INNOVATIVE: Journal Of Social Science Research
Volume 3 Nomor 2 Tahun 2023 Page 12190-12201
E-ISSN 2807-4238 and P-ISSN 2807-4246
Website: https://j-innovative.org/index.php/Innovative

Analisis Yuridis Terhadap Artificial Intelligence Pada Tindak Pidana Penyebaran Malware Di Indonesia

Fatmawati [1✉], Raihana [2]
(1) Jurusan Hukum, Fakultas Hukum, Universitas Lancang Kuning
(2) Jurusan Hukum, Fakultas Hukum, Universitas Muhammadiyah Riau
Email: fatmapanjaitan022@gmail.com [1✉]

Abstrak

Kemajuan ilmu pengetahuan dan pembangunan di era globalisasi dan modernisasi semakin menuntut. Demikian pula, penyebaran data dan akses ke media menjadi lebih sederhana dan lebih cepat. Internet adalah hasil dari kemajuan rasional dan kreatif yang dilakukan oleh manusia, dan keuntungan dari Internet sangat beragam, salah satunya adalah kumpulan jaringan yang menyediakan hiburan online. Perkembangan teknologi telah mengubah kehidupan masyarakat dan sebagai akibat dari perkembangan itu, dunia telah menambah dimensi kehidupan sejalan dengan perkembangan kejahatan teknologi. Studi ini menunjukkan bahwa penerapan kecerdasan buatan dalam kejahatan malware termasuk dalam kategori kejahatan komputer, karena komputer dan teknologi kecerdasan buatan digunakan sebagai alat untuk melakukan kejahatan. Hukum pidana yang dapat menjerat kegiatan tersebut antara lain KUHP, UU Hak Cipta, UU Pencucian Uang, UU Transfer Uang, UU Dokumen Dagang, Permencominfo No. 20 Tahun 2016 dan UU Terorisme. Namun, undang-undang Lex Specialis dan Lex Posterior ITE adalah undang-undang agresif yang paling cocok untuk mengatasi kejahatan ini, meskipun kelemahannya adalah istilah terkait malware dan kecerdasan buatan tidak disebutkan secara spesifik.

Kata Kunci: *Malware, Artificial Intelligence, Cyber Crime.*

Abstract

Advances in science and development in the era of globalization and modernization are increasingly demanding. Likewise, data dissemination and access to media becomes simpler and faster. The Internet is the result of rational and creative progress made by humans, and the advantages of the Internet are very diverse, one of which is a collection of networks that provide online entertainment. Technological developments have changed people's lives and as a result of these developments, the world has added a dimension of life in line with the development of technological crimes. This study shows that the application of artificial intelligence in malware crimes is included in the category of computer crimes, because computers and artificial intelligence technology are used as tools to commit crimes. Criminal laws that can ensnare these activities include the Criminal Code, Copyright Law, Money Laundering Law, Money Transfer Law, Trade Documents Law, Permencominfo No. 20 of 2016 and the Terrorism Law. However, the Lex Specialis and Lex Posterior ITE laws are the most suitable aggressive laws to tackle this crime, although the drawback is that the terms related to malware and artificial intelligence are not specifically mentioned.
Keywords: *Malware, Artificial Intelligence, Cyber Crime*

PENDAHULUAN

Internet memudahkan manusia untuk berinteraksi dan mencari informasi, batas ruang dan waktu menjadi hilang dengan adanya jaringan internet. Dengan adanya perkembangan teknologi informasi ini tidak menutup kemungkinan akan melahirkan tindak pidana baru, yang membedakan adalah kejahatan ini dilakukan dengan media maya atau media virtual dan dalam melakukan tindak pidana tersebut menggunakan teknologi sebagai alat bantu. Tindak pidana dalam bentuk media maya atau dunia virtual disebut *cyber crime*. *Cyber crime* adalah kejahatan di dunia maya atau dunia maya, yaitu kejahatan yang muncul sebagai akibat dari revolusi teknologi informasi. Cyber crime mengacu pada kejahatan yang berkaitan dengan dunia maya dan kejahatan yang melibatkan penggunaan komputer (Didik M Arief Mansur & Elisatris Gultom, 2005).

Cyber crime memiliki berbagai jenis tindak pidana, antara lain: *hacking* dan *cracking* (memasuki komputer atau sistem elektronik tanpa ijin), *carding* (mencuri nomor kartu kredit milik orang lain), *phising* (penipuan website yang namanya hampir sama dengan aslinya), *defacing* (mengalihkan website asli ke website lain), *spamming* (pengiriman informasi atau berita secara berulangulang), *malware* (program atau *software* jahat yang menyusup ke dalam komputer atau sistem komputer) dan masih banyak lagi bentuk tindak pidana *cyber crime* tersebut. Serangan *Malware* di Indonesia cukup memperihatinkan, hal ini dibuktikan berdasarkan data keamanan siber *Microsoft* pada

akhir 2018, Indonesia berada di posisi ke-3 negara yang paling banyak terkena *malware* di perangkat komputer. Berdasarkan data internal pusat keamanan siber perusahaan di Washington, AS, serangan siber yang paling banyak menyerang Indonesia adalah jenis *Malware*. *Malware* masih menjadi momok di dunia siber karena *malware* dibuat secara khususagar tersembunyi sehingga mereka bisa tetap berada di dalam sebuah sistem untuk periode waktu tertentu tanpa sepengetahuan pemilik sistem tersebut sehingga keamanan sebuah sistem tersebut tidak dapat mengetahui bahwa sistemnya telah terinfeksi *malware*. Era teknologi sekarang memasuki era kecerdasan buatan atau yang sering disebut *Artificial Intelligence* disingkat AI. AI mengacu pada simulasi kecerdasan manusia oleh mesin yang diprogram untuk berpikir secara manusiawi dan meniru tindakannya, kecerdasan buatan sendiri dicirikan oleh kemampuan untuk bernalar dan mengambil tindakan yang memiliki peluang terbaik untuk mencapai tujuan tertentu.

Pemanfaatan kekuatan teknologi AI bisa dibilang salah satu *item* agenda penting diiringi berkembangnya revolusi Industri 4.0 dimana kunci dari revolusi tersebut terletak pada *Big Data* dan AI. AI dalam banyak organisasi bisnis di seluruh dunia digunakan untuk mengontrol data perusahaan dan menggunakan pembelajaran mesin untuk memahami tren bisnis adalah hal biasa. Namun disisi lain peretas juga mengeksplorasi teknologi ini untuk membuat *malware* yang ditenagai AI yang dapat menyebarkan aplikasi berbahaya yang tidak bisa dilacak dalam muatan data yang tidak berbahaya. Teknik AI dapat menyembunyikan kondisi yang diperlukan untuk membuka muatan berbahaya sehingga hampir tidak mungkin untuk merekayasa ulang ancaman, teknik tersebut juga berpotensi melewati sistem deteksi intrusi *anti-virus* dan *malware* moderen. *Malware* berteknologi AI dapat dilatih untuk menunggu hingga terjadi tindakan spesifik yang memicu muatan bermusuhan. Ini mungkin digerakkan oleh pengenalan suara atau wajah, atau bahkan oleh properti geo-lokasi. Dapat dikatakan bahwa malware AI dapat dilatih untuk mendengarkan kata- kata tertentu atau suara orang yang ditargetkan

Salah satu hal sulit yang akan ditemukan dalam penangan hukum tindak pidana penyebaran malware adalah saat proses hukum terkandang menjadi terkendala karena pelaku tidak dapat ditemukan atau tidak ada orang/ kelompok yang dapat mempertanggungjawabkan kejahatan tersebut dan biasanya pelaku berasal dari luar negeri. Di Indonesia memang belum terjadi penyerangan deepfake atau modus malware-AI lainnya, namun serangan malware sudah marak terjadi dan teknologi AI saat ini sudah mulai berkembang sehingga membuat kita mawas diri akan hal keamanan siber (cyber security).

Berdasarkan kecenderungan tersebut, malware yang mengimplementasikan kecerdasan buatan belum diatur secara khusus dalam UU Informasi dan Elektronika atau disingkat UU ITE. Undang-undang tidak secara optimal mengatur penegakan hukum dalam kasus kejahatan dunia maya, terutama terkait malware yang diimplementasikan oleh kecerdasan buatan, sehingga penegakan hukum tidak seaktif dan represif mungkin. Oleh karena itu, penulis tertarik untuk membahas bagaimana mengatur kejahatan cyber-malware dengan menggunakan teknologi AI berdasarkan undang-undang ITE saat ini di Indonesia.

METODE PENELITIAN

Metode penelitian yang digunakan dalam penelitian ini adalah studi literatur (library research) (P. Andi, 2012). Jenis pendekatan penelitian yang digunakan oleh peneliti di dalam penelitian ini adalah penelitian hukum normatif dengan pendekatan teori dan asas hukum, terkhususnya dalam penelitian ini difokuskan pada pembahasan mengenai kekuatan-kekuatan sosial yang mempengaruhi hukum dan fungsi hukum di masyarakat. Penelitian hukum normatif didefinisikan penelitian yang mengacu kepada norma-norma hukum yang terdapat dalam peraturan perundang-undangan maupun putusan pengadilan. Penelitian hukum normatif bisa juga disebut sebagai penelitian hukum doctrinal (Jonaedi Effendi & Johnny Ibrahim, 2018). Pada dasarnya, globalisasi menciptakan berbagai tantangan dan permasalahan baru yang harus dijawab, dipecahkan dalam upaya memanfaatkan globalisasi untuk kepentingan kehidupan (Erwin Muslimin et al., 2022).

Prosedur dalam penelitian ini dilaksanakan dengan tahapan-tahapan yaitu mengumpulkan data Pustaka, membaca, mencatat, menelaah, mengumpulkan konsep atau naskah kemudian dilakukan elaborasi dan eksplanasi terhadap data atau teks yang terkumpul berkaitan dengan topik pembahasan utama di dalam penelitian ini. Hal ini sesuai dengan pendapat Zed (M. Zed, 2008) yang mengatakan bahwa riset Pustaka tidak hanya sebatas urusan membaca dan mencatat literatur atau buku, melainkan serangkaian kegiatan yang berkenaan dengan metode pengumpulan data Pustaka, membaca, mencatat serta mengolah suatu bahan penelitian.

HASIL DAN PEMBAHASAN

Perkembangan komputer saat ini merespon perubahan zaman dan apa yang terjadi dengan masyarakat dunia yang selalu ingin menemukan sesuatu yang baru melalui pengolahan, penelitian dan pengembangan serta membuat penemuan-penemuan baru yang kompleks dan modern dari hasil pemikiran mereka (Suisno, 2014). Kecerdasan buatan yang selanjutnya disebut AI merupakan sebuah studi tentang bagaimana membuat komputer melakukan hal-hal yang pada saat ini dapat dilakukan lebih baik oleh manusia. Banyaknya permasalahan kompleks yang dihadapi manusia saat ini membuat manusia bahkan komputer sulit untuk menyelesaikannya (Elaine Rich & Kevin Knight, 1991). Malware atau Malicous Software merupakan perangkat lunak yang secara eksplisit didesain untuk melakukan aktifitas berbahaya atau perusak perangkat lunak lainnya (S. Kramer & Bradfield, 2010). Keduanya merupakan buah dari perkembangan teknologi, AI yang merupakan hadiah dari inovasi teknologi pada akhirnya dapat menjadikan Malware yang merupakan bencana perkembangan teknologi menjadi senjata yang mematikan dan mengancam keamanan. Contoh dari tindak pidana Malware-AI sudah banyak terjadi seperti deepfake video atau voice, Jackpotting, phising spear dan masih banyak lagi.

Malware memiliki berbagai jenis dan perkembangan jenis malware semakin hari semakin beragam, dalam berbagai jenis terebut malware memilik nama yang berbeda. Secara garis besar modus operandi malware terangkum kedalam 4 insiden siber. Malware dalam 4 insiden siber tersebut digunakan untuk:

1. Penolak Akses

   Malware berbentuk virus juga dimanfaatkan pelaku untuk membuat serangan DDoS dengan cara menyebarkan file yang berisi virus di berbagai situs internet dengan rekayasa sosial yang membuat korban mengundu file tersebut dan membuat komputer tersebut terinfeksi virus. Ketika komputer telah terinfeksi virus DDoS maka akan secara otomatis virus terebut akan melaksanakan protokol serangan DDoS.

2. Pemerasan

   Terdapat beberapa malware yang dirancang untuk mengenskripsi data korban sehingga korban tidak memiliki akses untuk menggunakan datanya kembali. Untuk mendapatkannya kembali biasanya pelaku akan meminta korban untuk membayar tebusan berupa “kunci” untuk mengenkripsi data korban kembali. Ada beberapa pelaku yang memanfaatkan kepanikan korban sehingga pelaku melakukan pemerasan lebih yang menguras uang korban. Malware yang memiliki modus operandi ini adalah Ransomware, Lockscreen, Ransomware WannaCry hingga

Ransomware palsu dan berbagai nama ransomware yang memiliki nama yang beragam karena perkembangannya.

3. Spionase

   Spionase yang dilakukan mulai dari akses pada layar komputer, webcam (kamera pada komputer) hingga merekam ketikan keyboard (keyologger) kegiatan ini dapat disebut juga sebagai Spyware, program malware yang mampu memata-matai aktivitas pengguna komputer seseorang. Pelaku telah melakukan penerobosan akses tanpa seizin pemilik komputer sehingga hal ini telah melanggar hukum karena mebuat rasa tidak nyaman korban dan berpotensi menyalahgunakan informasi-informasi yang telah didapatkan korban. Biasanya pelaku menjual infromasi korban kepada penyedia layanan iklan sehingga dapat menampilkan iklan yang relevan. Kondisi terburuknya adalah pelaku dapat mengendalikan komputer dari jarak jauh karena telah memiliki akses komputer tersebut

4. Pencurian Informasi

   Pencurian informasi oleh malware adalah serangan yang paling umum dari ketiga modus operandi diatas karena cara kerja malware yang selalu bermuara kepada pencurian informasi. Pelaku yang menerapkan malware dalam serangannya telah merencanakan targetnya terlebih dahulu untuk menentukan jenis malware apa yang digunakan. Perkembangan teknologi sekarang yang memasuki revolusi industri 4.0 melibatkan banyak data didalamnya, akses serba digital menjadi target populer oleh cyber threat actor untuk melakukan serangan terhadapnya. Pencurian informasi data pribadi sangat populer belakangan tahun ini, karena pelaku dapat memanfaatkan data tersebut untuk berbagai insiden siber.

Perkembangan Malware melahirkan berbagai jenis modus operandi demi melaksanakan niat jahatnya, penerapan AI didalamnya dapat mengotomatisasi modus-modus sehingga memudahkan pelaku untuk melakukan kejahatan. Pembuat malware dapat memanfaatkan AI yang selanjutnya disebut Malware-AI digunakan untuk:

a. Menghasilkan jenis malware baru yang tak terdeteksi. Melalui algoritma dan pembelajaran mesin menghasilkan sebuah teknik yang dapat diciptakan kembali dan selalu meningkat untuk mempelajari jenis malware yang memiliki kemungkinan kecil untuk terdeteksi kemudian melakukan serangan dengan karakteristik yang sama.
b. Menyembunyikan malware dari jaringan. Malware dapat memonitor perilaku jaringan korban dan membangun pola yang sama seperti jaringan yang legal.
c. Mengkombinasi berbagai teknik serangan. Teknik yang dilakukan untuk

menggabungkan serangkaian teknik untuk menemukan opsi paling efektif agar tidak terdeteksi dan memprioritaskan alternatif dari serangan yang kurang berhasil

d. Menyesuaikan fitur/fokus malware berdasarkan kondisi lingkungan. Penyerang yang ingin menyerang sebuah browser tidak perlu lagi memasukkan daftar lengkap browser, pelaku hanya perlu menerapkan informasi umum saja karena dengan bantuan algoritma AI yang telah dilatih dan belajar, AI lebih memahami seluk beluk browser sehingga dengan mudah dapat menyusup.
e. Menerapkan mekanisme penghancuran diri dalam malware jika terdeteksi perilaku ganjil. Malware telah diterapkan penghancuran diri (self destruction) untuk menghindari deteksi.
f. Mendeteksi lingkungan yang mencurigakan. Malware dapat menghindari lingkungan yang mencurigakan seperti alat-alat yang digunakan oleh peneliti anti-malware dan menghentikan aktivitasnya untuk menghindari deteksi.
g. Meningkatkan kecepatan serangan. Kecepatan serangan bisa menjadi sangat penting, terutama dalam kasus-kasus seperti pencurian data. Algoritma dapat melakukan ekstraksi jauh lebih cepat daripada manusia, membuatnya lebih sulit untuk dideteksi dan hampir tidak mungkin dicegah - karena mesin dapat menyalin data dari perimeter yang dilindungi sebelum anti-malware dapat beraksi.
h. Membiarkan perangkat lain belajar bersama dan mengidentifikasi bentuk serangan yang paling efektif dalam satu jaringan botnet, masing-masing bot dimanfaatkan untuk menguji hasil teknik infiltrasi dalam satu waktu dan memberikan laporan untuk mempelajari target dalam waktu singkat.

Dengan kata lain penerapan AI dalam tindak pidana malware dapat dikatakan sebagai computer-related crime dimana teknologi AI dan komputer sebagai alat bantu kejahatan dalam meretas dan melakukan tindak kejahatan siber lainnya. Berdasarkan penelitian penulis, tindak pidana Malware-AI belum diatur secara gramatikal dalam peraturan undang-undang di Indonesia. Namun terdapat berbagai aturan pidana diluar UU ITE yang sekiranya mampu untuk menerat tindak pidana tersebut karena UU ITE merupakan peraturan yang paling baru dan paling khusus untuk menangani tindak pidana siber.

Lex Specialis derogat lege generali adalah asas yang mengandung makna bahwa hukum yang bersifat khusus (Lex Specialis) mengesampingkan hukum yang bersifat umum (Lex generali). Lex posterior derogat legi priori adalah asas penafsiran hukum yang menyatakan bahwa hukum yang terbaru (Lex Posterior) mengesampingkan hukum yang

lama (Lex prior). Undang-Undang Republik Indonesia nomor 11 tahun 2008 tentang informasi dan transaksi elektronik sebagaimana diubah dengan Undang-Undang nomor 19 tahun 2016 merupakan Lex Specialis dan Lex Posterior yang saat ini paling sesuai mengatur perbuatan Malware-AI. Penulis mengkaji beberapa pasal yang menurut penulis dapat diterapkan pada tindak pidana Malware-AI.

Pasal 31 ayat (2) UU ITE:

Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atas transmisi informasi elektronik dan/atau dokumen elektronik yang tidak bersifat publik dari, ke, dan di dalam suatu komputer dan/atau sistem elektronik tertentu milik orang lain, baik yang tidak menyebabkan perubahan apa pun maupun yang menyebabkan adanya perubahan, penghilangan, dan/atau penghentian informasi elektronik dan/atau dokumen elektronik yang sedang ditransmisikan.

Pasal (3) menyebutkan "Kecuali intersepsi sebagaimana dimaksud pada ayat (1) dan ayat (2), intersepsi yang dilakukan dalam rangka penegakan hukum atas permintaan kepolisian, kejaksaan, dan/atau institusi penegak hukum lainnya yang ditetapkan berdasarkan undang-undang."

Berdasarkan uraian pasal diatas mengenai penyadapan, perubahan dan pengilangan data diluar intersepsi yang dilakukan dalam rangka penegakan hukum adalah dilarang. Perbuatan Malware-AI dalam pelaksanaan tujuannya adalah untuk kepentingan pribadi demi mendapatkan keuntungan melalui jalan kriminal.

Pasal 32 ayat (1) UU ITE "Setiap orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu informasi elektronik dan/atau dokumen elektronik milik orang lain atau milik publik."

Pasal 32 ayat (2) UU ITE "Setiap orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun memindahkan atau mentransfer informasi elektronik dan/atau dokumen elektronik kepada sistem elektronik orang lain yang tidak berhak."

Pasal 32 ayat (3) UU ITE "Terhadap perbuatan sebagaimana dimaksud pada ayat (1) yang mengakibatkan terbukanya suatu informasi elektronik dan/atau dokumen elektronik yang bersifat rahasia menjadi dapat diakses oleh publik dengan keutuhan data yang tidak sebagaimana mestinya."

Berdasarkan uraian pasal diatas yang melarang perbuatan perusakan, pemindahan dan penghilangan data karena dapat mengakibatkan terbukanya suatu informasi yang bersifat rahasia menjadi dapat diakses oleh publik karena malfungsi sebuah program

yang sengaja dibentuk oleh pelaku. Malware-AI akan mengenskripsi data yang mana data tersebut dapat sewaktu-waktu disebarluaskan pelaku jika keinginannya tidak dapat dituruti.

Pasal 33 UU ITE "Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan tindakan apa pun yang berakibat terganggunya sistem elektronik dan/atau mengakibatkan sistem elektronik menjadi tidak bekerja sebagaimana mestinya." Menurut Pasal ini perbuatan yang dilarang adalah perbuatan yang dapat membuat sistem tidak dapat bekerja atau memperlambat sebuah sistem tersebut. Virus dan Worm yang merupakan produk dari Malware-AI memang diciptakan untuk mengganggu sistem komputer milik orang lain agar sistem komputer tersebut menjadi lambat bahkan bisa sampai sistem tersebut tidak berfungsi.

Pasal 34 ayat (1) UU ITE:

Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum memproduksi, menjual, mengadakan untuk digunakan, mengimpor, mendistribusikan, menyediakan, atau memiliki:

a. Perangkat keras atau perangkat lunak Komputer yang dirancang atau secara khusus dikembangkan untuk memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 33;
b. Sandi lewat Komputer, Kode Akses, atau hal yang sejenis dengan itu yang ditujukan agar Sistem Elektronik menjadi dapat diakses dengan tujuan memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 33."

Pasal 34 ayat (2) UU ITE "Tindakan sebagaimana dimaksud pada ayat (1) bukan tindak pidana jika ditujukan untuk melakukan kegiatan penelitian, pengujian Sistem Elektronik, untuk perlindungan Sistem Elektronik itu sendiri secara sah dan tidak melawan hukum."

Berdasarkan uraian pasal diatas Malware-AI termasuk kedalam penylahgunaan perangkat keras atau perangkat lunak yang dilarang didalam pasal tersebut. Perangkat keras yang tujuan awalnya bukan untuk kejahatan, disalahgunakan pelaku untuk memfasilitasi tindak kejahatan mereka. Sama halnya dengan perangkat lunak teknologi AI yang ditujukan untuk membantu manusia malah digunakan untuk menyerang dan membuat susah pekerjaan manusia. Salah satu teknik Jackpotting pada ATM merupakan bentuk nyata penyalahgunaan perangkat keras.

Pasal 36 UU ITE "Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan perbuatan sebagaimana dimaksud dalam pasal 27 sampai dengan pasal 34

yang mengakibatkan kerugian bagi orang lain." Pasal ini melarang perbuatan yang dilakukan dengan sengaja merugikan orang lain. Malware-AI banyak menimbulkan kerugian pihak lain karena Malware-AI menghambat aktifitas komputer korban, membuat korban tidak dapat menyelesaikan perkerjannya dan meminta tebusan untuk membebaskan file yang telah dikunci oleh pelaku Malware-AI.

Penyimpangan penerapan teknologi AI pada tindak pidana malware (Malware-AI) merupakan sisi gelap dalam berkembangnya teknologi. Masalah- masalah yang ditimbulkan rumit dan menyentuh berbagai aspek dalam satu kali aksi. Hukum sebagai alat pembaharuan sosial (a tool of social engineering) harus dapat memberikan jalan bagi perkembangan-perkembangan yang terjadi di masyarakat, terutama dalam perkembangan teknologi. Untuk itu pengaturan alih teknologi sebagai tolak ukur kemajuan negara miskin dan berkembang harus dapat diatur secara hukum tersendiri (O. C. Kaligis (Otto Cornelis), n.d.).

Perbuatan Malware-AI sendiri dapat dikriminalisasi menjadi tindak pidana siber atau kejahatan mayantara (cyber crime) karena telah memenuhi karakteristik cyber crime sebagaimana kejahatan tersebut telah diatur dalam hukum positif Indonesia. Namun hukum positif di Indonesia sebenarnya tidak terlalu kuat untuk menjerat pelaku tindak pidana Malware-AI karena dalam peraturan berbagai sektor yaitu KUHP, UU Hak Cipta, UU TPPU, UU Transfer dana, UU Dokumen Perusahaan, Permenkominfo no 20 tahun 2016 dan, UU terorisme maupun Undang-Undang ITE sebagai hukum positif terbaru sebagai pengenaan tindak pidana ini belum mengatur secara jelas dan rinci yang mana secara gramatikal tidak dituangkannya kata Malware dan juga kecerdasan buatan (Artificial Intelligence atau AI) didalam peraturan tersebut.

SIMPULAN

Penerapan KUHP untuk menerapkan penyimpangan AI dalam kejahatan malware dilakukan sesuai dengan ketentuan yang berlaku, meskipun secara gramatikal hal tersebut tidak tertuang dalam peraturan terkait yaitu UU ITE. Tindakan AI malware diklasifikasikan sebagai kejahatan komputer karena kecerdasan buatan dan teknologi komputer digunakan untuk melakukan kejahatan. Hukum pidana yang relevan menganggap penggunaan dan penyimpangan kecerdasan buatan sebagai kejahatan dunia maya terhadap malware. UU Pidana, UU Hak Cipta, UU TPPU, UU Pengiriman Uang, UU Surat Perusahaan, Permencominfo No. 20 Tahun 2016 dan UU Terorisme dapat diberlakukan terhadap UU ini namun mengacu pada Lex specialis derogat lege generali

dan Lex posterior derogat lege priori. UU ITE adalah Ahli Lex dan Lex berdasarkan ketentuan ini paling cocok untuk menuntut penggunaan kecerdasan buatan dan penyimpangan malware.

DAFTAR PUSTAKA

A. Kumedi Ja'far. (2010). PENGARUH GLOBALISASI TERHADAP PEMBANGUNAN HUKUM EKONOMI DIINDONESIA. ASAS, 2(2), 16.

Barda Nawawi Arief. (2005). Pembaharuan Hukum Pidana dalam Perspektif Kajian Perbandingan. Badan Penerbit Universitas Diponegoro.

DHARMA SETIAWAN PAGARALAM. (2014). IMPLIKASI GLOBALISASI DAN PENEGAKAN HUKUMPROGRESIF DI INDONESIA. KEADILAN PROGRESIF, 2(1), 24.

Erwin Muslimin, Deden Heri, & Mohamad Erihadiana. (2022). Kesiapan Merespon terhadap Aspek Negatifdan Positif Dampak Globalisasi Dalam Pendidikan Islam. Jurnal Dirosah Islamiyah, 4(1), 60.

Geofani Milthree Saragih. (2022a). Pancasila Sebagai Landasan Filosofis Pembentukan Peraturan Perundang-Undangan Di Indonesia. JUPANK : Jurnal Pancasila Dan Kewarganegaraan, 2(1), 20.

Geofani Milthree Saragih. (2022b). Tinjauan Yuridis Terhadap Tindak Lanjut Putusan Mahkamah Konstitusi Dalam Pengujian Undang-Undang Terhadap Undang-Undang Dasar 1945 Oleh Lembaga Negara DiIndonesia [Skripsi]. Universitas Riau.

Jonaedi Effendi, & Johnny Ibrahim. (2018). Metode Penelitian Hukum Normatif dan Empiris. Kencana.

M. Zed. (2008). Metode Penelitian Kepustakaan. Yayasan Obor Indonesia.

Mohammad Maiwan. (2014). MEMAHAMI POLITIK GLOBALISASI DAN PENGARUHNYA DALAM TATA DUNIA BARU: ANTARA PELUANG DAN TANTANGAN. Jurnal PAMATOR, 7(1), 2.

P. Andi. (2012). Metode Penelitian Kualitatif dalam Perspektif Rancangan Penelitian. Ar-Ruzz Media. Randy Pradityo. (2017). MENUJU PEMBAHARUAN HUKUM PIDANA INDONESIA: SUATU TINJAUAN SINGKAT. Jurnal Legislasi Indonesia, 14(2), 140.

Ratno Lukito. (2022). "Compare But Not to Compare": Kajian Perbandingan Hukum di Indonesia. Undang: Jurnal Hukum, 5(2), 287.

Sudarto. (1989). Hukum Pidana Jilid I A-B. Fakultas Hukum Universitas Diponegoro.

Sudiyana. (2016). PENGARUH GLOBALISASI TERHADAP PEMBANGUNAN EKONOMI DAN IMPLIKASIHUKUMNYA. JURNAL KAJIAN HUKUM, 1(1), 23.

Syprianus Aristeus. (2018). TRANSPLANTASI HUKUM BISNIS DI ERA GLOBALISASI TANTANGAN BAGI INDONESIA. Jurnal Penelitian Hukum DE JURE, 18(4), 515.