memengaruhi perilaku individu. Fokus utama adalah pada individu yang memiliki potensi berbuat jahat atau yang tidak terintegrasi dalam masyarakat akibat masalah biologis, psikologis, atau kurangnya kesempatan sosial ekonomi. Oleh karena itu, perbaikan di bidang sosial dan ekonomi menjadi syarat penting dalam mewujudkan pencegahan kejahatan yang efektif, sementara aspek biologis, psikologis, serta faktor *opportunity of criminal* dianggap sebagai faktor subsider.

Penelitian sebelumnya yang dilakukan oleh Setiawan et al. (2021) dengan judul "*Legal Strategy of Treating Telematics Crime in the Field Of Electronic Transactions In Global Trade*" yang menganalisis strategi hukum dalam penanggulangan kejahatan telematika di bidang transaksi elektronik di era perdagangan global. Penelitian tersebut berfokus pada kompleksitas permasalahan yang muncul akibat pesatnya perkembangan telematika, khususnya dalam pemanfaatan media transaksi melalui teknologi informasi yang terus berkembang tanpa diimbangi dengan keberadaan hukum yang memadai, seperti *cyber law*. Relevansi topik tersebut dengan teori *crime prevention* adalah bahwa upaya pencegahan kejahatan yang efektif harus memberikan perlindungan kepada masyarakat dari ancaman kejahatan dengan mengedepankan pendekatan yang bersifat non-punitif, yaitu melalui rehabilitasi pelaku dan pencegahan kejahatan di masa depan.

Penelitian ini memiliki perbedaan fokus, yaitu lebih menitikberatkan pada kejahatan ekonomi berbasis teknologi dalam konteks global. Penelitian ini bertujuan untuk mengembangkan konsep penanggulangan kejahatan berbasis teknologi dengan strategi makro yang bersifat multiaspek. Penelitian ini berfokus pada pengembangan kerangka kerja komprehensif untuk menanggulangi kejahatan siber yang kompleks. Pendekatan multidisiplin akan mengintegrasikan analisis makroekonomi, sosial, hukum, dan teknologi guna merumuskan strategi jangka panjang yang efektif. Urgensi penelitian ini terletak pada pentingnya kesadaran para pengambil kebijakan dan pemangku kepentingan dalam mengadopsi strategi makro yang holistik dalam menghadapi kejahatan ekonomi berbasis teknologi. Diharapkan dapat tercipta kebijakan yang lebih komprehensif dalam mengantisipasi dan menanggulangi kriminalitas di era ekonomi digital yang terus mengalami pertumbuhan yang pesat.

B. Metode Penelitian

Metode yang diterapkan dalam penelitian ini adalah yuridis normatif, Penelitian yuridis normatif merupakan penelitian hukum doktrinal yang berfokus pada kajian terhadap penerapan norma-norma hukum yang ada dalam sistem hukum positif. Pendekatan yang diterapkan dalam masalah ini meliputi pendekatan perundang-undangan (*statute approach*), pendekatan konseptual (*conceptual approach*), dan pendekatan komparatif (*comparative approach*) (Marzuki, 2010) Penelitian ini menganalisis secara lebih mendalam mengenai upaya penanggulangan kejahatan berbasis teknologi pada zaman transformasi digital yang memerlukan konsep yang bersifat multiaspek serta membandingkan aturan atau kebijakan suatu negara dengan aturan-aturan dari satu atau lebih negara lain mengenai penanggulangan kejahatan ekonomi berbasis teknologi .

Pengumpulan data dalam penelitian hukum normatif dilakukan dengan cara studi pustaka berupa data sekunder sebagai bahan dasar untuk diteliti dengan cara mengadakan penelusuran terhadap peraturan-peraturan dan literatur-literatur lain berkaitan dengan permasalahan yang diteliti atau sering disebut sebagai penelitian hukum kepustakaan (Soekanto & Mamudji, 2015).

C. Hasil dan Pembahasan

1. Analisis Upaya Penanggulangan Kejahatan Berbasis Teknologi Pada Era Perekonomian Global yang Bersifat Multiaspek

Analisis ekonomi dalam pencegahan kejahatan mencakup pendekatan untuk memahami bagaimana faktor-faktor ekonomi berperan dalam mendorong atau mengurangi tingkat kejahatan. Dalam hal ini, pencegahan kejahatan dapat dilihat sebagai investasi jangka panjang yang berhubungan dengan peningkatan kesejahteraan masyarakat, stabilitas sosial, dan pertumbuhan ekonomi. Pentingnya keberadaan program pencegahan kejahatan tersebut tidak dapat diremehkan, karena pencegahan kejahatan meningkatkan keselamatan publik, memajukan keadilan sosial, dan berkontribusi pada pembangunan berkelanjutan. Namun, di era meningkatnya biaya peradilan pidana dan prioritas yang saling bersaing ini, pemilihan, implementasi, perluasan, dan kelanjutan program pencegahan kejahatan telah mendapat perhatian lebih ketat, dan telah mendorong minat baru dalam "akuntabilitas berbasis hasil" dan bukti "apa yang berhasil". Oleh karena itu, ada peningkatan kesadaran dan pengakuan di antara para peneliti, pembuat kebijakan, dan praktisi bahwa program pencegahan kejahatan harus berbasis bukti, yaitu, didasarkan pada penelitian ilmiah yang menunjukkan strategi mana yang berhasil dan tidak berhasil untuk mencegah kejahatan (Byrne & Marx, 2011).

Keamanan siber (*cybersecurity*) dan pencegahan kejahatan siber (*cybercrime*) memiliki dimensi ekonomi yang signifikan. Kejahatan siber tidak hanya merusak data atau reputasi individu dan organisasi, tetapi juga memiliki dampak luas terhadap perekonomian, baik pada tingkat mikro (individu, perusahaan) maupun makro (ekonomi negara) (Ardiyanti, 2014). Kejahatan siber menimbulkan dampak finansial yang besar terhadap individu, perusahaan, dan negara. Kerugian akibat kejahatan siber dapat mencakup kerugian langsung maupun tidak langsung, yang dapat mempengaruhi ekonomi secara keseluruhan. Termasuk pencurian dana melalui peretasan rekening bank, penipuan online, dan peretasan kartu kredit. Misalnya, serangan ransomware yang mengenkripsi data dan menuntut tebusan dapat menyebabkan kerugian langsung yang signifikan bagi perusahaan dan individu.

Pencegahan kejahatan siber memerlukan investasi yang signifikan dalam teknologi, pelatihan, dan infrastruktur. Namun, meskipun pencegahan ini membutuhkan biaya awal yang tinggi, potensi kerugian yang dapat dihindari jauh lebih besar. Oleh karena itu, dari perspektif ekonomi, alokasi sumber daya untuk pencegahan kejahatan siber harus dipandang sebagai investasi jangka panjang (McIntosh & Li, 2012). Perusahaan dan organisasi perlu mengalokasikan anggaran untuk membeli perangkat lunak keamanan terbaru, memperbarui sistem, dan mengimplementasikan solusi berbasis teknologi canggih seperti enkripsi, firewall, dan deteksi intrusi otomatis. Teknologi AI

dan machine learning dapat membantu memonitor dan mendeteksi ancaman secara real-time, memungkinkan respon yang cepat terhadap potensi serangan.

Tamara Hubanova et al. (2021) menyatakan bahwa pencegahan kejahatan adalah upaya dan pengaruh yang ditargetkan dari subjek tertentu terhadap objek-objek kriminogenik spesifik, yang bersama dengan faktor-faktor lain (determinasi), mampu menciptakan fenomena yang menyebabkan kejahatan, motivasi kriminal, dan perilaku kriminal. Langkah-langkah pencegahan kejahatan mengaktifkan faktor-faktor anti-kriminogenik, di mana pengaruhnya secara bertahap menghilangkan determinasi kejahatan dan mencegah (mengurangi) manifestasi kriminal yang ditimbulkannya.

Faktor ekonomi atau lebih spesifiknya adalah sistem perekonomian berkorelasi positif terhadap berkembangnya kejahatan bisnis/ekonomi. Arus globalisasi yang cenderung menyeret sistem perekonomian pada ekonomi liberal dan kapitalis seringkali memaksa teknologi bermain dalam hukum pasar (Fakih, 2003). Secara nasional, terdapat sejumlah tantangan dalam membangun sistem keamanan siber yang efektif, antara lain kurangnya pemahaman di kalangan penyelenggara negara dan pihak terkait mengenai dunia siber, yang mengharuskan adanya pembatasan penggunaan layanan dengan server yang berlokasi di luar negeri serta penerapan sistem yang lebih aman. Selain itu, belum ada regulasi yang memadai untuk menangani serangan siber, tata kelola keamanan siber yang masih terfragmentasi dan kurang terkoordinasi, serta keterbatasan industri dalam memproduksi dan mengembangkan perangkat keras (*hardware*) yang berkaitan dengan teknologi informasi (Ardiyanti, 2014). Salah satu aspek teknologi dalam penanggulangan kejahatan saat ini, yaitu dengan menggunakan kecerdasan buatan atau *artificial intelligence* (AI) yang telah diprogram untuk berpikir dan meniru perbuatan manusia. Hal ini kemudian dimanfaatkan dalam bidang keamanan untuk mengumpulkan, menyaring, dan mengelola data yang terdapat dalam ruang informasi. Diharapkan langkah ini dapat meningkatkan kinerja kepolisian secara optimal, dengan pendekatan yang berkualitas, tepat waktu, dan efektif dalam memastikan keamanan nasional serta melindungi masyarakat. (Radulov N., 2019)

Terdapat berbagai metode yang dapat dimanfaatkan untuk mengaplikasikan AI dalam penanggulangan kejahatan, di antaranya melalui pengumpulan data, deteksi tindak pidana, pencegahan kejahatan siber, dan lain-lain. AI diyakini dapat membantu organisasi dalam mencegah kejahatan siber dengan melatih sistem untuk mengenali kata kunci atau topik yang terkait dengan konten berbahaya, yang kemudian digunakan untuk mendeteksi dan menghentikan potensi serangan siber (Radulov N., 2019). Namun, keterikatan Indonesia dengan sistem ekonomi global tidak serta merta melibas habis ideologi Ekonomi Indonesia (Ekonomi Pancasila) yang berkeadilan sosial. Dalam kaitannya dengan upaya penanggulangan kejahatan ekonomi berteknologi maka pengembangan sistem perekonomian dan teknologi penunjangnya seharusnya tidak hanya mementingkan aspek prospek yang berkaitan dengan profit atau hanya semata-mata berdasarkan keinginan/kepentingan pemilik modal saja, tetapi juga harus memperhatikan kepentingan masyarakat luas. Berkaitan dengan hal tersebut maka setiap pengembangan sistem ekonomi dan teknologi pendukungnya harus diimbangi dengan pengembangan sistem penanggulangan terhadap eksesnya. Dalam istilah lain, perlu ada pengembangan sistem penanggulangan kejahatan ekonomi berbasis teknologi dengan pendekatan "*Economic Prevention*" atau "*Techno Prevention*" (Arief, 2001).

Pemerintah perlu menerapkan kebijakan dan regulasi yang mendukung pencegahan kejahatan siber. Ini termasuk peraturan terkait perlindungan data pribadi (seperti GDPR di Eropa), pengawasan dunia maya, dan sistem peringatan dini untuk serangan siber. Pencegahan kejahatan siber adalah langkah ekonomi yang sangat penting, baik untuk perusahaan individu, sektor industri, maupun perekonomian negara secara keseluruhan (Prahassacitta, 2019). Meskipun membutuhkan biaya untuk implementasi dan pengelolaan sistem keamanan siber, biaya tersebut jauh lebih kecil dibandingkan dengan kerugian yang dihasilkan oleh serangan siber. Oleh karena itu, investasi dalam teknologi keamanan, pelatihan, serta kebijakan yang mendukung pencegahan

kejahatan siber harus dipandang sebagai langkah strategis untuk melindungi integritas ekonomi dan keberlanjutan pasar dalam

Penanggulangan kejahatan berbasis teknologi di Indonesia berlandaskan pada beberapa prinsip filosofis yang mencerminkan nilai-nilai keadilan, perlindungan hak asasi manusia, dan tanggung jawab negara dalam menjaga ketertiban sosial. Prinsip-prinsip ini membentuk dasar dari kebijakan dan strategi yang diterapkan dalam mengatasi kejahatan siber dan ekonomi berbasis teknologi. Pancasila, sebagai dasar negara Indonesia, menjadi landasan filosofi utama dalam berbagai kebijakan negara, termasuk dalam penanggulangan kejahatan berbasis teknologi. Indonesia menganut prinsip negara hukum yang tertuang dalam Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 (UUD NRI 1945) yang menegaskan bahwa negara Indonesia adalah negara yang berdasarkan hukum. Penanggulangan kejahatan berbasis teknologi di Indonesia harus dilandasi oleh supremasi hukum, di mana segala kebijakan dan tindakan penegakan hukum terkait teknologi harus berdasarkan pada hukum yang sah dan adil (Nahak, 2017).

Dalam konteks penanggulangan kejahatan berbasis teknologi, prinsip keadilan sosial menekankan pentingnya pemerataan akses terhadap teknologi yang aman, serta perlindungan terhadap kelompok rentan dari potensi eksploitasi atau kerugian akibat kejahatan berbasis teknologi. Sebagai negara berdaulat, Indonesia memiliki hak untuk mengatur dan melindungi ruang digitalnya, baik dari ancaman domestik maupun internasional. Penanggulangan kejahatan berbasis teknologi berkaitan dengan kemampuan negara untuk memastikan bahwa ruang digital tetap aman, baik untuk individu maupun untuk perekonomian digital secara keseluruhan. Kejahatan berbasis teknologi sering kali bersifat lintas batas negara. Oleh karena itu, penanggulangan kejahatan tersebut memerlukan kerjasama internasional yang erat. Indonesia, sebagai bagian dari komunitas internasional, perlu menjalin kerjasama dengan negara lain dan organisasi internasional dalam hal pertukaran informasi dan penegakan hukum terhadap kejahatan digital yang melibatkan pelaku di luar negeri. Dengan memadukan prinsip-prinsip ini, Indonesia dapat membangun sistem yang lebih baik dalam melawan kejahatan berbasis teknologi, memastikan perlindungan hak-hak individu, dan menjaga stabilitas ekonomi digital.

Penanggulangan kejahatan berbasis teknologi tidak hanya melibatkan dimensi teknis dan hukum, tetapi juga berkaitan erat dengan kondisi sosial yang melatarbelakangi kejahatan dan dampaknya terhadap masyarakat. Dalam perspektif sosiologi, penanggulangan kejahatan berbasis teknologi dilihat sebagai bagian dari upaya untuk memahami dan mengatasi faktor-faktor sosial yang memengaruhi terjadinya kejahatan, serta bagaimana teknologi dapat diterapkan untuk menciptakan perubahan sosial yang positif. Teori strain, yang dikembangkan oleh Robert Merton, menyatakan bahwa kejahatan sering kali muncul sebagai akibat dari ketegangan atau tekanan yang dialami oleh individu dalam masyarakat, terutama ketika mereka tidak dapat mencapai tujuan sosial yang diinginkan melalui cara yang sah (Manullang, 2023). Dalam konteks penanggulangan kejahatan berbasis teknologi, teori ini memberikan landasan untuk memahami bahwa teknologi dapat digunakan untuk mengurangi atau mengatasi ketegangan sosial tersebut. Teori Belajar Sosial (*Social Learning Theory*). Teori yang dikemukakan oleh Albert Bandura, berpendapat bahwa kejahatan sering kali terjadi karena individu belajar perilaku kriminal melalui interaksi sosial dengan orang lain yang terlibat dalam aktivitas kriminal (Wahyun & Fitriani, 2022). Dalam dunia yang semakin digital, teknologi memiliki potensi untuk memainkan peran besar dalam memodifikasi proses sosial ini. Teori Anomi (*Anomie Theory*) yang dikembangkan oleh Émile Durkheim menjelaskan bahwa kejahatan dapat muncul ketika ada ketidakcocokan antara tujuan masyarakat dan cara yang sah untuk mencapainya (Indahni et al., 2022). Dalam masyarakat modern, teknologi bisa menjadi faktor yang meningkatkan atau mengurangi ketegangan ini. Landasan sosiologis penanggulangan kejahatan berbasis teknologi menggambarkan bagaimana faktor-faktor sosial, budaya, dan struktural dapat memengaruhi terjadinya kejahatan, serta bagaimana teknologi dapat digunakan untuk menciptakan interaksi sosial yang lebih positif dan

mencegah kejahatan. Teknologi tidak hanya digunakan sebagai alat untuk mengawasi atau menghukum, tetapi juga sebagai sarana untuk memberdayakan masyarakat, membangun norma sosial yang positif, dan mengurangi ketegangan sosial yang menjadi penyebab kejahatan.

Kejahatan siber (*cybercrime*) adalah tindakan yang melanggar hukum yang dilakukan melalui media internet, dengan memanfaatkan teknologi canggih, komputer, dan telekomunikasi, baik untuk tujuan memperoleh keuntungan maupun tidak, yang pada akhirnya merugikan pihak lain. (Marufah et al., 2020). Kejahatan ini mencakup berbagai jenis tindakan ilegal yang berkaitan dengan pelanggaran terhadap kerahasiaan, integritas, dan keberadaan data serta sistem komputer (Chintia et al., 2018). Kejahatan siber (*cybercrime*) muncul akibat tindakan menyimpang dari pengguna media sosial yang memanfaatkan platform tersebut untuk tujuan yang merugikan dalam berbagai aspek kehidupan masyarakat (Djanggih & Hipan, 2018). Perkembangan ini memberikan dampak pada kehidupan sosial masyarakat, sementara di sisi lain, kemajuan yang dicapai juga turut memunculkan berbagai jenis kejahatan (Kristiani, 2014)

Dari sudut pandang sosiologis, kejahatan merupakan gejala sosial yang melibatkan interaksi antara individu dan masyarakat (Hartanto, 2015). Secara sosiologis, globalisasi telah mempengaruhi perilaku dan pola hidup masyarakat. Pengaruh tersebut tidak sebatas pada perubahan gaya hidup yang semakin serupa, tetapi juga membawa pergeseran pada sikap pandang terhadap nilai-nilai hidup. Kehadiran Teknologi Informasi dan Komunikasi (TIK) sebagai 'anak' sekaligus 'motor' transformasi global di abad modern ini telah mengubah masyarakat dengan menggoyangkan 'akar' institusionalnya, yaitu kehidupan antarpribadi manusia yang paling dasar di tempat kerja dan di dalam keluarga (Endeshaw, 2007). Beberapa gaya hidup global yang dipandang sebagai perilaku negatif antara lain *individualism, consumerism, pragmatism*. *Liberalism dan free live* seringkali dapat memicu terjadinya kejahatan ekonomi di negara-negara berkembang. Perbuatan *carding* sebagai varian dari *hacking,* misalnya mengapa perbuatan tersebut marak terjadi di negara-negara seperti Indonesia, ukraina dan sebagaimana bukan terjadi di negara-negara maju seperti yang ada di Eropa Barat dan Amerika? Nampaknya gaya hidup barat yang melanda di negara berkembang (akibat globalisasi) tidak diimbangi dengan kesejahteraan masyarakat (untuk memenuhi) gaya hidup modern, etika, dan rasa tanggung jawab sosial untuk menjaga ketertiban.

Sistem sanksi sosial juga dikenal dalam masyarakat dunia maya. Di *blacklist*-nya *Netter* (dalam hal ini selaku konsumen Indonesia oleh berbagai *online shop* di luar negeri (khususnya Amerika), sehingga tidak bisa mengakses sistem order barang melalui *e-commerce,* merupakan salah satu contoh untuk menanggulangi merebaknya perbuatan *carding*. Hanya saja cara ini kurang efektif meningat para *carder* adalah *hacker* yang selalu tertantang untuk menerobos sistem. Berdasarkan hal tersebut maka perlu disusun kode etik bagi para pengguna dan sistem pengawasan serta mekanisme penegakannya. Kejahatan ekonomi berbasis teknologi merupakan ancaman serius era perdagangan global. Sekalipun di bidang perekonomian dan teknologi Indonesia masih tergolong negara berkembang atau setidaknya sebagai *Newly Industrialized Countries* (NIC), namun realitanya pemanfaatan teknologi informatika di dunia bisnis (*e-banking*, *e-commerce, e-government*) telah diadaptasi secara penuh di Indonesia. Penerapan teknologi tersebut tentu saja dengan segala konsekuensinya, termasuk ekses-eksesnya yang berupa kejahatan bisnis modern (kata lain dari kejahatan ekonomi berteknologi). Terhadap merebaknya kejahatan jenis baru tersebut. Sebenarnya selama ini Indonesia telah melakukan berbagai upaya penanggulangan antara lain dengan memproses hukum pelaku kejahatan ekonomi berbasis teknologi dengan hukum pidana yang berlaku, memperbaharui peraturan perundang-undangan di bidang perekonomian, hingga meningkatkan kualitas lembaga peradilan dan sumber daya manusianya. Meskipun demikian, upaya-upaya tersebut masih belum membuahkan hasil yang diharapkan secara optimal, terbukti dengan masih bermunculannya kejahatan-kejahatan ekonomi berbasis teknologi. Bahkan kejahatan-kejahatan tersebut menunjukkan perkembangan baik kuantitasnya maupun kualitasnya.

2. Komparasi Penanggulangan Kejahatan Ekonomi Berbasis Teknologi di Amerika dan Eropa sebagai Dampak dari Transformasi Global dalam Perekonomian

Keamanan ekonomi berbasis teknologi menjadi salah satu tantangan terbesar bagi negara-negara di dunia, termasuk Amerika Serikat. Di Amerika Serikat, penanggulangan kejahatan ekonomi berbasis teknologi melibatkan kerjasama antara sektor publik (pemerintah) dan sektor swasta, serta didukung oleh regulasi yang ketat, teknologi canggih, serta lembaga penegak hukum**.** Amerika Serikat miliki berbagai langkah proaktif untuk menangani kejahatan berbasis teknologi melalui lembaga-lembaga seperti FBI, *Federal Trade Commission* (FTC), dan Departemen Kehakiman (DOJ). Negara ini menerapkan peraturan yang ketat terkait kejahatan siber, termasuk *Cybersecurity Information Sharing Act* (CISA) dan *California Consumer Privacy Act* (CCPA). Selain itu, Amerika Serikat secara rutin melakukan operasi internasional untuk mengatasi kejahatan dunia maya dengan bekerja sama dengan organisasi global seperti INTERPOL dan Europol. Menurut kajian Penulis, Negara ini cenderung mengutamakan regulasi hukum yang lebih maju dan penggunaan teknologi. Fokus utama mereka adalah pada pemantauan dan pencegahan melalui regulasi yang ketat terhadap sektor teknologi, serta investasi besar dalam penelitian keamanan siber (Triwahyuni & Wulandari, 2016). Penanggulangan kejahatan teknologi di AS juga mencakup pengembangan kecerdasan buatan (AI) dan pembelajaran mesin untuk mendeteksi ancaman secara lebih efektif.

Amerika Serikat memiliki berbagai peraturan yang mengatur kejahatan ekonomi berbasis teknologi, dengan fokus pada perlindungan data, sistem keuangan, serta transparansi ekonomi digital. Beberapa aturan yang penting adalah: *The Computer Fraud and Abuse Act* (CFAA**)** CFAA adalah salah satu undang-undang utama di AS yang mengatur kejahatan berbasis komputer, termasuk pencurian data, penipuan online, serta penggunaan perangkat teknologi untuk meretas dan mengakses sistem keuangan tanpa izin. Dalam konteks kejahatan ekonomi, CFAA digunakan untuk menuntut tindakan ilegal yang melibatkan pencurian data pribadi atau informasi finansial yang digunakan untuk penipuan. Selain itu, *The Electronic Fund Transfer Act* (EFTA) EFTA mengatur transaksi elektronik yang melibatkan transfer dana, seperti ATM, kartu kredit, dan transfer bank online. Kejahatan ekonomi yang melibatkan transaksi yang tidak sah atau penipuan menggunakan instrumen pembayaran elektronik seringkali dihukum berdasarkan undang-undang ini. Anti-*Money Laundering (AML) & Know Your Customer* (KYC) *Regulations* Kejahatan ekonomi berbasis teknologi sering kali melibatkan pencucian uang, yang dapat dilakukan melalui transaksi keuangan anonim atau jaringan digital. Regulasi AML dan KYC mengharuskan lembaga keuangan untuk melakukan verifikasi identitas nasabah dan melaporkan aktivitas yang mencurigakan. Regulasi ini juga berfokus pada pemantauan transaksi yang dapat menunjukkan adanya aktivitas ilegal.

Amerika Serikat membentuk sejumlah badan penegak hukum dan lembaga terkait yang berfokus pada penanggulangan kejahatan ekonomi berbasis teknologi. *Federal Bureau of* Investigation (FBI) FBI memiliki divisi khusus yang menangani kejahatan berbasis teknologi, termasuk penipuan keuangan dan cybercrime yang melibatkan penggunaan teknologi untuk mencuri uang atau data. FBI bekerja dengan sektor swasta dan lembaga internasional dalam memerangi kejahatan ekonomi berbasis teknologi yang sering kali bersifat lintas batas. Kemudian ada U.S. *Secret Service* berfokus pada kejahatan yang melibatkan peredaran uang palsu, pencurian identitas, serta penipuan kartu kredit yang memiliki peran penting dalam melindungi infrastruktur sistem pembayaran dan sistem keuangan digital yang dapat menjadi sasaran serangan.

Kerjasama antara pemerintah dan sektor swasta sangat penting dalam menghadapi kejahatan ekonomi berbasis teknologi, yang sering kali melibatkan organisasi besar atau teknologi yang kompleks. *Public-Private Partnerships* (PPP) Pemerintah AS bekerja sama dengan perusahaan teknologi dan keuangan untuk meningkatkan keamanan sistem pembayaran elektronik dan mencegah penipuan. Salah satu contohnya adalah *Cybersecurity and Infrastructure Security Agency* (CISA), yang bekerja dengan sektor swasta untuk meningkatkan proteksi terhadap sistem

kritis ekonomi dan finansial, serta mengidentifikasi ancaman ekonomi berbasis teknologi (Nugroho, 2018).

Penggunaan teknologi dalam penanggulangan kejahatan ekonomi berbasis teknologi sangat penting, mengingat sifat ancaman yang semakin kompleks dan terdistribusi. Teknologi *Blockchain Blockchain* memiliki potensi untuk mengurangi kejahatan berbasis teknologi yang terkait dengan transaksi finansial, termasuk penipuan dan pencucian uang. Penggunaan blockchain dalam sektor keuangan memberikan transparansi dan keamanan yang lebih tinggi dalam transaksi digital. Kecerdasan Buatan (AI) dan Pembelajaran Mesin AI dan pembelajaran mesin digunakan untuk mendeteksi pola-pola transaksi yang mencurigakan atau abnormal, seperti yang terjadi dalam penipuan kartu kredit atau penggelapan dana. Algoritma cerdas dapat membantu mendeteksi potensi kejahatan sebelum kerusakan yang lebih besar terjadi. Biometrik dan Otentikasi Multifaktor Penggunaan otentikasi biometrik (sidik jari, pengenalan wajah) dan otentikasi multifaktor (MFA) dapat mengurangi risiko pencurian identitas dan penipuan terkait transaksi elektronik.

Keamanan ekonomi berbasis teknologi di Eropa menjadi isu yang semakin mendesak seiring dengan perkembangan ekonomi digital yang pesat. Uni Eropa mengeluarkan peraturan seperti *General Data Protection Regulation* (GDPR) yang mengatur perlindungan data pribadi dan keamanan informasi yang mengharuskan perusahaan untuk melindungi data pribadi warganegara Uni Eropa. Meskipun berfokus pada privasi, GDPR juga memainkan peran penting dalam penanggulangan kejahatan berbasis teknologi, seperti pencurian identitas atau peretasan data pribadi. Pelanggaran terhadap GDPR dapat mengakibatkan denda yang sangat besar, yang memberi insentif kuat bagi perusahaan untuk memperkuat sistem keamanan mereka. Penulis berpendapat bahwa strategi Uni Eropa lebih mengutamakan kerja sama antar negara anggota dan fokus pada penyelarasan kebijakan dalam menghadapi kejahatan berbasis teknologi.

Penanggulangan kejahatan ekonomi berbasis teknologi di Eropa melibatkan berbagai lembaga yang bekerja untuk mengidentifikasi, menyelidiki, dan menuntut pelaku kejahatan, serta melindungi sistem keuangan dan data pribadi warga negara. *Europol dan European Cybercrime Centre* (EC3) EC3 berfokus pada penanggulangan kejahatan ekonomi berbasis teknologi di seluruh Eropa. Sebagai bagian dari Europol, EC3 mendukung negara-negara anggota dalam menyelidiki kejahatan siber yang melibatkan penipuan finansial, perdagangan ilegal data pribadi, dan serangan terhadap sistem pembayaran atau infrastruktur kritis. Selain itu, *National Data Protection Authorities* memiliki otoritas perlindungan data yang bertugas untuk menegakkan kepatuhan terhadap GDPR dan melindungi data pribadi warga negara dari penyalahgunaan dan kejahatan berbasis teknologi. Otoritas ini juga menangani keluhan individu yang merasa datanya telah disalahgunakan atau diakses tanpa izin. Mengingat sifat kejahatan ekonomi berbasis teknologi yang sering kali melibatkan pelaku lintas negara, kerjasama internasional sangat penting dalam penanggulangan kejahatan ini.

Penggunaan teknologi sangat penting dalam penanggulangan kejahatan ekonomi berbasis teknologi. *Blockchain* digunakan dalam sektor keuangan untuk menyediakan transparansi dan keamanan yang lebih tinggi dalam transaksi digital. Teknologi ini juga digunakan untuk mencegah pencucian uang dan penipuan dalam transaksi berbasis *cryptocurrency* (Anisah & Riyanto, 2022). Banyak negara Eropa mulai memanfaatkan *blockchain* untuk memperbaiki keamanan sistem pembayaran dan transparansi dalam transaksi digital. Kecerdasan Buatan (AI) dan Pembelajaran Mesin *(Machine Learning)* AI dan pembelajaran mesin digunakan untuk menganalisis pola transaksi yang mencurigakan atau abnormal, seperti dalam kasus penipuan kartu kredit atau perdagangan ilegal. Teknologi ini membantu lembaga keuangan dan penegak hukum untuk mendeteksi dan mengidentifikasi ancaman lebih cepat, serta meningkatkan respon terhadap potensi kejahatan ekonomi berbasis teknologi. Otentikasi Multifaktor dan Keamanan Digital Otentikasi multifaktor (MFA) digunakan untuk meningkatkan keamanan transaksi finansial online dan mengurangi risiko penipuan. Bank dan lembaga keuangan di Eropa menerapkan sistem MFA

untuk memastikan bahwa hanya individu yang sah yang dapat mengakses akun atau melakukan transaksi. Eropa memiliki serangkaian kebijakan dan lembaga yang berfokus pada perlindungan data, sistem pembayaran, dan integritas pasar, sambil mendukung edukasi dan kesadaran publik tentang potensi ancaman yang ada.

Dari komparasi beberapa negara di Amerika dan Eropa seperti tersebut di atas dapat terlihat bahwa penanggulangan kejahatan berbasis teknologi di berbagai negara sangat dipengaruhi oleh transformasi global dalam bidang perekonomian dan kemajuan teknologi. Negara-negara maju seperti AS dan Uni Eropa cenderung memiliki regulasi yang lebih ketat dan terintegrasi untuk menghadapi kejahatan berbasis teknologi, dengan fokus pada perlindungan data pribadi dan keamanan siber. Masing-masing negara mengadopsi pendekatan yang sesuai dengan kondisi sosial, ekonomi, dan politik mereka, dengan fokus yang berbeda pada regulasi, kolaborasi internasional, dan penguatan infrastruktur teknologi. Pendekatan makro dan multiaspek, yang menggabungkan kebijakan ekonomi, sosial, hukum, dan teknologi, akan menjadi kunci utama dalam menciptakan solusi yang efektif untuk menangani kejahatan berbasis teknologi secara global.

Dengan semakin berkembangnya teknologi dan ekonomi digital, Indonesia menghadapi tantangan besar dalam penanggulangan kejahatan ekonomi berbasis teknologi. Kejahatan ini mencakup berbagai bentuk, mulai dari penipuan finansial online, pencurian identitas, manipulasi pasar, hingga pencucian uang melalui platform digital dan *cryptocurrency*. Meskipun Indonesia telah memiliki berbagai regulasi yang mengatur teknologi dan ekonomi digital, seperti Undang-Undang Informasi dan Transaksi Elektronik (ITE), Peraturan Perlindungan Data Pribadi (PDP), dan Regulasi terkait Pencucian Uang, namun regulasi ini masih menghadapi beberapa kendala dalam menghadapi cepatnya perubahan teknologi dan kompleksitas kejahatan yang terjadi sehingga Perlu adanya Pembaruan dan Penyesuaian Regulasi yang relevan dengan perkembangan teknologi dan praktik kejahatan ekonomi berbasis teknologi terbaru. Misalnya peraturan terkait penggunaan *cryptocurrency* dan transaksi digital di Indonesia masih sangat terbatas dan ambigu, sementara penggunaan teknologi ini semakin meningkat (Nabila et al., 2024).

Keamanan siber (*cybersecurity*) menjadi masalah besar dalam konteks kejahatan ekonomi berbasis teknologi. Di Indonesia, banyak sektor yang masih rentan terhadap ancaman serangan siber, baik dalam sektor perbankan, *e-commerce*, maupun sektor publik yang menyimpan data sensitif. Ancaman terhadap Infrastruktur Keuangan Digital seperti Bank, lembaga keuangan, dan sektor *e-commerce* yang semakin berkembang di Indonesia menjadi sasaran potensial bagi penjahat dunia maya. Masih banyak lembaga keuangan yang belum menerapkan standar keamanan siber yang memadai, termasuk enkripsi data dan otentikasi multifaktor yang efektif. Penggunaan *cryptocurrency* yang tidak diawasi dengan baik dapat membuka peluang untuk pencucian uang, penipuan investasi, dan aktivitas ilegal lainnya. Di Indonesia, regulasi terkait *cryptocurrency* masih dalam tahap pengembangan, dan banyak pihak yang belum sepenuhnya paham risiko yang ditimbulkan oleh teknologi ini.

Penyelesaian kejahatan ekonomi berbasis teknologi memerlukan kolaborasi yang erat antara berbagai pihak, baik pemerintah, lembaga penegak hukum, sektor swasta, serta masyarakat. Saat ini, koordinasi antara lembaga penegak hukum seperti Polri, Badan Siber dan Sandi Negara (BSSN), dan lembaga lain yang terkait dengan keamanan digital masih belum optimal. Oleh karena itu, kerjasama internasional sangat penting. Indonesia perlu meningkatkan peran serta dalam organisasi internasional seperti Interpol, ASEANAPOL, dan APEC untuk menangani kejahatan yang melintasi batas negara.

Untuk menghadapi tantangan tersebut, Indonesia perlu memperbaharui dan mengadaptasi regulasi untuk mengikuti perkembangan teknologi dan praktik kejahatan yang baru, seperti pencucian uang melalui *cryptocurrency* atau kejahatan siber yang melibatkan kecerdasan buatan (AI). Perlindungan terhadap infrastruktur digital yang kritis, seperti sistem pembayaran, data keuangan, dan data pribadi. Bank dan lembaga keuangan perlu meningkatkan penerapan otentikasi

multifaktor, enkripsi, dan pemantauan transaksi secara real-time. Dengan menerapkan langkah-langkah strategis ini, Indonesia dapat lebih siap menghadapi tantangan penanggulangan kejahatan ekonomi berbasis teknologi di masa depan.

Penulis menggunakan beberapa teori yang relevan, teori-teori ini dapat memberikan pandangan mendalam tentang penyebab, dampak, dan cara-cara untuk mengatasi tantangan penanggulangan kejahatan ekonomi berbasis teknologi di Indonesia Teori kriminalitas teknologi atau teori kejahatan dunia maya menjelaskan bagaimana perkembangan teknologi mengubah cara-cara tradisional dalam melakukan kejahatan, termasuk kejahatan ekonomi berbasis teknologi. Selain itu, Teori Kejahatan Terorganisir Transnasional (*Transnational Organized Crime Theory*). Teori ini menjelaskan kejahatan yang melibatkan pelaku lintas negara dan menggunakan teknologi untuk mengelabui atau menghindari sistem hukum. Dalam konteks kejahatan ekonomi berbasis teknologi, banyak tindakan kriminal yang melibatkan pelaku di luar Indonesia, misalnya dalam kasus penipuan investasi online, pencucian uang melalui *cryptocurrency*, atau peretasan sistem perbankan.

D. Simpulan dan Saran

Upaya penanggulangan kejahatan berbasis teknologi di era perekonomian global selama ini cenderung dilakukan secara parsial. Ketidakterpaduan antara kebijakan ekonomi, sosial, politik, budaya, dan hukum dalam pemanfaatan serta pengembangan teknologi tinggi di Indonesia menjadi salah satu penyebab utama. Pendekatan yang tidak terintegrasi ini menyebabkan upaya penanggulangan kejahatan ekonomi berbasis teknologi tidak efektif. Oleh karena itu, upaya penanggulangan kejahatan yang hanya berfokus pada satu aspek, seperti hukum, akan sulit mengatasi kejahatan berbasis teknologi yang semakin kompleks. Hal ini terutama relevan dalam konteks kejahatan ekonomi berteknologi yang merupakan produk dari ekses transformasi global di bidang ekonomi dengan dimensi yang multivarian. Secara obyektif, hukum pidana di Indonesia masih dapat digunakan sebagai sarana untuk menanggulangi *cybercrime*, namun memiliki keterbatasan signifikan.

Strategi global dalam mengatasi kejahatan ekonomi berbasis teknologi di era transformasi digital menunjukkan perbedaan pendekatan antara Indonesia, Amerika, dan Eropa. Amerika lebih mengutamakan penegakan hukum yang ketat dan regulasi berbasis teknologi canggih, sementara Eropa menekankan perlindungan data pribadi dan kolaborasi antarnegara melalui kebijakan seperti GDPR. Di Indonesia, tantangan utama terletak pada penguatan regulasi yang adaptif, infrastruktur keamanan digital yang lebih baik, serta peningkatan literasi digital masyarakat. Untuk itu, Indonesia perlu memperkuat kerjasama internasional, meningkatkan penegakan hukum, dan memperbarui regulasi agar dapat bersaing dengan strategi yang diterapkan oleh negara-negara maju. Masing-masing kebijakan harus dipandang sebagai bagian yang saling melengkapi untuk menghasilkan solusi yang utuh dan integral. Globalisasi, yang memengaruhi berbagai aspek kehidupan, menuntut adanya koordinasi antar-kebijakan agar penanggulangan kejahatan ekonomi berbasis teknologi dapat berjalan secara efektif.

DAFTAR PUSTAKA

Anisah, M., & Riyanto, S. (2022). Pengaturan tindak pidana pencucian uang (TPPU) melalui cryptocurrency di Indonesia: Studi perbandingan negara Amerika Serikat, Kanada, dan Australia (Skripsi). Universitas Gadjah Mada.

Ardiyanti, H. (2014). Cyber-Security dan Tantangan Pengembangannya di Indonesia. *Politica, 5*(1), 95–110. https://doi.org/10.22212/jp.v5i1.336

Arief, B. N. (2001). *Masalah Penegakan Hukum dan Kebijakan Penanggulangan Kejahatan*. Bandung: PT Citra Aditya Bakti.

Byrne, J., & Marx, G. (2011). Technological Innovations in Crime Prevention and Policing: A Review of the Research on Implementation and Impact. *Journal of Police Studies, 3*(20), 17–40. https://www.ojp.gov/ncjrs/virtual-library/abstracts/technological-innovations-crime-prevention-and-policing-review

Chintia, E., Nadiah, R., Ramadhani, H. N., Haedar, Z. F., & Febriansyah, A. (2018). Kasus Kejahatan Siber yang Paling Banyak Terjadi di Indonesia dan Penanganannya. *JIEET (Journal of Information Engineering and Educational Technology), 2*(2), 65–69. https://doi.org/10.26740/jieet.v2n2.p65-69

Colarik, A. M. (2006). *Cyber Terrorism: Political dnd Economic Implications*. USA: Idea Group Publishing.

Djanggih, H., & Hipan, N. (2018). Pertimbangan Hakim dalam Perkara Pencemaran Nama Baik Melalui Media Sosial (Kajian Putusan Nomor: 324/Pid./2014/Pn.Sgm). *Jurnal Penelitian Hukum De Jure, 18*(1), 93–102. https://doi.org/10.30641/dejure.2018.V18.93-102

Endeshaw, A. (2007). *Hukum E-Commerce dan Internet dengan Fokus di Asia Pasifik* (M. S. Purwandari, Ed.). Yogyakarta: Pustaka Pelajar.

Fakih, M. (2003). *Runtuhnya Teori Pembangunan dan Globalisasi*. Yogyakarta: Insist Press dan Pustaka Pelajar.

Hartanto, H. D. (2015). Tindak Pidana Terhadap Konflik Antar Kampung dalam Perspektif Hukum Pidana. *Lex Crimen, 4*(7), 148–156. Retrieved from https://ejournal.unsrat.ac.id/index.php/lexcrimen/article/view/10104

Hubanova, T., Shchokin, R., Hubanov, O., Antonov, V., Slobodianiuk, P., & Podolyaka, S. (2021). Information Technologies in Improving Crime Prevention Mechanisms in the Border Regions of Southern Ukraine. *Journal of Information Technology Management*, 75–90. https://doi.org/10.22059/jitm.2021.80738

Indahni, A., Cassanti, R., & Manalu, R. M. U. (2022). Memperdagangkan Alibi dalam Perkara Keterlibatan Korupsi Menggunakan Teori Anomie dari Emile Durkheim. *HUMAYA: Jurnal Hukum, Humaniora, Masyarakat, dan Budaya, 21*(2), 21–33. https://doi.org/10.33830/humaya_fhisip.v2i1.3201

Kristiani, M. D. (2014). Kejahatan Kekerasan Seksual (Perkosaan) Ditinjau dari Perspektif Kriminologi. *Jurnal Magister Hukum Udayana, 7*(3), 371–382. https://doi.org/10.24843/JMHU.2014.v03.i03.p02

Manullang, C. J. (2023). Analisis Teori Kriminologi Strain dalam Kasus Balap Liar. *UNES Law Review, 5*(4), 3708–3723. https://doi.org/10.31933/unesrev.v5i4.683

Marufah, N., Rahmat, H. K., & Widana, I. D. K. K. (2020). Degradasi Moral Sebagai Dampak Kejahatan Siber Pada Generasi Millenial di Indonesia. *NUSANTARA: Jurnal Ilmu Pengetahuan Sosial, 7*(1), 191–201. https://doi.org/10.31604/nusantara

Marzuki, P. M. (2010). *Penelitian Hukum* (Cet. 6). Jakarta: Kencana Prenada Media Group.

McIntosh, C., & Li, J. (2012). *An Introduction to Economic Analysis in Crime Prevention: The Why, How, and So What*. National Crime Prevention Centre.

Nabila, A. P., Manabung, N. A., & Ramadhansha, A. C. (2024). Peran Hukum Internasional dalam Menanggulangi Cyber Crime Pada Kejahatan Transnasional. *Indonesian Journal of Law, 1*(1), 26–37. https://jurnal.intekom.id/index.php/inlaw/article/view/290

Nahak, S. (2017). Hukum Tindak Pidana Mayantara (Cyber Crime) dalam Perspektif Akademik. *Jurnal Prasada, 4*(1), 1–11. https://doi.org/10.22225/jhp.4.1.2017.1-11

Nugroho, K. A. (2018). Pengaruh Cyber Attack Terhadap Kebijakan Cyber Security Amerika Serikat. *Journal of International Relations, 4*(3), 393–401. https://doi.org/10.14710/jirud.v4i3.21048

Prahassacitta, V. (2019). Kejahatan Siber Sebagai Kejahatan Ekonomi dalam Revolusi Industri 4.0. *Binus University, Faculty of Humanities*. from https://business-law.binus.ac.id/2019/06/30/kejahatan-siber-sebagai-kejahatan-ekonomi-dalam-revolusi-industri-4-0/

Radulov, N. (2019). Artificial Intelligence and Security. *Security 4.0: International Scientific Journals, 3*(1), 3–5. https://stumejournals.com/journals/confsec/2019/1/3

Sambas, N., & Andriasari, D. (2019). *Kriminologi: Perspektif Hukum Pidana* (Tarmizi, Ed., 1st ed.). Jakarta: Sinar Grafika.

Setiawan, D. A., Rohman, A., Jambak, F. F., Umbara, A., & Mulia, M. O. M. O. (2021). The Legal Strategy of Treating Telematics Crimes in the Field of Electronic Transactions in Global Trade. *Jurnal Pembaharuan Hukum, 8*(3), 374. https://doi.org/10.26532/jph.v8i3.15743

Soekanto, S., & Mamudji, S. (2015). *Penelitian Hukum Normatif: Suatu Tinjauan Singkat* (Cet. 4). Jakarta: Raja Grafindo Persada.

Sudjito, B., Majid, A., Sulistio, F., Ruslijanto, & Audrey, P. (2016). Tindak Pidana Pornografi dalam Era Siber di Indonesia. *Jurnal Wacana, 19*(2), 1. https://doi.org/10.21776/ub.wacana.2016.019.02.1

Triwahyuni, D., & Wulandari, T. A. (2016). Strategi Keamanan Cyber Amerika Serikat. *Jurnal Ilmu Politik dan Komunikasi, VI*(1), 107–118. https://doi.org/10.34010/jipsi.v6i1.239

Wahyun, N., & Fitriani, W. (2022). Relevansi Teori Belajar Sosial Albert Bandura dan Metode Pendidikan Keluarga dalam Islam. *Qalam: Jurnal Ilmu Kependidikan, 11*(2), 60–66. https://doi.org/10.33506/jq.v11i2.2060

Wisnusubroto, A. (2010). *Strategi Penanggulangan Kejahatan Telematika*. Yogyakarta: Atmajaya Yogyakarta.