El-Dusturie: Jurnal Hukum dan Perundang-undangan
Vol.3, No.2, Juni (2024)

PENAL POLICY CYBERCRIME ARTIFICIAL INTELLIGENCE (AI) ERA *SOCIETY* 5.0 PRESFEKTIF *FIQIH JINAYAH*

Dewi Iriani
Institut Agama Islam Negeri Ponorogo
Dewiiriani@iainponorog.ac.ad

Abstract: Cybercrime is increasing in line with the advancements of the era, triggering the need for legal protection governing the use of Artificial Intelligence (AI). This research aims to develop a penal policy that provides protection for victims of AI-based cybercrime by addressing two main issues: 1) the concept of prohibiting AI-based cybercrime in the Society 5.0 era from the perspective of *Fiqh Jinayah* and 2) the urgency of penal policies in protecting victims of AI-based cybercrime in this era. Using a qualitative normative approach, the study analyzes legal frameworks, including Law Number 19 of 2016 on Electronic Information and Transactions, and integrates the theories of Penal Policy and *Fiqh Jinayah* as analytical foundations. The findings reveal that, from the *Fiqh Jinayah* perspective, AI-based cybercrime is categorized as *jarimah*, subjecting perpetrators to *hudud* punishments under Law Number 1 of 2024. Furthermore, the urgency of penal policies lies in strengthening government regulations, requiring official registration of all internet applications through the Ministry of Communication and Information (Kemeninfo). Recommendations include fostering inter-agency collaboration, involving IT experts in mapping hacking threats, and focusing on enhanced cybersecurity measures.

Keywords: *Penal Policy, Cybercrime, Fiqh Jinayah, Artificial Intelligence, Society 5.0 Era, ITE Law, Legal Protection*.

Abstrak: Kejahatan siber semakin meningkat seiring dengan perkembangan zaman. Hal ini memicu kebutuhan terhadap perlindungan hukum yang mengatur pemanfaatan *Artificial Intelligence* AI. Tujuan penelitian ialah membuat kebijakan pidana (*Penal Policy*) dengan memberikan perlindungan terhadap korban cybercrime berbasis AI. Fokus penelitian ini mengkaji rumusan masalah 1). Bagaimana Konsep Larangan Tindak Pidana Cybercrime Artificial Intelligence (AI) Era Society 5.0 Prespektif Fiqih Jinayah. 2) Bagaiamana Urgensi Penal Policy Perlindungan Hukum Terhadap Korban Cybercrime Berbasis Artificial Intelligence (AI) Di Era Society 5.0 ? Metode kajian penelitian berupa : penelitian normatif kualitatif menjelasakan kebijakan hukum piana untuk memberikan perlindungan korban Kejahatan AI, dengan mengunakan pendekatan Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik. Pendekatan konseptual yaitu teori Penal Policy dan Fiqih Jinayah sebagai dasar analisis. Adapun hasil penelitian ialah 1) Perspektif Konteks Fiqh Jinayah, hal ini termasuk dalam kategori jarimah dan pelaku dapat dikenakan hukuman hudud, melalui penerapan sanksi manusia sesuai dengan peraturan dalam Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik. 2) Urgensi penal policy dalam memberikan perlindungan hukum data korban cyber crime Artificial Intelligence (AI) di era society 5.0 sebagai berikut: Pemerintah memperkuat

regulasi aplikasi internet, dengan cara semua aplikasi web internet harus didaftarkan secara resmi di pemerintah melalui Kemeninfo. Rekomendasi dari penelitian Ini adalah 1) Pemerintah harus menjalin kolaborasi yang baik antar lembaga dan bekerja sama dengan pakar TI dalam memetakan ancaman peretasan dan memprioritaskan fokus pada peningkatan keamanan situs.

Kata Kunci: Penal Policy, Cybercrime, Fiqih Jinayah, Artificial Intelligence, Era Society 5.0, Undang-Undang ITE, Perlindungan Hukum

A. PENDAHULUAN

Perkembangan teknologi di Era s*ociety 5.0* memberikan manusia kemudahan dalam menjalankan kehidupan sosial. Meskipun demikian, disaat yang sama juga menjadi pemicu permasalahan baru, yaitu kejahatan di dunia maya. Salah satu tanda kemajuan tersebut adalah integrasi kehidupan sosial dengan dunia maya dengan kecerdasan buatan yang dikenal dengan *Artificial Intelligence* (AI) [1]. Teknologi AI adalah sebuah sistem buatan yang dapat menirukan kegiatan manusia dan memiliki kerangka berfikir layaknya manusia dalam menjalankan suatu pekerjaan.

Sebagaimana layaknya teknologi yang bermata dua, kecanggihan AI dapat membantu dan mempermudah aktifitas, namun ia juga memberikan ancaman serangan bagi manusia itu sendiri. Sering kali beberapa oknum memanfaatkannya untuk melakukan kejahatan yang biasa disebut dengan *cybercrime*. *Cybercrime* adalah tindak pidana dalam dunia maya, atau dunia virtual yang merupakan tindak pidana yang timbul akibat dari revolusi teknologi informasi.

Cybercrime merujuk pada suatu tindakan kejahatan yang berhubungan dunia maya (*cyberspace*), dan tindakan kejahatan yang menggunakan komputer seperti: 1) *hacking* dan *cracking*, 2) *carding*, 3) *phising*, 4) *defacing, 5) spamming, 6) malware* dan masih banyak lagi bentuk tindak pidana *cybercrime* tersebut[2]. Banyaknya kejahatan *cybercrime* yang terjadi membuat pemerintah mengeluarkan kebijakan tentang hukum pidana kejahatan AI melalui *penal policy. Penal policy* (kebijakan hukum pidana) atau dikenal dengan politik hukum pidana adalah suatu tindakan yang dilakukan oleh lembaga yang memiliki kewenangan untuk menanggulangi

[1] Syafiqotuzzuhda. *Problematika Hukum Perlindungan Konsumen Dalam Menghadapi Kejahatan Berbasis Artificial Intellegence*. Skripsi. Universitas Islam Negeri Maulana Malik Ibrahim. 2023. Hal. 1

[2] Donovan Typhano Rachmadie. *Regulasi Penyimpangan Artificial Intelligence Pada Tindak Pidana Malware Berdasarkan Undang-Udang Republik Indonesia Nomor 19 Tahun 2016*.Jurnal Recidive, Jurnal Hukum Pidana dan Penanggulanggan Kejahtan. Vol.9 No.2. 2020. Hal 28

kejahatan melalui pendekatan peraturan hukum pidana,[3] termasuk tindak pidana kejahatan teknologi.

Data tahun 2023 dari Badan Siber Sandi Negara (BSSN) menunjukkan bahwa Tim Pusat Kontak Siber BSSN menerima sebanyak 1.417 aduan dari berbagai sektor[4]. Tercatat 1.216 aduan atau 86% porsi terbesar dari aduan tersebut berada dalam sektor *Cybercrime* atau tindakan kriminal yang memanfaatkan teknologi mulai dari perangkat hingga jaringan internet. Adapun prosentase sisanya secara terpisah dan terbagi kecil-kecil masuk ke dalam *web defacement* (serangan untuk mengeksploitasi situs web dengan cara merusak, melakukan modifikasi atau menghapus isi web), *vulnerable indikator* dan lainnya.[5]

Kaitannya dengan hal tersebut, kejahatan dalam bentuk apapun termasuk dalam bidang AI bertentangan dengan dengan hukum positif maupun agama (islam). Tindak pidana kejahatan teknologi / *cybercrime* AI diatur dalam Pengaturan Undang-Undang Nomor 1 Tahun Tahun 2024 Tentang Informasi Dan Transaksi Elektronik, Undang-undang No. 36 Tahun 1999 tentang Telekomunikasi, Peraturan Presiden Nomor 53 Tahun 2017 Badan Siber dan Sandi Negara (BSSN), dan peraturan perundang-undangan lainnya. Sementara itu, dalam hukum islam, tindak kriminal masuk dalam kategori fikih pidana.

Kerugian yang ditimbulkan dalam bidang kejahatan *cybercrime* AI yang ada di Indonesia menimbulkan kerugian bagi korban cybercrime. Hal inilah yang menarik penulis untuk melakukan penelitian lebih lanjut terkait *Penal Policy Cybercrime Artificial Intelligence* (AI) Era S*ociety* 5.0 Presfektif Fiqih Jinayah dan Peraturan Perundang-Undangan di Indonesia. Dengan rumusan masalah 1). Bagaimana Konsep Larangan Tindak Pidana Cybercrime *Artificial Intelligence* (AI) Era S*ociety* 5.0 Prespektif Fiqih Jinayah. 2) Bagaiamana Urgensi Penal Policy Perlindungan Hukum Terhadap Korban *Cybercrime* Berbasis *Artificial Intelligence* (AI) Di Era *Society* 5.0. Untuk membedakan kajian penelitian *Penal Policy Cybercrime Artificial Intelligence* (AI) Era S*ociety* 5.0 Presfektif *Fiqih Jinayah*, dengan penelitian penulis lainnya terdahulu yaitu penulis membandingkan dengan penelitian yang dilakukan oleh:

Pertama, Khofidhotur Rovida dan Sasmini. Berjudul Konsep Pencegahan *Cyberbullying* Berbasis *Techno Prevention* Pada Era Society 5.0 di Indonesia. Diterbitkan di Jurnal Hukum Ius Quia Iustum, (2024), pp. 461-485 ISSN 0854-8498

[3] John Kenedi.*Kebijakan Hukum Pidana (Penal Policy) Dalam Sistem Penegakan Hukum Di Indonesia.* Yogyakarta: Pustaka Pelajar : 2017. Hal 59

[4] Hinsa Siburian, Dominggus Pakel. *Lanskap Kemanan Siber Indonesia Tahun 2023*. Penerbit Badan Siber Sandi Negara (BSSN). 2024. Hal 38.

[5] *Ibid*, 39.

(Print) 2527-502X (Online). Membahas mengenai perkembangan teknologi melalui penerapan techno prevention yang ideal di era Society 5.0, untuk mencegah masyarakat dari cyberbullying. Masalah yang dikaji 1) Bagaimana upaya yang dilakukan oleh pemerintah dalam suatu kebijakan baik dalam bentuk represif maupun preventif? 2) Bagaimana konsep ideal pencegahan *cyberbullying Artificial Intelligence* (AI) yang ideal di era Society 5. Hasil penelitian yakni 1) Kebijakan pemerintah secara reprensif dan preventif bersifat post factum dalam penggunaan hukum pidana. 2) Pencegahan *Artificial Intelligence* (AI) dapat dilakukan dengan penerapan *Techno Prevention* melalui metode *Matematis Komputerasi*, seperti metode *Algoritma Nearest Neighbour (ANN).* Metode penelitian digunakan memgkaji peraturan perundang-undangan dan konseptual. Perbedaan penelitian dengan penulis ialah fokus kajian penelitian, penulis membahas *Penal Policy Cybercrime Artificial Intelligence* (AI) Era S*ociety* 5.0 Presfektif *Fiqih Jinayah.* Sedangkan Khofidhotur Rovida dan Sasmini, fokus penelitian pada kajian Konsep Pencegahan *Cyberbullying* Berbasis *Techno Prevention* Pada Era Society 5.0 di Indonesia

Kedua, Farhan Aulia Harun, dan Lucky Nurhadiyanto. Judul penelitian Rekayasa Konten Pornografi Berbasis AI Image Generator dalam Perspektif Space Transition. Telah publis di jurnal Ranah Research : Journal of Multidisciplinary Research and Development Vol. 6, No. 3, Maret. 2024. Penggunaan AI Image Generator disalahgunakan untuk membuat film pornografi. *Rumusan masaalh yang diteliti 1) Faktor apa yang menyebabkan penyalahgunaan* AI Image Generator? Bagaimana perlindungan terhadap keamanan siber AI Image Generator? Hasil penelitian ialah 1) lemahnya keamanan ruang siber terhadap anonimitas dan fleksibilitas identitas , sehingga yang menyebabkan penyalahgunaan AI dalam pembuatan konten pornografi. 2) Meningkatkan kemananan siber agar pelaku pembuat konten pronografi dalam penyalahgunaan AI dapat terlacak keberadaanya. Metode penelitian dengan melakukan wawancara, dan observasi. Perbadaan penelitian Farhan Aulia Harun, dan Lucky Nurhadiyanto yaitu pada metode penelitian. Penulis meneliti normatif kualitatif dan library, sedangkan Farhan meneliti dengan melakukan wawancara. Serta kajian yang diteliti berbeda, Farhan mengkaji penyelagunaan AI untuk konten Pornografi sedangkan penulis mengkaji ***Penal Policy Cybercrime Artificial Intelligence* (AI) Era S*ociety* 5.0 Presfektif *Fiqih Jinayah***

B. METODE PENELITIAN

Metode kajian penelitian berupa : penelitian normatif kualitatif menjelasakan kebijakan hukum piana untuk memberikan perlindungan korban Kejahatan AI, dengan mengunakan pendekatan peraturan Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik. Pendekatan konseptual yaitu teori Penal Policy dan Fiqih Jinayah sebagai dasar analisis

C. HASIL DAN PEMBAHASAN

1. Konsep Larangan Tindak Pidana Cybercrime *Artificial Intelligence* (AI) Era S*ociety* 5.0 Presfektif Fiqih Jinayah

Cybercrime *Artificial Intelligence* (AI), merupakan kejahatan dunia maya pada era s*ociety* 5.0. Penyalahgunaan aplikasi AI dilakukan oleh pelaku kejahatan, termasuk dalam tindak pidana teknologi cybercrime. Pelaku akan memanfaatkan teknologi dengan cara illegal, tanpa izin dari orang lain atau korban[6]. Pelaku akan mengirimkan aplikasi tertentu melalui whatsapp kemudian korban yang tidak mengetahui akan membuka dan uang akan langsung hilang.

Menurut Agus Raharjo cara pelaku mempengaruhi korban dengan memasuki jaringan komputer melalui kode tertentu untuk membuka akses yang bisa menguras rekening korban. Pelaku melakukan perbuatan penyusupan sebagai kejahatan di ruang siber (*cyberpace*) perbuatan melawan hukum. Berbagai macam kejahatan *cybercrime* AI dibagi menjadi ;1). Kejahatan Dunia maya yang merupakan kerahasiaan data melaui komputer yakni ; masuk akun tanpa izin, data base komputer, menggunakan sistem dan Jaringan komputer tanpa izin, mencuri data penting, melakukan mata-mata dengan membocorkan data. 2) Kejahatan dunia maya dengan cara melakukan penipuan melalui komputer ialah: kartu kredit, penipuan terhadap bank, penawaran jasa, pemalsuan melalui komputer, mencuri indentitas, melakukan pemerasan terhadap korban.[7]

Selanjutnya, penulis akan membahas tindak pidana *cybercrime* AI dari presfektif fikih jinayah yang termasuk dalam aturan dalam hukum Islam. Hendara Gunawan mengungkapkan hukum Islam melarang suatu perbuatan yang merugikan orang lain. Teori *maqasid al-syari'ah* memiliki tujuan untuk

6 Angkasa. *Cybercrime Di Era Industri 4.0 Dan Masyarakat 5.0 Dalam Perspektif Viktimologi.* Jurnal Justiciabelen. Vol 2, No 02. 2022.

7. Muhammad Muslih, Said Sahabuddin, Tanzil Pengungkapan Kejahatan Hacking Mengakses Sistem Elektronik Milik Orang Lain Di Wilayah Hukum Polres Batanghari. Legalitas: Jurnal Hukum. Vol 15. No. 2. Desember. 2023. Hal 265

mewujudkan kemaslahatan (kemanfaatan) di dunia maupun di akhirat[8]. Konsep *maqasid al-syari'ah* melindungi *almasalih al-khamsah* (lima kebutuhan pokok dalam kehidupan manusia) mencakup *hifz al-din* (pemeliharaan agama), *hifz al-nafs* (jiwa), *hifz al-nasl* (keturunan atau kehormatan), *hifz almal* (harta), dan *hifz al-'aql* (akal).

Fikih Jinayah yang mengatur tentang tindak pidana kejahatan dapat mencakup pula tindak kriminal pada aspek *cyber crime* AI. Pernyataan ini didasarkan pada *qiyas* (analogi) dengan macam-macam kejahatan yang telah tercakup dalam fikih pidana seperti *syariqah, hirabah,* zina, dan lain sebagainya dimana para pelaku kejahatan *cyber crime* AI dapat dijatuhi hukuman *ta'zir* bahkan hukuman *hudud* apabila memiliki *illat* (kesamaan) dengan *jarimah hudud*. Tindak pidana seperti zina, *qozaf* (tuduhan palsu tentang perzinaan), *sariqah* (pencurian), *hirabah* (perampokan), *riddah* (murtad), *al-baghy* (pemberontakan), dan *syurb al-khamr* (minum-minuman keras) termasuk dalam *jarimah hudud* tersebut dalam al Qur'an.[9]

Salah satu kejahatan teknologi cyber crime AI adalah tindakan. Phising dalam kejahatan cybercrime AI, dimana maksudnya adalah upaya pelaku untuk melakukan kejahatan dengan cara menipu dan mencuri korban untuk mendapatkan data pribadi mulai dari alamat, nama lengkap, umur, akun masuk dan kode akun yang akan menguras rekening tabungan korban[10]. Sementara itu, secara umum, pencurian dalam perspektif fikih jinayah disebut dengan sariqah dimana pidana ini masuk dalam kategori jarimah hudud.

Pengertian sariqoh ialah mengabil harta (mal) yang bukan haknya, secara diam-diam tanpa sepengetahuan pemilik (akhzu al-mal li al-ghairi). Sementara itu, tindakan phising pada era Rasullulah belum dikenal karena belum adanya teknologi komputer. Ulama Imam Malik dan Hanabilah sepakat apabila mengambil harta dari orang lain disebut penipuan dan dikenakan hukuman had atau ta"zir yang melanggar aturan (nash). [11] Oleh karenanya, memformulasikan tindak pidana dalam dunia cyber perspektif fikih jinayah menjadi penting.

---

8. Hendra Gunawan. Tindak Kejahatan *Cyber Crime* Dalam Perspektif Fikih Jinayah. Jurnal El-Qanuniy Vol. 6 No. 1 Edisi Januari-Juni 2020. Hal 80

[9] Makhrus Munajat. *Hukum Pidana Islam; Fiqih Jinayat*. Yogyakarta: Pesantren Nawasea Press, 2020. Hal 105

[10] Aidil Fitrisuryani Yusi. *Kejahatan Dunia Maya (Cybercrime) Dalam Presfektif Hukum Islam Dan Hukum Positif Indonesia*. Justice Journal By Faculty Lawvol 17 No 1 (2024): Keadilan. 19

[11] Monica Shelsa Hanalisis. *Tindak Pidana Pencurian Data Pribadi Melalui Teknik Phising Ditinjau Dalam Prespektif Fiqih Jinaya, Hukum Pidana Islam*. Skripsi. Fakultas Syariah Dan Hukum Universitas Islam Negeri Walisongo Semarang. 2022. Hal 70

Menurut Abdul Qadir Audah, ada tiga hal yang termasuk kategori unsur umum dari jarimah yakni ; 1) unsur formal berlaku aturan dan ketentuan yang termasuk jarimah. 2) Unsur materiil, berupa perbuatan melawan hukum. 3) unsur moril berupa niat dari pelaku kejahatan jarimah (tindak pidana)[12]. Dari ketiga unsur tersebut penulis menguraikan pertanggungjwaban pidana oleh pelaku kejahatan cyber crime AI secara fiqih jinayah ialah; 1) secara unsur formal, pelaku kejahatan cyber crime AI harus memenuhi unsur : sudah baliq (dewasa), berakal sehat, ikhtiyar atau terdapat unsur melakukan perbuatan. 2) secara unsur materiil melakukan kejahatan atau kemaksiatan sebagai jarimah ta'zir (tindak pidana). 3) secara unsur moril adanya niat dalam melakukan kejahatan atau kemaksiatan yang melanggaran nash (aturan) yang berlaku.

Kaitannya dengan persoalan ini, maka solusi dari penulis untuk mencegah pelaku kejahatan *cyber crime* AI adalah *diqiyaskan* dengan *jarimah hudud* (hukuman yang sudah ditetapkan secara jelas dalam *nash* Al-Qur'an dan sunnah) melalui penerapan sanksi hukuman sesuai dengan peraturan perundang-undangan yang berlaku di Indonesia. selain itu, menerapkan hukuman *ta'dib* (edukatif) yang bersifat mendidik terhadap pelaku, *al-man'u* (pencegahan/antisipasi), atau *tankîf* (menakut-nakuti) dengan memberikan sanksi pemidanaan.

2. Urgensi Penal Policy Perlindungan Hukum Terhadap Korban *Cybercrime* Berbasis *Artificial Intelligence* (AI) Di Era *Society* 5.0

Pada masa modern perkembangannya, Artificial Intelligence (AI) memang membawa banyak manfaat dalam mendorong perkembangan industri. Akan tetapi, dengan adanya perkembangan teknologi informasi AI ini tidak menutup kemungkinan akan melahirkan tindak pidana baru akibat dari penyalahgunaan oleh pelaku kejahatan cybercrime[13].. Penyalahgunaan AI berbeda dengan tindak pidana lainnya, yang membedakan adalah kejahatan ini dilakukan dengan media maya atau media virtual. Dalam melakukan tindak pidana tersebut, menggunakan teknologi sebagai alat bantu. Hal ini sebagaimana dinyatakan oleh Barda Nawawi bahwa penyerangan melalui sistem teknologi dilakukan dengan

[12] Ahmad Muyasir. *Kejahatan Defecting: Studi Perbandingan Antara Undang-Undang ITE Dan Hukum Pidana Islamal MazaHib.* Vol. 3. No. 1,. Juni 2019

[13] Wansyah. *Penelitian Hukum, Pilihan Metode Dan Praktik Penulisan Artikel*. Edisi ke 3. Yogyakarta: Mira Buana Media. 2020. Hal 89

cara menggunakan media sosial sebagai sarana untuk merugikan orang lain.[14] Contoh lainnya dalam tindak pidana cyber crime adalah pertasan akun perbankan yang dimiliki korban kejahatan cyber crime. Pada era 5.0 ini, peretasan tersebut menggunakan jaringan akses internet. Pelaku tindak pidana cyber crime akan langsung mencuri data pribadi nasabah. [15]

Selain itu, tindak pidana *cyber crime* AI mempunyai banyak ragam sebagaimana berikut[16] :

a. *Malicious software (Malware*) yang artinya *software* yang tidak diinginkan dalam sistem komputer, biasanya *malware* dibuat untuk mencuri data informasi yang bahkan dapat merusak sebuah sistem komputer dengan menyusup ke sistem jaringan komputer.
b. *Defacing* adalah memindahkan data dari *website* asli ke akun website palsu.
c. *Deepfake* atau menggunakan video akun palsu yang dapat merentas kode OTP *(One Time Password*).
d. Pengiriman OTP melalui SMS.
e. *Hacking* dan *Cracking* yaitu pesan e-mail penipuan dari perusahaan yang sah misalnya, universitas, penyedia layanan internet, bank. Pesan dalam email ini biasaya mengarahkan seseorang kesitus web palsu, atau membuat seseorang untuk membocorkan informasi pribadi. Misalnya ; *password*, kartu kredit, atau *update* akun lainnya yang masuk sistem elektronik tanpa ijin.
f. *Carding* dilakukan denga cara mencuri nomor kartu kredit milik orang lain, dengan menawarkan program kartu keridit yang nanti uangnya akan beralih.
g. *Spamming* adalah mengirim informasi pesan terus berulang-ulang untuk mencuri data.
h. *Skimmer* merupakan modus kejahatan di bidang perbankan bertujuan mencuri informasi dari kartu debit atau kredit milik nasabah, menggunakan alat khusus bernama Skimmer

---

[14] Radya Dzuhrizha Rahmana And Adhitya Widya Kartika. *Penegakan Hukum Bagi Pelaku Pembuatan Dan Penyebaran Scam Page (Studi Di Kepolisian Daerah Jawa Timur).* Jurnal Risalah Hukum . Vol.18. No. 2. 2022. Hal 98.

[15] Putri Wahyu Widayanti. Tindak Pidana Pencurian Data Nasabah Dalam Bidang Perbankan Sebagai *Cyber Crime* Legacy : Jurnal Hukum Dan Perundang-Undangan Vol 2 No 2 - Agustus 2022. Hal 21

[16] Donovan Typhano Rachmadie. *Regulasi Penyimpangan Artificial Intelligence Pada Tindak Pidana Malware Berdasarkan Undang-Udang Republik Indonesia Nomor 19 Tahun 2016*. Jurnal Recidive Vol.9 No. 2 . 2020. Hal 129

i. *Phising* ialah penipuan *website* yang menyerupai sama persis denga akun asli.

Menurut data dari Kementerian Komunikasi dan Informatika Indonesia (Kominfo), terdapat 1,225 miliar serangan siber setiap harinya. yaitu 1) kejahatan *cyber crime* dengan pengambilan data di M-banking dimana selama tahun 2023 ini sudah ada 13.269 korban, 2) Kejahatan *cybe crime* peretasan data dalam sosial media melalui kode OTP atau Link dengan jumlah korban mencapai 12. 817, 3) kejahatan *deepfake* di tahun 2023 ada 95.820 laporan dari korban.[17] Uniknya, korban kejahatan *cyber crime* akan sulit mencari dan melacak pelaku, sebaliknya pelaku kejahatn *cyber crime* akan dengan mudah mencari korban *cyber crime.* Hal ini dikarenakan beberapa faktor ; 1) indentitas pelaku tidak bisa dilacak, mengggunakan nomer yang berbeda berbeda. 2). Pelaku kejaahatan cyber crime mengguasai perkembangan teknologi. 3). Korban kejahatan cyber crime mudah percaya dan tidak menguasai teknologi, menyebabkan pelaku kejahatan semakin banyak.[18]

Korban dari tindak pindana cyber crime memiliki hak jaminan perlidungan hukum. Menurut Setiono perlindungan hukum ialah upaya hukum untuk melindungi masyarakat dari tindakan kesewenang-wenangan oleh penguasa maupun oleh orang yang telah berbuat kerugian. Sedangkan Muchsin menyampaikan perlindungan hukum yaitu seseorang yang patut mendapatkan perlindungan sesuai dengan aturan undang-undang, dengan memberikan sanksi kepada pelaku yang membuat kerugian[19].

Philipus. M. Hardjo membagi dua jenis perlindungan hukum yakni : Pertama, perlindungan hukum preventif dimana maksudnya adalah Pemerintah memberikan perlindungan kepada masyarakat dengan pencegahan sebelum terjadinya pelanggaran. Kedua, perlindungan hukum represif. Upaya hukum terakhir inilah yang memberikan perlindungan kepada korban, dengan menerapkan sanksi pemidanaan bagi pelaku.[20]

---

[17] Yusuf. *Serangan Siber*. Https://Www.Kominfo.Go.Id/Content/Detail/57320/Siaran-Pers-No-412. Hmkominfo062024-Tentang-Indikasi-Serangan-Siber-Wamenkominfo-Fokus-Tangani-Dampak-Layanan Pemerintah/0/Siaran_Pers. Diakses Pada Tanggal 10 Juli 2024. Jam. 10.00 Wib.

[18] Andi Widiatno . *Cyberporn Dalam Pasar Digital Non-Fungible Tokens: Prespektif Undang-Undang Informasi Transaksi Elektronik Dan Pornografi.* Journal Justiciabelen. Vol 2. No. 2. 2022. Hal 90

[19] Ari Dermawan. Akmal. *Urgensi Perlindungan Hukum Bagi Korban Tindak Pidana Kejahatan Teknologi Informasi*. Journal Of Science And Social Research. 2019.Hal 46

[20] Fajar Kurniawan, Didik Suhariyanto, Hartana. *Perlindungan Konsumen Terhadap Pinjaman Onlineatas Penyebaran Data Pribadi.* Journal Of Social Science Research Vol 4. No. 1. 2024. Hal 13.

Kaitannya dengan hal ini, korban kejahatan tindak pidana *cybercrime* mempunyai hak-hak yang harus dipenuhi, yaitu meliputi: jaminan hukum, kepastian hukum, pendampingan hukum, mendapatkan fasilitasi pelayanan hukum, mendapatkan hak ganti kerugian[21]. Hak berikutnya bagi korban tindak pidana *cyber crime* berhak mendapatkan ganti rugi secara proposisonal dimana korban dapat menuntut ganti kerugian kepada pelaku kejahatan *cyber crime.* Korban dapat menuntut ganti kerugian secara materiil dan non materiil atas perbuatannya perbuatan perlaku sesuai dengan nominal kerugian (materiil) maupun melebihi kerugian (non materiil). Gagasan keadilan akibat tindak pidana *cyber crime* adalah sebagai upaya memberikan perlindungan hukum dalam sistem peradilan pidana berbasis masyarakat[22], dimana masyarakat akan merespon secara langsung, dengan memberikan peringatan kepada korban *cyber crime* untuk segera melaporkan ke aparat hukum.

Negara berkewajiban memberikan perlindungan hukum kepada korban kejaahatan *cyber crime*, dengan memberikan ganti kerugian yang dilakukan oleh pelaku dan menghukum pelaku kejahatan *cyber crime.* negara berkewajiban untuk memberikan ganti rugi pada korban tindak pidana pidana *cyber crime*.[23] Pemberian ganti kerugian kepada korban kejahatan *cyber crime* berorientasi pada hukum progresif yang memberikan keadilan restoratif. korban kejahatan *cyber crime* dapat melaporkan pelaku kejahatan *cyber crim*e ke kepolisian dengan syarat yang harus dipenuhi antara lain: Perbuatan merugikan kroban, sering dilakukan secara berulang, menimbulkan reaksi atas perbuatan pelaku, terdapat bukti kuat.[24] Keadilan restoratif berfungsi sebagai upaya untuk memulihkan korban akibat adanya kerugian yang dialami akibat tindak pidana *cyber crime*.

---

[21] Muhammad Kamran And Maskun Maskun. *Penipuan Dalam Jual Beli Online: Perspektif Hukum Telematika*. Balobe Law Journal. Vo. 1,.No. 1. 2021. Hal 4

[22] Henny Saida Flora, Tiromsi Sitanggang, Berlian Simarmata, Ica Karina *Keadilan Restoratif Dalam Melindungi Hak Korban Tindak Pidana Cyber: Manifestasi Dan Implementasi.* Jurnal Ius Constituendum. Vol. 8 No. 2. 2023. Hal 180

[23] Nurul Adhha Asep Saepudin Jahar, Raju Moh Hazmi. *Construction Of Legal Justice, Certainty, And Benefits In The Supreme Court Decision*. Cita Hukum. Vol. 9. No. 1. 2021. Hal 162.

[24] Heny Novyanti, Pudji Astuti. *Jerat Hukum Penyalahgunaan Aplikasi Deepfake Ditinjau Dari Hukum Pidana* Jurnal Novum. Hukum Jurusan Hukum Universitas Negeri Surabaya. 2021. Hal 85

Techno Prevention salah satu teknologi kecerdasan buatan (Artificial Intelligence/ AI) melalui suara, gambar, bahasa untuk berkeativitas [25]. Teknologi tersebut disalahgunakan untuk *cyber crime,* kercedasan buatan lainnya adalah Deepfakes untuk memanipulasi foto atau video yang digunakan dalam pembuatan konten porno.[26] *Techno Prevention* dapat juga digunakan untuk mendiketsi secara awal dari pelaku cbyer crime, dan mencegah korban cyber crime Artificial Intelligence/AI) [27]. Penyalahgunaan AI menimbulkan kerugian dan dampak yang serius bagi korban dan masyarakat yang menonton, penyalahgunaan AI oleh pelaku cyber crime harus mendapatkan perhatian serius dari pemerintah. Untuk itu diperlukan perlindungan hukum bagi korban AI, dan saknsi hukuman bagi pelaku cyber crime.[28]

Analisis penulis terhadap perlindungan hukum data korban *cyber crime artificial intelligence* (AI) adalah bertujuan untuk meminimalisasi adanya potensi tindak pidana *cyber* secara prefentif. Pelaku kejahatan *cyber crime artificial intelligence* (AI) di era *society* 5.0 selain mendapatkan sanksi hukuman penjara juga diwajibkan untuk menganti kerugian korban tindak pidana *cyber*. Ganti kerugian lebih ditujukan pada korban tindak pidana cyber *crime* AI, ganti kerugian tersebut merupakan penerapan keadilan restoratif. Sehingga, akan memberikan jaminan kepastian hukum.

Seringkali korban kejahatan *cyber crime* kesulitan mengukapkan pelaku tindak pidana cyber crime dikarenakan indentitas pelaku memakai no HP yang berbeda-beda. Maka korban kejahatan *cyber crime* akan sulit untuk mendapatkan uangnya kembali dan kesulitan pula untuk mendapatkan ganti kerugian. Oleh karenanya negara harus hadir untuk memberikan

[25] Nabila Syahrani Lestari Kebijakan Formulasi Hukum Pidana Atas Praktik Deepfake Dilihat Dari Perspektif Kejahatan Siber Dan Pornografi. Skripsi. Fakultas Universitas Sriwjaya. Palembang. 20224. Hal 10

[26] Nadila Criswara. *Analisis Yuridis Kekerasan Gender Berbasis Online (KGBO) dengan Deepfakes Ditinjau dari Hukum Positif*. Proceedings Series on Social Sciences & Humanities, Volume 17 Proceedings of Seminar International Legal Development in Twenty-First Century Era. Hal 299

[27] Khofidhotur Rovida, Sasmini. *Konsep Pencegahan Cyberbullying Berbasis Techno Prevention Pada Era Society 5.0 di Indonesia*. Jurnal Hukum Ius Quia Iustum, (2024), pp. 461-485 ISSN 0854-8498 (Print) 2527-502X (Online). Hal 482

[28] Farhan Aulia Harun, Lucky Nurhadiyanto. *Rekayasa Konten Pornografi Berbasis AI Image Generator dalam Perspektif Space Transition*. Ranah Research : Journal of Multidisciplinary Research and Development Vol. 6, No. 3, Maret. 2024. Hal 418 .

perlindungan hukum, dan menindak tegas pelaku kejahatan tindak pidana *cyber crime* sesuai dengan undang-undang yang berlaku.

Pengaturan Undang-Undang Nomor 1 Tahun Tahun 2024 Tentang Informasi Dan Transaksi Elektronik, diharapkan dapat memberikan perlindungan hukum bagi masyarakat yang menggunakan teknologi. Selain itu, memberikan perlindungan hukum terhadap korban *cybercrime* dapat memberikan rasa aman bagi yang menggunakan teknologi informasi dalam beraktivitas di dunia maya. Untuk lebih mempermudah pemahaman aturan mengenai larangan dan sanksi atas tindak pidana *cyber crime*, penulis akan menjelaskan aturan yang tercantup pada Undang-Undang Nomor 1 Tahun 2024 Tentang Informasi Dan Transaksi Elektronik

a. Pasal 30 ayat 1 sampai 3 Undang-Undang Nomor 1 Tahun 2024 Tentang Informasi Dan Transaksi Elektronik dijelaskan tentang larangan mengakses komputer, dan/atau sistem elektronik milik orang lain secara sengaja untuk diambil keuntungannya.[29]
b. Kemudian sanksi pada pelaku dijelaskan pada Pasal 46 ayat 1 sampai 3 Undang-Undang Nomor 1 Tahun 2024 Tentang Informasi Dan Transaksi Elektronik, mengatur mengenai ketentuan pidana bagi pelaku kejahatan dunia maya. Adapun ancaman pidanya, mulai dari 6 (enam) tahun sampai 8 (delapan) tahun penjara dengan denda mulai dari Rp600.000.000,00 (enam ratus juta rupiah) sampai Rp800.000.000,00 (delapan ratus juta rupiah).[30]
c. Dalam hal kejahatan media sosial, sesuai dengan ketentuan Pasal 4 ayat (2) Undang-Undang Nomor 1 Tahun Tahun 2024 tentang Informasi dan Transaksi Elektronik disebutkan bahwa Pemerintah melindungi kepentingan umum dari segala jenis gangguan sebagai akibat penyalahgunaan Informasi Elektronik dan Transaksi Elektronik yang mengganggu ketertiban umum, sesuai dengan ketentuan Peraturan Perundang-Undangan.[31]

Dengan adanya Undang-Undang Nomor 1 Tahun Tahun 2024 tentang Informasi dan Transaksi Elektronik tersebut, diharapkan dapat memberikan rasa aman dan dapat melindungi bagi mereka yang menggunakan teknologi.

[29] Lihat Pasal 30 ayat 1 sampai 3 Undang-Undang Nomor 1 Tahun 2024 Tentang Informasi Dan Transaksi Elektronik

[30] Lihat Pasal 46 ayat 1 sampai 3 Undang-Undang Nomor 1 Tahun 2024 Tentang Informasi Dan Transaksi Elektronik

[31]Lihat Pasal 4 ayat (2) Undang-Undang Nomor 1 Tahun Tahun 2024 tentang Informasi dan Transaksi Elektronik

Di samping itu, dalam keadaan tertentu dan membahayakan, bagi mereka yang menjadi korban kejahatan teknologi juga berhak mendapatkan perlindungan hukum.

Penggunaan hukum pidana di Indonesia sebagai sarana untuk menanggulangi kejahatan tampaknya tidak menjadi persoalan. Hal ini, terlihat dari praktiknya dalam perundang-undangan yang menunjukkan bahwa penggunaan hukum pidana merupakan bagian dari kebijakan atau politik hukum yang dianut di Indonesia. Penggunaan hukum pidana sebagai suatu hal yang wajar dan normal bahkan menjadi sebuah kebutuhan, seolah-olah eksistensinya tidak perlu lagi dipersoalkan.

Selain itu terdapat aturan lain berkaitan dengan perlindungan data korban, yaitu Peraturan Presiden Nomor 53 Tahun 2017 Tentang Badan Siber dan Sandi Negara (BSSN) BSSN merupakan hasil dari penggabungan beberapa entitas pemerintah sebelumnya, antara lain Lembaga Sandi Negara (Lemsaneg), Direktorat Keamanan Informasi, Direktorat Jenderal Aplikasi Informatika Kementerian Komunikasi dan Informatika (Kemenkominfo), serta Indonesia Security Incident Response Team on Internet Infrastructure (IdSIRTII) [32]. BSSN dibentuk pada tanggal 13 April 2021 melalui Peraturan Presiden (Perpres) Nomor 28 Tahun 2021 Tentang Badan Siber Dan Sandi Negara (BSSN)[33]. Tujuan dari BSSN ialah memberikan rasa aman dan perlindungan data siber secara nasional. Dengan demikian, kejahatan cyber crime sangat berbahaya, dapat menyebabkan kerugian bagi masyarakat. Maka diperlukannya *penal policy* (kebijakan hukum pidana).

Barda Nawawi menjelaskan *penal policy* Usaha adalah kebijakan dalam membuat aturan hukum pidana, mempunyai tujuan untuk menanggulangi kejahatan. *Penal policy* lebih dikenal dengan kebijakan hukum pidana, yang diartikan penaggulangan kejahatan melalui politik hukum atau kebijakan. Bagian dari penal policy ialah: kebijakan penegakan hukum (*law enforcement policy*), kebijakan kriminal, kebijakan penanggulangan kejahatan.[34] Pendekatan melaui *penal policy* diperlukan pendekatan budaya, moral, pendidikan, kerjasama berbagai pihak, kerjasama dengan negara luar. *Penal policy* untuk menanggulangi kejaharan melalui aturan undang-undang hukum

[32] Lihat Peraturan Presiden Nomor 53 Tahun 2017 Tentang Badan Siber dan Sandi Negara (BSSN)

[33] Lihat Peraturan Presiden (Perpres) Nomor 28 Tahun 2021 Tentang Badan Siber Dan Sandi Negara (Bssn

[34] Barda Nawawi. Tindak Pidana Mayantara: *Perkembangan Cyber Crime Di Indonesia*. Jakarta; Rajagrafindo Persada. 2006. Hal 183.

pidana, sebagai upaya melindungi masyarakat (*social welfare*)[35]. *Penal policy* dapat digunakan dalam penaggulangan kejahatan *cyber crime, selain penal policy digunakan pula teori krimonologi untuk mengukur* setiap jenis kejahatan siber *(cyber crime) yang* mempunyai spesifikasi yang berbeda. Agus Rahardjo membagi 4 (empat) jenis teori kriminologi yakni : 1)Teori anomi, untuk mencari sebab orang melakukan tindak pindana. 2) Teori asosiasi diferensial, karakteristik pelaku kejahatan. 3) Teori kontrol sosial, faktor sosial masyarakat untuk berbuat kejahatan. 4. Teori netralisasi, alasan seseorang berbuat kejahatan[36]. *Penal policy* digunakan mengubah kebijakan aturan undang-undang pidana khususnya yang mengatur kejahatan *cyber crime*

Kejahatan *cyber crime* yang semakin canggih dan semakin banyak korban yang dirugikan secara finansial maka penulis menggangap diperlukannya urgensi penal policy dalam memberikan perlindungan hukum data korban *cyber crime Artificial Intelligence* (AI) di era *society* 5.0 sebagai berikut:

1. Pemerintah memperkuat regulasi aplikasi internet, dengan cara semua aplikasi web internet harus didaftarkan secara resmi di pemerintah melalui Kemeninfo. Pemerintah selalu memantau aplikasi yang terdaftar, apabila terbukti melakukan kejahatan cyber crime pada aplikasi yang terdafar maupun tidak terdaftar pemerintah akan bertindak tegas dengan menutup akun dan memberikan saknsi.
2. Melakukan sosialisasi untuk tidak membalas atau langsung memblokir, kiriman undangan maupun lainnya yang dikirimkan melalui media sosial.
3. Kerjasama antara Kemeninfo dan parat penegak hukum yaitu kepolisian memiliki ahli siber untuk melacak keberadaan pelaku kejahatan, dan mau menerima laporan masyarakat atas data yang dicuri sehingga mengakibatkan kehiangan uang.
4. Melibatkan pertisipasi masyarakat, bagi masyarakat yang merasa dirugikan atau mengetahui akun fake (palsu) dapat segera melaporkan ke kepolisian
5. Penegakan hukum dengan melaksanakan sanksi maksimal, bagi pelaku kejahatan cyber crime. Perlindungan hukum bagi korban *cyber crime* dengan mendapatkan pelayanan dan bantuan hukum.

---

[35] Nugroho Wisnu Pujoyono. *Penal Policy Dalam Upaya Preventif Kejahatan Carding Di Indonesia.* Jurnal Panji Keadilan, Jurnal Ilmiah Nasional Mahasiswa Hukum Universitas Muhammadiyah Bengkulu. 2020. Hal 77

[36] Hardianto Djanggih, Nurul Qamar. *Penerapan Teori-Teori Kriminologi Dalam Penanggulangan Kejahatan Siber (Cyber Crime).* Jurnal Pandeta. Volume 13. Number 1. June 2018. Hal 23

D. Penutup

A. Kesimpulan

1. Konteks *Fiqh Jinayah*, hal ini termasuk dalam kategori jarimah dan pelaku dapat dikenakan hukuman hudud, melalui penerapan sanksi manusia sesuai dengan peraturan dalam Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik.
2. Urgensi penal policy dalam memberikan perlindungan hukum data korban *cyber crime Artificial Intelligence* (AI) di era *society* 5.0 sebagai berikut: Pemerintah memperkuat regulasi aplikasi internet, dengan cara semua aplikasi web internet harus didaftarkan secara resmi di pemerintah melalui Kemeninfo. Pemerintah selalu memantau aplikasi yang terdaftar, apabila terbukti melakukan kejahatan cyber crime pada aplikasi yang terdafar maupun tidak terdaftar pemerintah akan bertindak tegas dengan menutup akun dan memberikan saknsi.

B. Rekomendasi

1. Pemerintah harus menjalin kolaborasi yang baik antar lembaga dan bekerja sama dengan pakar TI dalam memetakan ancaman peretasan dan memprioritaskan fokus pada peningkatan keamanan situs.
2. Diperlukan regulasi yang ketat dan komprehensif untuk aplikasi internet dan kerja sama antara berbagai pihak dalam penegakan hukum dan melibatkan partisipasi masyarakat.

Daftar Pustaka

Al Quran Al Karim Dan Terjemahannya Dengan Literasi. Surat An-Nisa Ayat 4 Departemen Agama Ri. Semarang . Pt. Karya Toha. 2024.

Al Quran Al Karim dan Terjemahannya Dengan Literasi. *Surat Al-Mudatsir ayat 38*. Departemen Agama RI. Semarang. PT. Karya Toha. 2024.

Al Quran Al Karim dan Terjemahannya Dengan Literasi. *Surat Fatir ayat 18*. Departemen Agama RI. Semarang. PT. Karya Toha. 2024.

Angkasa. *Cybercrime Di Era Industri 4.0 Dan Masyarakat 5.0 Dalam Perspektif Viktimologi.* Jurnal Justiciabelen. Vol 2, No 02. 2022.

_____. Windiasih, Rili. Juanda, Ogiandhafiz. *Efektivitas Rancangan Undang-Undang Penghapusan Kekerasan Seksual Sebagai Hukum Positif Dalam Perspektif Viktimologi*. Jurnal USM Law Review. Vol. 4. No. 1. June 2021.

Asep Saepudin Jahar, Nurul Adhha. Hazmi, Raju Moh. *Construction Of Legal Justice, Certainty, And Benefits In The Supreme Court Decision*. Cita Hukum. Vol. 9. No. 1. 2021

Criswara, Nadila. *Analisis Yuridis Kekerasan Gender Berbasis Online (KGBO) dengan Deepfakes Ditinjau dari Hukum Positif*. Proceedings Series on Social Sciences & Humanities, Volume 17 Proceedings of Seminar International Legal Development in Twenty-First Century Era.

Djanggih, Hardianto. Qamar, Nurul. *Penerapan Teori-Teori Kriminologi Dalam Penanggulangan Kejahatan Siber (Cyber Crime).* Jurnal Pandeta. Volume 13. Number 1. June 2018.

Flora, Henny Saida. Sitanggang, Tiromsi. Simarmata, Berlian. Karina, Ica. *Keadilan Restoratif Dalam Melindungi Hak Korban Tindak Pidana Cyber: Manifestasi Dan Implementasi.* Jurnal Ius Constituendum. Vol. 8 No. 2. 2023.

Gunawan, Hendra. Tindak Kejahatan Cyber Crime Dalam Perspektif Fikih Jinayah. Jurnal El-Qanuniy Vol. 6 No. 1 Edisi Januari-Juni 2020Kamran, Muhammad. Maskun. *Penipuan Dalam Jual Beli Online: Perspektif Hukum Telematika*. Balobe Law Journal. Vo. 1,.No. 1. 2021.

Hanalisis, Monica Shelsa. *Tindak Pidana Pencurian Data Pribadi Melalui Teknik Phising Ditinjau Dalam Prespektif Fiqih Jinaya, Hukum Pidana Islam*. Skripsi. Fakultas Syariah Dan Hukum Universitas Islam Negeri Walisongo Semarang. 2022

Harun, Farhan Aulia. Nurhadiyanto, Lucky. *Rekayasa Konten Pornografi Berbasis AI Image Generator dalam Perspektif Space Transition*. Ranah Research : Journal of Multidisciplinary Research and Development Vol. 6, No. 3, Maret. 2024.

Kenedi, John. *Kebijakan Hukum Pidana (Penal Policy) Dalam Sistem Penegakan Hukum Di Indonesia.* Yogyakarta: Pustaka Pelajar : 2017.

Kurniawan, Fajar. Suhariyanto, Didik. Hartana. *Perlindungan Konsumen Terhadap Pinjaman Onlineatas Penyebaran Data Pribadi.* Journal Of Social Science Research Vol 4. No. 1. 2024.

Munajat, Makhrus. *Hukum Pidana Islam; Fiqih Jinayat*. Yogyakarta: Pesantren Nawasea Press, 2020.

Muyasir, Ahmad. *Kejahatan Defecting: Studi Perbandingan Antara Undang-Undang ITE Dan Hukum Pidana Islamal MazaHib.* Vol. 3. No. 1. Juni 2019

Muslih, Muhamma. Sahabuddin, Said. Tanzil. *Pengungkapan Kejahatan Hacking Mengakses Sistem Elektronik Milik Orang Lain Di Wilayah Hukum Polres Batanghari.* Legalitas: Jurnal Hukum. Vol 15. No. 2. Desember. 2023.

Nawawi, Barda. *Tindak Pidana Mayantara: Perkembangan Cyber Crime di Indonesia*. Jakarta; RajaGrafindo Persada. 2020.

Novyanti, Pudji Astuti Jerat Hukum Penyalahgunaan Aplikasi *Deepfake* Ditinjau Dari Hukum Pidana. Jurnal Novum. Hukum Jurusan Hukum Universitas Negeri Surabaya. 2021.

Pujoyono, Nugroho Wisnu. *Penal Policy Dalam Upaya Preventif Kejahatan Carding Di Indonesia.* Jurnal Panji Keadilan, Jurnal Ilmiah Nasional Mahasiswa Hukum Universitas Muhammadiyah Bengkulu. 2020

Rachmadie, Donovan Typhano. *Regulasi Penyimpangan Artificial Intelligence Pada Tindak Pidana Malware Berdasarkan Undang-Udang Republik Indonesia Nomor 19 Tahun 2016.*Jurnal Recidive, Jurnal Hukum Pidana dan Penanggulanggan Kejahtan. Vol.9 No.2. 2020.

Rahmana, Radya Dzuhrizha. Kartika, Adhitya Widya. *Penegakan Hukum Bagi Pelaku Pembuatan Dan Penyebaran Scam Page (Studi Di Kepolisian Daerah Jawa Timur).* Jurnal Risalah Hukum . Vol.18. No. 2. 2022.

Rovida, Khofidhotur. Sasmini. *Konsep Pencegahan Cyberbullying Berbasis Techno Prevention Pada Era Society 5.0 di Indonesia*. Jurnal Hukum Ius Quia Iustum, (2024), pp. 461-485 ISSN 0854-8498 (Print) 2527-502X (Online).

Siburian, Hinsa. Pakel, Dominggus. *Lanskap Kemanan Siber Indonesia Tahun 2023*. Penerbit Badan Siber Sandi Negara (BSSN). 2024.

Syafiqotuzzuhda. *Problematika Hukum Perlindungan Konsumen Dalam Menghadapi Kejahatan Berbasis Artificial Intellegence.* Skripsi. Universitas Islam Negeri Maulana Malik Ibrahim. 2023.

Suharyadi. Sampara, Said. Ahmad, Kamri. *Kejahatan Dunia Maya (Cyber Crime) Dalam Prespektif Hukum Islam*. Journal Of Lex Generalis. Vol.1. No.5, Oktober. 2020.

Wansyah. *Penelitian Hukum, Pilihan Metode Dan Praktik Penulisan Artikel*. Edisi ke 3. Yogyakarta: Mira Buana Media. 2020.

Widayanti, Putri Wahyu. Tindak Pidana Pencurian Data Nasabah Dalam Bidang Perbankan Sebagai *Cyber Crime* Legacy : Jurnal Hukum Dan Perundang-Undangan Vol 2 No 2 - Agustus 2022.

Widiatno, Andi . *Cyberporn Dalam Pasar Digital Non-Fungible Tokens: Prespektif Undang-Undang Informasi Transaksi Elektronik Dan Pornografi.* Journal Justiciabelen. Vol 2. No. 2. 2022.

Website/Internet;

Yusuf. *Serangan Siber*. Https://Www.Kominfo.Go.Id/Content/Detail/57320/Siaran-Pers-No-412. Hmkominfo062024-Tentang-Indikasi-Serangan-Siber-Wamenkominfo-Fokus-Tangani-Dampak-Layanan Pemerintah/0/Siaran_Pers.

Peraturan Perundang-Undangan

Undang-Undang Nomor 1 Tahun 2024 Tentang Informasi Dan Transaksi Elektronik

Peraturan Presiden Nomor 53 Tahun 2017 Tentang Badan Siber dan Sandi Negara (BSSN)

Peraturan Presiden (Perpres) Nomor 28 Tahun 2021 Tentang Badan Siber Dan Sandi Negara (BSSN)