PERLINDUNGAN HUKUM TERHADAP KORBAN PENYALAHGUNAAN DATA PRIBADI : PENGGUNAAN TEKNIK DEEPFAKE

Sayid Muhammad Rifki Noval[1)]
[1)] *Dosen Fakultas Hukum Universitas Islam Nusantara, Bandung*

ABSTRACT

This article aims to determine solutions to prevent widespread deepfake videos nowadays. Video manipulation may happen to someone who has published his pictures and videos on the internet, mainly on social media. The biggest concern of deepfake abuse is the manipulation to produce pornographic videos by putting someone's face on the existing porn videos. The current legal provisions regarding pornographic video production and distribution can be found under several regulations in Indonesia. However, this article tries to prevent the production of porn videos using deep-fake technique through legal instruments. The method was statue approach, case approach, analytical approach, and comparative approach. The result of this research is the implementation of the Right to be Forgotten regulated in Law No.19 of 2016 of Amendment to Law No.11 of 2008 on Electronics Information and Transactions. This provision allows a person to apply for the deletion of his/her personal information published on the internet to prevent it from being used in creating deepfake porn videos.

Keywords: *Privacy, Deepfake, Right to be Forgotten.*

1. PENDAHULUAN

Tidak dapat dipungkiri, apabila saat ini masyarakat tengah menghadapi "tsunami informasi" yang hadir dari berbagai sumber media. Keadaan tersebut patut diakui telah menghadirkan kemudahan bagi masyarakat dalam mendapatkan informasi. Walaupun pada satu sisi, perlu diantisipasi hadirnya potensi masalah yakni berupa informasi yang tidak benar, termasuk di dalamnya *fake news* maupun informasi sejenis yang dikenal dengan istilah *hoax*. Di Indonesia sendiri, Kementerian Komunikasi dan Informasi merilis bahwa terdapat 1.731 hoax sejak Agustus 2018-April 2019 [1]. Ketika proses Pemilihan Umum Presiden Indonesia pada tahun 2019, calon Presiden Joko Widodo sempat mendapatkan fitnah dengan hadirnya foto DN Aidit bersama dirinya [2], serupa dengan pesaingnya Calon Presiden Prabowo Subiantopun mendapakan fitnah serupa dengan hadirnya foto dengan latar belakang lambang palu arit [3].Maraknya penyebaran hoax tidak hanya meningkat dari jumlah, namun juga lahir dalam berbagai macam bentuk. Tidak berhenti pada format artikel dan foto, saat ini hoax pun turut hadir dalam format video, salah satu contohnya adalah video mengenai kapal pembawa alat berat tenggelam yang sesungguhnya merupakan peristiwa yang terjadi pada waktu yang berbeda [4].

Namun dewasa ini lahir satu fenomena yang berpotensi melahirkan hoax model baru. Apabila selama ini video hoax kerap berlangsung dengan menggunakan video yang tidak sesuai dengan tempat dan waktu sesungguhnya. Saat ini, dengan perkembangan teknologi telah dimungkinkan hadirnya manipulasi video yang dapat merekayasa ucapan ataupun adegan yang seolah dilakukan oleh seseorang sehingga terlihat sebagai video asli. Tentu dibutuhkan kemampuan khusus agar dapat melakukan manipulasi terhadap suatu video, namun berbeda halnya jika telah terdapat aplikasi yang memungkinkan hal tersebut terjadi. Pada akhir bulan Agustus 2019, pengguna internet dikejutkan dengan hadirnya aplikasi penukar wajah bernama Zao. Aplikasi yang berasal dari negara Tiongkok ini memanfaatkan teknik *deepfake* untuk mengubah wajah artis pada suatu video dengan wajah pengguna aplikasi tersebut [5]. Aplikasi ini menjadi ramai diperbincangkan karena telah menunjukkan kemampuan *Aritificial Intelligence* (AI) untuk dapat melahirkan "video" yang nyaris tidak terdeteksi sebagai hasil rekayasa.Dapat dibayangkan jika teknik *deepfake* ini dipergunakan dengan tujuan yang tidak benar, seperti propaganda, pornografi atau terkait isu privasi. Masyarakat tentu akan menghadapi disinformasi, mengingat pada umumnya masyarakat berpikir bahwa video merupakan informasi dengan nilai validitas yang kuat, sehingga video dengan hasil teknik *deepfake* ini akan dinilai sebagai sebuah kebenaran.

Sesungguhnya permasalahan mengenai *deepfake* telah hadir jauh sebelum aplikasi Zao dirilis, tercacat beberapa peristiwa sempat dikaitkan dengan teknik ini diantara yakni video Presiden Gabon, Ali Bongo [6], atau video Mantan Presiden Amerika Serikat, Barack Obama dengan komedian Jordan Peele [7] dan beberapa video porno yang menggunakan wajah aktris-aktris seperti Gal Gadot, Scarlett Johansson, Taylor Swift dan

[1] Korespondensi penulis: Sayid Muhammad Rifki Noval, juristdomain@gmail.com

Maisie Williams [8]. Pada dasarnya istilah *Deepfake* digunakan untuk menunjuk video yang melapisi wajah *hyper-realistic* kepada tubuh orang lain dengan tujuan untuk membuat video baru menggunakan representasi palsu [9].Penjelasan lainnya menyatakan bahwa *deepfake* adalah penggabungan dari dua kata yakni antara *"deep learning*" dan "*fake", deepfakes* merujuk pada *photo-realistic audiovisual* yang diproduksi dengan bantuan *deep learning*. Istilah ini mengacu pada penyalahgunaan guna tujuan illegal dan tidak etis. Istilah ini berasal dari pengguna situs Reddit dengan nama *deepfakes* yang merupakan akun pertama yang secara publik mendokumentasikan upaya mengganti wajah seseorang secara sintetis dengan wajah orang lainnya, yakni pertukaran wajah dalam video porno [10]. Jika telusuri lebih jauh, satu potensi dapat lahir beriringan dengan video porno yang menggunakan teknik *deepfake*, yaitu fenomena yang dikenal dengan istilah *Revenge Pornography/ image-based sexual abuse* atau yang dikenal dengan istilah balas dendam pornografi. Perbuatan mengirimkan informasi pribadi (konten pornografi) tentang pasangannya dengan motif balas dendam untuk disebarluaskan. Hal itu dimungkinkan terjadi karena dokumentasi yang pernah dilakukan bersama dengan pasangannya/ dengan persetujuan pasangannya atau secara diam-diam tanpa diketahui pasangannya. Dengan kepemilikan gambar atau video yang dimiliki oleh seseorang terhadap pasangannya, semakin memudahkan untuk dilakukan manipulasi video, karena kuantitas serta kualitas informasi menjadi salah satu faktor penting untuk dapat menghasilkan video *deepfake* yang terlihat seperti asli. Internet menjadi salah satu alasan mengapa *revengeporn* dan *deepfake* ini kian luas penyebarannya, sebagaimana yang diungkapkan oleh Grebowicz bahwa *the Internet fundamentally changes the social meaning of pornography by embedding it squarely in the epistemological shift from knowledge to information, and the political shift to information becoming democratically accessible to everyone* [11].

Terkait dengan permasalahan diatas, maka diperlukan instrument hukum yang dapat melindungi seseorang agar tidak menjadi korban pembuatan video dengan teknik *deepfake*, terutama pembuatan video porno. Tulisan ini tidak akan membahas secara teknis bagaiamana *deepfakes* ini dilakukan, tidak juga secara dalam melakukan pembahasan tentang sanki hukum yang dapat diterapkan kepada pelaku pembuatan video porno dengan teknik *deepfake*, namun menghadirkan alternatif pencegahan melalui instrument hukum agar meminimalisir hadirnya penyebaran video hasil *deepfake*

2. METODE PENELITIAN

Metode penelitian yang digunakan dalam penelitian ini adalah yuridis normatif dengan pendekatan undang-undang (*statue approach)*, kasus (*case approach)*, analitis (*analytical approach)*, dan perbandingan (*comparative approach)*. Sumber data yang digunakan dalam tulisan ini adalah data sekunder. Adapun yang dengan data sekunder terdiri dari : a) bahan hukum primer, yaitu bahan-bahan hukum yang mengikat seperti Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) ; b) bahan hukum sekunder, yaitu bahan-bahan hukum yang memberikan penjelasan terhadap bahan hukum primer, seperti doktrin, karya-karya ilmiah para sarjana, jurnal, dan tulisan-tulisan lain yang bersifat ilmuah. Penelitian terhadap bahan hukum sekunder ini dimaksudkan untuk membantu menganalisis dan memahami bahan hukum primer, dan c) bahan hukum tersier, yaitu bahan-bahan hukum yang memberikan petunjuk maupun penjelasan terhadap bahan hukum primer dan bahan hukum sekunder. Contohnya data internet yang berkaitan dengan masalah dalam tulisan ini. Analisis data dilakukan secara deskriptif-kualitatif. Spesifikasi penelitian ini menggunakan deskriptif analitis.

3. HASIL DAN PEMBAHASAN

Kehadiran teknik manipulasi audio-visual ini sesungguhnya telah diprediksi oleh David Brin pada tahun 1998 dengan memperingatkan bahwa teknologi pembuktian melalui foto akan segera ditinggalkan, masyarakat akan dengan cepat mencapai titik ketika komputer yang dikontrol oleh para ahli dapat melakukan penyesusaian gambar, pixel demi pixel miskroskopis dan tidak meninggal petunjuk. Bahkan saat ini telah banyak transformasi teknologi serupa yang tidak hanya berlangsung di ranah gambar namun turut pada bidang *audio-visual*. National Public Radio (NPR), The Verge dan media lainnya telah merilis berita tentang perusahaan Kanada bernama Lyrebird yang telah menemukan cara untuk menciptakan kembali suara seseorang dan membuatnya untuk dapat mengatakan apapun. Menggunakan algoritma komputer untuk menangkap fitur-fitur khas suara seseorang dari contoh suara yang berdurasi singkat. Program tersebut kemudian dapat menghasilkan suara seseorang yang dituju, kemudian akan dianalisis dan memerintahkannya untuk mengatakan konten yang diperintahkan. Google turut menjadi salah satu perusahaan yang telah menghasilkan teknologi simulasi ragam suara serta Project VoCo dari Adobe yang dapat mengedit ucapan

manusia layaknya Photoshop yang mengubah gambar digital [12]. Saat ini, kekhwatiran David Brin telah terjadi secara perlahan. Perkembangan teknologi telah semakin berkembang hingga memungkinkan dilakukannya proses manipulasi video, yang dikenal dengan istilah *deepfake* dan berpotensi diterapkan pada konten pornografi.

Sebagaimana telah dinyatakan dalam pendahuluan, bahwa artikel ini tidak akan menjelaskan mengenai aturan serta sanksi hukum terhadap perbuatan penyebaran video porno, mengingat telah hadir beragam ketentuan dalam aturan hukum di Indonesia yang dapat menjeratnya. Pasal 282 ayat (1) Kitab Undang-Undang Hukum Pidana mengenai kejahatan terhadap kesusilaan, Pasal 27 ayat (1) UU ITE serta Pasal 4 ayat (1) Undang-Undang Nomor 44 Tahun 2008 tentang Pornografi telah mengatur perihal tersebut. Permasalahan mendesak yang sesungguhnya perlu mendapatkan perhatian adalah upaya pencegahan agar tidak dilakukannya teknik *deepfake,* sehingga menghasilkan manipulasi video terhadap diri seseorang. Setidaknya dapat diidentifikasi beberapa jenis video *deepfake* yang beredar saat ini, *pertama* adalah video asli yang dilakukan proses "penempelan" wajah orang lain terhadap wajah asli seseorang pada video tersebut, sehingga video yang dihasilkan seolah-olah benar dilakukan oleh wajah baru yang digunakan- video porno dengan wajah Galgadot menjadi contoh bentuk video *deepfake* ini. Permasalahan lainnya, sebagaimana yang telah disebutkan sebelumnya bahwa terdapat potensi masalah tambahan yakni balas dendam pornografi. Anastasia Powel dan Nicola Henry menjelaskan setidaknya terdapat tiga kategori dari balas dendam pornografi itu yaitu, 1) *the creation of nude or sexual images without consent;* 2) *the distribution or sharing of nude or sexual images without consent* (*including images that were self-created by the victim or consensually created with another person)*; 3) *the threat of distribution of nude or sexual images* [13]. Jenis *kedua*, adalah merekayasa ucapan serta mimik muka pada sebuah video sehingga seolah-olah orang dalam video tersebut yang telah mengucapkan kata-kata tersebut – jenis ini yang terjadi pada Mantan Presiden Barack Obama. Kedua jenis video *deepfake* tersebut dapat dilakukan karena terdapat sumber informasi, baik video atau gambar yang tersedia dalam internet, data tersebut dapat diperoleh melalui artikel internet atau media social seseorang.

Video *deepfake* Galgadot dan Barack Obama dapat terjadi karena mudahnya untuk mendapatkan dokumentasi Video dan Foto keduanya. Teknologi AI telah berevolusi dengan begitu cepat sehingga aplikasi yang dirancang untuk membuat *deepfake* saat ini tersedia secara luas. Aplikasi ini tidak hanya menurunkan ambang batas teknis yang diperlukan dalam membuat video manipulasi, tetapi juga memungkinkan untuk membuat video porno palsu tokoh publik dan individu menjadi lebih lazim. Saat ini, siapapun yang telah terpublikasi dalam gambar digital dapat membintangi pornografi di luar kehendaknya [14]. Hal ini menjadi mungkin terjadi terhadap seseorang yang gemar untuk mempublikasinya foto dirinya melalui media sosial atau aplikasi lainnya. Menurut data hasil Survei Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) tahun 2018, alasan utama masyarakat menggunakan internet adalah melakukan komunikasi lewat pesan sebanyak 24,7% dan 18,9% untuk bersosial media [15], dengan tingginya aktifitas tersebut dapat dibayangkan betapa rentannya masyarakat Indonesia untuk menjadi korban *deepfake* ini.

Solusi pencegahan terhadap ancaman ini seolah mudah untuk dilakukan, apabila foto atau video diri seseorang terpublikasi melalui akun media sosial pribadinya, karena pada umumnya terdapat fitur yang disediakan oleh aplikasi untuk melakukan penghapusan file tersebut. Namun bagaimana jika foto dan video seseorang telah tersebar secara umum dan/atau diluar kendali subjek dokumentasi tersebut ?. Pertanyaan ini serupa dengan pandangan Peter Fleischer tentang kendali subjek data terhadap data tersebut apabila telah terpublikasi di internet. Lebih lanjut Fleischer membagi kondisi tersebut kedalam tiga kategori yakni, (1) *If I post something online, do i have the right to delete it again ?;* (2) *If i posting something and someone else copies it and re-post it on their own site, do i have the right to delete it ?;* (3) *If someone else posts something about me, do i have a right to delete it ?* [16]. Kategori pertama yang diberikan Peter Fleischer mudah untuk melakukan proses penghapusan data, karena subjek data memiliki akses kontrol terhadap sumber data tersebut. Namun berbeda terhadap kategori kedua dan ketiga, mengingat subjek data tidak memiliki kewenangan terhadap data tersebut. Subjek data perlu melakukan permohonan terhadap pihak yang telah melakukan *re-post* data dan mempublikasikan data yang terdapat subjek data didalamnya.

Masalah akan muncul apabila permohonan penghapusan data tersebut ditolak, sehingga berpotensi untuk mengancam seseorang menjadi korban video *deepfake*. Foto diri seseorang sesungguhnya termasuk dalam kategori data pribadi yang secara hukum seharusnya dilindungi. Tidak mudah sesungguhnya untuk dapat mendefinisikan secara utuh mengenai privasi. Pada umumnya privasi dapat dikategorikan dalam 3 (tiga) tipe dasar yaitu : 1) *Pysical Privacy;* 2) *Information Privacy;* 3) *Organizational Privacy*. Lebih lanjut, guna

memastikan data privasi yang kerap berbenturan dengan data publik, dapat dihat dilihat pembagiannya yakni : 1) *Privacy of our Communications*, 2) *Privacy of our behavior,* 3) *Privacy of our person*. [17]. Pembagian tersebut pada dasarnya menempatkan foto dan video seseorang sebagai bagian dari data priibadi yang perlu dilindungi secara khusus, sebagaimana beberapa negara telah memiliki aturan khusus terkait data pribadi- Indonesia sendiri hingga saat ini tengah dalam proses untuk mensahkan Rancangan Undang-Undang Data Pribadi [18].

Di Negara Eropa, perlindungan data pribadi telah berjalan dengan baik. Warga negara Eropa dapat mengajukan permohonan untuk dipenuhinya apa yang dikenal dengan istilah *right to be forgotten* (RTBF). RTBF dikenal banyak pihak setelah pada tahun 2010, setelah seseorang warga negara Spanyol Mario Costeja Gonzalez mengajukan penghapusan informasi dirinya tentang pelelangan rumah guna melunasi hutang jaminan sosial yang dialaminya pada tahun 1998 kepada mesin pencarian Google. Informasi pelelangan rumah tersebut dapat ditemui pada hasil teratas mesin pencarian Google apabila dituliskan nama dirinya. Pemberitaan Gonzalez tersebut dapat ditelusuri akibat langkah digitalisasi yang dilakukan oleh surat kabar Spanyol, La Vanguardia terhadap arsip-arsip beritanya- termasuk didalamnya berita tentang Gonzalez . Perjuangan Gonzalez, berakhir dengan diputuskannya perusahaan Google untuk *de-index* artikel pemberitaan tentang pelelangan rumahnya. Selain, karena peristiwa tersebut telah lama terselesaikan oleh Gonzales, putusan tersebut didasarkan terkait ketentuan yang berlaku di *European Union* (EU) [19]. Putusan RTBF pada kasus Gonzales tersebut didasarkan ketentuan yang terkandung dalam Directive 95/46/EC, yang memberikan perlindungan kepada warga negaranya atas penggunaan data pribadi yang tidak sesuai. Setelah kasus Gonzalez tersebut marak dibicarakan, EU segera merumuskan ketentuan baru dan sejak Mei 2018 ketentuan mengenai RTBF diatur dalam Art.17 *General Data Protection Regulation* (GDPR) dengan judul "*Right to erasure ('right to be forgotten')* yang memiliki sedikit perbedaan dengan RTBF sebelumnya.

Instrumen hukum serupa RTBF atau *Right to Erasure* sesungguhnya telah diadopsi dalam sistem hukum Indonesia, dengan istilah "hak untuk dilupakkan" yang terdapat dalam Pasal 26 ayat (3) dan (4) UU ITE. Secara lengkap ketentuan tersebut yaitu :

(3) Setiap Penyelenggara Sistem Elektronik wajib menghapus Informasi dan Elektronik yang tidak relevan yang berada di bawah kendalinya atas permintaan orang yang bersangkutan berdasarkan penetapan pengadilan ;
(4) Setiap Penyelenggara Sistem Elektronik wajib menyediakan mekanisme penghapusan Informasi Elektronik yang sudah tidak relevan.

Hak untuk dilupakan tidak sepenuhnya serupa dengan konsep RTBF, perbedaan mendasar yang membedakan keduanya berada hasil pemenuhan hak tersebut. Pada RTBF, informasi tersebut akan hilang dari hasil mesin pencarian namun tetap dapat ditemukan pada tautan asli informasi data tersebut berada, sehingga RTBF kerap disebut sebagai langkah untuk menyulitkan seseorang untuk mengakses informasi tentang seseorang pada hasil situs mesin pencarian. Konsep Hak untuk dilupakan mengambil langkah yang berbeda dengan menghapus data tersebut sehingga tidak hanya dilakukan penghapusan dari hasil situs mesin pencari namun turut dilakukan pada tautan asli sumber data tersebut. Namun, terdapat kendala yang dapat dihadapi oleh seseorang yang hendak menghindari ancaman teknik *deepfake* terhadap dirinya, mengigat RTBF dan Hak untuk dilupakan memiliki syarat yang harus dipenuhi agar informasi tersebut dihapuskan. RTBF merujuk pada putusan *Court of Justice of the European Union* (CJEU) pada kasus Gonzalez mensyarakat informasi tersebut *inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes* [20]. Sementara Hak untuk dilupakan mensyaratkan informasi tersebut "tidak relevan". Tidak mudah tentunya untuk dalam mendasarkan ketidakrelevanan suatu informasi ketika informasi tersebut belum diproses dalam bentuk video porno atau manipulasi video lainnya sehingga ketakutan akan hadirnya ancaman terhadap diri seseorang tehadap potensi penggunaan informasi yang tidak sesuai sebaiknya menjadi pertimbangan dalam menerapkan pemberlakuan hak untuk dilupakan, dengan mendasarkan perlindungan hukum serta pengakuan terhadap hak atas data pribadi yang dimiliki oleh setiap individu. Masalah lainnya yang harus dihadapai oleh masyarakat Indonesia, karena hingga saat ini Peraturan Menteri terkait Hak Untuk Dilupakkan belum terbit.

4. KESIMPULAN

Upaya mencegah hadirnya video manipulasi dengan teknik *deepfake* dapat dilakukan dengan membatasi publikasi dokumentasi pribadi baik dalam bentuk foto ataupun video secara berlebihan. Apabila data tersebut telah terpublikasi, maka langkah yang dapat dilakukan adalah dengan melakukan proses seleksi data, sehingga tidak tersedia secara berlebihan informasi dokumentasi diri seseorang. Namun apabila data diri

subjek data terpublikasi pada penyelenggara sistem elektronik yang tidak dibawah kendali subjek data, maka subjek data dapat berupa mengajukan pemenuhan "Hak untuk dilupakan" sebagaimana yang diatur dalam Pasal 26 ayat (3) UU ITE guna mengajukan penghapusan data terkait informasi pribadi dirinya guna menghindari tersedianya sumber foto atau video yang dapat digunakan video *deepfake.*

5. DAFTAR PUSTAKA

[1] Tsarina Maharani, " Kominfo Identifikasi 486 Hoax Sepanjang April 2019, 209 terkait Politik", Detik, 1 Mei 2019, [Online]. Tersedia : https://news.detik.com/berita/d-4532182/kominfo-identifikasi-486-hoax-sepanjang-april-2019-209-terkait-politik [Diakses 13 September 2019].

[2] Seno Tri Sulistiyo, "Sembari tunjukkan Foto PKI, Jokowi : Fitnah keji seperti ini dalam rangka berpolitik", Tribunnews, 14 Desember 2018, [Online]. Tersedia : https://www.tribunnews.com/pilpres-2019/2018/12/14/sembari-tunjukkan-foto-pki-jokowi-fitnah-keji-seperti-ini-dalam-rangka-berpolitik [Diakses 14 September 2019].

[3] Adib M Asfar (ed)," Foto Prabowo dan logo palu arit, asli atau editan ? cek faktanya", Solopos, 5 Februari 2019, [Online]. Tersedia : https://www.solopos.com/foto-prabowo-dan-logo-palu-arit-asli-atau-editan-cek-faktanya-969903 [Diakes 13 September 2019].

[4] Ilham Safutra (ed), "Video kapal pembawa alat berat tenggelam jadi hoax ibu kota baru", Jawa Pos, 9 September 2019, [Online]. Tersedia : https://www.jawapos.com/hoax-atau-bukan/09/09/2019/video-kapal-pembawa-alat-berat-tenggelam-jadi-hoax-ibu-kota-baru/ [Diakses 13 September 2019].

[5] Tanayastri Dini Isna, "Duduki peringkat teratas aplikasi gratis IOS, ternyata aplikasi ini berbahaya !", Warta Ekonomi, 2 September 2019, [Online]. Tersedia : https://www.wartaekonomi.co.id/read244595/duduki-peringkat-teratas-aplikasi-gratis-ios-ternyata-aplikasi-ini-berbahaya.html [Diakses : 15 September 2019].

[6] Drew Harwell, "Top AI researcher race to detect 'deepfake' videos : 'we areoutgunned'", The Washingtonpost, 12 Juni 2019, [Online]. Tersedia : https://www.washingtonpost.com/technology/2019/06/12/top-ai-researchers-race-detect-deepfake-videos-we-are-outgunned/ [Diakses : 15 September 2019].

[7] Danielee Keats Citron, "Sexual Privacy", The Yale Law Journal, Vol. 128, pp. 1921-1922, 2019.

[8] Donie O'Sullivan, "When seeing is no longer believing : Inside the Pentagon's race againt deepfake videos, CNN, 2019, [Online]. Tersedia : https://edition.cnn.com/interactive/2019/01/business/pentagons-race-against-deepfakes/ [Diakses : 15 September 2019].

[9] Russel Spivak, ""Deepfakes": The newest way to commit one of the oldest crime", Georgetown Law Technology Review, Vol. 3.2, pp. 339, 2019.

[10] Giorgio Patrini, Francesco Cavalli, dan Henry Ajder, "The state of deepfakes : reality under attack", Deeptrace B.V, Amsterdam, Annual Report V.2.3, pp.3, 2018.

[11] Margaret Grebowicz, "Why Internet Porn Matters", Stanford University Press, California, pp.2, 2013.

[12] Marc Jonathan Blitz, "Lies, Line Drawing, and (Deep) Fake News", Oklahoma Law Review, Volume 71:1, pp.104-105, 2018.

[13] Anastasia Powell, "Sexual Violence in A Digital Age", Palgrave Studies in Cybercrime and Cybersecurity, Palgrave Macmillan, United Kingdom, pp.119-120, 2017.

[14] Rebecca A Delfino, "Pornographic Deepfakes- Revenge Porn's Next Tragic Act", Fordham Law Review, Vol 88, pp.5, 2019.

[15] Laporan Survei 2018, "Penetrasi & profil perilaku pengguna internet di Indonesia, Asosiasi Penyelenggara Jasa Internet Indonesia, Ver : S 20190518, 2019.

[16] Peter Fleischer dalam Jeffrey Rosen, " The Right to be forgotten", Standford law review symposium, The Privacy Paradox : Privacy and its conflingting values, 3 Februari 2012.

[17] Terence Craig dan Marr E. Ludloff, "Privacy and Big Data : The Player, Regulators and Stakeholders, O'Reilly Media, Sebastopol, pp.14-15, 2011.

[18] CNN, "RUU Data Pribadi Terancam Tak Selesai Dibahas Tahun Ini", CNN, 2019, [Online], Tersedia : https://www.cnnindonesia.com/teknologi/20190807122353-185-419154/ruu-data-pribadi-terancam-tak-selesai-dibahas-tahun-ini [Diakses : 16 September 2019].
[19] Chelsea E. Carbone, "To be or not to be Forgotten : Balancing the right to know with the right to privacy in the digital age", Virginia Journal of Social Policy & the Law, Vol. 22:3,pp. 533-535, 2015.
[20] McKay Cunningham, "Privacy Law That Does Not Protect Privacy, Forgetting the Right to be Forgotten, Bufallo Law Review,Vol.65, pp.496. 2017.

6. UCAPAN TERIMA KASIH

Terimakasuh kepada Kementerian Riset, Teknologi dan Pendidikan Tinggi Republik Indonesia yang telah membiayai penelitian penulis melalui Program Hibah Penelitian Dasar Unggulan Perguruan Tinggi (PDUPT) periode tahun 2019, hingga akhirnya menjadikannya materi dalam penulisan karya tulis ini.