Media Hukum Indonesia (MHI)
Published by Yayasan Daarul Huda Krueng Mane
https://ojs.daarulhuda.or.id/index.php/MHI/index

May-2025. Vol. 2, No. 6
e-ISSN: 3032-6591
pp 145-150

Revolusi Digital dan Tantangan Kriminologis: Analisis terhadap Tren Kriminalitas dalam Era Digitalisasi

The Digital Revolution and Criminological Challenges: An Analysis of Crime Trends in the Era of Digitalization

Jonner Marulitua Butarbutar
Universitas Bung Karno
Email: jonnerbutarbutar@gmail.com

Abstract: Purpose: This study aims to analyse the impact of the digital revolution on the emergence and transformation of criminal behaviours. It focuses on understanding how digitalization has influenced the nature, method, and scope of crimes, particularly in the context of cybercrime, digital fraud, data exploitation, and hacking. Research Methodology: The research adopts a qualitative approach, utilizing literature review and theoretical analysis. Various contemporary criminological theories are employed to interpret the changing patterns of criminality in the digital era. Results: The study reveals that the digital revolution has significantly altered criminal behaviour. New types of crimes have emerged, characterized by their transnational nature, anonymity, and reliance on technological tools. These developments challenge traditional law enforcement mechanisms and demand updated frameworks for crime prevention and investigation. Conclusion: The evolution of crime in the digital age necessitates urgent reforms in legal, regulatory, and security systems. Traditional approaches are no longer sufficient to address the complexities of digital crime. A multidisciplinary and adaptive response is crucial. Limitations: This study is limited by its reliance on secondary data and theoretical frameworks. Further empirical research is needed to validate the findings and explore region-specific crime patterns in more detail. Contribution: The study provides a conceptual foundation for policymakers and legal practitioners to develop technology-based, forward-looking criminal justice policies. It also contributes to the academic discourse on the intersection between digital transformation and criminology.

Article History
Received: April 30, 2025
Revised: May 10, 2025
Published: May 17, 2025

Keywords :
digital revolution, cybercrime, digital criminology, technological transformation, data security.

https://doi.org/10.5281/zenodo.15493512

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi dalam dua dekade terakhir telah melahirkan apa yang disebut sebagai Revolusi Digital. Perubahan ini ditandai dengan integrasi teknologi digital ke dalam seluruh aspek kehidupan manusia, termasuk dalam bidang ekonomi, sosial, politik, pendidikan, hingga budaya. Internet, kecerdasan buatan (AI), *big data*, *Internet of Things (IoT)*, dan teknologi *blockchain* merupakan beberapa pilar utama yang menopang transformasi ini.

Revolusi digital bukan hanya membawa kemudahan dan efisiensi dalam aktivitas manusia, tetapi juga menciptakan bentuk-bentuk tantangan baru yang kompleks dan multidimensi. Salah satu tantangan yang cukup krusial namun sering kali terabaikan adalah meningkatnya bentuk-bentuk kejahatan digital atau *cybercrime*. Di era ini, kejahatan tidak lagi terbatas pada ruang fisik. Dunia maya telah menjadi medan baru yang subur bagi pelaku kriminal, baik individu maupun kelompok terorganisir. Fenomena seperti peretasan data, penipuan daring, eksploitasi seksual anak secara digital, penyebaran hoaks dan propaganda melalui media sosial, serta penyalahgunaan kecerdasan buatan untuk membuat konten palsu (*deepfake*) merupakan wujud nyata bagaimana transformasi digital membuka celah baru dalam tindakan kriminal. Bahkan, dalam beberapa kasus, dampak kejahatan digital lebih luas dan destruktif dibanding kejahatan konvensional karena bersifat lintas batas, sulit dilacak, dan

May-2025. Vol. 2, No. 6
e-ISSN: 3032-6591
pp 145-150

berdampak sistemik terhadap keamanan publik maupun infrastruktur negara. Dalam konteks tersebut, kriminologi sebagai ilmu sosial yang mengkaji penyebab, bentuk, dan penanggulangan kejahatan dituntut untuk ikut berkembang dan beradaptasi dengan tantangan era digital. Pendekatan kriminologi klasik yang berfokus pada perilaku menyimpang di ruang fisik tidak lagi cukup untuk menjelaskan dinamika kejahatan masa kini. Diperlukan pendekatan baru yang mampu menjembatani antara aspek teknologi dan aspek sosial-budaya dalam memahami kompleksitas kejahatan digital. Oleh karena itu, artikel ini hadir untuk mengkaji bagaimana revolusi digital memengaruhi pola dan bentuk kriminalitas, serta bagaimana ilmu kriminologi dapat menjawab tantangan tersebut dengan strategi analisis dan pendekatan yang relevan. Dengan pemahaman yang lebih mendalam, diharapkan masyarakat dan negara dapat lebih siap dalam merespons gelombang perubahan kriminalitas yang terjadi di era digital sekarang dan ke depan.

Tinjauan pustaka dan pengembangan hipotesis

Revolusi digital merupakan salah satu tonggak penting dalam sejarah peradaban manusia modern. Dengan hadirnya internet, teknologi informasi, dan komunikasi digital, dunia mengalami transformasi yang luar biasa cepat dalam berbagai aspek kehidupan. Digitalisasi telah merombak cara manusia berinteraksi, bertransaksi, bekerja, belajar, bahkan dalam hal mengelola negara dan pemerintahan. Namun, kemajuan tersebut juga membawa dampak negatif yang tidak dapat diabaikan, khususnya dalam bidang kriminalitas. Fenomena kejahatan yang muncul di era digital sangat berbeda dari bentuk kejahatan konvensional. Pelaku kejahatan kini tidak perlu lagi bertatap muka dengan korban, tidak membutuhkan senjata fisik, dan dapat beroperasi dari mana saja secara anonim. Bentuk kejahatan seperti penipuan digital, pencurian identitas, peretasan sistem (hacking), serangan ransomware, perdagangan ilegal melalui dark web, hingga penyebaran disinformasi dan propaganda berbasis algoritma adalah contoh nyata bagaimana dunia digital menjadi medan baru bagi aktivitas kriminal. Kejahatan digital ini berkembang pesat karena didukung oleh beberapa faktor penting. Pertama, pesatnya pertumbuhan pengguna internet yang belum diimbangi dengan kesadaran dan literasi digital yang memadai. Kedua, lemahnya regulasi hukum siber di banyak negara, termasuk Indonesia, membuat banyak celah hukum yang dapat dimanfaatkan pelaku kejahatan. Ketiga, kompleksitas teknologi yang digunakan membuat aparat penegak hukum kesulitan untuk mendeteksi dan membuktikan tindak kriminal secara teknis dan forensik. Selain itu, kejahatan digital juga memiliki sifat *borderless* atau lintas batas negara, yang menyulitkan proses penindakan karena harus melibatkan kerja sama internasional. Tidak jarang pelaku berada di satu negara, korban di negara lain, dan server yang digunakan untuk melakukan serangan berada di negara ketiga. Hal ini menunjukkan bahwa revolusi digital tidak hanya menciptakan dunia yang lebih terkoneksi, tetapi juga dunia yang lebih rentan terhadap kejahatan transnasional yang kompleks dan sulit dijangkau. Latar belakang inilah yang menjadi dasar pentingnya pembahasan dalam artikel ini. Dengan menggunakan pendekatan kriminologi kontemporer, tulisan ini bertujuan untuk menelaah secara kritis bagaimana revolusi digital memengaruhi dinamika kriminalitas, serta bagaimana sistem hukum dan masyarakat perlu beradaptasi dalam menghadapi bentuk kejahatan baru yang terus berkembang seiring kemajuan teknologi.

Perkembangan teknologi digital yang semakin masif telah memunculkan bentuk-bentuk kriminalitas baru yang tidak hanya lebih canggih, tetapi juga lebih kompleks dan sulit terdeteksi. Kejahatan tidak lagi terbatas pada ruang fisik, melainkan telah berpindah ke dunia maya yang tidak mengenal batas wilayah, waktu, dan identitas konvensional. Di tengah dinamika ini, muncul sejumlah pertanyaan mendasar yang perlu dijawab secara ilmiah untuk memahami, mengantisipasi, dan merespons tantangan yang ditimbulkan oleh revolusi digital terhadap bidang kriminologi.

Penelitian ini disusun dengan tujuan untuk memberikan pemahaman yang lebih komprehensif mengenai dinamika kejahatan dalam konteks revolusi digital serta bagaimana kriminologi sebagai sebuah disiplin ilmu dapat menyesuaikan diri dalam menganalisis fenomena tersebut. Tujuan-tujuan yang ingin dicapai dalam penelitian ini adalah sebagai berikut:

1. Menganalisis pengaruh revolusi digital terhadap transformasi pola dan bentuk kejahatan Penelitian ini bertujuan untuk mengkaji bagaimana kemajuan teknologi digital mengubah cara kejahatan dilakukan, termasuk bagaimana pelaku memanfaatkan celah teknologi untuk menjalankan aksinya dan bagaimana korban terekspos risiko baru di ranah digital.

May-2025. Vol. 2, No. 6
e-ISSN: 3032-6591
pp 145-150

2. Mengidentifikasi dan mengklasifikasikan jenis-jenis kejahatan yang muncul di era digital Penelitian ini juga bertujuan untuk menguraikan berbagai bentuk kejahatan digital *(cybercrime)*, baik yang bersifat individu maupun terorganisir, termasuk modus operandi yang digunakan serta karakteristik umum dari pelaku dan korban kejahatan digital.
3. Mengeksplorasi pendekatan kriminologi kontemporer yang relevan untuk menganalisis kejahatan digital. Tujuan ini diarahkan untuk mengevaluasi sejauh mana teori-teori kriminologi klasik dan modern dapat diaplikasikan pada konteks kejahatan digital, sekaligus membuka ruang bagi pengembangan pendekatan baru dalam kajian *cybercriminology*.
4. Mengkaji efektivitas regulasi hukum dan kebijakan publik dalam menanggulangi kejahatan digital di Indonesia. Penelitian ini juga bertujuan untuk menilai kesesuaian instrumen hukum dan kebijakan negara dalam merespons fenomena kejahatan digital yang terus berkembang, serta memberikan saran strategis guna memperkuat sistem perlindungan hukum terhadap masyarakat digital.
5. Memberikan kontribusi ilmiah bagi pengembangan kajian kriminologi digital dan penyusunan kebijakan keamanan siber ke depan. Penelitian ini diharapkan dapat menjadi referensi konseptual dan praktis bagi akademisi, pembuat kebijakan, serta aparat penegak hukum dalam mengembangkan pemahaman dan strategi penanggulangan kejahatan digital yang berbasis pada pendekatan multidisipliner.

Dengan capaian tujuan-tujuan tersebut, diharapkan penelitian ini mampu menjadi landasan teoritis sekaligus praktis dalam menghadapi tantangan kejahatan digital yang terus berevolusi seiring dengan kemajuan revolusi digital di masa kini dan masa depan.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif-deskriptif untuk menggambarkan secara mendalam dan menyeluruh fenomena kejahatan digital dalam konteks revolusi digital. Metode ini memungkinkan penulis untuk menelusuri dimensi sosial, hukum, dan teknologi dari kejahatan digital, serta mengeksplorasi relevansi pendekatan kriminologis dalam merespons tantangan tersebut.

Penelitian ini merupakan studi kepustakaan *(library research)* yang berfokus pada pengumpulan dan analisis data sekunder dari berbagai sumber ilmiah dan institusional. Data yang digunakan berasal dari buku, jurnal akademik, laporan penelitian, regulasi hukum, dan dokumentasi lembaga keamanan siber nasional dan internasional.

Digunakan pendekatan analisis isi *(content analysis)* dan analisis tematik, untuk mengevaluasi isi dokumen secara kritis dan mengidentifikasi tema-tema utama terkait kejahatan digital, pola pelaku, dan respons institusi penegak hukum serta sistem hukum di era digital.

Analisis dalam penelitian ini dibingkai dengan teori-teori dalam cybercriminology, seperti: *routine activity theory* untuk menjelaskan bagaimana kejahatan digital terjadi karena bertemunya pelaku termotivasi, target yang sesuai, dan ketiadaan pengawas dan *strain theory* untuk menjelaskan tekanan sosial yang mendorong individu menggunakan teknologi sebagai pelarian atau sarana kejahatan. *Social Learning Theora*, untuk menunjukkan bagaimana pelaku mempelajari teknik kejahatan digital dalam komunitas daring.

Teknik Pengumpulan Data Data dikumpulkan melalui studi literatur pada jurnal-jurnal seperti *Cyberpsychology, Behavior, and Social Networking, Journal of Cybersecurity* dan *International Journal of Cyber Criminology*. Analisis dokumen hukum seperti Undang-Undang ITE, Peraturan BSSN, laporan tahunan Kemenkominfo, dan publikasi resmi dari Interpol dan UNODC. Observasi tidak langsung terhadap media sosial, forum *dark web*, dan berita daring untuk mendeteksi tren dan modus kejahatan digital terbaru.

Sebagai ilustrasi konkret dalam penelitian ini, digunakan kasus kebocoran data BPJS Kesehatan tahun 2021, di mana sekitar 279 juta data penduduk Indonesia diduga diperjualbelikan di forum hacker internasional. Kasus ini mengungkap lemahnya keamanan siber institusi publik, rendahnya kesadaran terhadap perlindungan data pribadi, serta tantangan penegakan hukum digital di Indonesia. Kasus ini juga memperlihatkan bagaimana pelaku menggunakan teknik digital canggih untuk mengakses sistem, serta bagaimana negara mengalami kesulitan dalam membuktikan pelanggaran dan menuntut pelaku

May-2025. Vol. 2, No. 6
e-ISSN: 3032-6591
pp 145-150

lintas negara. Contoh lain adalah penyebaran hoaks politik di media sosial menjelang pemilu yang dilakukan secara sistematis melalui bot, akun palsu, dan algoritma untuk memengaruhi opini publik. Ini merupakan bentuk kejahatan digital berbasis manipulasi informasi yang masuk dalam ranah *cyber* propaganda dan menjadi tantangan besar dalam menjaga demokrasi digital yang sehat.

Validitas data dijaga dengan menggunakan triangulasi sumber dan teori, serta seleksi literatur berdasarkan kredibilitas penerbit dan relevansi topik. Perbandingan antara data hukum, ilmiah, dan jurnalistik juga dilakukan untuk membentuk analisis yang obyektif dan menyeluruh.

HASIL DAN PEMBAHASAN

Di bagian Pembahasan dari jurnal "Revolusi Digital dan Tantangan Kriminologis" yang sudah dilengkapi dengan analisis kasus nyata serta pelanggaran terhadap UU yang relevan di Indonesia:

Dinamika Kejahatan Digital di Era Revolusi Digital

Revolusi digital telah mengubah cara manusia hidup dan berinteraksi. Namun, kemajuan ini turut melahirkan bentuk-bentuk kejahatan baru yang memanfaatkan celah dalam sistem digital. Kejahatan yang dahulu dilakukan secara langsung kini bisa dilakukan dari jarak jauh, anonim, dan dalam hitungan detik. Kriminalitas digital tidak lagi bergantung pada kekerasan fisik, melainkan pada kecanggihan teknologi dan keterampilan siber. Kejahatan digital mencakup berbagai bentuk, seperti:

a) *Hacking* (peeretasan sistem komputer)
b) *Pishing* (penipuan identitas)
c) *Data breach* (kebocoran data pribadi)
d) *Cyberbullving* dan kejahatan berbasis media sosial
e) Penyebaran hoaks dan disinformasi
f) Perdagangan ilegal di *dark web*
g) Pencucian uang digital *(cryptocurrency)*

Studi Kasus: Kebocoran Data BPJS Kesehatan

Pada tahun 2021, masyarakat Indonesia dikejutkan oleh dugaan kebocoran data 279 juta penduduk dari server BPJS Kesehatan. Data tersebut mencakup nama lengkap, NIK, alamat, nomor HP, hingga data keluarga, yang kemudian dijual di forum hacker internasional. Penelusuran menunjukkan bahwa data tersebut kemungkinan besar diambil dari kelemahan sistem keamanan internal.

Analisis Kriminologis:

Kasus ini mencerminkan lemahnya pengawasan sistem keamanan siber lembaga negara.Dalam perspektif routine activity theory, pelaku menemukan celah karena tidak adanya *"guardian"* atau pengawasan yang cukup atas sistem digital. Dalam strain theory, pelaku bisa jadi termotivasi oleh tekanan ekonomi atau ideologis, dan melihat kejahatan digital sebagai jalan keluar.

Pelanggaran Hukum:

Pasal 30, 32, dan 33 UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE), sebagaimana diubah dalam UU No. 19 Tahun 2016:

Pasal 30 (1): Setiap orang dilarang mengakses komputer atau sistem elektronik milik orang lain tanpa izin.

Pasal 32 (2): Dilarang dengan sengaja dan tanpa hak mengubah, menambah, mengurangi, mentransmisikan, merusak, menghilangkan data elektronik.

Pasal 33: Dilarang melakukan gangguan sistem elektronik yang mengakibatkan sistem tidak berfungsi.UU Perlindungan Data Pribadi (UU PDP No. 27 Tahun 2022) juga dilanggar, khususnya pada Pasal 58 yang mengatur sanksi terhadap pihak yang lalai dalam mengamankan data pribadi.

Studi Kasus: Penyebaran Hoaks Politik Menjelang Pemilu

Jelang Pemilu 2019 dan 2024, penyebaran berita palsu dan ujaran kebencian melalui media sosial meningkat tajam. Modus yang digunakan termasuk manipulasi informasi, penggunaan bot, dan akun palsu untuk menyerang lawan politik atau memecah belah masyarakat.

Analisis Kriminologis:

Kejahatan ini termasuk dalam kategori *cyber* propaganda, di mana informasi dimanipulasi untuk memengaruhi opini publik.

May-2025. Vol. 2, No. 6
e-ISSN: 3032-6591
pp 145-150

Mengacu pada *social learning theory*, pelaku belajar dari komunitas daring lain yang telah berhasil melakukan propaganda serupa, bahkan lintas negara.

Pelanggaran Hukum:

Pasal 28 ayat (2) UU ITE: Melarang penyebaran informasi yang menimbulkan rasa kebencian atau permusuhan berdasarkan SARA.

Pasal 14 dan 15 UU No. 1 Tahun 1946 tentang Peraturan Hukum Pidana: Melarang penyiaran berita bohong yang dapat menimbulkan keonaran di masyarakat.Tantangan Penegakan Hukum dan Adaptasi Kriminologi Penegakan hukum atas kejahatan digital menghadapi sejumlah tantangan besar:

a) *Anonymity*: Pelaku kejahatan dapat menyembunyikan identitasnya melalui VPN, enkripsi, atau server luar negeri.
b) *Borderless Crime*: Kejahatan digital sering kali bersifat lintas negara, yang mempersulit kerja sama penegakan hukum.
c) Keterbatasan SDM: Aparat penegak hukum dan institusi negara belum sepenuhnya memiliki kapasitas teknis dan forensik digital yang memadai.
d) Keterlambatan regulasi: Hukum sering tertinggal dari teknologi yang terus berkembang.Oleh karena itu, kriminologi harus bertransformasi untuk mengadopsi pendekatan multidisipliner, memanfaatkan teknologi dalam riset kriminalitas, serta menjalin kerja sama global dalam menganalisis dan menanggulangi kejahatan digital.

Studi Kasus

Dalam konteks kejahatan digital dan manipulasi informasi, studi yang dilakukan oleh Adya Danaditya (2021) mengenai aktivisme digital di Indonesia menunjukkan bahwa media sosial seperti *twitter* tidak hanya menjadi alat perjuangan, tetapi juga rentan terhadap bentuk-bentuk kejahatan digital. Studi tersebut mengangkat kasus protes terhadap kebijakan investasi minuman beralkohol yang ramai diperbincangkan di *twitter*. Melalui analisis jaringan, ditemukan adanya praktik hashtag *hijacking*, yaitu terstruktur dan diduga dilakukan oleh pihak-pihak tertentu untuk mendistorsi opini publik. Fenomena ini termasuk ke dalam bentuk kejahatan siber yang berdampak langsung terhadap kebebasan berekspresi dan hak atas informasi. Tidak hanya itu, keterlibatan akun bot dalam percakapan daring juga menandakan adanya operasi manipulasi yang bisa mempengaruhi persepsi masyarakat secara masif dan cepat. Temuan ini memperkuat urgensi pendekatan kriminologi kontemporer dalam menganalisis ancaman-ancaman baru yang lahir dari ruang digitalpengambilalihan tagar aktivis oleh kelompok oposisi untuk mengaburkan pesan utama gerakan tersebut.

SIMPULAN

Revolusi digital telah membawa transformasi besar dalam berbagai aspek kehidupan sosial, termasuk dalam lanskap kejahatan dan sistem hukum. Kejahatan tidak lagi terbatas pada ruang fisik, melainkan telah menjelma dalam bentuk-bentuk baru yang kompleks di ruang siber. Dari peretasan, penyebaran informasi palsu, hingga manipulasi opini publik melalui media sosial—semuanya menjadi tantangan kriminologis yang nyata di era digital ini. Studi kasus mengenai manipulasi digital dalam aktivisme *twitter* di Indonesia menunjukkan bahwa ruang digital tidak hanya menjadi medium ekspresi, tetapi juga ladang subur bagi praktik-praktik kriminal yang sulit dilacak dengan pendekatan hukum konvensional. Keterlibatan akun bot, hashtag hijacking, dan kampanye informasi sistematis menjadi bukti bahwa ancaman terhadap hak-hak sipil kini hadir dalam wajah baru yang tersembunyi di balik algoritma dan jaringan digital. Oleh karena itu, diperlukan pendekatan kriminologi yang lebih adaptif dan interdisipliner untuk memahami dinamika kejahatan digital secara holistik. Kriminologi kontemporer harus mampu menjangkau realitas virtual yang terus berubah, memperkuat kerja sama antara lembaga hukum, teknologi, dan masyarakat sipil, serta mendorong pembaruan regulasi yang responsif terhadap zaman. Tanpa pembaruan paradigma ini, sistem hukum akan selalu tertinggal satu langkah di belakang para pelaku kejahatan digital

KETERBATASAN PENELITIAN

Menghadapi tantangan kejahatan digital, diperlukan langkah strategis yang menyeluruh dan progresif. Pertama, pemerintah perlu memperkuat regulasi dan kebijakan yang relevan dengan

May-2025. Vol. 2, No. 6
e-ISSN: 3032-6591
pp 145-150

perkembangan teknologi informasi, termasuk pembaruan UU ITE yang lebih berorientasi pada perlindungan hak digital dan keadilan sosial. Kedua, aparat penegak hukum harus dibekali dengan pelatihan khusus dalam bidang digital forensik dan investigasi siber agar mampu merespons kejahatan dengan cepat dan akurat.

Ketiga, kerja sama lintas sektor antara pemerintah, akademisi, perusahaan teknologi, dan masyarakat sipil sangat penting untuk menciptakan ekosistem digital yang aman dan bertanggung jawab. Edukasi publik mengenai literasi digital juga harus digencarkan agar masyarakat tidak hanya menjadi pengguna teknologi, tetapi juga subjek yang kritis dan sadar hukum dalam ruang digital. Terakhir, kriminologi sebagai disiplin ilmu harus terus mengembangkan pendekatan analisis yang inovatif dan kontekstual, agar mampu memahami dan merespons wajah baru kejahatan dalam era revolusi digital secara efektif.

REFERENSI

Arief, Barda Nawawi. Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan. Jakarta: Kencana, 2020.

Brenner, Susan W. “Cybercrime Metrics: Old Wine, New Bottles?” Virginia Journal of Law and Technology, Vol. 9, No. 4, 2004.

Budiyanto, Eko. “Kejahatan Siber dan Tantangannya terhadap Sistem Peradilan Pidana.” Jurnal Hukum dan Peradilan, Vol. 6, No. 2, 2017, hlm. 239–256.

Canggara, Hafied. Komunikasi Digital: Sebuah Pengantar. Jakarta: Rajawali Pers, 2021.

Indonesia. Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), jo. UU No. 19 Tahun 2016.

Nugroho, Riant. Kebijakan Publik di Negara Berkembang. Yogyakarta: Pustaka Pelajar, 2017.

Nurwati, Irna. “Kajian Kriminologis Kejahatan Siber di Indonesia.” Jurnal Kriminologi Indonesia, Vol. 14, No. 1, 2019, hlm. 1–12.

Wall, David S. “Cybercrime, Media and Insecurity: The Shaping of Public Perceptions of Cybercrime.” International Review of Law, Computers & Technology, Vol. 22, No. 1-2, 2008.Yar, Majid. Cybercrime and Society. London: SAGE Publications, 2013.

Zulkarnain, Zainuddin. Kriminologi dan Kejahatan Modern. Bandung: Refika Aditama, 2022