

Penerapan Doktrin Vicarious Liability Untuk Pertanggungjawaban Pelaku Tindak Pidana Dunia Maya

Wiwin Ariesta^{1*}, Tuti¹

¹Universitas Merdeka Pasuruan

e-mail: *wiwin_ariesta@yahoo.com, tuti.unmer@gmail.com

ABSTRAK

Perkembangan teknologi yang semakin pesat telah memunculkan kemajuan dalam peradaban manusia dengan hadirnya dunia digital atau dunia maya (cyberspace). Hal ini dapat memberikan banyak kemudahan bagi manusia, namun di sisi lain juga menimbulkan permasalahan yang kita kenal sebagai cybercrime. Semakin banyak jenis tindak pidana yang baru dalam cyberspace maka dibutuhkan penegakan hukum oleh cyberpolice dengan menggunakan cyberlaw yang sudah ada saat ini. Hadirnya dunia metaverse dengan interaksi antar avatarnya telah menimbulkan suatu jenis interaksi baru yang hadir dalam dunia virtual. Hubungan antar avatar ini tidak saja terjadi secara positif namun ternyata bisa juga memunculkan tindak kejahatan yang dilakukan dalam dunia metaverse. Untuk itu dibutuhkan pembaharuan hukum yang lebih baik agar dapat melakukan penegakan hukum digital (digital law enforcement) dan meminta pertanggungjawaban pidana pada pelaku yang melakukan kejahatan cybercrime. Penggunaan blended law antara hukum konvensional dan cyberlaw yang diterapkan melalui doktrin vicarious liability dengan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik diharapkan dapat menjerat pelaku tindak pidana dalam dunia maya ini.

Kata kunci: cybercrime; cyberlaw; metaverse; avatar; vicarious liability.

ABSTRACT

Rapid technological developments have brought progress in human civilization to present the digital world or cyberspace. On the one hand, this can provide many conveniences for humans, but on the other hand, it can cause problems known as cybercrime. There are many types of new crimes that are necessary to enforce the law by the cyber police using the existing cyber law. The existence of a digital world in the form of a metaverse whose interaction model uses an avatar has given rise to a new type of interaction in the virtual world. The relationship between these avatars does not only occur in a positive way but also can actually lead to crimes committed in the metaverse. Therefore, better legal reform is needed in order to be able to enforce the digital law and ask for criminal accountability for perpetrators who commit cybercrime. The use of blended law between conventional law and cyber law which is applied through the Vicarious liability doctrine in Undang-Undang Number 11 of 2008 concerning Information and Electronic Transactions is expected to be able to arrest perpetrators of criminal acts in this virtual world

Keywords: cybercrime; cyber law; metaverse; avatar; vicarious liability.

PENDAHULUAN

Revolusi Industri 4.0 telah mendorong semua bidang menuju digitalisasi, dimana terjadi perkembangan yang sangat pesat dalam bidang teknologi dan dunia maya (cyberspace). Berbagai bidang maupun kegiatan yang sebelumnya dilakukan secara konvensional, dalam era sekarang mengalami disrupsi sehingga muncul dalam bentuk elektronik atau digital. Hal-hal terkait kejahatan dan penegakan hukum pun tidak terlepas dari imbas disrupsi tersebut. Sehingga dalam perjalanan waktu muncullah istilah seperti *cybercrime*, *cyberlaw*, dan *cyberpolice* yang berkaitan dengan keadaan maupun fenomena-fenomena yang terjadi di dunia maya khususnya dalam bidang hukum.

Sebagai salah satu dampak dari pandemi covid-19, masyarakat menjadi lebih aktif dalam berinteraksi di dunia maya, mengingat pemerintah sempat menerapkan pembatasan sosial skala besar sehingga berdampak pada kurangnya interaksi antar manusia dalam kehidupan sehari-hari. Banyak orang beralih aktivitas dari offline ke online, tidak hanya pada taraf pemenuhan kebutuhan

sehari-hari seperti berbelanja, bekerja, sekolah, melainkan juga kebutuhan untuk berwisata. Adanya gagasan traveling online kemudian menarik banyak minat masyarakat yang mulai hobi berselancar di dunia maya.

Kasus *cybercrime* yang terjadi awal Desember 2021 yang lalu patut menjadi perhatian, saat itu seorang perempuan bernama Nina Jane Patel melaporkan kasus pelecehan seksual yang dia alami sewaktu dia berada dalam platform beta VR dari Meta, Horizon Worlds. Saat itu ada beberapa *avatar* laki-laki yang menyerangnya dan melakukan perabaaan yang mengakibatkan korban membeku ketakutan. Kasus ini memang sudah dilaporkan dan telah mendapatkan perhatian dari Wakil Presiden Horizon, Vivek Sharma, sebagai feedback untuk memperbaiki keamanan di Meta. Dengan cara meningkatkan penggunaan fitur Safe Zone, yaitu fitur untuk memblokir *avatar* lain sehingga para pengguna dapat hidup dalam 'bubble' mereka masing-masing serta dapat berinteraksi dengan lebih aman.

Cybercrime merupakan pengembangan bentuk kejahatan yang sebelumnya tidak dikenal dalam dunia konvensional, hal ini timbul dilatarbelakangi dengan banyaknya aktivitas dalam dunia maya yang pada akhirnya memunculkan para pelaku kejahatan yang mengambil celah dan kesempatan untuk melakukan berbagai tindak pidana lewat dunia maya.

According to the U.S. Department of Justice (the "DOJ"), the term cybercrime refers to any illegal activity for which a computer is used as its primary means of commission, transmission, or storage. The list of criminal activities made possible by the widespread use of computers has grown exponentially in recent decades, and includes such acts as dissemination of computer viruses, network intrusion, identity theft, and even electronic bullying, stalking, and terrorism.

Berbagai jenis dari *Cybercrime* yang dikenal saat ini terbagi atas tiga kualifikasi umum, yaitu :

- a. Kejahatan Dunia Maya yang berkaitan dengan kerahasiaan, integritas dan keberadaan data dan sistem komputer:
 1. *Illegal access* (akses secara tidak sah terhadap sistem komputer);
 2. *Data interference* (mengganggu data komputer);
 3. *System interference* (mengganggu sistem komputer);
 4. *Illegal interception in the computers, systems and computer networks operation* (intersepsi secara tidak sah terhadap komputer, sistem, dan jaringan operasional komputer);
 5. *Data Theft* (mencuri data);
 6. *Data leakage and espionage* (membocorkan data dan memata-matai);
 7. *Misuse of devices* (menyalahgunakan peralatan komputer).
- b. Kejahatan Dunia Maya yang menggunakan komputer sebagai alat kejahatan:
 1. *Credit card fraud* (penipuan kartu kredit);
 2. *Bank fraud* (penipuan terhadap bank);
 3. *Service Offered fraud* (penipuan melalui penawaran suatu jasa);
 4. *Identity Theft and fraud* (pencurian identitas dan penipuan);
 5. *Computer-related fraud* (penipuan melalui komputer);
 6. *Computer-related forgery* (pemalsuan melalui komputer);
 7. *Computer-related betting* (perjudian melalui komputer);
 8. *Computer-related Extortion and Threats* (pemerasan dan pengancaman melalui komputer).
- c. Kejahatan Dunia Maya yang berkaitan dengan isi atau muatan data atau sistem komputer:
 1. *Child pornography* (pornografi anak);
 2. *Infringements Of Copyright and Related Rights* (pelanggaran terhadap hak cipta dan hak-hak terkait);

3. *Drug Traffickers* (peredaran narkoba), dan lain-lain.

Banyaknya kasus *cybercrime* menimbulkan tuntutan pembaharuan hukum dalam dunia maya sehingga muncullah *cyberlaw*, yakni istilah untuk hukum yang terkait dengan penggunaan teknologi informasi dan komunikasi. Ada juga istilah-istilah lain yang diberikan untuk hukum yang mengatur kegiatan-kegiatan yang dilakukan dalam dunia maya (*cyberspace*) ini seperti *the law of internet*, *the law of information technology*, *the telecommunication law*, dan *lex informatica*.

Pembukaan UUD 1945 yang menjwai pengaturan HAM dalam Batang Tubuh UUD 1945 dan peraturan perundang-undangan lain sebagai hukum positif, pada setiap alinea mencerminkan Hak Azasi Manusia. Jika dalam pembukaan UUD alinea pertama dan kedua tercermin pengakuan adanya kebebasan dan keadilan maka alinea ketiga dan keempat mencerminkan adanya persamaan dalam bidang politik, Ekonomi, Hukum, sosial dan budaya. Ini berarti substansi Hak Azasi Manusia dalam Pembukaan UUD 1945 amat luas, termasuk salah satunya hak perlindungan bagi warga negara untuk dijamin keamanannya oleh negara.

Dalam tatanan hukum bidang teknologi dan informasi di Indonesia telah diatur dalam Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik *juncto* Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (selanjutnya disebut dengan UU ITE). Bagi negara kita, UU ITE ini menjadi salah satu bagian dari sistem hukum positif negara Indonesia. Hadirnya bentuk hukum yang baru ini adalah akibat dari perkembangan teknologi dan globalisasi sehingga memunculkan pengayaan pada bidang hukum sektoral yang menjadi dinamika hukum tersendiri sebagai bagian dari sistem hukum nasional.

Mabes Polri memang sudah mempunyai unit khusus *cybercrime* untuk menangani kejahatan dalam dunia maya, namun dengan semakin banyaknya tindak kejahatan dalam dunia maya ujung-ujungnya menuntut kehadiran *cyberpolice* agar dapat melakukan penegakan hukum terhadap pelaku *cybercrime*. Dalam hal ini UU ITE akan menjadi panduan dan payung hukum yang dapat digunakan oleh *cyberpolice* untuk menangani berbagai kasus *cybercrime* yang terjadi di Indonesia.

Saat ini dunia maya sudah berkembang lebih jauh lagi dengan hadirnya dunia *metaverse*, suatu lompatan teknologi yang mulai dikembangkan juga oleh Mark Zuckerberg.

Metaverse: the internet considered as an imaginary area without limits where you can meet people in virtual reality (= images and sounds, produced by a computer, that seem to represent a real place or situation):

The metaverse is a virtual world where humans, as avatars, interact with each other in a three-dimensional space that mimics reality

Metaverse merupakan konsep dunia virtual yang memungkinkan seseorang membuat *avatar* (sebutan bagi karakter dalam platform *metaverse*) dirinya dan masuk ke sana untuk melakukan hal-hal sebagaimana yang mereka lakukan dalam dunia konvensional. Jadi mereka bisa bekerja, rapat bersama kolega, jalan-jalan dengan teman, bahkan juga bisa bermain bersama-sama secara virtual. Tetapi sebagaimana interaksi yang terjadi dalam dunia konvensional, maka di dunia *metaverse* interaksi yang terjadi tidak hanya yang bersifat positif saja, tapi bisa juga yang bersifat negatif dengan munculnya tindak kejahatan seperti kasus Nina Jane Patel di atas.

Patut diperhatikan bahwa dalam hal ini baik hukum konvensional maupun *cyberlaw* yang ada saat ini (dalam hal ini adalah UU ITE) masih belum mampu memberikan perlindungan hukum bagi korban maupun menindak pelaku tindak pidana di dunia maya dalam kasus seperti itu. Disini penulis akan mengulas dengan mengambil sudut pandang

dari penegakan hukum terhadap pelaku tindak pidana di dunia *metaverse*, kemudian melakukan penganalogian terhadap *avatar* sebagai subjek hukum sehingga memberikan legalitas bagi penegak hukum untuk dapat menindaknya. Berikutnya doktrin *Vicarious liability* dapat dipergunakan untuk mengaitkan pertanggungjawaban pidana dari *avatar* di dunia *metaverse* dengan otak pelaku tindak pidana yang berada di dunia konvensional.

Dalam tinjauan *ius constituendum*, peristiwa pelecehan seksual di dunia *metaverse* ini seyogyanya dapat memantik pemikiran yang lebih luas. Kejahatan yang terjadi di dunia maya saat ini bukan lagi sekedar kejahatan sebatas yang terjadi melalui Facebook, Instagram, Tiktok, atau media sosial lainnya saja. Ragam tindak pidana mulai dari yang sederhana seperti penipuan, pemerasan, pembajakan akun, sampai berbagai jenis perkembangan *cybercrime* seharusnya sudah harus diantisipasi oleh hukum. Para penegak hukum di Indonesia dapat mengambil kasus *cybercrime* di atas dan menjadikannya sebagai bahan perencanaan untuk mengantisipasi *cybercrime* di dunia *metaverse*. Jika teknologi telah maju sedemikian pesatnya maka hukum juga harus turut berlari untuk mengujarnya.

Kasus tersebut mungkin tidak akan berhenti pada titik itu saja, bisa saja ada kemungkinan kelak pelaku kejahatan mengembangkan bentuk-bentuk kejahatan yang lebih canggih. Seperti kejahatan yang sebelumnya dilakukan dalam dunia konvensional semacam pemerasan, penipuan, penghinaan, pemerkosaan atau tindak pidana lainnya dapat dilakukan juga terhadap *avatar-avatars* yang melakukan aktifitas di dunia *metaverse*. Jika *avatar* pelaku melakukan penipuan dengan menggunakan tipu daya, bujuk rayuan maupun intimidasi, maka kebijakan *Safe Zone* yang diterapkan menjadi tidak begitu bermakna untuk melindungi korban.

Selanjutnya kalau melihat bahwa konsep awal dunia *metaverse* memang ditujukan untuk meningkatkan interaksi manusia lintas batas secara positif, artinya orang-orang dari berbagai negara dapat saja melakukan pertemuan di dunia *metaverse*. Namun di masa yang akan datang, ini dapat menimbulkan kemungkinan bahwa interaksi tersebut akan disalahgunakan sebagai sarana melakukan kejahatan. Ada potensi *avatar-avatars* itu dapat melakukan tindak pidana ekonomi seperti menjual rahasia dagang, praktek *insider's trading*, dan sebagainya. Atau bahkan melakukan tindak pidana yang berhubungan dengan keamanan negara seperti menjual rahasia negara, membocorkan data sistem pertahanan negara, dan lain-lain. Jika mereka melakukan hal-hal semacam itu, *cyberlaw* kita saat ini masih belum bisa menjangkau untuk melakukan penindakan hukum terhadap pelakunya. Sehingga penting bagi para penegak hukum saat ini untuk secara serius memikirkan lebih lanjut bagaimana upaya dari *cyberpolice* agar dapat melakukan penegakan hukum di dunia digital (*digital law enforcement*) terhadap kasus kejahatan atau tindak pidana yang terjadi di dunia *metaverse* di kemudian hari.

METODE PENELITIAN

Dalam melakukan penelaahan untuk membahas permasalahan yang dikemukakan penulis akan memakai metode penelitian hukum (*legal research methods*). Peter Mahmud Marzuki mengatakan bahwa penelitian hukum dilakukan untuk mencari pemecahan atas suatu isu hukum yang dihadapi, dengan kemampuan untuk melakukan identifikasi masalah hukum, melakukan penalaran hukum, melakukan analisa atas masalah yang dihadapi serta memberikan pemecahan masalah hukum tersebut. Jadi ini bukan sekedar menerapkan aturan hukum yang ada saja tapi juga untuk menciptakan hukum agar dapat mengatasi masalah yang dihadapi.

HASIL DAN PEMBAHASAN

Jika terjadi *cybercrime* dalam dunia *metaverse* maka salah satu kesulitan utama yang dihadapi oleh *cyberpolice* adalah bagaimana menindak pelaku tindak pidana tersebut, mengingat yang menjadi pelaku dalam hal ini berbentuk *avatar*. Subjek hukum yang kita kenal selama ini hanya mengacu pada *natuurlijke persoon* dan *rechtspersoon*, sedangkan bentuk karakter atau *avatar* belum mempunyai legalitas untuk dikategorikan sebagai subjek hukum. Namun berdasarkan kenyataan yang terjadi, *avatar* tersebut mampu melakukan suatu tindakan termasuk melakukan kejahatan atau tindak pidana. Karena itu perlu dipikirkan suatu cara agar dapat melakukan

penegakan *cyberlaw* (*digital law enforcement*) terhadap para pelaku tindak pidana tersebut walaupun mereka berbentuk *avatar*. Karena itu disini penulis ingin mengajukan gagasan untuk memberlakukan *blended law*, artinya pemberlakuan kombinasi hukum konvensional dan *cyberlaw* untuk menindak pelaku tindak pidana pada *avatar* yang melakukan kejahatan di dunia *metaverse*.

Kejahatan selain dilakukan oleh manusia juga dapat dilakukan oleh korporasi sebagai subjek hukum. Mengenai pembebanan pertanggungjawaban pidana terhadap kejahatan yang dilakukan oleh korporasi itu sendiri ada beberapa teori atau ajaran yang dapat dijadikan dasar dalam pembebanan pertanggungjawaban pidana tersebut. Teori atau ajaran tersebut adalah Teori Identifikasi (*Identification Theory*), Teori Pertanggungjawaban Pidana Mutlak (*Strict Liability*), dan Teori Pertanggungjawaban Pidana Pengganti (*Vicarious liability*). Dalam teori identifikasi, perbuatan pidana yang dilakukan oleh pejabat senior diidentifikasi sebagai perbuatan pidana yang dilakukan oleh korporasi. Teori ini juga dikenal dengan teori *alter ego* (*alter ego theory*) atau teori organ yang dapat diartikan secara sempit maupun secara luas, sebagaimana dikemukakan oleh Barda Nawawi Arief, yaitu : dalam arti sempit (Inggris) : hanya perbuatan pejabat senior (otak korporasi) yang dapat dipertanggungjawabkan kepada korporasi. Dalam arti luas (Amerika Serikat) : tidak hanya pejabat senior/direktur saja, tetapi juga agen dibawahnya.

Strict liability merupakan salah satu bentuk pembebanan pertanggungjawaban kepada korporasi atas tindak pidana yang dilakukan oleh seseorang yang bekerja pada korporasi tersebut. Menurut doktrin pertanggungjawaban mutlak ini, suatu pertanggungjawaban pidana dapat dibebankan kepada pelaku tindak pidana tertentu, tanpa perlu dibuktikan ada tidaknya unsur kesalahan (baik itu kesengajaan ataupun kelalaian). Dengan kata lain, pertanggungjawaban pidana oleh pelaku tidak dipermasalahkan dalam *strict liability*.

Sistim hukum di Indonesia juga mengenal doktrin *Vicarious liability* yang diartikan sebagai pertanggungjawaban pengganti, doktrin ini merupakan pengecualian dari asas *Geen Straft Zonder Schuld* (tiada suatu pidana tanpa adanya kesalahan). Doktrin tersebut juga telah diakomodir serta dirumuskan dalam Konsep KUHP 2008 pada Pasal 38 Ayat (2) yang menyebutkan “Dalam hal ditentukan oleh Undang-Undang, setiap orang dapat dipertanggung-jawabkan atas tindak pidana yang dilakukan oleh orang lain”. Selama ini penegakan hukum di Indonesia banyak memakai doktrin *Vicarious liability* yang diterapkan untuk menjerat korporasi yang melakukan kejahatan. Dalam pengertian bahwa di satu sisi korporasi diposisikan sebagai *rechtspersoon* sehingga mampu melakukan tindakan hukum dan dapat dimintai pertanggungjawaban hukum juga. Di sisi lain, juga ada pihak-pihak lain yang dapat dimintai pertanggungjawaban pidana berkaitan dengan terjadinya kejahatan korporasi.

Sebagaimana diungkapkan juga dalam Konsep KUHP 2010 yang memberikan pendirian untuk beban pertanggungjawaban pidana yang pelakunya adalah korporasi, maka akan dibebankan baik kepada korporasinya juga pada pengurusnya yang mempunyai kedudukan fungsional di dalam struktur organisasi korporasi tersebut, yakni pengurus yang sesuai dengan ketetapan anggaran dasar korporasi mempunyai kewenangan bertindak untuk dan atas nama korporasi (*intra vires*) baik di dalam maupun di luar pengadilan. Karenanya dapat disimpulkan bahwa walaupun bentuk korporasi itu bukan orang (*natuurlijke persoon*) dalam arti sebenarnya namun hukum memandang korporasi sebagai subjek hukum yang berbentuk badan hukum (*rechtspersoon*) yang merupakan subjek perwakilan dari orang yang membentuknya. Jadi korporasi yang dipersamakan sebagai orang ini mampu bertindak sebagai subjek hukum juga, artinya disini korporasi bisa melakukan tindakan hukum yang nantinya dapat menimbulkan hak dan kewajiban hukum juga baginya.

Analogi semacam ini kelak dapat dipergunakan juga oleh para penegak hukum di dunia *metaverse* untuk menjangkau karakter *avatar* yang melakukan kejahatan, sebab walaupun *avatar* ini berbentuk virtual namun dia memiliki kemampuan untuk melakukan suatu tindakan hukum,

karena *avatar* tersebut adalah subjek perwakilan dari orang yang menciptakannya. Jika dikaitkan kembali dengan penggunaan doktrin *Vicarious liability* maka untuk meminta pertanggungjawaban hukum atas subjek hukum yang melakukan tindak pidana, jika pelakunya adalah *avatar* di dunia *metaverse* pertanggungjawaban tindak pidana selain dikenakan pada *avatar* tersebut juga dapat dibebankan pada penciptanya yang berada di dunia konvensional. Sebab *avatar* tersebut merupakan subjek perwakilan yang melakukan tindakannya semata-mata berdasarkan pada perintah dari orang dari dunia konvensional yang menciptakan dan menjalankan karakter *avatar* tersebut di dunia *metaverse*.

Jadi dalam hal ini *cyberpolice* dapat melakukan penindakan terhadap pelaku tindak pidana di dunia *metaverse* terhadap *avatarnya* maupun terhadap otak pelakunya (penciptanya) yang berada di dunia konvensional dengan menggunakan kaidah hukum yang terkait, baik menggunakan hukum konvensional maupun *cyberlaw* (UU ITE). Jika kita hendak menerapkannya terhadap kasus Nina Jane Patel, maka dalam hal ini *cyberpolice* terlebih dahulu dapat melakukan pelacakan jejak digital terhadap *avatar-avatars* yang melakukan tindak pidana pelecehan seksual terhadap korban. Langkah berikutnya, sesuai dengan konsep penganalogian subjek hukum dan doktrin *Vicarious liability*, maka *avatar* yang melakukan tindak pidana beserta manusia pelaku tindak pidananya dapat dikenakan pertanggungjawaban pidana. Karena telah melanggar ketentuan hukum sebagaimana yang diatur dalam Pasal 282 KUHP bahwa tindak pidana kejahatan terhadap kesopanan tergolong sebagai perbuatan yang dilarang, pada Pasal 27 UU ITE tentang tindak pidana terhadap muatan yang melanggar kesusilaan, serta pada Pasal 4 Ayat 1 jo Pasal 1 Undang-Undang Nomor 44 Tahun 2008 tentang Pornografi mengenai larangan konten yang melanggar norma kesusilaan dalam masyarakat, yang dengan secara eksplisit memuat kekerasan seksual.

Dengan demikian model penerapan penegakan hukum semacam ini kelak akan dapat juga dipergunakan untuk mengantisipasi ragam jenis *cybercrime* yang terjadi di dunia *metaverse* termasuk juga melakukan penegakan hukumnya. *Cyberpolice* dapat melakukan penegakan hukum *cyberlaw* yang lebih responsif terhadap kemajuan teknologi dengan cara melakukan *blended law* agar pelaku tindak pidana dapat dimintai pertanggungjawabannya, sehingga dapat menjamin keamanan dan kepastian hukum bagi masyarakat.

KESIMPULAN

Kemajuan *cybertechnology* yang semakin canggih memang semakin memudahkan kehidupan manusia di satu sisi, tetapi di sisi lain ternyata dapat menimbulkan masalah seperti munculnya jenis-jenis *cybercrime* yang masih belum terjangkau oleh hukum konvensional dan *cyberlaw* yang ada pada saat ini. Untuk menanggulangi *cybercrime* diperlukan gerak cepat dari *cyberpolice* agar dapat menyikapi berbagai tantangan yang muncul akibat timbulnya bentuk-bentuk kejahatan yang baru seperti halnya yang terjadi di dunia *metaverse*. *Digital law enforcement* sangat dibutuhkan untuk melakukan penegakan hukum di dunia maya, serta diperlukan juga pembaharuan dalam *cyberlaw* untuk mengantisipasi pelaku tindak pidana yang berasal dari dunia maya. Dalam upaya menjerat pelaku tindak pidana di dunia maya seperti di dunia *metaverse*, bisa menggunakan *blended law* yang merupakan kombinasi dari hukum konvensional dan *cyberlaw*. Salah satu caranya adalah dengan melakukan penganalogian pada *avatar* sebagai subjek hukum agar hukum dapat menjangkau pelaku tindak pidana yang belum mempunyai keabsahan sebagai subjek hukum. Berikutnya doktrin *Vicarious liability* dapat dipakai juga untuk meminta pertanggungjawaban pidana dari pencipta *avatar* yang berada di dunia konvensional, agar otak pelaku tindak pidana tersebut tidak dapat menghindarkan diri dari pertanggungjawabannya atas *avatar* yang mewakili dirinya di dunia *metaverse*.

DAFTAR PUSTAKA

Penjelasan Umum Undang-Undang Nomor 19 tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik.

Arief, Barda Nawawi. (2003). Kapita Selekta Hukum Pidana. Jakarta : Rajawali Pers

Budhijanto, Danrivanto. (2017). Revolusi Cyberlaw Indonesia: Pembaruan dan Revisi Undang-

Undang Informasi dan Transaksi Elektronik 2016. Bandung: Refika Aditama.

Mewengkang, Indriani Berlian, Robert N. Warong, dan Michael Kuntag. (2021). "Kajian Yuridis Cyber Crime Penanggulangan Dan Penegakan Hukumnya." *Lex Crimen*. Vol.X No.5. Hal.26-35

Mulasari, Laila. (2012). "Ajaran Pertanggungjawaban Pidana Korporasi Dalam Kebijakan Hukum Pidana Di Bidang Mayantara." *Jurnal Ilmiah Hukum Dan Dinamika Masyarakat*. Vol.9 No.2. Hal.113-120.

Marzuki, Peter Mahmud. (2021). *Penelitian Hukum*. Jakarta: Kencana.

Subagyo, Agus. (2018). "Sinergi Dalam Menghadapi Ancaman Cyber Warfare." *Jurnal Pertahanan & Bela Negara*. Vol.5 No.1. Hal.89-108.

Sudiyana. (2019). *Problematika Hukum Dalam Transaksi Elektronik dan Upaya Penyelesaiannya*. QISTIE. Vol.12 No.2. Hal.178-196.

Ariesta, Wiwin and M. Mashuri, "Legal Protection For Citizens Rights ' From Quarantine Areas Secretly And Without a Basis During The Covid19 Pandemic," vol. 1, no. 1, pp. 177–184, 2022.

<https://dictionary.cambridge.org/dictionary/english/metaverse>, diakses tanggal 22 Maret 2022.

<https://kepaniteraan.mahkamahagung.go.id/glosarium-hukum/1895-vicarious-liability>, diakses tanggal 23 Maret 2022.

<https://legaldictionary.net/cybercrime/>, diakses tanggal 22 Maret 2022.

<https://www.cnnindonesia.com/teknologi/20211220141432-185-736240/percobaan-metaverse-berbuah-aksi-pelecehan-seks-virtual>, diakses tanggal 22 Maret 2022.