REGULASI PENYIMPANGAN *ARTIFICIAL INTELLIGENCE* PADA TINDAK PIDANA *MALWARE* BERDASARKAN UNDANG-UDANG REPUBLIK INDONESIA NOMOR 19 TAHUN 2016

Donovan Typhano Rachmadie, Supanto
E-mail : donovanrachmad@yahoo.co.id

Abstrak

Penelitian ini bertujuan untuk mengetahui pengaturan pidana penerapan *artificial intelligence* pada tindak pidana *malware* berdasarkan Undang-Undang nomor 19 tahun 2016 tentang perubahan atas Undang-Undang nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik. Penelitian ini termasuk jenis penelitian hukum normatif yang bersifat preskriptif dengan pendekatan undang-undang (*statue approach*) dan pendekatan konseptual (*conseptual approach*). Penelitian menggunakan bahan hukum primer, sekunder dan bahan non hukum yang berkaitan. Perkembangan teknologi telah merubah kehidupan masyarakat, akibat perkembangan tersebut dunia menambah dimensi kehidupan yang mana hal itu selaras dengan berkembangnya kejahatan teknologi. Dalam penelitian ini menghasilkan bahwa penerapan AI dalam tindak pidana *malware* merupakan kategori *computer-related crime* karena pemanfaatan komputer dan teknologi AI sebagai alat bantu dalam melakukan kejahatan. Aturan-aturan pidana yang dapat menjerat perbuatan tersebut adalah KUHP, UU Hak Cipta, UU TPPU, UU Transfer Dana, UU Dokumen Perusahaan, Permenkominfo no 20 tahun 2016 dan UU Terorisme. Namun UU ITE sebagai *lex specialis* dan *lex posterior* merupakan hukum positif yang paling tepat dalam menjerat tindak pidana tersebut meskipun terdapat kelemahan bahwa tidak disebutkan secara eksplisit pengaturan mengenai *malware* dan AI.

Kata Kunci : *Malware; Artificial Intelligence*/Kecerdasan Buatan; *Cyber Crime*; UU ITE.

Abstract

This study aims to determine the criminal regulation for the application of artificial intelligence in criminal acts of malware based on criminal law in Indonesia, especially in Law number 19 of 2016 concerning amendments to Law number 11 of 2008 concerning Information and Electronic Transactions. This research is a type of normative legal research that is prescriptive in nature with the law approach (statue approach) and conceptual approach (conceptual approach). The study uses primary, secondary and related non-legal material. Technological developments have changed people's lives, as a result of these developments the world added a dimension of life which was in harmony with the development of technological crime. The results showed that the application of AI in malware criminal acts is a category of computer-related crime due to the use of computers and AI technology as a tool in committing crimes. Criminal rules that can ensnare such acts are the Criminal Code, the Copyright Act, the TPPU Law, the Fund Transfer Act, the Company Document Law, the Ministry of Communication and Information No. 20 of 2016 and the Terrorism Law. However, the ITE Law as lex specialis and lex posterior is the most positive positive law in ensnaring these crimes despite the weakness that there is no explicit mention of the regulation regarding malware and AI.

Keywords : *Malware; Artifical Intelligence; Cyber Crime; ITE Law.*

A. Pendahuluan

Teknologi merupakan salah satu bentuk nyata bahwa manusia telah berkembang dan beradab, dengan hadirnya teknologi peradaban dan perilaku manusia berubah menjadi lebih efisien dan lebih mudah. Manusia selalu berusaha untuk menciptakan sesuatu yang dapat mempermudah

aktivitasnya, hal inilah yang mendorong perkembangan teknologi yang telah banyak menghasilkan alat sebagai piranti untuk mempermudah kegiatan manusia, bahkan menggantikan peran manusia dalam suatu fungsi tertentu. Teknologi memegang peran penting di era globalisasi pada saat ini, dimana teknologi telah menjadi bagian yang tidak dapat dipisahkan dalam kehidupan sehari-hari. Perkembangan teknologi telah merubah struktur masyarakat dari yang bersifat lokal menuju ke arah masyarakat yang berstruktur global. Perubahan ini disebabkan oleh kehadiran teknologi informasi. Perkembangan teknologi informasi itu berpadu dengan media dan komputer yang kemudian melahirkan piranti baru yang disebut internet (Wahid dan Labib, 2005: 103).

The United State Supreme Court mendefinisikan internet sebagai *International Network Of Intercontnected Computer*, artinya jaringan internasional dari komputer-komputer yang saling berhubungan (Wahid dan Labib, 2010: 31). 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 tindak pidana dalam dunia maya atau dunia virtual yang merupakan tindak pidana yang timbul akibat dari revolusi teknologi informasi. *Cyber crime* merujuk pada suatu tindakan kejahatan yang berhubungan dunia maya (*cyberspace*) dan tindakan kejahatan yang menggunakan komputer (Didik M Arief Mansur dan Elisatris Gultom, 2005: 3).

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. Menurut data Kominfo, Indonesia mendapat 1,225 miliar serangan siber setiap harinya. Data tersebut didapat dari Kementerian Komunikasi dan Informatika yang diperkuat oleh Kementerian Koordinator Bidang Politik, Hukum, dan Keamanan, seperti tertulis dalam siaran pers dari ESET (Ayu Yuliani, 2017).

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 khusus agar 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 mansia pada mesin yang di program untuk berikir manusia dan meniru tindakannya, karakteristik AI sendiri adalah kemampuannya untuk merasionalisasi 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 (Marty Puranik, 2019).

Pada tahun 2017, Rumah Sakit Harapan Kita dan Rumah Sakit Dharmais di Jakarta menjadi korban serangan *Malware* berjenis Ransomware WannaCry yang juga melanda dunia. Serangan yang dilakukan adalah dengan cara mengunci komputer atau mengenskripsi semua data korban sehingga tidak dapat diakses kembali. Hal itu membuat pelayanan kedua rumah sakit tersebut terhenti. Untuk dapat membuka kembali data tersebut, korban diminta membayar tebusan dalam bentuk bitcoin (mata uang virtual) sebesar US$300 atau sekitar 4 Juta Rupiah atau data mereka lenyap (Lesthia Kertopati, 2017). Penggunaan AI pada *Malware* yang paling menggemparkan adalah teknologi *deepfake* yang dapat menghasilkan tiruan realistis dari suara, wajah dan bagian tubuh lain untuk digunakan menipu korbannya. Sebuah CEO Perusahaan Energi Jerman berhasil ditipu menggunakan *deepfake video* senilai 3,8 Miliyar. Pelaku berhasil memndahkan uang tersebut, alhasil penegak hukum setempat kehilangan jejaknya (Catherine Stupp, 2019). 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 tren tersebut *malware* yang menerapkan AI belum diatur secara khusus didalam Undang-Undang Informasi dan Elektronik atau disingkat sebagai UU ITE. Di dalam peraturan tersebut belum mengatur secara optimal tentang penegakan hukum atas tindak pidana siber khususnya *malware* yang diterapkan AI didalamnya, sehingga belum timbul penegakan hukum yang bersifat prefentif dan represif secara maksimal. Oleh karena itu penulis tertarik membahas bagaimana pengaturan mengenai tindak pidana siber *malware* yang menerapkan teknologi AI didalamnya menurut UU ITE yang berlaku di Indonesia sekarang.

B. Rumusan Masalah

Bagaimana penerapan regulasi hukum pidana dalam mengatur tindak pidana *Malware* berteknologi *Artificial Intelligence* berdasarkan Undang-Undang Nomor 19 Tahun 2016 di Indonesia?

C. Metode Penelitian

Penelitian ini merupakan penelitian yuridis normatif sehingga dalam penulisan ini penulis menggunakan data sekunder. Data sekunder diperoleh dari bahan-bahan kepustakaan dan bahan hukum serta bahan non-hukum lain. Teknik pengumpulan data dilakukan dengan studi kepustakaan atau studi dokumen (*library research*) dengan cara mengkaji dan mempelajari buku-buku, dokumen, laporan dan hasil penelitian lain yang berkaitan. Kemudian data tersebut dianalisis dengan metode silogisme melalui pola berpikir deduktif melalui pendekatan undang- undang (*statue approach*) dan pendekatan konseptual (*Conseptual approach*) untuk mengkaji isu hukum mengenai penerapan dan penyimpangan AI pada tindak pidana siber *Malware* untuk menghasilkan pengolahan data kualitatif terkait tindak pidana siber *malware* yang menggunakan teknologi AI dalam UU ITE.

D. Hasil Penelitian dan Pembahasan

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 and Shivashankar Nair, 2009: 3). *Malware* atau *Malicous Software* merupakan perangkat lunak yang secara eksplisit didesain

untuk melakukan aktifitas berbahaya atau perusak perangkat lunak lainnya (Kramer and Bradfield, 2010: 105). 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 (OECD, 2008: 14):

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 (Yasin K, 2018).

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 (Ondrej, 2018: 7) :

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.

Kitab Undang-Undang Hukum Pidana (KUHP)	1) Pasal 335 tentang Pengancaman 2) Pasal 362 tentang pencurian 3) Pasal 378 tentang penipuan dan penggelapan 4) Pasal 406 tentang perusakan atau *hacking*
Undang-Undang Nomor 28 Tahun 2014 Tentang Hak Cipta	1) Pasal 45 tentang izin penggandaan terhadap program komputer 2) Pasal 46 tentang larangan melakukan penggandaan tanpa izin 3) Mengenai pelanggaran kode etik profesi komputer dan informatika

Undang-Undang Republik Indonesia Nomor 36 Tahun 1999 Tentang Telekomunikasi	1) Pasal 22 tentang perbuatan tanpa hak 2) Pasal 40 tentang penyadapan
Undang-Undang Nomor 8 Tahun 2010 Tentang Pencegahan Dan Pemberantasan Tindak Pidana Pencucian Uang	1) Pasal 3 dan 4 tentang pelaku pencucian uang aktif 2) Pasal 5 tentang pelaku pencucian uang pasif
Undang-Undang nomor 3 tahun 2011 tentang Transfer Dana	1) Pasal 79 tentang larangan kegiatan transfer dana tanpa izin 2) Pasal 80 tentang penyalahgunaan perintah transfer dana 3) Pasal 81 tentang pencurian dana 4) Pasal 82 tentang penerima hasil curian transfer dana 5) Pasal 83 tentang manipulasi perintah transfer dana 6) Pasal 84 tentang perusakan sistem transfer dana 7) Pasal 85 tentang perbuatan tanpa hak
Undang-Undang nomor 8 tahun 1997 tentang Dokumen Perusahaan	1) Pasal 12 tentang pengalihan dokumen perusahaan 2) Pasal 13 tentang legalisasi pengalihan dokumen perusahan
Permenkominfo nomor 20 tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik	1) Pasal 68 tentang pelanggaran data pribadi 2) Pasal 69 tentang ancaman data pribadi di tempat umum 3) Pasal 70 tentang alat kejahatan pelanggaran data pribadi 4) Pasal 71 tentang perbuatan melawan hukum oleh pihak ketiga 5) Pasal 72, 73 dan 74 tentang Penyalahgunaan data pribadi 6) Pasal 75 tentang pemalsuan data pribadi 7) Pasal 76 tentang pidana tambahan 8) Pasal 77 tentang tindak pidana data pribadi oleh korporasi
Undang- Undang no 5 tahun 2018 tentang perubahan atas Undang- Undang no 15 tahun 2003 penetapan peraturan pemerintah pengganti Undang- Undang no 1 tahun 2002 tentang pemberantasan tindak pidana terorisme menjadi Undang-Undang	1) Pasal 6 tentang tindak pidana terorisme 2) Pasal 8 huruf I tentang pembajakan pesawat udara 3) Pasal 11 tentang penyedia dana teroris

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, 2012:3).

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.

E. Simpulan

Implenetasi hukum pidana terhadap perbuatan penerapan penyimpangan AI pada kejahatan *malware* telah sesuai dengan peraturan yang berlaku meskipun belum disebutkan secara gramatikal pada peraturan terkait yaitu UU ITE. Perbuatan *Malware*-AI dikategorikan sebagai *computer-related crime* karena dalam melakukan kejahatan menggunakan teknologi AI dan komputer.

Aturan-Aturan pidana yang tepat unuk menjerat penerapan dan penyimpangan *Artificial Intelligence* sebagai tindak pidana siber pada *Malware*. KUHP, UU Hak Cipta, UU TPPU, UU Transfer dana, UU Dokumen Perusahaan, Permenkominfo no 20 tahun 2016 dan, UU terorisme dapat diterapkan pada perbuatan ini, namun mengacu pada *Lex specialis derogat lege generali* dan *Lex posterior derogat legi priori*. UU ITE merupakan *Lex specialis* dan *Lex posterior* atas peraturan-peraturan tersebut adalah yang paling tepat untuk menjerat pelaku tindak pidana penerapan dan penyimpangan *Artificial Intelligence* pada *Malware*.

F. Saran

Memasukkan ketentuan AI dan *Malware* dalam UU ITE dengan cara merevisi UU tersebut, karena diperlukan adanya peraturan-peraturan yang lebih khusus lagi terhadap penerapan dan penyimpangan AI sebagai tindak pidana siber pada *Malware* sebagai bentuk antisipatif terhadap

perbuatan yang mengakibatkan kerugian banyak orang, karena efeknya yang belum terasa bukan berarti kejahatan ini merupakan kejahatan yang dianggap sepele. Aturan-aturan pidana harus lebih mengigit pelaku tindak pidana siber dan merumuskan hal-hal yang memungkinkan untuk dilakukan lagi dengan teknik lain sebagai tindakan preventif atas kejahatan tersebut. Karena menurut penulis kejahatan ini merupakan bom waktu yang dapat sewaktu-waktu meledak dan akan mengganggu ketertiban umum dengan skala yang lebih besar lagi, maka dari itu diperlukan respon cepat dan tanggap dalam menangani kasus-kasus seperti ini. Meningkatkan kesadaran dalam semua lini lapisan masyarakat dan penegak hukum akan pentingnya perkembangan teknologi, karena tak ayal perkembangan ini memunculkan suatu dimensi baru yang menghasilkan tindak kejahatan baru yang memaksa kita untuk meningkatkan keamanan digital kita dan pula bagi penegak hukum agar tidak gagap dalam menghadapi gelombang baru kejahatan ini.

G. Daftar Pustaka

Abdul Wahid dan Mohammad Labib. 2005,.*Kejahatan Mayantara (Cyber Crime),* Jakarta: PT. Refika Aditama.

Catherine Stupp. 2019. Stupp. 2019. “Fraudster Used AI to Mimic CEO’s Voice in nusual Cybercrime Case”.https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402. Diakses pada 19 Maret 2020 pukul 13.52 WIB.

Didik M Arief Mansur dan Elisatris Gultom. 2005. *Cyber Law* Aspek Hukum Teknologi Informasi. Bandung: Refika Aditama.

Elaine Rich. dan Kevin Knight. 1991. *Artificial Intelligence*. New York: McGraw-Hill.

Kaligis, O. C. (Otto Cornelis) & Indonesia. Undang-Undang tentang Informasi dan Transaksi Elektronik 2012, *Penerapan Undang-Undang nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik dalam prakteknya*, Cet. 1, Yarsif Watampone, Jakarta.

Kramer, S. & Bradfield, J. C. 2010. “A general definition of malware”. *Journal in Computer Virology*, *6* (2), 105–114.

Marty Puranik. 2019. *AI*-Powered Malware, Smart Phising and Open Source Attack, Oh My! The New Wave of Hacking in 2019 and How to Prevent. https://www.cpomagazine.com/cyber-security/ai-powered-malware-smart-phishing-and-open-source-attacks-oh-my-the-new-wave-of-hacking-in-2019-and-how-to-prevent/ diakses pada 29 Oktober 2019 pukul 22.59 WIB.

Ondrej Kubovic. 2018. “Can Artificial Intelligence Power Future Malware?”. https://www.welivesecurity.com/wpcontent/uploads/2018/08/Can_AI_Power_Future_Malware.pdf. *ESET Wihte Paper*. Diakses pada 29 Oktober 2019 pukul 00.15 WIB.

Organisation for Economic Co-Operation and Development (OECD). 2008. “Malicious Software (Malware): Security Threat to the Internet Economy”. *Ministerial Background Report DSTI/ICCP/REG(2007)5/FINAL*. Seoul, Korea.

Undang-Undang Nomor 19 tahun 2016 tentang perubahan atas Undang-undang nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik

Yasin K. Pengertian DDOS dan Bagaimana menanggulanginya. https://www.niagahoster.co.id/blog/ddos-adalah/. Diakses pada 5 juni 2020 pukul 23:01 WIB.

Yuliani, Ayu. 2017. Indonesia Diserang Hacker Miliaran Kali Tiap Hari. https://kominfo.go.id/content/detail/11956/indonesia-diserang-hacker-miliaran-kali-tiap-hari/0/sorotan_media (diakses pada 28 Oktober 2019 pukul 07.27 WIB.