BAB I

PENDAHULUAN

A. LATAR BELAKANG

Perkembangan teknologi yang semakin pesat telah mendorong peningkatan kehadiran *Artificial Intelligence* (AI) dalam aktivitas kehidupan manusia. AI dapat memberikan banyak manfaat dalam membantu pekerjaan manusia, baik dari segi kecepatan maupun keakuratan. Namun, teknologi ini juga memicu munculnya aplikasi *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 menampilan perkataan atau perbuatan tertentu dari seseorang yang sebetulnya tidak pernah terjadi.

Deepfake merupakan salah satu teknologi yang tergolong baru, 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

[1] Grace Shao. *What 'DEEPFAKE' are and how they may be dangerous*. (https://www.cnbc.com /2019/10/14/what-is-DEEPFAKE-and-how-it-might-be-dangerous.html. Diakses pada 24 September 2023, Pukul 07:47 WIB.)

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, 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. Parahnya *deepfake* tanpa persetujuan juga banyak dimanfaatkan untuk melakukan hal-hal yang merugikan. Salah satu bentuk penyalahgunaan *deepfake* tanpa persetujuan ialah *deepfake* pornografi. Diawal tahun 2022 publik sempat dikejutkan dengan beredarnya video syur 61 detik mirip Nagita Slavina yang beredar

[2] Elva Rini, *DEEPFAKE App: Pengertian, Cara Kerja, dan Manfaatnya*. (https://beta.kompas.tv/amp/article/248655/videos/Deepfake-app-pengertian-cara-kerja-dan manfaatnya?page=3. Diakses pada 24 September 2023, Pukul 08:30 WIB.)

di internet.[3] 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 menganggu keluarganya.

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 pemilik data.[4] 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 menunjukan bahwa meskipun digunakan untuk keperluan yang tidak membahayakan pada prinsipnya *deepfake* tetap harus dibuat berdasarkan persetujuan dari pemilik data.

Permasalahannya dalam praktik dilapangan *deepfake* seringkali dibuat tanpa persetujuan pemilik data dan dimanfaatkan untuk hal-hal negatif yang merugikan bagi pemilik data. Kerugian yang ditimbulkan

---

[3] Rana Ayyub, *I Was The Victim of A Deepfake Porn Plot Intended To Silence Me*. (https://www. huffingtonpost.co.uk/entry/deepfake-porn_uk_5bf2c126e4b0f32bd58ba316. Diakses pada 25 September 2023, Pukul 13.50 WIB.)

[4] Rachel Metz, *How a Deepfake Tom Cruises on Tik Tok turned into a very real AI company*. (https://edition.cnn.com/2021/08/06/tech/tom-cruise-Deepfake-tiktok-company/index.html. Diakses pada 25 September 2023 Pukul 10:06 WIB.)

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 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.

Untuk melindungi masyarakat dari penyalahgunaan kecerdasan buatan, pemerintah di seluruh dunia telah menerapkan perlindungan hukum terhadap penyalahgunaan teknologi *deepfake*. Perlindungan hukum ini bertujuan untuk mencegah orang membuat dan mendistribusikan konten palsu untuk tujuan jahat. Sebagai contoh, di Amerika Serikat, Pemerintah telah mengesahkan Undang-Undang Larangan *Deepfake* Berbahaya yang mengkriminalisasi produksi dan distribusi *deepfake* berbahaya.

Di Indonesia untuk menangani masalah ini, ada berbagai Undang-Undang yang dapat digunakan untuk melindungi pengguna dari penyalahgunaan *artificial intelligence* (AI). Undang-undang tersebut meliputi : Undang-Undang Dasar 1945, Kitab Undang-Undang Hukum Perdata, Kitab Undang-Undang Hukum Pidana, Undang-Undang No. 19 tahun 2016 Tentang Perubahan atas Undang-Undang No. 11 tahun 2008 Tentang Informasi dan Transaksi Elektronik, Undang-Undang No. 27 tahun

2022 tentang Pelindungan Data Pribadi, Undang-undang No. 44 Tahun 2008 tentang Pornografi, Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, dan Peraturan Menteri Komunikasi dan Informatika Republik Indonesia No. 20 tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik.

Sedangkan menurut Barda Nawawi Arief dalam perspektif hukum pidana, upaya dari penaggulangan *cybercrime* dapat dilihat dari beberapa aspek, diantaranya yaitu aspek kebijakan kriminalisasi (formulasi tindak pidana), aspek pertanggungjawaban pidana atau pemidanaan (termasuk aspek alat bukti/ 3 pembuktian), dan aspek yurisdiksi.[5] 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.[6] Adapun jenis data pribadi dibedakan menjadi 2, yakni data pribadi yang bersifat umum dan data pribadi yang bersifat khusus.[7] 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

[5] Siregar, Bonanda Japatani. "*Problem Dan Pengaturan Cybercrime Melalui Aktifitas Internet Dalam Kasus Sara Di Pilkada Serentak 2018*." Jurnal Penelitian Pendidikan Sosial Humaniora, Vol. 3(1), 2018

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

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

sebagainya. Dalam penggunaan teknik *deepfake* untuk membuat foto, video, atau audio *deepfake* diperlukan data berupa gambar wajah, mimik dan gestur, bahkan suara seseorang 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 dilanggar haknya sebagaimana dimaksud pada ayat (1) dapat mengajukan gugatan atas kerugian yang ditimbulkan berdasarkan Undang-Undang ini.[8]

Sehubungan dengan permasalahan tersebut, jika ditijau dari hukum Islam, dapat dikaji ke dalam ranah fiqh siyasah dusturiyah yakni hukum yang mengatur hubungan antara warga negara dengan lembaga negara satu dengan warga negara dan lembaga negara lainnya dalam batasan administratif warga negara.[9] Suyuthi Pulungan menyebutkan bahwa yang

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

[9] Smith dan Rhona K.M., *Hukum Hak Asasi Manusia*, Yogyakarta: PUSHAM UII, 2008, hlm. 238

dimaksud dengan fiqh siyasah dusturiyah adalah siyasah yang berhubungan dengan peraturan mengenai bentuk pemerintahan dan batasan kekuasaannya, tata cara pemilihan kepala negara, batasan kekuasaan yang lazim bagi pelaksana urusan umat, serta mengatur mengenai ketetapan hak yang wajib bagi individu dan masyarakat, sekaligus mengatur hubungan antara penguasa dan rakyat.[10]

Bilamana ditinjau dari hukum Islam, data pribadi meliputi kehormatan, kemuliaan dan martabat manusia yang tidak dapat dicabut. Ketika data disalahgunakan, maka menimbulkan bahaya (mudharat) berupa rusaknya harkat dan martabat individu (hifz-nafs), padahal syariat Islam berusaha semaksimal mungkin untuk menciptakan kemaslahatan bagi umat manusia. Urgensi regulasi pelindungan data pribadi membuat hukum menjamin privasi dan kerahasiaan setiap individu serta pengumpul data untuk lebih menghormati informasi pribadi yang dikumpulkan dan tidak menyebarkannya kepada pihak ketiga.[11] Hal tersebut sesuai dengan firman Allah SWT dalam surah An-Nur Ayat 27 sebagai berikut:

يَٰٓأَيُّهَا ٱلَّذِينَ ءَامَنُواْ لَا تَدۡخُلُواْ بُيُوتًا غَيۡرَ بُيُوتِكُمۡ حَتَّىٰ تَسۡتَأۡنِسُواْ وَتُسَلِّمُواْ عَلَىٰٓ أَهۡلِهَاۚ ذَٰلِكُمۡ خَيۡرٞ لَّكُمۡ لَعَلَّكُمۡ تَذَكَّرُونَ ٢٧

Artinya: “Hai orang-orang yang beriman, janganlah kamu memasuki rumah yang bukan rumahmu sebelum meminta izin dan memberi salam

[10] Suyuthi Pulungan, Fiqih Siyasah, *Ajaran, Sejarah dan Pemikiran*, Jakarta: PT. Raja Grafindo Persada, 1997, hlm. 40

[11] Mohammad Farid Fad, “*Pelindungan Data Pribadi dalam Perspektif Sadd Dzari’ah,*” Muamalatuna 13, no. 1 (2021): 61

kepada penghuninya. Yang demikian itu lebih baik bagimu, agar kamu (selalu) ingat" (QS. An-Nur: 27)[12]

Berdasarkan penjelasan tersebut, kemudian muncul pertanyaan bagaimanakah perlindungan hukum terhadap data pribadi berupa foto, video, atau audio atas wajah dan/atau yang suaranya digunakan untuk membuat *deepfake*, serta bagaimanakah tindakan hukum yang dapat dilakukan jika data pribadi tersebut digunakan tanpa persetujuan pemilik data pribadi, kemudian bagaimana perspektif fiqih siyasah dusturiyah terhadap perlindungan data pribadi dalam penyalahgunaan teknologi *deepfake*. Oleh karena itu penting untuk dilakukan penelitian mengenai **SISTEM PENEGAKAN HUKUM PERLINDUNGAN DATA PRIBADI TERHADAP PENGGUNAAN TEKNOLOGI *DEEPFAKE* DALAM PERSPEKTIF PERBUATAN MELAWAN HUKUM.**

B. RUMUSAN MASALAH

Berdasarkan uraian latar belakang di atas, maka dapat diambil rumusan masalah sebagai berikut:

1. Bagaimana perlindungan hukum terhadap penyalahgunaan teknologi *deepfake* dalam perspektif perbuatan melawan hukum?
2. Bagaimana tindakan hukum yang dapat dilakukan dalam penggunaan teknologi *deepfake* tanpa persetujuan pemilik data pribadi?

[12] "Al-Qur'an" n.d., v. an-Nur: 27

3. Bagaimana perlindungan data pribadi dalam penggunaan teknologi *deepfake* menurut perspektif fiqh siyasah dusturiyah?

C. TUJUAN PENELITIAN

Berdasarkan rumusan masalah di atas, maka penulis menentukan tujuan penelitian sebagai berikut:

1. Untuk mengetahui perlindungan hukum terhadap data pribadi dari penggunaan teknologi *deepfake* dalam perspektif perbuatan melawan hukum.
2. Untuk mengetahui tindakan hukum yang dapat dilakukan seseorang yang data pribadinya digunakan dalam penggunaan teknologi *deepfake* tanpa persetujuannya.
3. Untuk mengetahui perlindungan data pribadi dalam penggunaan teknologi *deepfak* dalam perspektif fiqh siyasah dusturiyah.

D. MANFAAT PENELITIAN

Hasil penelitian ini diharapkan dapat memberikan manfaat sebagai berikut:

1. Manfaat Teoritik

   Hasil penelitian ini diharapkan dapat memberikan sumbangsih pengetahuan dan dapat memberikan kontribusi dalam pengembangan ilmu pengetahuan khususnya bidang Hukum Tata Negara, terutama yang berkaitan dengan aspek hukum perlindungan data pribadi terhadap

penggunaan teknologi *deepfake* dalam perspektif perbuatan melawan hukum.

2. Manfaat Praktik

   a. Bagi Masyarakat:

      Dengan adanya penelitian ini diharapkan masyarakat dapat memiliki pengetahuan mengenai perlindungan hukum data pribadi dari penggunaan teknologi *deepfake* agar kedepannya dapat dengan bijak dalam bertindak baik sebagai *source subject*, pengguna data pribadi, maupun sebagai pihak yang memanfaatkan media sosial.

   b. Bagi Pengguna Data Pribadi Dalam Teknologi *Deepfake*:

      Pengguna data pribadi dalam teknologi *deepfake* dengan adanya penelitian ini, diharapkan dapat memiliki pengetahuan bahwa penggunaan data pribadi seseorang tanpa persetujuan dapat terkualifikasi sebagai suatu perbuatan melawan hukum yang menimbulkan tanggung jawab hukum.

   c. Bagi Penyelenggara Sistem Elektronik:

      Dengan adanya penelitian ini diharapkan penyelenggara sistem elektronik penyedia jasa media sosial sebagai pihak ketiga dapat 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 Pemerintah:

Penelitian ini diharapkan dapat bermanfaat bagi pemerintah terkait dengan hukum perlindungan data pribadi terhadap penggunaan teknologi *deepfake* dalam perspektif perbuatan melawan hukum. Serta dapat dijadikan referensi dan bahan evaluasi guna meningkatkan perlindungan data pribadi dari penyalahgunaan *deepfake*.

e. Bagi Peneliti Selanjutnya:

Penelitian ini diharapkan dapat dijadikan bahan acuan dan referensi bagi siapapun yang akan melakukan penelitian yang serupa, sehingga dapat menjadi tolak ukur bagi peneliti selanjutnya.

E. PENEGASAN ISTILAH

1. Penegasan Konseptual

Berikut adalah beberapa penegasan istilah yang dapat berguna dalam memahami konsep-konsep yang berkaitan dengan *deepfake* dan teknologi terkaitnya :

a. *Deepfake*: *Deepfake* adalah istilah yang mengacu pada teknik yang menggunakan kecerdasan buatan (AI), khususnya teknik *deep learning*, untuk menciptakan citra atau video palsu yang tampak sangat nyata. *Deepfake* sering digunakan untuk menggantikan wajah atau suara seseorang dalam video atau gambar.

b. Kecerdasan Buatan (*Artificial Intelligence*-AI): AI adalah bidang ilmu komputer yang berfokus pada pengembangan sistem komputer yang dapat melakukan tugas-tugas yang biasanya memerlukan kecerdasan manusia, seperti pemahaman bahasa alami, pengambilan keputusan, dan pembelajaran.
c. *Deep Learning*: *Deep learning* adalah subbidang dari machine learning yang menggunakan jaringan saraf tiruan (*neural networks*) dengan banyak lapisan (*deep layers*) untuk melakukan tugas-tugas yang kompleks, seperti pengenalan wajah atau suara.
d. Manipulasi Multimedia: Istilah ini merujuk pada proses mengedit atau mengubah gambar, video, atau suara secara digital. Dalam konteks *deepfake*, manipulasi multimedia mencakup pembuatan konten palsu yang tampak sangat nyata.
e. Deteksi *Deepfake*: Ini adalah usaha untuk mengidentifikasi dan mendeteksi konten *deepfake*, yaitu konten yang telah dimanipulasi menggunakan teknik *deep learning*.
f. Privasi: Privasi merujuk pada hak individu untuk menjaga informasi pribadi mereka dari akses dan penggunaan yang tidak diizinkan. Dalam konteks *deepfake*, privasi sering kali terkait dengan pemalsuan atau penyalahgunaan citra atau video pribadi.
g. Etika Teknologi: Etika teknologi adalah bidang yang mempertimbangkan aspek moral dan prinsip-prinsip etika dalam pengembangan, penggunaan, dan dampak teknologi.

h. Hukum dan Regulasi: Ini merujuk pada undang-undang dan peraturan yang mengatur penggunaan teknologi, termasuk *deepfake*. Hukum dan regulasi dapat mencakup perlindungan terhadap penyalahgunaan teknologi dan sanksi hukum.

2. Penegasan Operasional

Deepfake adalah sebuah teknologi yang digunakan untuk memanipulasi konten audio atau visual dengan tujuan menciptakan video palsu yang terlihat sangat nyata. Teknologi terkait lainnya termasuk *face swapping, voice cloning*, dan manipulasi gambar, yang dapat digunakan untuk tujuan serupa. Teknologi *deepfake* menggunakan kecerdasan buatan dan *machine learning* untuk menggabungkan dan memanipulasi data yang ada. Dalam konteks *deepfake*, teknologi *deep learning* digunakan untuk menganalisis dan membandingkan pola visual dalam video, serta mengidentifikasi tanda-tanda manipulasi atau rekayasa.

Teknologi *deepfake* terus berkembang dengan cepat, membuatnya semakin sulit untuk membedakan antara video asli dan *deepfake*. Penggunaan *deepfake* yang tidak etis dan berpotensi merugikan telah menimbulkan kekhawatiran tentang privasi, keamanan, dan integritas informasi. Untuk mengatasi tantangan yang ditimbulkan oleh teknologi *deepfake*, regulasi dan teknologi deteksi *deepfake* terus dikembangkan. Regulasi bertujuan untuk melindungi individu dan pemegang hak cipta, serta memastikan kepatuhan terhadap hukum yang berlaku. Sementara

itu, teknologi deteksi *deepfake* menggunakan pendekatan seperti analisis kehilangan informasi, pemodelan 3D, analisis statistik, dan deteksi anomali.

Namun, seiring dengan perkembangan *deepfake,* deteksi yang efektif juga membutuhkan penelitian dan pengembangan berkelanjutan dalam teknologi deteksi *deepfake*. Hal ini penting untuk memastikan bahwa *deepfake* dapat diidentifikasi dan tindakan yang tepat dapat diambil untuk mencegah penyebaran *deepfake* yang berbahaya.

F. METODE PENELITIAN

1. Jenis Penelitian

Permasalahan yang diangkat pada penelitian ini menggunakan metode penelitian yuridis normatif (metode penelitian hukum normatif) atau juga dikenal dengan penelitian hukum *doctrinal* atau kepustakaan, dalam Anglo Amerika disebut dengan *legal research* yaitu penelitian internal dalam disiplin ilmu hukum.[13] Metode penelitian yuridis normatif adalah penelitian hukum kepustakaan yang dilakukan dengan cara meneliti bahan-bahan kepustakaan atau data sekunder belaka.[14]

Penelitian ini dilakukan guna untuk mendapatkan bahan-bahan berupa: teori-teori, konsep-konsep, asas-asas hukum serta peraturan

[13] Ronny Hanitijo Soemitro, *Metode Penelitain Hukum, Metodologi Penelitian Ilmu Sosial, (Dengan Orientasi Penelitian Bidang Hukum),* Pelatihan Metodologi Ilmu Sosial, Bagian Hukum dan Masyarakat FH Undip, 1999, hlm. 15

[14] Soerjono Soekanto dan Sri Mahmudji, *Penelitian Hukum Normatif, Suatu Tinjauan Singkat*, Jakarta: Raja Grafindo Persada, 2003, hlm. 13

hukum yang berhubungan dengan pokok bahasan. Ruang lingkup penelitian hukum normatif menurut Soerjono Soekanto meliputi:

a. Penelitian terhadap asas-asas hukum.
b. Penelitian terhadap sistematika hukum.
c. Penelitian terhadap taraf sinkronisasi hukum secara vertikal dan horizontal.
d. Perbandingan hukum.
e. Sejarah hukum.

Dalam penelitian ini, ruang lingkup penelitian ini akan dilakukan penelitian dengan cara menarik asas hukum, dimana dilakukan terhadap hukum positif tertulis maupun tidak tertulis.[15] Penelitian ini dapat digunakan untuk menarik asas-asas hukum dalam menafsirkan peraturan peundang-undangan. Selain itu, penelitian ini juga, dapat digunakan untuk mencari asas hukum yang dirumuskan baik secara tersirat maupun tersurat.[16]

2. Metode Pendekatan

Metode pendekatan yang dipergunakan dalam penyusunan tesis ini adalah penelitian yuridis normatif (metode penelitian hukum normatif). Metode penelitian yuridis normatif adalah penelitian hukum kepustakaan yang dilakukan dengan cara meneliti bahan-bahan pustaka atau data sekunder belaka. Dengan menggunakan metode berpikir

[15] Soerjono Soekanto, *Pengantar Penelitian Hukum*, Jakarta: UI Press, 1996, hlm. 63
[16] Bambang Sunggono, *Metodologi Penelitian Hukum*, Jakarta: Raja Grafindo Persada, 2003, hlm. 27-28

deduktif (cara berpikir dalam penarikan kesimpulan yang ditarik dari sesuatu yang sifatnya umum yang sudah dibuktikan bahwa dia benar dan kesimpulan itu ditujukan untuk sesuatu yang sifatnya khusus).[17]

Dengan demikian objek yang dianalisis dengan pendekatan yang bersifat kualitatif adalah metode penelitian yang mengacu pada norma-norma hukum yang terdapat dalam peraturan perundang-undangan.[18]

3. Sumber Data

Untuk memecahkan serta menyelaraskan isu terkait masalah hukum dalam penelitian, suatu penelitian memerlukan sumber-sumber penelitian yang disebut bahan hukum, baik primer maupun sekunder.[19] Adapun yang termasuk jenis-jenis sumber bahan hukum dalam penelitian ini yakni:

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

a. Undang-Undang Dasar 1945;
b. Kitab Undang-Undang Hukum Perdata;
c. Kitab Undang-Undang Hukum Pidana;
d. Undang-Undang No. 19 tahun 2016 Tentang Perubahan atas Undang-Undang No. 11 tahun 2008 Tentang Informasi dan Transaksi Elektronik;

[17] Sedarmayanti & Syarifudin Hidayat, *Metodologi Penelitian*, Bandung: Mandar Maju, 2002, hlm. 23

[18] Soerjono Seokanto dan Sri Mamudji, *Op.Cit*, hlm. 14

[19] Johny Ibrahim, *Op.Cit*., hlm. 141

e. Undang-Undang No. 27 tahun 2022 tentang Pelindungan Data Pribadi;
f. Undang-undang No. 44 Tahun 2008 tentang Pornografi;
g. Undang-Undang No. 28 tahun 2014 tentang Hak Cipta.
h. Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik; dan
i. Peraturan Menteri Komunikasi dan Informatika Republik Indonesia No. 20 tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik;

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.[20] 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 diataranya:

a. Buku-buku hukum;
b. Al-Qur'an
c. Hadis
d. Jurnal-jurnal hukum;

[20] Elizabeth Nurhaini Butarbutar, *Op.Cit*,, hlm. 136

e. Karya tulis hukum atau pandangan ahli hukum yang termuat dalam media masa; dan

f. Surat kabar.

4. Teknik Pengumpulan Data

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*.[21] 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. Analisis Data

Dalam penelitian, metode pengolahan dan analisis data seringkali disesuaikan dengan jenis data yang digunakan. Pada penelitian hukum normatif, proses pengolahan dan analisis data dari bahan hukum primer hingga tersier sangat terkait dengan berbagai interpretasi dalam ranah keilmuan hukum. Data yang dikumpulkan selama penelitian akan melalui serangkaian tahapan sebagai berikut:

[21] Soerjono Soekanto dan Sri Mamudji, *Op. Cit.*, hlm. 23

a. Editing: Tahap awal di mana data dari daftar pustaka atau referensi dikaji ulang untuk memastikan kecocokan dan relevansinya dalam konteks penelitian.
b. Classifying: Penting untuk mengklasifikasikan dengan cermat setiap data, informasi, interpretasi, opini, dan teori yang terkait dengan penelitian.
c. Verifying: Langkah verifikasi membantu memastikan kefaktualan dan keabsahan data, informasi, atau sumber kepustakaan yang digunakan dalam penelitian.
d. Concluding: Tahap akhir di mana peneliti menyimpulkan hasil penelitian dan menarik kesimpulan dari seluruh proses penelitian, menjawab permasalahan yang mendasari studi sesuai dengan latar belakang yang telah diuraikan.

Setelah mengumpulkan data, langkah selanjutnya adalah melakukan analisis mendalam untuk mendapatkan kesimpulan dan jawaban atas tujuan penelitian. Analisis data ini bertujuan untuk menyelidiki, menafsirkan, dan memverifikasi fenomena atau objek penelitian sesuai dengan yang telah diuraikan sebelumnya.

6. Keabsahan Data

Dalam menguji keabsahan data, salah satu metode yang dapat digunakan adalah triangulasi, yaitu memverifikasi data dengan menggunakan instrumen lain untuk membandingkan fenomena atau perspektif terhadap dokumen seperti buku, literatur, perundang-

undangan, dan lain sebagainya. Dalam konteks skripsi ini, penulis perlu menganalisis peraturan perundang-undangan, literatur, serta situasi politik dan hukum di Indonesia yang relevan dengan penelitian yang dilakukan.

G. SISTEMATIKA PEMBAHASAN

Untuk memberikan gambaran yang jelas dalam skripsi ini, peneliti membagi menjadi lima bab, dimana antara bab satu dengan bab lainnya saling berkaitan, sehingga penulisan skripsi ini merupakan satu kesatuan yang tidak dapat dipisah-pisahkan. Adapun sistematikanya adalah sebagai berikut:

1. Bagian awal

   Bagian awal skripsi ini memuat hal-hal yang bersifat formalitas tentang halaman sampul depan, halaman judul, halaman persetujuan, halaman pengesahan, motto, persembahan, kata pengantar, daftar isi, daftar tabel, daftar gambar, daftar lampiran, dan abstrak.

2. Bagian Inti

   Bagian ini terdiri dari:

   BAB I Pendahuluan, terdiri dari (a) latar belakang masalah, (b) rumusan masalah, (c) tujuan penelitian, (d) manfaat penelitian, (e) penegasan istilah, (f) metode penelitian, (g) sistematika pembahasan.

BAB II Kajian Pustaka yang terdiri dari pembahasan mengenai (a) kajian fokus pertama, (b) kajian fokus kedua dan seterusnya, (c) hasil penelitian terdahulu.

BAB III Pada bab ini penulis akan menjawab rumusan masalah pertama mengenai perlindungan hukum terhadap penyalahgunaan teknologi *deepfake* dalam perspektif perbuatan melawan hukum.

BAB IV Pada bab ini penulis akan menjawab rumusan masalah kedua mengenai tindakan hukum yang dapat dilakukan dalam penyalahgunaan teknologi *deepfake* tanpa persetujuan pemilik data pribadi.

BAB V Pada bab ini penulis akan menjawab rumusan maslah ketiga mengenai perlindungan data pribadi dalam penyalahgunaan teknologi *deepfake* menurut perspektif fiqh siyasah dusturiyah.

BAB VI Penutup, terdiri dari kesimpulan dan saran.