

**ASPEK HUKUM PERLINDUNGAN DATA PRIBADI *SOURCE SUBJECT*
TERHADAP PENGGUNAAN TEKNIK DEEPPAKE DALAM
PERSPEKTIF PERBUATAN MELANGGAR HUKUM**



SKRIPSI

Diajukan Sebagai Syarat Untuk Memperoleh Gelar Sarjana Hukum

Pada Program Kekhususan Hukum Perdata

Fakultas Hukum Universitas Sriwijaya

Oleh :

BELA RENATA

02011181823448

**FAKULTAS HUKUM
UNIVERSITAS SRIWIJAYA**

INDRALAYA

2022

UNIVERSITAS SRIWIJAYA

FAKULTAS HUKUM

INDRALAYA

HALAMAN PENGESAHAN SKRIPSI

NAMA : BELA RENATA
NIM : 02011181823448
PROGRAM KEKHUSUSAN : HUKUM PERDATA

JUDUL SKRIPSI

**ASPEK HUKUM PERLINDUNGAN DATA PRIBADI *SOURCE SUBJECT*
TERHADAP PENGGUNAAN TEKNIK DEEPPAKE
DALAM PERSPEKTIF PERBUATAN MELANGGAR HUKUM**

Secara Substansi Telah Diuji dan Dinyatakan Lulus

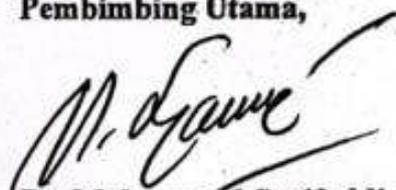
Dalam Ujian Skripsi/Komprehensif

Indralaya, 2022

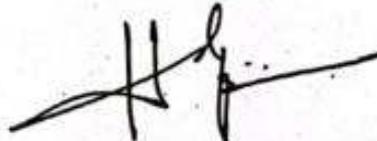
Menyetujui :

Pembimbing Utama,

Pembimbing Pembantu,



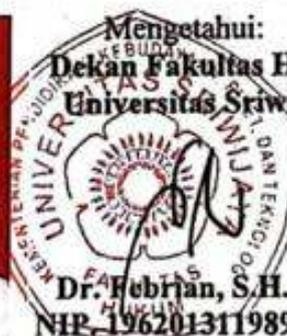
Dr. Muhammad Syaifuddin, S.H., M.Hum.
NIP. 197307281998021001



Helena Primadianti S, S.H., M.H.
NIP. 198609142009022004



Mengetahui:
**Dekan Fakultas Hukum
Universitas Sriwijaya,**



Dr. Febrina, S.H., M.S.
NIP. 196201311989031001

SURAT PERNYATAAN

Saya yang bertanda tangan dibawah ini:

Nama : Bela Renata
NIM : 02011181823448
Tempat/Tanggal Lahir : Megang Sakti II, 02 Februari 2000
Fakultas : Hukum
Strata Pendidikan : S1
Program Studi : Ilmu Hukum
Program Kekhususan : Hukum Perdata

Dengan ini menyatakan bahwa skripsi ini tidak memuat bahan-bahan yang sebelumnya telah diajukan untuk memperoleh gelar di Perguruan Tinggi manapun tanpa mencantumkan sumbernya. Skripsi ini tidak memuat bahan-bahan yang sebelumnya telah dipublikasikan atau ditulis oleh siapapun tanpa menyantumkan sumbernya.

Dengan demikian pernyataan ini telah saya buat dengan sebenarnya, apabila terbukti Saya telah melakukan hal-hal yang bertentangan dengan pernyataan ini, Saya bersedia menanggung segala akibat yang timbul dikemudian hari sesuai dengan ketentuan yang berlaku.

Indralaya, 2022

Yang Menyatakan :



Bela Renata
02011181823448

MOTTO:

**“The Future Belongs to Those
Who Believe in The Beauty of Their Dreams”**

Skripsi ini kupersembahkan kepada:

- 1. Allah SWT**
- 2. Kedua Orangtuaku tersayang
“Mama” dan “Abah” terima kasih
untuk semua kasih sayang dan
pengorbanannya serta setiap do’a
yang selalu mengiringi setiap
langkahku menuju pintu kesuksesan.**
- 3. Kakek dan Nenek tercinta**
- 4. Keluarga besarku yang selalu
mendo’akanku serta memberikan
dukungan dan semangat untuk
menuntaskan skripsi ini**
- 5. Sahabat-sahabatku yang tidak bisa
disebutkan satu persatu**
- 6. Almamaterku Fakultas Hukum
Universitas Sriwijaya.**

KATA PENGANTAR

Segala puja dan puji bagi Allah SWT yang telah memberikan nikmat, hidayah serta pertolongan sehingga penulisan skripsi ini dapat diselesaikan dengan baik. Selanjutnya sholawat serta salam tak hentinya dihaturkan kepada nabi Muhammad SAW yang telah membawa kita dari zaman kegelapan hingga zaman yang terang-benderang dipenuhi dengan ilmu pengetahuan seperti sekarang ini. Skripsi ini berjudul **“Aspek Hukum Perlindungan Data Pribadi *Source Subject* Terhadap Penggunaan Teknik Deepfake Dalam Perspektif Perbuatan Melanggar Hukum”**.

Skripsi ini dibuat untuk memenuhi salah satu syarat dalam mengikuti ujian skripsi/komprehensif untuk memperoleh gelar sarjana hukum di Fakultas Hukum Universitas Sriwijaya Indralaya. Penulis memahami dan menyadari bahwa skripsi ini masih jauh dari kata sempurna, oleh karenanya penulis sangat mengharapkan saran dan masukan guna untuk kesempurnaan skripsi ini.

Akhir kata penulis menyampaikan terima kasih kepada seluruh pihak yang telah memberikan bimbingan, arahan, ilmu, bantuan, dukungan serta doa sehingga terselesaikannya skripsi ini. Semoga skripsi ini dapat berguna bagi siapa saja yang membacanya, serta dapat memberikan manfaat bagi perkembangan ilmu pengetahuan khususnya di bidang ilmu hukum.

Indralaya, 2022



Bela Renata
02011181823448

UCAPAN TERIMA KASIH

Setelah melalui proses yang sangat panjang maka dalam kesempatan yang baik ini penulis mengucapkan Alhamdulillah, segala puji dan syukur kepada Allah SWT, karena atas berkat rahmat dan karunia-Nya lah penulis dapat menyelesaikan skripsi ini dengan baik, serta shalawat dan salam tidak lupa penulis haturkan kepada Baginda Nabi Muhammad SAW, keluarga serta para sahabatnya yang telah memberikan tauladan dan dinantikan syafaatnya di hari kiamat kelak.

Penulis dapat menyelesaikan skripsi ini atas bimbingan dan bantuan dari yang terhormat Bapak Dr. Muhammad Syaifuddin, S.H., M.Hum selaku pembimbing utama dan Ibu Helena Primadianti Sulistyaningrum, S.H., M.H selaku pembimbing kedua, terima kasih atas saran dan masukan serta kritik kepada penulis dalam melakukan penulisan skripsi ini. Serta ucapan terima kasih penulis kepada:

1. Kedua Orangtuaku, khususnya Mama terima kasih atas jasa, doa, dukungan yang selalu menjadi penyemangatku sejak awal perkuliahan hingga penyelesaian skripsi dan terima kasih atas kasih sayang dan cinta yang begitu berharga dan tidak akan sanggup membalasnya dalam segala aspek kehidupanku;
2. Bapak Dr. Febrian, S.H., M.S. selaku Dekan Fakultas Hukum Universitas Sriwijaya;
3. Bapak Dr. Mada Apriandi, S.H., M.CL. selaku Wakil Dekan I Fakultas Hukum Universitas Sriwijaya;
4. Bapak Dr. Ridwan S.H., M.H. selaku Wakil Dekan II Fakultas Hukum Universitas Sriwijaya;
5. Bapak DRS. H. Murzal Zaidan, S.H, M.Hum. selaku Wakil Dekan III Fakultas Hukum Universitas Sriwijaya;
6. Bapak Dr. Muhammad Syaifuddin, S.H., M.Hum. selaku Kepala Bagian Program Kekhususan Perdata atas segala pembelajaran ilmu, tenaga dan waktu yang telah diluangkan kepada penulis untuk menyelesaikan skripsi ini;
7. Bapak Dr. H. KN. Sofyan Hasan, S.H., M.H. selaku Dosen Pembimbing Akademik, Terima kasih atas pengarahan dan segala masukan yang telah diberikan selama kegiatan perkuliahan hingga saat ini;

8. Seluruh Dosen Fakultas Hukum Universitas Sriwijaya yang telah senantiasa dengan ikhlas mengajari, mendidik, memberikan ilmu dan pengetahuannya kepada penulis;
9. Seluruh staff & Karyawan di lingkungan Fakultas Hukum Universitas Sriwijaya yang telah berdedikasi penuh dalam menciptakan Fakultas Hukum Universitas Sriwijaya menerapkan Pelayanan Publik yang Prima;
10. Sahabat, adik dan teman terbaik dari awal menempuh pendidikan di Fakultas Hukum Universitas Sriwijaya (Alifia Laila Fitri, Tarisa Aprilliani, Nadia Shahab, Inja Takbir Marsela, Mellinia E.P, Nadiah Syahirah, Dwi Marlia, Lingga Agistin, Yuli Astuti, dan Nailah Hanifah) terimakasih untuk kebersamaannya, semoga kita semua berkumpul kembali di Jannah-Nya Allah;
11. BO Ramah, menjadi rumah bagi penulis dan membantu penulis dalam membentuk karakter pada diri semoga kita semua berkumpul kembali di Jannah-Nya Allah;
12. BO LAWCUS, menjadi wadah bagi penulis untuk mengembangkan kemampuan penulis khususnya dalam bidang kepenulisan dan debat, serta mempertemukan penulis dengan komunitas pencinta sastra dan literasi;
13. U-READ, menjadi wadah bagi penulis untuk mengembangkan kemampuan manajemen kegiatan dan organisasi serta memberikan penulis pengalaman, relasi dan teman-teman yang menginspirasi;
14. Kak Al-Walid, Kak Wafi, Kak Robin, Kak Irvan, dan Mbak Refi yang telah memberikan kesempatan bagi penulis untuk dapat berkembang dan belajar banyak hal baru yang bermanfaat, serta memberikan saran, dukungan, doa, bimbingan dan ilmunya dalam membantu penulis mengerjakan skripsi sampai penulisan skripsi ini dapat selesai;
15. Seluruh teman, adik, dan kakak tingkat yang tidak bisa penulis sebutkan satu-persatu yang telah memberikan saran, pengalaman, ilmu, semangat dan doa sehingga penulisan skripsi ini dapat diselesaikan.

Akhir kata terhadap semua doa, dukungan dan bantuan yang telah diberikan kepada penulis. Semoga silaturahmi tetap terjaga dan Semoga Allah SWT dapat menerima kebaikan dan amal saleh dan memberikan pahala yang berlipat ganda. Semoga ilmu yang penulis dapatkan menjadi ilmu yang berkah dan skripsi ini bermanfaat bagi kita semua. Aamiin.

DAFTAR ISI

HALAMAN JUDUL	i
HALAMAN PENGESAHAN	ii
SURAT PERNYATAAN	iii
MOTTO	iv
KATA PENGANTAR.....	v
UCAPAN TERIMA KASIH	vi
DAFTAR ISI.....	viii
DAFTAR GAMBAR.....	xi
ABSTRAK	xii
BAB I PENDAHULUAN.....	1
A. Latar Belakang	1
B. Rumusan Masalah	9
C. Tujuan Penelitian	9
D. Manfaat Penelitian	10
E. Ruang Lingkup Penelitian.....	11
F. Kerangka Teori.....	11
1. Teori Perlindungan Hukum.....	12
2. Teori Perbuatan Melanggar Hukum.....	14
G. Kerangka Konseptual	15
1. Hak atas Privasi.....	15
2. Perlindungan Data Pribadi	18
3. Deepfake Sebagai Informasi Digital	19
4. <i>Source Subject</i>	21
H. Metode Penelitian.....	23
1. Jenis Penelitian.....	23
2. Pendekatan Penelitian	24
3. Jenis dan Sumber Bahan-Bahan Hukum.....	25
4. Teknik Pengumpulan Bahan-Bahan Hukum.....	27

5. Teknik Analisis Bahan-Bahan Hukum	27
6. Penarikan Kesimpulan	28
BAB II TINJAUAN PUSTAKA.....	29
A. Hak Privasi.....	29
1. Definisi Privasi.....	29
2. Dimensi Privasi	33
3. Pengaturan Hak atas Privasi.....	38
B. Data Pribadi.....	40
1. Definisi Data Pribadi.....	40
2. Perlindungan Data Pribadi	43
3. Asas dan Prinsip Perlindungan Data Pribadi	47
C. Deepfake	50
1. Definisi Deepfake.....	50
2. Teknologi yang Mendasari Deepfake	52
3. Manfaat, Risiko, dan Dampak Penggunaan Deepfake.....	58
D. Perbuatan Melanggar Hukum	71
1. Perkembangan Perbuatan Melanggar Hukum.....	71
2. Unsur-Unsur Perbuatan Melanggar Hukum.....	75
3. Keterkaitan antara Perbuatan Melanggar Hukum dengan Hukum Pidana.....	76
BAB III PEMBAHASAN	78
A. Perlindungan Hukum terhadap Data Pribadi <i>Source Subject</i> dari Penggunaan Teknik Deepfake dalam Perspektif Perbuatan Melanggar Hukum.....	78
1. Keterkaitan Deepfake dengan Berbagai Aspek Hukum.....	78
2. Perlindungan Hukum Preventif terhadap Data Pribadi <i>Source Subject</i> dari Penggunaan Teknik Deepfake Berdasarkan Undang-Undang No. 27 Tahun 2022 tentang Pelindungan Data Pribadi.....	89

3. Perlindungan Hukum Represif terhadap Data Pribadi <i>Source Subject</i> dari Penggunaan Teknik Deepfake Berdasarkan Pasal 1365 Kitab Undang-Undang Hukum Perdata	95
B. Tindakan Hukum yang Dapat Dilakukan <i>Source Subject</i> yang Data Pribadinya Digunakan dalam Penggunaan Teknik Deepfake Tanpa Persetujuannya	117
1. Tindakan Hukum Perdata dan Pidana Berdasarkan Undang-Undang No. 27 Tahun 2022 tentang Pelindungan Data Pribadi.....	117
2. Tindakan Hukum Perdata Berdasarkan Undang-Undang No. 19 Tahun 2016 tentang Perubahan atas Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik	119
3. Tindakan Hukum Menuntut Tanggung Jawab Perdata Layanan Penyedia Sistem Elektronik Media Sosial, Mesin Pencari, dan Aplikasi Pembuat Deepfake	120
a) Tindakan Pemutusan Akses (<i>Take Down</i>) Berdasarkan Peraturan Menteri Komunikasi dan Informatika No. 5 Tahun 2020 tentang Penyelenggara Sistem Elektronik Lingkup Privat	129
b) Tindakan Mewujudkan Hak untuk Dilupakan (<i>Right To Be Forgotten</i>) Berdasarkan Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.....	135
BAB IV PENUTUP	139
A. Kesimpulan	139
B. Saran	140
DAFTAR PUSTAKA	143
LAMPIRAN	

DAFTAR GAMBAR

Gambar 1.1	3
Gambar 1.2	54
Gambar 1.3	55
Gambar 1.4	55

ABSTRAK

Penelitian dengan judul "Aspek Hukum Perlindungan Data Pribadi *Source Subject* terhadap Penggunaan Teknik Deepfake dalam Perspektif Perbuatan Melanggar Hukum". Penelitian ini bertujuan untuk mengetahui dan menganalisis perlindungan hukum data pribadi *source subject* dari penggunaan teknik deepfake dalam perspektif perbuatan melanggar hukum dan untuk mengetahui tindakan hukum yang dapat dilakukan *source subject* yang data pribadinya digunakan dalam teknik deepfake tanpa persetujuannya. Metode penelitian yang digunakan dalam skripsi ini adalah penelitian yuridis normatif, dengan pendekatan perundang-undangan (*statute approach*) dan pendekatan konseptual (*conceptual approach*). Hasil penelitian menunjukkan bahwa secara preventif penggunaan data pribadi *source subject* harus dilakukan berdasarkan persetujuan pemilik data, yang jika tidak terpenuhi maka pemrosesan data pribadi dianggap batal demi hukum. Sedangkan secara represif penggunaan data pribadi *source subject* tanpa persetujuan terhadap penggunaan teknik deepfake yang merugikan telah memenuhi unsur-unsur yang termuat dalam Pasal 1365 Kitab Undang-Undang Hukum Perdata sehingga dapat dikategorikan sebagai perbuatan melanggar hukum. Adapun tindakan hukum yang dapat dilakukan *source subject* yang data pribadinya digunakan tanpa persetujuan untuk membuat sebuah deepfake, selain dapat melakukan tindakan hukum perdata dan tindakan hukum pidana. *Source subject* juga dapat melakukan tindakan hukum pemutusan akses (*take down*) dan/atau tindakan hukum mewujudkan hak untuk dilupakan (*the right to be forgotten*) yang terdiri dari hak untuk dihapus (*right to erasure*) dan hak untuk dikeluarkan dari daftar mesin pencari (*right to delisting*).

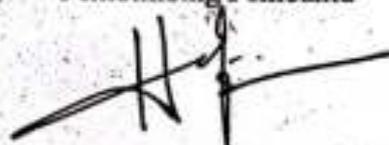
Kata kunci: Perlindungan Hukum, Data Pribadi, Deepfake, Tindakan Hukum.

Pembimbing Utama



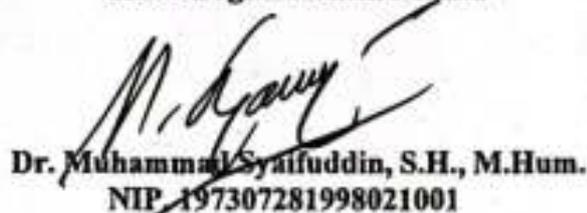
Dr. Muhammad Syaifuddin, S.H., M.Hum.
NIP. 197307281998021001

Pembimbing Pembantu



Helena Primadianti, S.H., M.H.
NIP. 198609142009022004

Ketua Bagian Hukum Perdata



Dr. Muhammad Syaifuddin, S.H., M.Hum.
NIP. 197307281998021001

BAB I

PENDAHULUAN

A. Latar Belakang

Perkembangan *artificial intelligence* (AI) atau yang biasa disebut kecerdasan buatan dewasa ini semakin pesat dan sangat cepat. *Artificial intelligence* kini tidak hanya berbentuk robot humanoid, melainkan juga memungkinkan sistem komputer, perangkat lunak, dan program untuk dapat mengambil keputusan serta bertindak selayaknya manusia. Salah satu hasil kreasi *artificial intelligence* yang sedang marak dibicarakan ialah **deepfake**. Deepfake berasal dari kata *deep Learning* dan *fake* yang dapat diartikan sebagai sebuah informasi audio visual palsu berupa foto, video, atau audio, yang dibuat melalui metode *deep learning*. *Deep learning* sendiri merupakan bagian dari *artificial intelligence* yang merujuk kepada pengaturan algoritma, yang secara mandiri dapat belajar dan membuat keputusan cerdas.¹ Secara sederhana deepfake dapat diartikan sebagai suatu audio visual palsu yang menampilkan perkataan atau perbuatan tertentu dari seseorang yang sebetulnya tidak pernah terjadi.

¹ Grace Shao, *What 'DEEPFAKE' are and how they may be dangerous*, CNBC, 13 September 2019, <https://www.cnbc.com/2019/10/14/what-is-DEEPFAKE-and-how-it-might-be-dangerous.html>, diakses pada 04 Desember 2021, Pukul 07:47 WIB.

Deepfake meskipun merupakan audio visual palsu yang dibuat menggunakan *artificial intelligence* bukan berarti deepfake dapat dengan mudah dilihat kepalsuannya secara kasat mata. Justru sebaliknya, deepfake dapat terlihat sangat nyata dan asli bergantung dari banyaknya data yang digunakan. Semakin banyak data berupa sampel suara dan gambar wajah dari *source subject* (individu yang wajah dan/atau suaranya ditampilkan dalam deepfake) digunakan, maka akan semakin baik dan nyata deepfake yang dihasilkan.

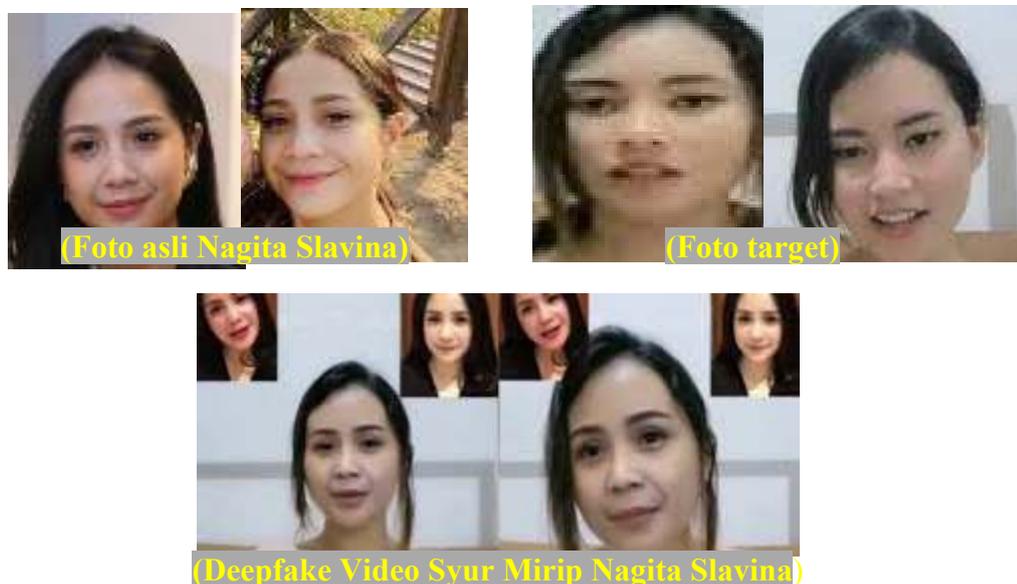
Awalnya pembuatan deepfake hanya dapat dilakukan oleh professional dan digunakan untuk industri perfilman misalnya pada saat aktor yang bersangkutan tidak dapat secara langsung hadir dalam proses syuting. Seperti yang terjadi pada film *Fast and Furious* dimana karakter Bryan (Paul Walker) digantikan perannya oleh aktor lain dikarenakan Paul meninggal dunia sebelum proses syuting berakhir.² Tetapi seiring berkembang serta meluasnya penggunaan teknologi, kini pembuatan deepfake bukan lagi menjadi hal yang hanya dapat dilakukan oleh professional karena telah dapat dibuat dengan cara yang lebih praktis menggunakan aplikasi-aplikasi yang tersedia gratis di internet seperti: DeepFaceLab, FaceSwap, MyFakeApp, Reface dan lain-lain. Hal tersebut semakin di dukung dengan keberadaan media sosial yang memberikan kemudahan akses bagi masyarakat luas untuk dapat memperoleh data berisikan gambar wajah atau sampel suara dari foto, video, atau audio milik orang lain yang tersebar di internet terutama foto-foto publik figur seperti politisi, artis,

² Elva Rini, *DEEPFAKE App: Pengertian, Cara Kerja, dan Manfaatnya*, Kompas TV, 5 Januari 2022, <https://beta.kompas.tv/amp/article/248655/videos/Deepfake-app-pengertian-cara-kerja-dan-manfaatnya?page=3>, diakses pada 10 Januari 2022, Pukul 09: 30 WIB.

influencer dan lain sebagainya. Faktor-faktor itulah yang mempermudah orang-orang dalam membuat deepfake dan memanfaatkannya untuk berbagai tujuan. Sayangnya kemudahan tersebut seringkali disalahgunakan untuk membuat deepfake tanpa persetujuan pemilik data yakni *source subject*. Parahnya deepfake tanpa persetujuan juga banyak dimanfaatkan untuk melakukan hal-hal yang merugikan terutama bagi *source subject*. Salah satu bentuk penyalahgunaan deepfake tanpa persetujuan ialah deepfake pornografi. Di awal tahun 2022 publik sempat dikejutkan dengan beredarnya video syur 61 detik mirip nagita slavina yang beredar di internet.³

Gambar 1.1

Deepfake Video Syur Mirip Nagita Slavina



Sumber: Liputan6, CNN, dan Idependensia.

³ Wahyu Sibarani, *Deepfake Bikin Oknum Pembuat Video Porno Leluasa Gunakan Wajah Artis*, SINDONEWS.com, 22 Januari 2022, <https://tekno.sindonews.com/read/663809/207/deepfake-bikin-oknum-pembuat-video-porno-leluasa-gunakan-wajah-artis-1642777284>, diakses pada 25 Januari 2022, Pukul 10:11 WIB.

Video tersebut sempat dilaporkan kepada pihak kepolisian dan setelah melalui proses penyelidikan video tersebut ternyata adalah video deepfake pornografi yang menggunakan wajah artis Indonesia Nagita Slavina. Suami dari Nagita Slavina mengaku bahwa video deepfake tersebut berkaitan dengan pencemaran nama baik dan telah mengganggu keluarganya. Hal serupa juga pernah terjadi pada salah satu reporter asal India Rana Ayyub. Pada tahun 2018 setelah ia mendukung kampanye menuntut keadilan bagi anak korban pemerkosaan, Rana justru diserang dengan video deepfake pornografi berisikan dirinya, keadaan menjadi semakin buruk saat video tersebut disebar oleh akun *fanspage* salah satu pendukung politikus yang mendukung pelaku dari peristiwa pemerkosaan tersebut, yang menyebabkan video deepfake pornografi Rana tersebar luas di internet dan dilihat hampir oleh seluruh masyarakat India saat itu, berbagai bentuk komentar negatif bahkan melecehkan mulai membanjiri Instagram, Facebook, hingga WhatsApp pribadinya miliknya. Saat itu Rana menderita stress dan tekanan yang sangat besar akibat deepfake pornografi berisikan dirinya, hingga ia harus dilarikan ke rumah sakit karena serangan panik.⁴ Terlepas dari itu nama baiknya sebagai seorang jurnalis saat itu telah tercemar. Bahkan ketika ia mencoba melaporkan ia justru tidak ditanggapi dengan baik oleh pihak kepolisian. Selain itu deepfake juga disalahgunakan sebagai modus penipuan. Menggunakan deepfake kloning pelaku telah berpura-pura sebagai CEO perusahaan energi asal Amerika Serikat yang memerintahkan

⁴ Rana Ayyub, *I Was The Victim of A Deepfake Porn Plot Intended To Silence Me*, Huffpost UK, 2018, https://www.huffingtonpost.co.uk/entry/deepfake-porn_uk_5bf2c126e4b0f32bd58ba316, diakses pada 17 Agustus 2022, Pukul 13.50 WIB.

manager perusahaan energi tersebut untuk mengirimkan uang sebesar US\$ 243.000 ke rekening pelaku. Sayangnya setelah uang tersebut dikirimkan, baru diketahui bahwa penelfon bukanlah CEO perusahaan dan bahwa suara tersebut merupakan hasil dari deepfake klonik audio yang menirukan suara asli dari CEO perusahaan bersangkutan.⁵ Tidak hanya itu, deepfake tanpa persetujuan juga dimanfaatkan untuk manipulasi data pinjaman online, dimana salah satu syarat pinjaman online ialah mengambil foto diri beserta KTP calon peminjam. Dalam hal ini teknik deepfake digunakan untuk menukar dan mencocokkan wajah serta KTP di foto dengan gambar wajah dari *source subject*.⁶ Akibatnya *source subject* yang digunakan datanya tanpa persetujuan untuk membuat deepfake tersebut menjadi terganggu dan dirugikan karena mengalami penagihan utang tanpa pernah meminjam, bahkan beberapa memilih membayar karena takut dengan ancaman pihak pinjaman online. Penyalahgunaan deepfake yang dibuat tanpa persetujuan *source subject* juga pernah digunakan dalam proses pengadilan sebagai alat bukti palsu, penyebaran berita bohong, serta penggiring opini politik.

Meskipun penggunaan deepfake tidak selamanya disalahgunakan seperti yang terjadi pada deepfake parodi Tom Cruises yang menampilkan Tom sebagai sarana hiburan dan tidak menyakiti atau membahayakan Tom sebagai *source*

⁵ Andi Nugroho, *Deepfake Voice, Teknik Baru Penjahat Siber Rampok Uang*, Cyberthreat.Id, 09 Oktober 2019, hlm. 1, <https://cyberthreat.id/read/3287/DEEPFAKE-Voice-Teknik-Baru-Penjahat-Siber-Rampok-Uang>, diakses pada 25 Januari 2022, Pukul 09:58 WIB.

⁶ Hafsah Amalia Afnan, *Skripsi, Perlindungan Hukum Penyalahgunaan Artificial Intelligence Deepfake Pada Layanan Pinjaman Online*, Fakultas Hukum Universitas Muhammadiyah Surakarta, 2022, hlm. 6..

subject.⁷ Namun dalam prosesnya, saat deepfake parodi Tom Cruises diterima baik oleh pengguna internet, pembuat deepfake tersebut mengatakan bahwa apabila Tom merasa tidak terima atau nyaman atas pembuatan deepfake menggunakan wajah dan suaranya maka ia akan menghapus video-video tersebut, meskipun kemudian Tom mengizinkannya bahkan berkolaborasi. Hal ini menunjukkan bahwa meskipun digunakan untuk keperluan yang tidak membahayakan pada prinsipnya deepfake tetap harus dibuat berdasarkan persetujuan dari pemilik data atau *source subject*. Permasalahannya dalam praktik lapangan deepfake seringkali dibuat tanpa persetujuan *source subject* selaku pemilik data dan dimanfaatkan untuk hal-hal negatif yang merugikan bagi *source subject*. Kerugian yang ditimbulkan terjadi karena apapun yang terjadi di dalam suatu deepfake senantiasa merujuk dan dianggap sebagai perbuatan dari individu yang ditampilkan di dalamnya. Hal ini menjadi sangat rentan bagi *source subject* sebagai pemilik data karena ia harus menanggung segala bentuk konsekuensi dan kerugian yang timbul dari deepfake tersebut. Bahkan jika digunakan untuk keperluan hiburan seperti industri perfilman, iklan, penyiaran ataupun parodi, penggunaan data pribadi dari seseorang tetap harus dilindungi karena menyangkut hak atas privasi bagi individu terkait, sehingga diperlukan izin sebelum menggunakannya.

⁷ Rachel Metz, *How a Deepfake Tom Cruises on Tik Tok turned into a very real AI company*, CNN BUSINESS, 06 Agustus 2021, hlm. 1, <https://edition.cnn.com/2021/08/06/tech/tom-cruise-Deepfake-tiktok-company/index.html> , diakses pada 26 Januari 2022 Pukul 08:06 WIB.

Di Indonesia sendiri data pribadi diatur di dalam Undang-Undang No. 27 Tahun 2022 tentang Pelindungan Data Pribadi yang baru disahkan beserta Undang-Undang terkait lainnya seperti: Undang-Undang No. 7 Tahun 1971 tentang Ketentuan Pokok Kearsipan, Undang-Undang No.8 Tahun 1997 tentang Dokumen Perusahaan, Undang-Undang No. 7 Tahun 1992 jo Undang-Undang No. 10 Tahun 1998 tentang Perbankan, Undang-Undang No. 36 Tahun 1999 tentang Telekomunikasi, Undang-Undang No. 36 Tahun 2009 tentang Kesehatan dan Undang-Undang No. 19 Tahun 2016 tentang perubahan atas Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.⁸ Meskipun demikian peraturan tersebut tidak secara khusus mengatur penggunaan data pribadi dalam pembuatan deepfake. Data pribadi sendiri diartikan sebagai data tentang orang perseorangan baik yang teridentifikasi atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik dan/atau nonelektronik.⁹ Adapun jenis data pribadi dibedakan menjadi 2 yakni data pribadi yang bersifat umum dan data pribadi yang bersifat khusus.¹⁰ Pada data pribadi yang bersifat khusus salah satunya jenisnya ialah data biometrik yang berkaitan dengan fisik, fisiologis, atau karakteristik perilaku individu seperti gambar wajah, suara, gestur tubuh dan lain sebagainya. Dalam penggunaan teknik deepfake untuk membuat foto, video, atau audio deepfake diperlukan data berupa gambar wajah, mimik dan gestur, bahkan suara seseorang

⁸ Edmon Makarim, *Pengantar Hukum Telematika (Suatu Kompilasi Kajian)*, Jakarta : PT. Raja Grafindo Persada, 2005, hlm. 177.

⁹ Pasal 1 ayat (1) Undang-Undang No. 27 Tahun 2022 tentang Pelindungan Data Pribadi.

¹⁰ Pasal 4 ayat (1) Undang-Undang No. 27 Tahun 2022 tentang Pelindungan Data Pribadi.

yang merupakan bagian dari data pribadi yang bersifat khusus yakni data biometrik tersebut. Meskipun saat ini untuk memperoleh informasi yang berkaitan dengan data pribadi seseorang seperti foto, video, atau audio atas individu yang tersebar di internet atau media sosial bukan hal yang sulit, tidak berarti bahwa informasi tersebut dapat dengan bebas digunakan tanpa seizin pemiliknya apalagi digunakan untuk hal-hal yang merugikan bagi individu tersebut. Hal ini selaras dengan apa yang diatur di dalam Undang-Undang Informasi dan Transaksi Elektronik bahwa *(1) kecuali ditentukan lain oleh Peraturan Perundang-Undangan, penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan Orang yang bersangkutan, (2) setiap orang yang melanggar haknya sebagaimana dimaksud pada ayat (1) dapat mengajukan gugatan atas kerugian yang ditimbulkan berdasarkan Undang-Undang ini.*¹¹ Sehingga kemudian muncul pertanyaan bagaimanakah sebetulnya perlindungan hukum terhadap data pribadi *source subject* yang data pribadi berupa foto, video, atau audio atas wajah dan/atau suaranya digunakan untuk membuat deepfake, serta bagaimanakah tindakan hukum yang dapat dilakukan jika data pribadi tersebut digunakan tanpa persetujuannya. Oleh karena itu penting untuk dilakukan penelitian mengenai **ASPEK HUKUM PERLINDUNGAN DATA PRIBADI SOURCE SUBJECT TERHADAP PENGGUNAAN TEKNIK DEEPPAKE DALAM PERSPEKTIF PERBUATAN MELANGGAR HUKUM.**

¹¹ Pasal 26 Undang-Undang No 19 tahun 2016 Tentang Perubahan atas Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

B. Rumusan Masalah

Berdasarkan latar belakang sebagaimana yang telah dijabarkan di atas maka dapat dirumuskan permasalahan sebagai berikut :

1. Bagaimana perlindungan hukum terhadap data pribadi *source subject* dari penggunaan teknik deepfake dalam perspektif perbuatan melanggar hukum?
2. Bagaimana tindakan hukum yang dapat dilakukan *source subject* yang data pribadinya digunakan dalam penggunaan teknik deepfake tanpa persetujuannya?

C. Tujuan Penelitian

Berdasarkan rumusan masalah diatas maka tujuan yang hendak di capai dalam penulisan skripsi ini adalah :

1. Untuk mengetahui perlindungan hukum terhadap data pribadi *source subject* dari penggunaan teknik deepfake dalam perspektif perbuatan melanggar hukum.
2. Untuk mengetahui tindakan hukum yang dapat dilakukan *source subject* yang data pribadinya digunakan dalam penggunaan teknik deepfake tanpa persetujuannya.

D. Manfaat Penelitian

Kegunaan dari hasil penelitian ini diharapkan dapat memberikan manfaat sebagai berikut:

1. Manfaat Teoritik

Pengembangan ilmu hukum perdata khususnya perbuatan melanggar hukum dalam kaitannya dengan perlindungan data pribadi *source subject* terhadap penggunaan teknik deepfake.

2. Manfaat Praktik

- a. Bagi *source subject* diharapkan bermanfaat memiliki pengetahuan terkait perlindungan hukum data pribadi miliknya dari penggunaan teknik deepfake tanpa persetujuan, serta tindakan hukum yang dapat dilakukan untuk mengembalikan hak-haknya jika terjadi pelanggaran.
- b. Bagi pengguna data pribadi dalam teknik deepfake diharapkan dapat memiliki pengetahuan bahwa penggunaan data pribadi seseorang tanpa persetujuan dapat terqualifikasi sebagai suatu perbuatan melanggar hukum yang menimbulkan tanggung jawab hukum.
- c. Bagi penyelenggara sistem elektronik penyedia jasa media sosial sebagai pihak ketiga diharapkan memiliki pengetahuan mengenai hak dan kewajiban sebagai pihak yang menghimpun data pribadi milik penggunanya, serta diharapkan dapat menjadi dasar pertimbangan dalam membuat ketentuan internal terkait larangan penggunaan data pribadi dan penyebarluasan informasi terkait data pribadi tanpa persetujuan.

- d. Bagi masyarakat informasi dan teknologi diharapkan dapat memiliki pengetahuan mengenai perlindungan hukum data pribadi dari penggunaan teknik deepfake agar kedepannya dapat dengan bijak dalam bertindak baik sebagai *source subject*, Pengguna data pribadi, maupun sebagai pihak yang memanfaatkan media sosial.

E. Ruang Lingkup Penelitian

Berdasarkan judul penelitian dan permasalahan dalam penelitian ini, maka ruang lingkup penelitian akan berfokus pada kajian mengenai:

1. Perlindungan hukum terhadap data pribadi *source subject* dari penggunaan teknik deepfake dalam perspektif perbuatan melanggar hukum.
2. Tindakan hukum yang dapat dilakukan *source subject* yang data pribadinya digunakan dalam penggunaan teknik deepfake tanpa persetujuannya.

F. Kerangka Teori

Kerangka teori pada dasarnya merupakan landasan teori atau dasar pemikiran yang sangat penting dalam menyusun penelitian. Kerangka teori diperlukan guna mempermudah penulis untuk menentukan arah serta tujuan penelitian, dan sebagai dasar penelitian supaya tahapan yang ditempuh berikutnya dapat jelas serta konsisten. Atau secara sederhananya sebagai alat untuk menjelaskan, dan mengolah data untuk memperoleh kesimpulan.¹² Kerangka teori dalam penulisan karya ilmiah hukum memiliki beberapa ciri yakni:

¹² Rifa'I Abubakar, *Pengantar Metodologi Penelitian*, Yogyakarta: SUKA-Press, 2021, hlm. 31.

- a) Teori-teori hukum;
- b) Asas-asas hukum;
- c) Doktri hukum; dan
- d) Ulasan pakar hukum berdasarkan pembedangan kekhususannya.¹³

Adapun teori-teori yang penulis gunakan dalam menyusun penelitian ini diantaranya:

1. Teori Perlindungan Hukum

Sebagai negara hukum, Indonesia mengedepankan supremasi hukum (kekuasaan tertinggi ada ditangan hukum) dalam menegakan kebenaran serta keadilan, dan bahwa tidak ada kekuasaan yang tidak dipertanggungjawabkan. Selaras dengan Pasal 1 ayat (3) Undang-Undang Dasar Kesatuan Republik Indonesia Tahun 1945 yang menyatakan bahwa Indonesia merupakan negara hukum. Dalam negara hukum, keberadaan hukum berfungsi untuk menjamin keadilan bagi masyarakat, sehingga sudah sepatutnya aturan-aturan dalam hukum mencerminkan keadilan dalam pergaulan hidup antar masyarakatnya.

Definisi perlindungan hukum menurut Satijipto Raharjo ialah sebuah bentuk pemberian pengayoman akan Hak Asasi Manusia atau yang sering disingkat sebagai HAM yang dirugikan atau dicerai orang lain, dan adapun perlindungan yang diberikan kepada masyarakat tersebut tidak lain adalah agar masyarakat dapat menikmati keseluruhan hak-hak yang diberikan oleh hukum.¹⁴

¹³ Zainuddin Ali, *Metode Penelitian Hukum* Jakarta: Sinar Grafika, 2016, Cet. 8, hlm. 79.

¹⁴ Satijipto Raharjo, *Ilmu Hukum*, Bandung: PT. Citra Aditya Bakti, 2021, Cet.9, hlm. 53.

Menurut Philipus M. Hadjon, yang dimaksud dengan Perlindungan Hukum adalah perlindungan terhadap harkat, martabat, dan pengakuan akan hak-hak asasi manusia yang dimiliki atau melekat kepada subyek hukum berdasarkan ketentuan hukum dari kesewenangan. Di sisi lain Hetty Hasanah mengartikan Perlindungan Hukum sebagai segala upaya yang menjamin adanya kepastian hukum, hal ini dikarenakan ia berkeyakinan bahwa kepastian hukum dapat memberikan perlindungan hukum terhadap pihak-pihak yang melakukan suatu perbuatan hukum.¹⁵

Perlindungan Hukum yang diperuntukan bagi masyarakat dari negara umumnya mempunyai dua sifat, yakni bersifat pencegahan (*preventif/prohibited*) dan bersifat hukuman (*represif/sanction*), namun dalam beberapa sumber juga menambahkan sifat pengarah (*persuasive*).¹⁶ Perlindungan hukum preventif adalah suatu tindakan pengendalian sosial yang bertujuan guna mencegah atau paling tidak mengurangi kemungkinan terjadinya hal-hal yang tidak dikehendaki kedepannya. Sedangkan perlindungan hukum represif bertujuan guna menyelesaikan sengketa yang telah terjadi serta penanganannya di lembaga peradilan. Singkatnya perlindungan hukum preventif merupakan upaya yang digunakan sebelum terjadinya pelanggaran terhadap hak-hak seorang individu, adapun perlindungan hukum represif adalah upaya yang dilakukan ketika pelanggaran terhadap suatu hak telah terjadi.

¹⁵ Hetty Hasanah, *Perlindungan Konsumen dalam Perjanjian Pembiayaan Konsumen atas Kendaraan Bermotor dengan Fidusia*, Jurnal UNIKOM, 2004, <http://jurnal.unikom.ac.id/vol3/perlindungan.html>, diakses pada 28 Januari 2022 Pukul 09:05 WIB.

¹⁶ Rizky P.P Karo karo dan Teguh Prasetyo, *Pengaturan Perlindungan Data Pribadi di Indonesia: Perspektif Teori Keadilan Bermartabat*, Bandung: Nusa Media, 2020, hlm. 50.

2. Teori Perbuatan Melanggar Hukum

Hampir seluruh aspek kehidupan manusia diatur oleh hukum. Semakin tinggi kepentingan manusia terhadap sesuatu maka semakin diperlukan keberadaan hukum yang dapat memberikan batasan terhadap perilaku manusia tersebut guna memperoleh kehidupan yang damai dan sejahtera. Hukum sendiri dapat diartikan sebagai sekumpulan peraturan yang berisi perintah dan larangan yang dibuat oleh pihak yang berwenang sehingga dapat dipaksakan pemberlakuannya dan berfungsi untuk mengatur masyarakat demi terciptanya ketertiban disertai dengan sanksi bagi pelanggarnya. Dalam ilmu hukum, kita mengenal adanya perbuatan melanggar hukum (PMH). Pada awalnya perbuatan melanggar hukum hanya terfokus pada perbuatan yang melanggar hukum tertulis saja atau yang dikenal dengan perbuatan melanggar hukum dalam arti sempit. Adapun saat ini dimulai sejak dikeluarkannya putusan Hoge Raad pada 31 Januari 1919, perbuatan melanggar hukum dapat diidentifikasi sebagai perbuatan yang lebih luas yakni perbuatan melanggar undang-undang, perbuatan yang bertentangan dengan hak-hak orang lain, perbuatan yang bertentangan dengan nilai-nilai kesusilaan dan kesopanan serta perbuatan yang melanggar asas-asas umum dalam lapangan hukum.¹⁷

¹⁷ Subekti, *Hukum Perjanjian*, Jakarta: Intermasa, 2010, Cet.23, hlm. 2.

Dalam ilmu hukum dikenal 3 (tiga) kategori dari perbuatan melanggar hukum sebagai berikut:

1. Perbuatan melanggar hukum karena kesengajaan,
2. Perbuatan melanggar hukum tanpa kesalahan (tanpa unsur kesengajaan maupun kelalaian), dan
3. Perbuatan melanggar hukum karena kelalaian.¹⁸

Perbuatan melanggar hukum di Indonesia diatur dalam Buku III Kitab Undang-Undang Hukum Perdata Pasal 1365-1380, termasuk ke dalam perikatan yang timbul dari undang-undang. Perbuatan Melanggar Hukum yang dijadikan dasar gugatan ganti rugi, disebutkan di dalam pasal 1365 KUHPerdata, yang menyatakan bahwa *tiap perbuatan melanggar hukum yang menimbulkan kerugian terhadap orang lain, mewajibkan orang yang karena salahnya menimbulkan kerugian itu, mengganti kerugian tersebut.*

G. Kerangka Konseptual

1. Hak atas Privasi

Hak atas privasi tidak secara eksplisit di cantumkan di dalam konstitusi Undang-Undang Dasar Negara Republik Tahun 1945 (UUD NRI 1945), melainkan tertera secara implisit pada Pasal 28 huruf (G) ayat (1) UUD NRI 1945 yang menerangkan bahwa *setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah*

¹⁸ Indah Sari, *Perbuatan Melanggar Hukum (PMH) dalam Hukum Pidana dan Hukum Perdata*, Jurnal Ilmiah Hukum Dirgantara, Volume 11 No. 1, September 2019, hlm. 53.

kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi.

Rumusan pada Pasal tersebut selaras dengan *Article 12 Universal Declaration of Human Rights* (UDHR) yang selanjutnya di adopsi dalam *Article 17 International Covenant on Civil and Political Rights* (ICCPR) yang secara jelas memuat jaminan terhadap hak atas privasi.

Jika merujuk pada putusan Mahkamah Konstitusi (MK) Nomor 50/PUU-VI/2008 tentang Perkara Pengujian Undang-Undang No 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), MK memberikan terjemahan terhadap kata *privacy* dalam Article 12 UDHR dan Article 17 ICCPR sebagai **urusan pribadi** atau **masalah pribadi** yang sesuai dengan apa yang tertera di dalam Pasal 28 huruf (G) ayat (1) UUD NRI 1945.¹⁹ *Article 12 UDHR* berbunyi *No one shall be subjected to arbitrary interference with his **privacy**, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.*²⁰ yang diterjemahkan menjadi, *tidak seorang pun boleh diganggu **urusan pribadinya**, keluarganya, rumah tangganya, atau hubungan surat-menyuratnya, dengan sewenang-wenang, juga tidak diperkenankan melakukan pelanggaran atas kehormatannya dan nama baiknya. Setiap orang berhak mendapat perlindungan hukum terhadap gangguan-gangguan atau pelanggaran seperti ini.*

¹⁹ Wicaksana Dramanda, *Apakah Hak atas Privasi Termasuk HAM?*, Hukum Online.COM, 22 Mei 2014, <https://www.hukumonline.com/klinik/a/apakah-hak-atas-privasi-termasuk-ham-lt4f5f850ec2388>, diakses pada 28 Januari 2022, Pukul 21:08 WIB.

²⁰ *International Covenant On Civil and Political Rights*, United Nations, General Assembly resolution 2200A (XXI), 1966.

Adapun *Article 17 ICCPR* menyatakan: 1. *No one shall be subjected to arbitrary or unlawful interference with his **privacy**, family, home or correspondence, nor honour and reputation*", 2. *"Everyone has the right to the protection of the law against such interference or attacks."*²¹ Diterjemahkan menjadi 1. *Tidak ada seorang pun yang boleh dicampuri secara sewenang-wenang atau secara tidak sah dicampuri **masalah pribadi**, keluarga, rumah atau korespondensinya, atau secara tidak sah diserang kehormatan dan nama baiknya*, 2. *Setiap orang berhak atas perlindungan hukum terhadap campurtangan atau serangan tersebut.*

Uraian tersebut menjelaskan bahwa hak atas privasi sebetulnya sudah dijamin di dalam UUD NRI 1945 namun yang dikenal sebagai hak atas pribadi. Lebih lanjut menurut Danrivanto Budhijanto suatu perlindungan atas hak pribadi atau hak privat sebagai hak asasi manusia dapat meningkatkan diantaranya: nilai-nilai kemanusiaan, hubungan antara individu dan masyarakat, kemandirian dalam otonomi untuk dapat melakukan dan kontrol mendapat kepantasan, dan meningkatkan toleransi serta menjauhkan dari perlakuan diskriminasi, dan terakhir dapat membatasi kekuasaan pemerintah.²² Hak atas privasi juga sangat berkaitan dengan kebutuhan spiritual manusia yakni untuk dihargai perasaan, pikiran serta hak untuk dapat menikmati kehidupannya yang dikenal dengan *"the right to be let alone"*.²³

²¹ *Ibid.*

²² Danrivanto Budhijanto, *Hukum Telekomunikasi, Penyiaran & Teknologi Informasi: Regulasi & Konvergensi*, Bandung: PT. Refika Aditama, 2010, hlm. 4.

²³ Samuel Warren & Louis D. Brandeis, *"The Right To Privacy"*, Harvard Law Review, Volume 4, No. 5, 1890, hlm.1, dikutip oleh Sinta Dewi dalam jurnal *Konsep Perlindungan Hukum atas Privasi*

2. Perlindungan Data Pribadi

Perlindungan data pribadi seringkali dihubungkan sebagai bagian dari perlindungan atas hak pribadi atau privasi. Hal tersebut merujuk kepada pendapat Schermer, menurutnya setidaknya ada tujuh dimensi paling umum dalam wacana hukum guna mengetahui hak atas privasi yakni:

1. Tubuh;
2. Pikiran;
3. Rumah;
4. Perilaku intim;
5. Korespondensi;
6. Kehidupan keluarga; dan,
7. Personal data.²⁴

Data pribadi berdasarkan Pasal 1 ayat (1) Undang-Undang tentang Pelindungan Data Pribadi diartikan sebagai *data tentang seseorang baik yang teridentifikasi dan/atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik dan.atau nonelektronik*. Pentingnya personal data atau data pribadi sebagai dimensi ruang privat adalah akibat langsung dari menjamurnya teknologi informasi dan komunikasi. Sering kali hal ini meningkatkan kategori untuk menindaklanjuti tiga 'ruang privasi' yaitu Privasi Jasmani, Privasi

dan Data Pribadi Dikaitkan dengan Penggunaan Cloud Computing di Indonesia, Fakultas Hukum Universitas Padjadjaran, Vol. 5, No.1, 2016.

²⁴ Bart Willem Schermer, *Software agents, surveillance, and the right to privacy: a legislative framework for agentenabled surveillance*, Leiden: Leiden University Press, 2007, hlm. 74.

Relasional, dan Privasi Informasi. Privasi Jasmani mencakup privasi dari (1) tubuh, (2) pikiran, dan (3) perilaku intim. Privasi Relasional meliputi privasi dari (3) perilaku intim, (4) rumah, (5) korespondensi, dan (6) kehidupan keluarga. Sedangkan Privasi Informasi terdiri dari (7) data pribadi, dan (5) korespondensi. Adapun yang dimaksud privasi informasi atau (*information privacy*) menurut Allan Westin ialah suatu hak individu, grup atau lembaga guna menentukan apakah informasi berkenaan dengan diri mereka perlu dikomunikasikan ataukah tidak kepada pihak lain.²⁵

3. Deepfake sebagai Informasi Digital

Suatu informasi di tengah perkembangan teknologi seperti sekarang ini tidak hanya berupa informasi konvensional seperti yang kita peroleh melalui televisi ataupun surat kabar melainkan juga informasi digital yang berkaitan erat dengan penggunaan komputer dan internet. Menurut Shannon dan Weaver dalam sudut pandang ilmu eksata, suatu informasi tidak muncul secara tiba-tiba melainkan merupakan hasil dari sistem pemrosesan atau pengolahan data sebagai bahan permulaannya.²⁶ Sehingga, suatu informasi lahir dari data-data yang berisikan fakta yang digunakan sebagai input baik itu berupa kata-kata, angka, gambar, pencitraan, suara, maupun gerak atau sensor, yang di proses atau telah mengalami perubahan baik bentuk atau penambahan nilai menjadi bentuk

²⁵ Alan F. Westin., *Privacy and Freedom*, Washington and Lee Law Review, Volume 25, ISSUE 1 Article 20, 1967, hlm. 7, dikutip oleh Sinta Dewi dalam *Perlindungan Privasi dan Data Pribadi dalam Era Ekonomi Digital di Indonesia*, Fakultas Hukum Padjadjaran, 2018, hlm.95.

²⁶ Shinta Dewi, *CYBERLAW Perlindungan Privasi Atas Informasi Pribadi Dalam E-Commerce Menurut Hukum Internasional*, Bandung: Widya Padjadjaran, 2009, hlm. 7.

yang lebih berarti sesuai konteksnya.²⁷ Sedangkan yang dimaksud dengan **digital** berdasarkan Kamus Besar Bahasa Indonesia (KBBI) diartikan sebagai sesuatu yang berkaitan dengan angka-angka untuk sistem perhitungan tertentu atau berhubungan dengan penomoran. Sehingga informasi digital dapat disimpulkan sebagai segala bentuk informasi yang disimpan, diproduksi, dikelola, didistribusikan, serta dikomunikasikan dalam format digital yang dapat berbentuk teks, angka, audio ataupun visual.

Berdasarkan kesimpulan tersebut deepfake dikategorikan sebagai salah satu bentuk informasi digital yang dibuat dengan data-data berisikan fakta berupa wajah, mimik, dan gestur *source subject* yang kemudian di proses untuk menghasilkan audio atau video yang memberikan informasi tertentu tentang hal yang sebetulnya tidak pernah dilakukan oleh individu yang menjadi *source subject* tersebut. Dalam proses pembuatannya, untuk menghasilkan video deepfake yang terlihat realistis diperlukan ratusan bahkan ribuan data berupa gambar mimik dan wajah individu yang bersangkutan. Artinya diperlukan ratusan bahkan ribuan data yang berkaitan dengan data pribadi *source subject* untuk membuat sebuah video deepfake. Adapun fitur wajah seseorang pada dasarnya merupakan bagian dari data pribadi dari setiap individu yang dapat mengidentifikasi identitasnya.

²⁷ Tansah Rahmatullah, *Kajian Mengenai Privasi Dalam Informasi Digital Dihubungkan Dengan Directive 95/46/EC dan Directive 2002/58/EC of The European Parliament and of The Council*, ResearchGate, 2017, hlm. 66.

Sehubungan dengan konteks privasi pada informasi digital, maka pendapat Alan Westin dalam *privacy and freedom* adalah yang paling mungkin diterapkan, ia menjelaskan privasi dalam kaitannya dengan kerahasiaan sebagai suatu klaim individu, kelompok, atau lembaga untuk menentukan kapan, bagaimana dan sejauh mana informasi tentang mereka dikomunikasikan kepada orang lain.²⁸ Artinya hanya individu terkaitlah yang memiliki hak untuk menentukan kapan waktu ia ingin mengkomunikasikan, atau siapa saja yang dapat mengakses ataupun bagaimana cara ia mengkomunikasikan informasi digital yang berkaitan dengan data pribadinya (*informacy privacy*). Sehingga dalam penggunaan informasi yang berkenaan dengan data pribadi seseorang perlu mendapatkan izin dari individu yang bersangkutan terlebih dahulu meskipun data tersebut tersebar di internet dan mudah didapatkan. Hal ini juga berkaitan dengan standarisasi privasi setiap orang yang dapat saja berbeda, bagi seseorang suatu tindakan mungkin telah melewati privasinya tetapi bagi orang lain dengan kebudayaan lain mungkin akan berbeda.

4. Source Subject

Source subject atau *source person* dapat diartikan sebagai subjek sumber atau individu yang gambar wajah atau sampel suara atas dirinya diperlukan sebagai data sumber dalam membuat deepfake. Secara umum dalam pembuatan deepfake terdapat 3 komponen yakni : *Source* atau Sumber, *Target* atau Destinasi, dan *Result* atau Hasil. Keseluruhan komponen tersebut biasanya

²⁸ Shinta Dewi, *Perlindungan Privasi ...*, *Loc.Cit.*

adalah data berupa gambar. *Source* merupakan data gambar dari individu yang akan digunakan wajahnya dan ditransfer kepada gambar *Target* yang kemudian akan menghasilkan gambar atau video gabungan antara wajah *Source* dan tubuh dari *Target* sebagai *Result* atau hasil akhirnya.²⁹ Dikarenakan belum adanya sebutan khusus bagi individu yang wajahnya digunakan dalam pembuatan ataupun hasil Deepfake itu sendiri sehingga dalam beberapa tulisan sering disebut sebagai *source subject* atau *source person* atau *source face*.

Source subject memiliki risiko yang lebih rentan dalam suatu deepfake dibandingkan individu lain yang digunakan datanya sebagai *Target* atau destinasi, karena biasanya hanya bagian badan dari target yang akan digunakan sedangkan wajah dan suara menggunakan data milik *source subject*, sehingga apapun yang terjadi di dalam foto, video maupun audio deepfake akan teridentifikasi dan tertuju kepada *source subject* meskipun kenyataannya *source subject* tidak pernah melakukan atau mengucapkan hal-hal seperti yang terdapat di dalam suatu deepfake. Terutama terhadap deepfake yang dibuat tanpa persetujuan *source subject*, dimana *source subject* tidak memiliki kendali terhadap bagaimana data pribadinya akan digunakan dalam sebuah deepfake, karena informasi terkait data pribadinya dipakai tanpa sepengetahuannya.

²⁹ Mariëtte van Huijstee, Pieter van Boheemen dan Djurre Das, *Tackling Deepfake in European Policy*, European Parliament, 2021, hlm. 11, [https://www.europarl.europa.eu/RegData/etudes/STUD/2021/690039/EPRS_STU\(2021\)690039_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2021/690039/EPRS_STU(2021)690039_EN.pdf), diakses 05 Februari 2022, Pukul 07:54 WIB.

H. Metode Penelitian

Metode Penelitian merupakan hal yang krusial dalam pengembangan ilmu pengetahuan dan teknologi, hal ini dikarenakan penelitian senantiasa bertujuan untuk mencari serta mengungkapkan kebenaran yang sistematis, metodologis dan konsisten. Dalam prosesnya, penelitian perlu dilakukan dengan analisa serta konsistensi agar menghasilkan konstruksi ilmiah terhadap data yang sebelumnya telah dikumpulkan dan diolah.³⁰ Dengan kata lain ilmu pengetahuan dan teknologi merupakan hasil dari penelitian yang dilakukan menggunakan metode penelitian. Metode penelitian yang digunakan akan berbeda sesuai dengan jenis penelitian yang dilakukan tidak terkecuali penelitian hukum yang memiliki jenis, sifat serta tujuan tersendiri dibanding ilmu pengetahuan lain.³¹ Penelitian hukum bukan merupakan bagian dari ilmu eksak ataupun ilmu humaniora. Selain itu, penelitian hukum bertujuan guna menentukan aturan hukum, prinsip hukum, dan doktrin hukum yang dibutuhkan untuk menjawab kebutuhan hukum di masyarakat. Adapun metode penelitian yang digunakan dalam melakukan penelitian ini ialah sebagai berikut :

1. Jenis Penelitian

Jenis penelitian hukum dibedakan menjadi 2 jenis yakni penelitian hukum empiris dan penelitian hukum normatif.³² Adapun penelitian ini dilakukan

³⁰ Soerjono Soekanto dan Sri Mamudji, *Penelitian Hukum Normative Suatu Tinjauan Singkat*, Jakarta: Raja Grafindo Persada, 2015, Cet. 17, hlm. 1.

³¹ *Ibid.*, hlm. 20.

³² Elizabeth Nurhaini Butarbutar, *Metode Penelitian Hukum*, Bandung: PT. Refika Aditama, 2018, hlm. 79.

dengan menggunakan metode penelitian hukum normatif yaitu suatu penelitian hukum yang berfokus pada norma hukum dimana data yang digunakan didapat dari membaca serta menganalisa bahan tertulis.

2. Pendekatan Penelitian

Pendekatan penelitian hukum merupakan penelitian yang memiliki obyek hukum, dapat berupa suatu ilmu, atau aturan-aturan yang bersifat dogmatis ataupun hukum yang berkaitan dengan pola perilaku dan kehidupan masyarakat. Intinya pendekatan penelitian ialah kegiatan ilmiah yang berdasarkan atas metode, sistematika serta pemikiran tertentu, bertujuan untuk mempelajari satu atau lebih gejala hukum dengan cara menganalisa. Menurut Jhony Ibrahim, pendekatan yang dapat di gunakan dalam penelitian hukum normatif ialah sebagai berikut :

- 1) Pendekatan Perundang-Undangan atau (*Statute approach*);
- 2) Pendekatan Konseptual atau (*Conceptual Approach*);
- 3) Pendekatan Kasus atau (*Case Approach*);
- 4) Pendekatan Analitis atau (*Analytical Approach*);
- 5) Pendekatan Perbandingan atau (*Comparative Approach*);
- 6) Pendekatan Historis atau (*Historical Approach*); dan
- 7) Pendekatan Filsafat atau (*Philosophical Approach*).³³

³³ Jhony Ibrahim, *Teori dan Metodologi Penelitian Hukum Normatif*, Malang: Bayu Media, 2013, hlm. 300.

Dalam penelitian ini, pendekatan yang di gunakan ialah jenis pendekatan perundang-undangan (*Statute approach*), dan pendekatan konseptual (*Conceptual Approach*). Pendekatan perundang-undangan (*Statute approach*), merupakan pendekatan yang dilakukan dengan cara menelaah seluruh undang-undang serta regulasi yang berkaitan dengan isu hukum yang sedang diteliti.³⁴ Adapun yang dimaksud dengan pendekatan konseptual (*Conceptual Approach*) adalah pendekatan yang beranjak dari pandangan-pandangan serta doktrin-doktrin yang berkembang di dalam hukum.³⁵ Dengan mempelajari pandangan-pandangan serta doktrin-doktrin dalam ilmu hukum tersebut diharapkan peneliti akan dapat menemukan ide-ide yang kemudian memunculkan pengertian-pengertian, konsep-konsep, dan asas-asas hukum yang sesuai dengan isu yang sedang diteliti.

3. Jenis dan Sumber Bahan-Bahan Hukum

Untuk memecahkan serta menyelaraskan isu terkait masalah hukum dalam penelitian, suatu penelitian memerlukan sumber-sumber penelitian yang disebut bahan hukum, baik primer maupun sekunder.³⁶ Adapun yang termasuk jenis-jenis sumber bahan hukum dalam penelitian ini yakni:

a. Bahan hukum primer yaitu bahan-bahan hukum yang mengikat, diantaranya:

1) Undang-Undang Dasar 1945;

³⁴ Petter Mahmud Marzuki, *Penelitian Hukum*, Edisi Revisi, Jakarta: Kencana, 2014, hlm. 133.

³⁵ *Ibid.*, hlm. 177.

³⁶ Johny Ibrahim, *Op.Cit.*, hlm. 141.

- 2) Kitab Undang-Undang Hukum Perdata;
 - 3) Undang-Undang No. 19 tahun 2016 Tentang Perubahan atas Undang-Undang No. 11 tahun 2008 Tentang Informasi dan Transaksi Elektronik;
 - 4) Undang-Undang No. 27 Tahun 2022 tentang Pelindungan Data Pribadi;
 - 5) Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik; dan
 - 6) Peraturan Menteri Komunikasi dan Informatika Republik Indonesia No. 20 tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik;
 - 7) Peraturan Menteri Komunikasi dan Informatika No. 5 Tahun 2020 tentang Penyelenggara Sistem Elektronik Lingkup Privat.
- b. Bahan hukum sekunder, Bahan hukum sekunder diperlukan karena suatu penelitian tidak cukup hanya bergantung pada bahan hukum primer perlu bahan hukum sekunder untuk menjelaskan bahan hukum primer.³⁷ Adapun bahan hukum sekunder biasanya dapat berupa pendapat hukum (doktrin), teori-teori yang berasal dari literatur hukum, hasil penelitian, artikel ilmiah, ataupun website yang berhubungan dengan penelitian. Dalam penelitian ini bahan hukum sekunder yang digunakan di antaranya :
- 1) Buku - buku hukum;
 - 2) Jurnal - jurnal hukum;

³⁷ Elizabeth Nurhaini Butarbutar, *Op.Cit.*, hlm. 136.

- 3) Karya tulis hukum atau pandangan ahli hukum yang termuat dalam media masa; dan
- 4) Surat kabar.

4. Teknik Pengumpulan Bahan-Bahan Hukum

Dalam penelitian ini, teknik pengumpulan bahan-bahan hukum yang digunakan ialah penelitian kepustakaan (*library research*) atau yang sering dikenal sebagai penelitian literatur, *legal research*, ataupun *legal research instruction*.³⁸ Penelitian kepustakaan disebut demikian dikarenakan bahan-bahan hukum yang digunakan dapat diperoleh di perpustakaan seperti: buku-buku, peraturan perundang-undangan, keputusan pengadilan (yurisprudensi), teori-teori hukum, doktrin- doktrin atau pendapat para ahli, rancangan undang-undang yang berkaitan dengan permasalahan yang diteliti dan sebagainya.

5. Teknik Analisis Bahan-Bahan Hukum

Teknik analisis bahan hukum merupakan penjelasan dari semua bahan penelitian yang telah dihimpun dan dijelaskan sebelumnya secara sistematis dan terstruktur. Penjelasan tersebut dijabarkan secara logis berdasarkan pemikiran penulis. Terdapat beberapa jenis teknik analisis bahan-bahan hukum dalam melakukan penelitian, adapun dalam penelitian ini digunakan teknik analisis kualitatif. Teknik analisis kualitatif merupakan metode analisis bahan-bahan hukum yang dilakukan dengan cara mengelompokkan dan memilah bahan-bahan

³⁸ Soerjono Soekanto dan Sri Mamudji, *Op. Cit.*, hlm. 23.

hukum yang didapat dari penelitian lapangan menurut kualitas dan kebenarannya untuk kemudian disusun secara sistematis.³⁹

6. Penarikan Kesimpulan

Penarikan Kesimpulan dalam penelitian ini dilakukan melalui teknik penarikan kesimpulan dengan cara berfikir deduktif, yang diawali dengan cara berfikir mendasar terhadap hal-hal yang bersifat umum, kemudian diambil kesimpulan secara khusus agar dapat mencapai tujuannya yakni berupa rumusan untuk menjawab permasalahan.⁴⁰

³⁹ Abdulkadir Muhammad, *Hukum dan Penelitian Hukum*, Cet. I, Bandung : PT. Citra AdityaBakti, 2004, hlm.5.

⁴⁰ Soerjono Soekanto, *Pengantar Penelitian Hukum*, Jakarta:UI-Press, 2010, hlm. 67.

DAFTAR PUSTAKA

BUKU

- Abubakar, Rifa'i. 2021. *Pengantar Metodologi Penelitian*. Yogyakarta: SUKA-Press.
- Ali, Achmad. 2015. *Menguak Tabir Hukum (Suatu Kajian Filosofis dan Sosiologis)*. Jakarta: Penerbit Toko Gunung Agung.
- Agustina, Rosa. 2004 *Perbuatan Melawan Hukum*. Jakarta: Fakultas Hukum Universitas Indonesia.
- Ali, Zainuddin. 2016. *Metode Penelitian Hukum (Cet. 8)*. Jakarta: Sinar Grafika.
- Amiruddin dan Zainal Asikin. 2018. *Pengantar Metode Penelitian Hukum (Cet. 10)*. Jakarta: Rajawali Pers.
- Badruzaman, Miriam Darus dkk. 2016. *Kompilasi Hukum Perikatan*. Bandung: PT Citra Aditya Bakti.
- Budhijanto, Danrivanto. 2010. *Hukum Telekomunikasi, Penyiaran & Teknologi Informasi: Regulasi & Konvergensi*. Bandung: PT. Refika Adhitama.
- Butarbutar, Elizabeth Nurhaini. 2018. *Metode Penelitian Hukum*. Bandung: PT. Refika Aditama.
- Dewi, Shinta. 2018. *Perlindungan Privasi dan Data Pribadi dalam Era Ekonomi Digital di Indonesia*. Fakultas Hukum Padjadjaran.
- Dewi, Shinta. 2009. *CYBERLAW Perlindungan Privasi Atas Informasi Pribadi Dalam E-Commerce Menurut Hukum Internasional*. Bandung: Widya Padjadjaran.
- Fuady, Munir. 2013. *Perbuatan Melawan Hukum Pendekatan Kontemporer (cet-4)*. Bandung: PT Citra Aditya Bakti.
- HS, Salim. 2019. *Perkembangan Hukum Kontrak Innominaat di Indonesia*. Jakarta: Grafika.

- Ibrahim, Johny. 2013. *Teori dan Metodologi Penelitian Hukum Normatif*. Malang : Bayu Media.
- Karo karo, Rizky P.P dan Teguh Prasetyo. 2020. *Pengaturan Perlindungan Data Pribadi di Indonesia: Perspektif Teori Keadilan Bermartabat*, Bandung: Nusa Media.
- Makarim, Edmon. 2005. *Pengantar Hukum Telematika (Suatu Kompilasi Kajian)*, Jakarta : PT. Raja Grafindo Persada.
- Marzuki, Petter Mahmud. 2014. *Penelitian Hukum (Edisi Revisi)*. Jakarta: Kencana.
- Muhammad, Abdulkadir. 2004. *Hukum dan Penelitian Hukum (Cet. I)*. Bandung: PT. Citra AdityaBakti.
- Prodjodikoro, Wirjono. 2018. *Perbuatan Melanggar Hukum Dipandang dari Sudut Hukum Perdata (edisi revisi)*. Bandung: CV Bandarmaju,
- Purwanto. 2007. *Penelitian Tentang Perlindungan Hukum Data Digital*. Jakarta: Badan Pembinaan Hukum Nasional.
- Satijipto, Raharjo. 2021. *Ilmu Hukum*. Bandung: PT. Citra Aditya Bakti.
- Schermer, Bart Willem. 2007. *Software agents, surveillance, and the right to privacy: a legislative framework for agentenabled surveillance*. Leiden: Leiden University Press.
- Soekanto, Soerjono. 2010. *Pengantar Penelitian Hukum*. Jakarta: UI-Press.
- Soekanto, Soerjono dan Sri Mamudji. 2015. *Penelitian Hukum Normative Suatu Tinjauan Singkat (Cet. 17)*. Jakarta: Rajawali Pres.
- Subekti. 2010. *Hukum Perjanjian*. Cet. 23. Jakarta: Intermasa.

JURNAL/PENELITIAN

- Aengus, Collins. 2019. *IRGC Forged Authenticity: Governing Deepfake Risks*. EPFL International Risk Governance Center.
- Afnan, Hafsa Amalia. 2022. *Perlindungan Hukum Penyalahgunaan Artificial Intelligence Deepfake Pada Layanan Pinjaman Online*. Skripsi Fakultas Hukum Universitas Muhammadiyah Surakarta.
- Bateman, Jon. 2020. *Deepfakes and Synthetic Media in the Financial System: Assessing Threat Scenario*. Carnegie Endowment for International Peace.

Diakses pada 26 April 2022.
<https://carnegieendowment.org/2020/07/08/deepfakes-and-synthetic-media-in-financial-system-assessing-threat-scenarios-pub-82237>.

Bennett, Thomas D.C.. 2019. *Triangulating Intrusion in Privacy Law*, Oxford Journal of Legal Studies, Vol. 39, No. 4, pp. 751–778.

BPHN. 2019. *Naskah Akademik Rancangan Undang-Undang Perlindungan Data Pribadi*. bphn.go.id. Diakses pada 04 April 2022.
https://www.bphn.go.id/data/documents/na_perlindungan_data_pribadi.pdf.

Chesney and Citron. 2018. *Deep Fakes: A Looming Challenge For Privacy, Democracy, and National Security*. SSRN Scholarly Paper Rochester, NY: Social Science Research Network, 2018, hlm. 1771-1778. Diakses pada 25 April 2022. <https://papers.ssrn.com/abstract=3213954>.

Delfino, Rebecca A. 2019. *Pornographic Deepfakes: The Case for Federal Criminalization of Revenge Porn's Next Tragic Act*. Fordham Law Review, Vol. 88, No. 3.

Dobber, Tom dkk. 2020. *Do (Microtargeted) Deepfakes Have Real Effects on Political Attitudes?*. The International Journal of Press/Politics, Vol. 26, No. 1. Diakses pada 29 April 2022. [Do \(Microtargeted\) Deepfakes Have Real Effects on Political Attitudes? \(sagepub.com\)](https://www.sagepub.com/journalsPermissions.nav).

European Union Agency for Fundamental Rights and Council of Europe. 2014. *Handbook on European Data Protection Law*. Belgium.

Kietzmann, Jan dkk. 2020. *Deepfakes: Trick or Treat?*. Business Horizons: ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING.

Maddocks, Ophie. 2020. *A Deepfake Porn Plot Intended to Silence Me: Exploring Continuities between Pornographic and 'Political' Deep Fakes*. Porn Studies, Vol. 7, No. 4. Diakses pada 28 April 2022.
<https://doi.org/10.1080/23268743.2020.1757499>.

Nurmatasari, Ni Nyoman Ari Diah dan Nyoman A. Martana. 2019. *Perlindungan Hukum Terhadap Data Pribadi Peminjaman Dalam Layanan Aplikasi Pinjaman Online*. Kertha Wicara: Journal Ilmu Hukum. Vol. 8, No. 12, P. 1-14. Diakses pada 20 April 2022.
<https://ojs.unud.ac.id/index.php/kerthawicara/article/view/50656>.

Rahmatullah, Tansah. 2017. *Kajian Mengenai Privasi Dalam Informasi Digital Dihubungkan Dengan Directive 95/46/EC dan Directive 2002/58/EC of The European Parliament and of The Council*. ResearchGate.

- Realussion. 2021. *AI-Generated Facial Photos For 3D Human Creation*. Headshot Plugin.
- Rini, Regina. 2020. *Deepfakes and the Epistemic Backstop*. Philosopher's Imprint, Vol. 20, No. 24. Diakses pada 30 April 2022. [Deepfakes and the Epistemic Backstop \(umich.edu\)](https://www.umich.edu).
- Sari, Indah. 2019. *Perbuatan Melanggar Hukum (PMH) dalam Hukum Pidana dan Hukum Perdata*. *Jurnal Ilmiah Hukum Dirgantara*, Vol. 11 No.1.
- Schofield, Carina B. Paine and Adam N. Joinson, 2010. *Privacy, Trust, and Disclosure Online*. ResearchGate. Diakses pada 01 April 2022. https://www.researchgate.net/profile/Ulf-Dietrich-Reips/publication/223956483_Privacy_Trust_and_Self-Disclosure_Online/links/0fcfd50c7d4a4de98a000000/Privacy-Trust-andSelf-Disclosure-Online.pdf?origin=publication_detail.
- Segal, Aya Yadlin and Yael Oppenheim. 2021. *Whose Dystopia Is It Anyway? Deepfakes and Social Media Regulation*. *Convergence*, Vol.27, No. 1, 2021. Diakses pada 29 April 2022. [Whose dystopia is it anyway? Deepfakes and social media regulation \(sagepub.com\)](https://www.sagepub.com)
- Šepec, Miha and Melanija Lango. 2020. *Virtual Revenge Pornography as a New Online Threat to Sexual Integrity*. *Balkan Social Science Review*, Vol. 15. Diakses pada 26 April 2022 <https://doi.org/10.46763/BSSR20150118sh>.
- Sokolov, S.S dkk. 2020. *Modern Social Engineering Voice Cloning Technologies*. 2020 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EICoN Rus). Diakses pada 19 April 2022. [Modern Social Engineering Voice Cloning Technologies | IEEE Conference Publication | IEEE Xplore](https://ieeexplore.ieee.org/abstract/document/9222222).
- Supriyadi, Daniar. 2018. *Data Pribadi dan Dua Dasar Legalitas Pemanfaatannya*, *Jurnal Unsyiah.ac.id*, Vol.20, No.2, 2018.
- Whittaker, L dkk. 2020. *All around Me Are Synthetic Faces': The Mad World of AI-Generated Media*. Departemen: IT Trends.
- Yuwinanto, Helmy Prasetyo. 2015. *Privasi Online dan Keamanan Data*. Departemen Informasi dan Perpustakaan FISIP. Universitas Airlangga.
- Zhu, Bingquan dkk. 2020. *Deepfakes for Medical Video De-Identification: Privacy Protection and Diagnostic Information Preservation*. *Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society*. Diakses pada 25 April 2022. <https://doi.org/10.1145/3375627.3375849>,

UNDANG-UNDANGAN/PERJANJIAN INTERNASIONAL

Kitab Undang-Undang Hukum Perdata

Kitab Undang-Undang Hukum Acara Pidana

Undang-Undang tentang Perlindungan Data Pribadi

Undang-Undang No 28 Tahun 2014 tentang Hak Cipta

Undang-Undang No 19 tahun 2016 Tentang Perubahan atas Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Peraturan Pemerintah No.71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik

Peraturan Menteri Komunikasi dan Informatika No.5 Tahun 2020 tentang Penyelenggara Sistem Elektronik Lingkup Privat

Peraturan Menteri Komunikasi dan Informatika No. 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik

United Nations. 1982. Internasional Covenant On Civil and Political Rights

INTERNET

Anjar, Angelina dan Philipus Parera. 2022. "Cek Faktas #50 Deepfake di Ruang Pengadilan". TEMPO.CO. Diakses pada 10 Januari 2022. <https://newsletter.tempo.co/read/1308716/cekfakta-50-Deepfakes-di-ruang-pengadilan/full&view=ok>.

Arif, Zainal. 2022. "Video Syur Nagita Slavina, Begini Ulasan Pakar IT Universitas Dinamika Sitkom", Surabaya.tribunnews.com. Diakses pada 14 Agustus 2022. <https://surabaya.tribunnews.com/2022/01/27/deepfake-video-syur-nagita-slavina-begini-ulasan-pakar-it-universitas-dinamika-stikom-surabaya>.

Ayyub, Rana. 2018. "I Was The Victim of A Deepfake Porn Plot Intended To Silence Me". Huffpost UK. Diakses pada 17 Agustus 2022. https://www.huffingtonpost.co.uk/entry/deepfake-porn_uk_5bf2c126e4b0f32bd58ba316.

Clarke, Roger. 2016. *Introduction to Dataveillance and Information Privacy, and Definitions of Terms*, AEShareNet, Diakses pada 02 April 2022. <http://www.rogerclarke.com/DV/>.

- Debusman, Bernd. 2021. "Deepfake: Tak sekedar teknologi untuk iseng, tapi diklaim sebagai 'masa depan pembuatan konten'. BBC. Diakses pada 11 Januari 2022. <https://www.bbc.com/indonesia/majalah-56318804>.
- Deepfacelab.cloud, "*Terms of Use*". Diakses pada 05 Oktober 2022. <https://deepfacelab.cloud/terms/>.
- Darmanda, Wicaksana. 2014. "Apakah Ha katas Privasi Termasuk HAM?". Hukum Online.COM. Diakses pada 28 Januari 2022. <https://www.hukumonline.com/klinik/a/apakah-hak-atas-privasi-termasuk-ham-lt4f5f850ec2388>.
- Ettema, Yori. 2021. "Deepmemory". YoriEttema.nl. Diakses pada 25 April 2022. <https://yorie.nl/deepmemory/>.
- Huijstee, Mariëtte van dkk. 2021. "Tackling Deepfake in European Policy". European Parliament. Diakses 20 Februari 2022. [https://www.europarl.europa.eu/RegData/etudes/STUD/2021/690039/EP_RS_STU\(2021\)690039_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2021/690039/EP_RS_STU(2021)690039_EN.pdf).
- IndiaToday. 2018. "I was vomiting: Journalist Rana Ayyub reveals horrifying account of deepfake porn plot". IndiaToday App Magazine. Diakses pada 17 Agustus 2022. <https://www.indiatoday.in/trending-news/story/journalist-rana-ayyub-deepfake-porn-1393423-2018-11-21>.
- Johnson, Dave. 2022. "What is a deepfake? Everthing you need to know about the AI-powered fake media". Businessinsider.com. Diakses pada 10 Agustus 2022, <https://www.businessinsider.com/guides/tech/what-is-deepfake?amp>.
- KOMINFO, 2017. "Penebar Hoax Bisa Dijerat Segudang Pasal". Viva.co.id. Diakses pada 14 Agustus 2022. https://www.kominfo.go.id/content/detail/8863/penebar-hoax-bisa-dijerat-segudang%20pasal/0/sorotan_media.
- Metz, Rachel. 2021. "How a Deepfake Tom Cruises on Tik Tok turned into a very real AI company". CNN BUSINESS. Diakses 11 Januari 2022. <https://edition.cnn.com/2021/08/06/tech/tom-cruise-deepfake-tiktok-company/index.html>.
- NPP/CR-21. 2016. "Ini Bedanya Konsep Right to be forgotten di Indonesia dengan Negara Lain". Hukum online. Diakses pada 11 September 2022. <https://www.hukumonline.com/berita/a/ini-bedanya-konsep-iright-to-be-forgotten-i-di-indonesia-dengan-negara-lain-lt586214ee33609>.
- Nugroho, Andi. 2021. "Facebook Kembangkan Alat Deteksi Deepfake". Cyberthreat.id. Diakses pada 09 September 2022.

<https://cyberthreat.id/read/11917/Facebook-Kembangkan-Alat-Deteksi-Deepfake>.

Nugroho, Andi. 2019. "Deepfake Voice, Teknik Baru Penjahat Siber Rampok Uang". Cyberthreat.Id. Diakses pada 10 Januari 2022. <https://cyberthreat.id/read/3287/Deepfakes-Voice-Teknik-Baru-Penjahat-Siber-Rampok-Uang>.

Palmai, Kitti. 2021. "Teknologi Kloning suara kian diminati aktor hingga penjahat siber, seperti apa kecanggihannya?". BBC NEWS INDONESIA. Diakses pada 03 September 2022. <https://www.bbc.com/indonesia/majalah-57804303.amp>.

Prastiwi, Devira. 2022. "4 Pokok Perkembangan Terkini Kasus Video Syur Mirip Nagita Slavina". Liputan6. Diakses pada 01 September 2022. <https://m.liputan6.com/news/read/4861620/4-perkembangan-terkini-kasus-video-syur-mirip-nagita-slavina>.

Rini, Elva. 2022. "Deepfakes App: Pengertian, Cara Kerja, dan Manfaatnya". Kompas TV. Diakses 10 Januari 2022. <https://beta.kompas.tv/amp/article/248655/videos/deepfake-app-pengertian-cara-kerja-dan-manfaatnya?page=3>.

Riparbelli, Victor. 2020. "Synthesia Insights: Case Study - David Beckham / Malaria No More / RGA". Synthesia. Diakses pada 28 April 2022. <https://www.synthesia.io/post/case-study-david-beckham-malaria-no-more-rga>

Sasse, Ben. 2018. "S.3805 - 115th Congress (2017-2018): Malicious Deep Fake Prohibition Act of 2018". CONGRESS.GOV. Diakses pada 29 April 2022. <https://www.congress.gov/bill/115th-congress/senate-bill/3805/text?format=txt>.

Shao, Grace. 2019. "What 'deepfakes' are and how they may be dangerous". CNBC. Diakses pada 04 Desember 2021. <https://www.cnbc.com/2019/10/14/what-is-Deepfakes-and-how-it-might-be-dangerous.html>.

Sibarani, Wahyu. 2022. "Deepfake Bikin Oknum Pembuat Video Porno Leluasa Gunakan Wajah Artis". SINDONESIAWS.com. Diakses pada 25 Januari 2022. <https://tekno.sindonews.com/read/663809/207/deepfake-bikin-oknum-pembuat-video-porno-leluasa-gunakan-wajah-artis-1642777284>.

Tech at Meta. 2019. "Facebook Is Building the Future of Connection with Lifelike Avatars". Facebook Technology. Diakses pada 12 Agustus 2022. <https://tech.fb.com/ar-vr/2019/03/codec-avatars-facebook-reality-labs/>.

- Tribun-Video. 2022. "Penyebaran Video Syur 61 Detik Mirip Nagita Slavina Ditangkap, Raffi Murka & Anggap Sudah Kelewatan". Tribun-Vide.com. Diakses pada 01 September 2022. <https://video.tribunnews.com/view/314467/penyeban-video-syur-61-detik-mirip-nagita-slavina-ditangkap-raffi-murka-anggap-sudah-kelewatan>.
- United Nations. 1966. Internasional Covenant On Civil and Political Rights, General Assembly resolution 2200A (XXI). Diakses pada 15 Januari 2022. <https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights>.
- Wyndham, Simon. 2021. "Bruce Willis starts as a deepfake in new phone ad", RedShark News. Diakses pada 11 Agustus 2022. <https://www.redsharknews.com/bruce-willis-stars-as-a-deepfake-in-new-phone-ad>.