SKRIPSI

PERLINDUNGAN HUKUM TERHADAP KORBAN PENYALAHGUNAAN DATA PRIBADI AKIBAT *DEEPFAKE*

Disusun untuk memperoleh gelar Sarjana Hukum

Oleh:

Rizal Wahyu Setyawan

18.0201.0020

PROGRAM STUDI ILMU HUKUM

FAKULTAS HUKUM

UNIVERSITAS MUHAMMADIYAH MAGELANG

2025

BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Perkembangan teknologi digital memberikan banyak sekali manfaat dalam kehidupan manusia. Teknologi AI (*Artificial Intelligence*) seperti *deep learning* telah melahirkan fenomena baru yang dikenal dengan istilah *deepfake*, yaitu konten digital hasil rekayasa AI (*Artificial Intelligence*) yang secara visual atau audio sangat menyerupai aslinya, sehingga sulit dibedakan dari kenyataan. Teknologi ini, meskipun memiliki potensi positif dalam bidang hiburan dan pendidikan, namun juga berpotensi disalahgunakan untuk kepentingan yang merugikan seseorang, seperti pencemaran nama baik, penipuan, pemerasan, bahkan kejahatan seksual berbasis digital.

Penyalahgunaan *deepfake* berkaitan dengan pelanggaran terhadap data pribadi, karena teknologi ini seringkali mengambil dan memanipulasi wajah, suara, atau perilaku seseorang tanpa izin. Saat ini di Indonesia, kesadaran dan regulasi mengenai perlindungan data pribadi mulai berkembang, salah satunya melalui Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Namun, penerapan undang-undang ini masih menghadapi berbagai tantangan, terutama dalam menanggapi kasus-kasus yang melibatkan teknologi *deepfake*.

Namun demikian, ketiadaan norma yang terkait penyalahgunaan teknologi *deepfake* menimbulkan celah hukum yang dapat dimanfaatkan oleh pelaku untuk menghindari pertanggungjawaban. Ketika data ini digunakan tanpa persetujuan

pemiliknya, hal tersebut dapat melanggar hak privasi individu dan menimbulkan dampak hukum maupun psikologis bagi korban. Selain itu, masyarakat umum pun masih banyak yang belum memahami ancaman *deepfake* terhadap privasi dan reputasi seseorang.

Permasalahan ini semakin kompleks ketika pengaturan hukum yang ada belum sepenuhnya mampu mengantisipasi perkembangan teknologi tersebut. Hal ini menciptakan gap regulasi, di mana pelaku kejahatan digital dengan mudah memanfaatkan celah hukum untuk melakukan tindakan manipulatif yang merugikan pihak lain. Oleh karena itu, sangat perlu dilakukan kajian mendalam mengenai bagaimana hukum di Indonesia memberikan perlindungan terhadap korban penyalahgunaan data pribadi akibat *deepfake,* serta sejauh mana hukum yang ada mampu mengantisipasi dan menangani permasalahan tersebut secara efektif. Dalam konteks ini, perlindungan hukum menjadi sangat penting sebagai bentuk jaminan negara atas hak asasi warga negara dalam menjaga integritas dan privasi data pribadinya.

Penelitian ini bertujuan untuk menganalisis secara yuridis perlindungan hukum terhadap penyalahgunaan data pribadi akibat fenomena *deepfake*, mengidentifikasi kelemahan regulasi yang ada, serta memberikan penguatan kebijakan hukum yang adaptif terhadap perkembangan teknologi. Melalui penelitian ini, maka penulis ingin mengkaji perlindungan hukum di Indonesia terhadap penyalahgunaan data pribadi dalam konteks *deepfake*.

1.2 Rumusan Masalah

Berdasarkan latar belakang tersebut, dapat diketahui rumusan masalah yang timbul dalam penelitian ini sebagai berikut:

1. Bagaimana perkembangan penyalahgunaan data pribadi melalui *deepfake*?
2. Bagaimana perlindungan hukum terhadap korban penyalahgunaan teknik *deepfake* terhadap data pribadi?

1.3 Tujuan Penelitian

Penelitian bertujuan untuk mengkaji ketentuan hukum pidana yang berlaku di Indonesia terkait perlindungan data pribadi, khususnya dalam konteks penyalahgunaan teknologi *deepfake*, serta bagaimana perlindungan yang didapatkkan oleh korban penyalahgunaan data pribadi secara hukum. Tujuan penelitian ini dapat dibedakan menjadi dua, yaitu tujuan teoritis dan tujuan praktis. Tujuan teoritis penelitian ini dapat dirumuskan sebagai berikut:

1. Untuk menganalisis konsep dan teori hukum yang berkaitan dengan perlindungan data pribadi dalam konteks perkembangan teknologi digital, khususnya *deepfake*.
2. Untuk mengkaji dasar-dasar normatif mengenai hak atas privasi dan perlindungan hukum bagi korban penyalahgunaan data pribadi menurut peraturan perundang-undangan yang berlaku.
3. Untuk memberikan kontribusi ilmiah terhadap pengembangan ilmu hukum, khususnya hukum siber dan hukum perlindungan data pribadi di era digital.

Sedangkan tujuan praktis pada penelitian ini dapat dirumuskan sebagai berikut:

1. Untuk memberikan gambaran mengenai bentuk perlindungan hukum yang dapat diberikan kepada korban penyalahgunaan data pribadi akibat teknologi *deepfake*.
2. Untuk mengidentifikasi kekosongan hukum atau kelemahan regulasi dalam menangani penyalahgunaan data pribadi melalui teknologi *deepfake* di Indonesia.
3. Untuk memberikan rekomendasi kepada pembuat kebijakan dan aparat penegak hukum dalam merumuskan langkah-langkah preventif dan represif guna melindungi korban penyalahgunaan teknologi *deepfake*.
4. Untuk meningkatkan kesadaran masyarakat mengenai risiko penyalahgunaan data pribadi dan pentingnya perlindungan hukum di era kecerdasan buatan.

Subjek yang mendapatkan manfaat dari penelitian ini adalah korban penyalahgunaan data pribadi, masyarakat umum, pembuat kebijakan/legislator, lembaga perlindungan data dan keamanan siber, lembaga bantuan hukum dan organisasi masyarakat sipil, akademisi, peneliti, mahasiswa hukum, serta penegak hukum seperti aparat kepolisian, jaksa, dan hakim.

1.4 Manfaat Penelitian

Berdasarkan latar belakang masalah tersebut, dapat diketahui manfaat penelitian yang timbul, yaitu memberikan kontribusi terhadap pengembangan ilmu hukum pidana, khususnya dalam ranah kejahatan siber yang melibatkan teknologi *deepfake*. Manfaat penelitian ini dapat dibedakan menjadi dua, yaitu

manfaat teoritis dan manfaat praktis. Penelitin ini dapat memberikan manfaat teoritis sebagai berikut:

1. Menambah keilmuan di bidang hukum, khususnya dalam pengembangan teori hukum siber, perlindungan data pribadi, dan regulasi terhadap kecerdasan buatan AI seperti teknologi *deepfake*.
2. Memberikan kontribusi ilmiah terhadap pengembangan kajian hukum yang membahas perlindungan terhadap hak privasi individu di era digital.
3. Mengidentifikasi dan menganalisis kekosongan normative yang ada dalam sistem hukum Indonesia dalam menghadapi kejahatan berbasis teknologi *deepfake*, serta menawarkan landasan teoritis untuk pengembangan regulasi yang lebih responsif.

Sedangkan, penelitian ini juga dapat memberikan manfaat praktis bagi beberapa pihak sebagai berikut:

1. Memberikan informasi dan panduan hukum kepada masyarakat, khususnya para korban, tentang bentuk perlindungan hukum yang dapat ditempuh dalam kasus penyalahgunaan data pribadi akibat *deepfake*.
2. Menyediakan rekomendasi konkret bagi pembuat kebijakan (legislator dan pemerintah) dalam menyusun atau merevisi peraturan perundang-undangan yang relevan dengan perlindungan data pribadi dan penggunaan teknologi AI.
3. Membantu aparat penegak hukum (kepolisian, jaksa, hakim) dalam menangani kasus *deepfake* dengan memahami aspek hukum, pembuktian, serta bentuk pertanggungjawaban pelaku.

4. Mendukung lembaga bantuan hukum dan LSM dalam melakukan advokasi serta perlindungan terhadap korban kejahatan digital.
5. Meningkatkan kesadaran masyarakat umum tentang pentingnya menjaga data pribadi dan mengenali ancaman *deepfake*, serta langkah preventif yang bisa diambil.

BAB II
TINJAUAN PUSTAKA

2.1 Penelitian Terdahulu

Pada penelitian ini, peneliti ingin menganalisis mengenai perlindungan hukum terhadap korban penyalahgunaan data pribadi akibat *deepfake*. Peneliti mengambil kajian skripsi yang sesuai dengan penelitian ini dari Hafsha Amalia Afnan (2022), Bela Renata (2022), Rusyda Aisyah (2023), dan Wachid Muhammad Rohman (2023). Pada penelitian ini peneliti juga mengambil kajian sebuah jurnal dari Cindy Natalia (2024).

Hafsha Amalia Afnan (2022), mahasiswa Fakultas Hukum, Universitas Muhammadiyah Surakarta, menulis skripsi berjudul *Perlindungan Hukum Penyalahgunaan Artificial Intelligence Deepfake pada Layanan Pinjaman Online*. Tujuan penelitiannya untuk mengetahui perlindungan hukum terhadap penyalahgunaan atau pemalsuan data pribadi dengan menggunakan teknologi *artificial intelligence deepfake*, ternyata telah diatur dalam Pasal 35 UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang secara tegas melarang pemalsuan data atau informasi elektronik dengan tujuan apapun.

Meskipun penyalahgunaan teknologi *deepfake* belum diatur secara khusus dalam UU 11/2008 maupun dalam peraturan perundang-undangan yang ada. UU ITE memberikan hak kepada korban untuk mengajukan gugatan kepada pengadilan apabila data atau informasi pribadi seseorang dipalsukan dengan *deepfake* untuk mengajukan pinjaman online. Namun demikian, peraturan mengatur mengenai penggunaan teknologi *artificial intelligence deepfake* pada

level undang-undang belum dimiliki, sehingga untuk mengisi kekosongan hukum, dibutuhkan pengaturan yang spesifik yang mendetail mengenai penggunaan teknologi *deepfake* dan penyalahgunaannya terhadap data pribadi, karena 17 perlindungan data pribadi sendiri diakui dalam hukum Indonesia sebagai hak asasi warga negara.

Bela Renata (2022), mahasiswa Fakultas Hukum, Universitas Sriwijaya Indralaya, menulis skripsi berjudul *Aspek Hukum Perlindungan Data Pribadi Source Subject Terhadap Penggunaan Teknik Deepfake dalam Perspektif Perbuatan Melanggar Hukum*. Tujuan penelitiannya untuk mengetahui dan menganalisis perlindungan hukum data pribadi *source subject* dari penggunaan teknik *deepfake* yang melanggar hukum serta tindakan hukum yang dapat dilakukan *source subject* data pribadi jika tanpa persetujuannya.

Hasil dari penelitian ini menunjukkan bahwa penggunaan data pribadi *source subject* secara preventif harus dilakukan berdasarkan persetujuan pemilik data karena jika tidak terpenuhi pemrosesan data pribadi dianggap batal demi hukum. Namun, penggunaan data pribadi *source subject* secara represif tanpa persetujuan terhadap penggunaan teknik *deepfake* yang merugikan telah memenuhi unsur-unsur yang terdapat pada Pasal 1365 Kitab Undang-Undang Hukum Perdata. Sehingga, dikategorikan sebagai perbuatan yang melanggar hukum.

Rusyda Aisyah (2023), mahasiswa Ilmu Hukum, Fakultas Hukum, Universitas Brawijaya, menulis skripsi berjudul *Analisa Yuridis Perlindungan Hukum Terhadap Data Pribadi Pengguna Media Sosial Terkait Penyalahgunaan*

Teknologi Deepfake. Tujuan penelitiannya untuk mengetahui bentuk perlindungan hukum yang diterima oleh seseorang ketika terjadi penyalahgunaan data pribadi pengguna media sosial menggunakan teknologi *deepfake* di Indonesia serta untuk mengetahui bentuk pengaturan yang tepat berkaca dari ketentuan yang ada di Tiongkok. Hasil penelitian ini dapat diketahui bahwa, Indonesia memiliki peraturan perundang-undangan yang dapat dikaitkan dengan perlindungan hukum terhadap korban penyalahgunaan data pribadi melalui teknologi *deepfake*.

Namun, hal itu terdapat kelemahan seperti ketidakjelasan prosedur persetujuan, absennya kewajiban verifikasi identitas, dan ketidakjelasan mekanisme penghapusan. Mengatasi hal ini, perlu adanya ketentuan yang mengatur prosedur persetujuan dengan jelas, verifikasi identitas sebelum penggunaan layanan, mekanisme penghapusan yang terperinci, pelabelan pada konten *deepfake*, dan penanganan rumor palsu. Oleh sebab itu, perlindungan dan implementasi hak individu serta mencegah potensi dampak negatif di masyarakat. Pemerintah perlu membentuk peraturan perundang-undangan khusus terkait layanan teknologi *deepfake* dengan mempertimbangkan contoh dari negara lain, seperti Tiongkok.

Wachid Muhammad Rohman (2023), mahasiswa Ilmu Hukum, Fakultas Hukum, Universitas Muhammadiyah Surakarta, menulis skripsi berjudul *Perlindungan Hukum Atas Data Pribadi dalam Penerapan Artificial Intelligence pada Sistem Perbankan*. Tujuan penelitiannya untuk mengetahui perlindungan hukum terhadap korban penyalahgunaan data pribadi dengan teknik *deepfake* yang ditinjau dari perspektrif UU Perlindungan Data Pribadi tahun 2022.

Teknologi AI yang canggih memberikan banyak sekali manfaat dalam aktifitas perbankan di Indonesia. Sehingga, nasabah atau calon nasabah tidak perlu datang ke bank untuk membuka rekening, nasabah atau calon nasabah sudah dapat melakukan pinjaman kredit di online, karena dengan adanya AI yang diterapkan dalam sistem perbankan.

Namun, perkembangan teknologi yang sangat pesat ini juga memiliki dampak buruk bagi perbankan seperti penyalahgunaan data pribadi atau kemungkinan terjadi kebocoran data pribadi milik nasabah. Kebocoran data pribadi yang disebabkan oleh AI di suatu bank, maka pihak bank dapat dimintakan pertanggungjawaban atas tindakan tersebut. Sehingga, sangat diperlukan untuk merumuskan aturan yang mengatur tentang penggunaan AI di Indonesia, khususnya dalam dunia perbankan agar lebih memberi kepastian hukum.

Cindy Natalia (2024), mahasiswa Fakultas Hukum, Universitas Udayana, menulis jurnal berjudul *Perlindungan Hukum bagi Korban Pornografi Deepfake dalam Konteks Hukum Indonesia*. Tujuan penelitiannya untuk menyelidiki strategi yang dapat diadopsi oleh peraturan hukum untuk mengatasi tantangan *deepfake pornography*. Perubahan hukum yang diperlukan untuk memberikan perlindungan yang lebih kuat bagi korban, serta langkah-langkah teknis yang dapat diambil untuk meningkatkan kemampuan identifikasi dan penegakan hukum terhadap *deepfake*. Selain itu, memberikan kontribusi dalam meningkatkan kesadaran dan upaya dalam menangani fenomena tersebut secara efektif dan berkelanjutan.

Bentuk pengaturan perlindungan hukum bagi korban *deepfake pornography* mencakup beberapa undang-undang seperti UU No. 19 Tahun 2016 dan UU No. 44 Tahun 2008 meskipun masih ada tantangan dalam identifikasi pelaku, pengumpulan bukti, dan kesadaran publik yang perlu diatasi. Sehingga, perlunya merancang pengaturan constituendum seperti penyempurnaan Undang-Undang Pornografi untuk secara eksplisit mencakup *deepfake pornography* sebagai bentuk pelanggaran, disertai dengan penyediaan sumber daya dan pelatihan bagi lembaga penegak hukum.

Penelitian mengenai penyalahgunaan teknologi *deepfake* dalam konteks hukum terus berkembang seiring meningkatnya risiko pelanggaran data pribadi di era digital. Lima penelitian sebelumnya yang ditulis oleh Hafsha Amalia Afnan (2022), Bela Renata (2022), Rusyda Aisyah (2023), Wachid Muhammad Rohman (2023), dan Cindy Natalia (2024) memberikan kontribusi penting dalam melihat berbagai sudut permasalahan. Masing-masing mengkaji *deepfake* dari aspek sektoral yang berbeda: layanan pinjaman online, perbuatan melawan hukum atas data pribadi, penyalahgunaan di media sosial, sistem perbankan, hingga konten pornografi. Kelima penelitian tersebut umumnya menekankan kelemahan regulasi positif di Indonesia dan mendesak perlunya pembentukan peraturan khusus yang secara eksplisit mengatur penggunaan dan penyalahgunaan teknologi *deepfake*.

Berbeda dengan penelitian-penelitian tersebut, penelitian ini secara spesifik menyoroti perlindungan hukum terhadap korban penyalahgunaan data pribadi melalui teknologi *deepfake* dengan pendekatan normatif yang didasarkan pada teori perlindungan hukum Satjipto Rahardjo. Pendekatan ini memosisikan

hukum sebagai alat yang tidak semata-mata menjamin kepastian, tetapi juga keadilan dan kemanfaatan bagi korban. Fokus saya tidak terbatas pada sektor tertentu, melainkan menempatkan individu sebagai subjek hukum yang harus dilindungi dari potensi kerugian akibat manipulasi teknologi digital.

Dari teori Satjipto Rahardjo, penulis melihat bahwa perlindungan hukum terhadap korban bukan hanya soal keberadaan norma hukum formal, tetapi juga bagaimana hukum merespons kebutuhan riil masyarakat. Penelitian ini mengisi kekosongan teoritis dalam diskursus hukum positif yang cenderung kaku, serta mendorong pendekatan hukum yang responsif, kontekstual, dan berorientasi pada hak asasi manusia, khususnya perlindungan atas data pribadi. Pendekatan ini diharapkan dapat menjadi dasar dalam merumuskan regulasi nasional terkait *deepfake* di masa mendatang.

2.2 Landasan Teori

2.2.1 Perlindungan Hukum

Perlindungan hukum merupakan segala upaya yang diberikan oleh hukum untuk melindungi hak asasi manusia dari tindakan yang melanggar hukum. Menurut Satjipto Rahardjo, perlindungan hukum tidak hanya berarti perlindungan normatif (aturan hukum), tetapi juga jaminan atas keadilan dan rasa aman bagi warga negara dalam menjalani kehidupannya, termasuk dalam ruang digital.

Perlindungan hukum terbagi menjadi dua, yaitu perlindungan preventif dan perlindungan represif. Perlindungan preventif merupakan perlindungan hukum yang diberikan sebelum terjadi pelanggaran hukum untuk mencegah terjadinya pelanggaran hak atau tindakan sewenang-wenang dari pihak lain,

termasuk dari pemerintah maupun aparat hukum, seperti pemerintah harus memberikan aturan yang jelas dan transparan sebelum mengambil tindakan terhadap warga negara. Sedangkan, perlindungan represif merupakan perlindungan hukum yang diberikan setelah terjadinya pelanggaran hukum untuk memulihkan hak-hak yang dilanggar dan memberikan keadilan bagi pihak yang dirugikan, seperti seseorang yang menjadi korban penipuan, kekerasan, atau pencurian itu bisa langsung melaporkan kejadian ke polisi setempat agar proses hukum dapat segera dimulai.

Perlindungan hukum yang dimaksut di dalam konteks terhadap korban penyalahgunaan data pribadi akibat *deepfake* ini, bahwa korban harus mendapatkan hak atas pemulihan nama baik, kerahasiaan identitas, serta korban harus dijamin ganti rugi materiil dan imateriil atas penyalahgunaan data pribadi. Selanjutnya, Undang-Undang harus mampu memberikan perlindungan secara menyeluruh terhadap aspek keamanan dan memberikan hak ketika terjadi penyalahgunaan data pribadi. Contoh kasus seperti yang terjadi dalam penggunaan *deepfake* ini terjadi pada seorang seorang wanita yang berasal dari Prancis telah tertipu Rp13 Miliar untuk pengobatan kanker sang aktor idola Brad Pitt. Selain itu, contoh kasus lainnya yang menipu sejumlah penggemar Taylor Swift dengan menjual *Le Creuset* palsu menggunakan video promosi.

2.2.2 *Deepfake*

Deepfake merupakan teknologi yang memanfaatkan kecerdasan buatan atau AI (*Artificial Intelligence*) untuk memanipulasi foto, video, bahkan suara seseorang sehingga terlihat seperti sangat nyata. Namun, teknologi ini menjadi

sangat berbahaya apabila digunakan untuk membuat konten palsu yang merusak reputasi seseorang, menyebarkan hoaks atau berita palsu, melakukan pemerasan atau penipuan dengan video atau audio yang direkayasa. *Deepfake* dapat menjadi alat kejahatan bila digunakan untuk memalsukan identitas, menyebarkan konten seksual nonkonsensual, atau menjatuhkan martabat seseorang dengan rekaman palsu.

Deepfake dapat menimbulkan banyak resiko dan tantangan hukum, seperti mencuri atau menyalahgunakan identitas seseorang. Sayangnya, perlindungan hukum di Indonesia mengenai *deepfake* ini masih belum spesifik. Adapun upaya pencegahan dan penanggulangan yang dapat dilakukan dengan memverifikasi fakta dan sumber informasi sebelum menyebarkan konten mencurigakan, atau bisa dengan mengedukasi publik tentang bahaya dan ciri-ciri *deepfake*.

2.2.3 Hukum Pidana

Hukum pidana merupakan bagian dari hukum publik yang berfungsi sebagai sarana dalam melindungi kepentingan hukum yang penting, seperti nyawa, kehormatan, harta benda, dan data pribadi. Hukum pidana bekerja melalui ancaman pidana untuk menimbulkan efek jera bagi pelanggar dan melindungi masyarakat dari perbuatan berbahaya.

Menurut Moeljatno, hukum pidana terdiri dari hukum pidana materiil, hukum pidana formil, dan hukum pelaksanaan pidana. Hukum pidana materiil merupakan aturan-aturan yang menentukan perbuatan apa yang dilarang dan ancaman hukumannya. Hukum pidana formil merupakan hukum yang mengatur

tata cara penegakan hukum pidana. Sedangkan, hukum pelaksanaan pidana merupakan hukum yang mengatur pelaksanaan pidana terhadap pelaku kejahatan.

2.2.4 Data Pribadi sebagai Objek Perlindungan Hukum

Data pribadi adalah bagian dari hak privasi yang termasuk dalam ruang lingkup perlindungan hukum pidana jika digunakan tanpa izin untuk merugikan orang lain. Dalam konteks hukum pidana, penyalahgunaan data pribadi dapat digolongkan menjadi kejahatan terhadap privasi, pemalsuan identitas, penipuan berbasis digital, dan kejahatan siber (*cybercrime*). Perlindungan data pribadi diatur dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), yang bertujuan untuk menjamin hak privasi setiap individu.

UU PDP membagi data pribadi menjadi dua, yaitu data pribadi yang bersifat umum dan spesifik. Data pribadi yang bersifat umum seperti nama lengkap, jenis kelamin, kewarganegaraan, agama, status perkawinan, serta data lain yang dapat digunakan untuk mengidentifikasi seseorang. Sedangkan data pribadi yang bersifat spesifik seperti data kesehatan, biometrik, genetika, catatan kejahatan, data keuangan, dan data lain yang pemrosesannya dapat mengakibatkan dampak yang lebih besar bagi seseorang.

2.2.5 Unsur Pidana dalam Penyalahgunaan Data Pribadi akibat *Deepfake*

Penyalahgunaan data pribadi melalui *deepfake* dapat memenuhi unsur tindak pidana jika mengandung perbuatan yang melawan hukum seperti mengambil atau memanfaatkan data pribadi tanpa hak, kesengajaan atau kelalaian, kerugian atau potensi kerugian bagi korban, serta niat jahat seperti pemerasan,

pencemaran nama baik, atau penipuan. Pasal-pasal yang dapat dikenakan untuk hal ini, antara lain:

1. Pasal 32-33 UU ITE : Perubahan atau pengambilan data elektronik tanpa izin
2. Pasal 27 ayat (1) UU ITE : Konten bermuatan asusila
3. Pasal 310 dan 311 KUHP : Pencemaran nama baik dan fitnah
4. Pasal 378 KUHP : Penipuan

Berdasarkan UU PDP, mengenai *deepfake* ini terdapat dalam Pasal 66 UU PDP, yaitu setiap orang dilarang membuat data pribadi palsu atau memalsukan data pribadi dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian bagi orang lain. Selanjutnya, orang yang melanggar ketentuan tersebut dapat dipidana dengan pidana penjara paling lama 6 tahun dan/atau pidana denda paling banyak Rp6 miliar.

BAB III
METODE PENELITIAN

3.1 Jenis Penelitian

Penelitian ini adalah penelitian normatif, yang fokus untuk membahas terkait dengan perlindungan hukum bagi korban penyalahgunaan data pribadi. Selain itu, untuk mengkaji efektivitas perlindungan hukum terhadap individu yang dirugikan akibat manipulasi data pribadi melalui teknologi *deepfake* dan analisis terhadap aturan hukum yang berlaku di Indonesia. Penelitian ini memusatkan perhatian pada tiga aspek utama, yaitu:

1. Analisis terhadap kerangka hukum yang mengatur pelindungan data pribadi di Indonesia, terutama Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) dan kaitannya dengan teknologi digital, khususnya *deepfake*.
2. Identifikasi bentuk-bentuk penyalahgunaan data pribadi melalui *deepfake*, seperti pencemaran nama baik, pornografi nonkonsensual, penipuan identitas, atau manipulasi opini publik, serta implikasi hukumnya terhadap korban dan pelaku.
3. Evaluasi terhadap kelemahan dan kekosongan hukum (legal gap) dalam regulasi yang ada, serta upaya perlindungan hukum yang dapat diberikan, baik melalui mekanisme hukum pidana, perdata, maupun administratif.

3.2 Pendekatan Penelitian

Penelitian ini menggunakan pendekatan undang-undang, yaitu pendekatan yang mengkaji hukum sebagai norma yang hidup dalam sistem perundang-

undangan Perlindungan Data Pribadi. Penelitian ini juga mengkaji asas-asas hukum, serta putusan pengadilan yang relevan dalam memberikan perlindungan terhadap data pribadi dari ancaman penyalahgunaan teknologi *deepfake*. Sehingga, dapat diketahui fokus utama pada pendekatan penelitian ini yaitu menganalisis peraturan perundang-undangan, asas hukum, serta putusan pengadilan terkait.

Pendakatan deskriptif kualitatif merupakan penelitian yang menghasilkan data deskriptif dari sumber data yang dapat diamati (Moleong, 2011:4). Data yang akan diolah termasuk data kualitatif, sehingga memerlukan penjelasan secara deskriptif. Pada penelitian ini dikatakan kualitatif karena data yang dikumpulkan berupa kata-kata, kalimat, bukan angka-angka.

3.3 Objek Penelitian

Objek dalam penelitian ini adalah norma hukum positif yang mengatur mengenai perlindungan data pribadi dalam konteks penyalahgunaan teknologi *deepfake*. Penelitian ini difokuskan pada analisis terhadap aturan hukum yang berlaku di Indonesia, serta kesesuaiannya dalam memberikan perlindungan hukum terhadap individu yang dirugikan akibat manipulasi data pribadi melalui teknologi *deepfake*. Secara spesifik, objek penelitian ini meliputi:

1. Peraturan Perundang-Undangan Nasional yang menjadi dasar hukum perlindungan data pribadi dan penanggulangan kejahatan digital, antara lain:
    1) Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP).

2) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) beserta perubahannya.
3) Kitab Undang-Undang Hukum Pidana (KUHP) yang relevan dengan pelanggaran privasi, pencemaran nama baik, atau pemalsuan identitas

2. Konsep dan asas hukum terkait data pribadi, privasi, persetujuan (*consent*), dan penyalahgunaan teknologi, yang dijadikan dasar dalam menilai efektivitas perlindungan hukum yang ada.
3. Putusan Pengadilan (jika tersedia) yang berkaitan dengan pelanggaran data pribadi, manipulasi digital, atau kasus *deepfake*, sebagai bahan analisis yuridis terhadap penerapan norma hukum.
4. Kesenjangan hukum (legal gap) dan potensi kebutuhan harmonisasi regulasi dalam menghadapi perkembangan teknologi digital seperti *deepfake*, baik dari segi hukum nasional maupun perbandingan dengan hukum internasional.

3.4 Sumber Data Penelitian

Sumber data penelitian ini menggunakan data sekunder yang dapat dibedakan menjadi dua, yaitu:

1. Bahan Hukum Primer : Bahan hukum yang memiliki kekuatan mengikat dan menjadi dasar utama dalam analisis hukum. Bahan hukum ini meliputi:

    1) Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP)
    2) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik beserta perubahan-perubahannya

3) Kitab Undang-Undang Hukum Pidana (KUHP)**,** khususnya ketentuan yang terkait dengan pelanggaran privasi, pencemaran nama baik, dan pemalsuan identitas
4) Peraturan pelaksana dari UU PDP dan UU ITE, seperti Peraturan Pemerintah atau Peraturan Menteri
5) Putusan pengadilan (jika tersedia) terkait pelanggaran data pribadi dan/atau pemanfaatan teknologi *deepfake*.

2. Bahan Hukum Sekunder : Bahan hukum yang memberikan penjelasan terhadap bahan hukum primer, serta membantu memahami konsep hukum dan interpretasinya. Bahan hukum ini meliputi:
   1) Buku teks atau literatur hukum yang membahas perlindungan data pribadi, hukum siber dan kejahatan digital, serta teori privasi dan keamanan informasi
   2) Artikel dalam jurnal ilmiah hukum yang relevan
   3) Opini hukum, pendapat ahli, dan pandangan akademisi terkait penyalahgunaan teknologi *deepfake* dalam konteks hukum

3.5 Teknik Pengambilan Data

Teknik pengumpulan data difokuskan pada penelusuran atau menelaah bahan-bahan hukum melalui studi kepustakaan. Teknik pengumpulan data ini tidak menggunakan wawancara atau observasi lapangan, karena fokus utama adalah menelaah norma hukum tertulis dan teori hukum dari berbagai literatur. Sehingga, data yang dikumpulkan dalam penelitian ini diambil dari berita CNBC Indonesia dan CBS News.

3.6 Teknik Analisis Data

Teknik analisis data yang digunakan pada penelitian ini adalah menganalisis data secara kualitatif normatif. Teknik ini dilakukan dengan menelaah, mengkaji, dan menafsirkan bahan hukum yang telah dikumpulkan melalui studi kepustakaan, guna memperoleh pemahaman sistematis terhadap ketentuan hukum yang mengatur perlindungan data pribadi dalam konteks penyalahgunaan oleh teknologi *deepfake*. Langkah-langkah analisis yang dilakukan adalah sebagai berikut:

1. Klasifikasi Bahan Hukum

   Bahan hukum yang telah dikumpulkan (primer, sekunder, dan tersier) diklasifikasikan berdasarkan relevansinya terhadap:

   1) Perlindungan hukum data pribadi
   2) Kejahatan siber dan penyalahgunaan teknologi *deepfake*
   3) Instrumen hukum nasional dan internasional

2. Interpretasi Hukum

   Setelah diklasifikasikan, dilakukan interpretasi terhadap peraturan perundang-undangan yang berlaku dengan menggunakan beberapa metode penafsiran, seperti:

   1) Interpretasi gramatikal, melihat arti kata atau frasa dalam peraturan
   2) Interpretasi sistematis, menafsirkan ketentuan dalam konteks keseluruhan sistem hukum
   3) Interpretasi teleologis, memahami maksud dan tujuan lahirnya norma hukum tersebut

4) Interpretasi historis, dengan melihat latar belakang pembentukan regulasi

3. Analisis Kesesuaian dan Kecukupan Hukum

Data hukum yang dianalisis kemudian dievaluasi untuk menjawab pertanyaan penelitian, yaitu:

1) Apakah regulasi yang ada saat ini cukup mengatur dan melindungi individu dari penyalahgunaan data pribadi melalui *deepfake*?
2) Apa saja kelemahan atau kekosongan hukum (legal gap) yang perlu diisi?

4. Penyusunan Argumentasi Hukum

Dari hasil analisis, disusun argumentasi hukum yang logis dan sistematis untuk:

1) Menjelaskan permasalahan hukum yang ada
2) Menyusun rekomendasi perbaikan atau pembaruan hukum
3) Memberikan solusi terhadap perlindungan hukum korban penyalahgunaan data pribadi akibat *deepfake*.

BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan hasil penelitian dan analisis terhadap peraturan perundang-undangan yang berlaku di Indonesia, maka dapat disimpulkan bahwa:

1. Perlindungan hukum terhadap korban penyalahgunaan data pribadi akibat teknologi *deepfake* di Indonesia belum optimal. Meskipun Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) telah mengatur prinsip-prinsip dasar pelindungan data pribadi, namun tidak secara eksplisit menyebutkan penyalahgunaan data visual dan audio oleh teknologi *deepfake* sebagai pelanggaran yang spesifik.
2. UU ITE dan KUHP dapat digunakan untuk menjerat pelaku penyebaran *deepfake* dalam konteks pencemaran nama baik, penipuan, atau pelanggaran kesusilaan. Namun, pasal-pasal tersebut bersifat umum dan belum mengatur secara khusus tentang rekayasa citra atau suara yang merupakan hasil teknologi berbasis kecerdasan buatan (AI).
3. Terdapat kekosongan hukum (legal gap) dalam regulasi Indonesia yang belum mengantisipasi dampak negatif teknologi manipulatif seperti *deepfake*, khususnya terkait data biometrik (seperti wajah dan suara) sebagai bagian dari data pribadi sensitif.

5.2 Saran

Penelitian ini mengkaji tentang perlindungan hukum terhadap korban penyalahgunaan data pribadi akibat *deepfake*. Supaya perlindungan hukum

terhadap penyalahgunaan data pribadi akibat *deepfake* dapat ditingkatkan, penulis memberikan beberapa saran sebagai berikut:

1. Pemerintah perlu menyusun peraturan pelaksana UU PDP yang secara khusus mengatur tentang data biometrik, wajah, dan suara sebagai objek perlindungan hukum, serta menetapkan sanksi administratif maupun pidana atas penyalahgunaannya dalam bentuk *deepfake*.
2. Perlu dilakukan revisi atau penambahan ketentuan dalam UU ITE atau KUHP untuk secara eksplisit memasukkan tindakan manipulasi digital atau pemalsuan identitas melalui *deepfake* sebagai bentuk kejahatan terhadap privasi dan identitas digital.
3. Penegakan hukum perlu diperkuat melalui peningkatan kapasitas digital forensik, termasuk pelatihan aparat penegak hukum dan lembaga peradilan dalam mengenali, membuktikan, dan menangani konten *deepfake* secara efektif.
4. Masyarakat perlu diberikan edukasi digital secara masif mengenai pentingnya menjaga data pribadi, risiko penyalahgunaan teknologi *deepfake*, serta langkah-langkah hukum yang dapat ditempuh apabila menjadi korban.

DAFTAR PUSTAKA

Afnan, Hafsha Amalia. 2022. *Perlindungan Hukum Penyalahgunaan Artificial Intelligence Deepfake pada Layanan Pinjaman Online*. Surakarta: Universitas Muhammadiyah Surakarta.

Aisyah, Rusyda. 2023. *Analisa Yuridis Perlindungan Hukum Terhadap Data Pribadi Pengguna Media Sosial Terkait Penyalahgunaan Teknologi Deepfake.* Malang: Universitas Brawijaya.

Cerullo, Megan. 2024. *AI-generated ads using Taylor Swift's likeness dupe fans with fake Le Creuset giveaway*. New York: CBS News.

Chesney, R., & Citron, D. (2019). *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*. California Law Review, 107(6), 1753–1819.

Hasibuan, Linda. 2025. *Wanita Ini Kena Tipu Brad Pitt AI, Duit Rp 13 Miliar Ludes*. CNBC Indonesia.

Koopman, Marissa. Rodriguez, Andrea Macarulla. and Geradts, Zeno. 2018. *Detection of Deepfake Video Manipulation*. University of Amsterdam & Netherlands Forensic Institute.

Moleong, Lexy J. 2011. *Metodologi Penelitian Kualitatif*. Bandung: PT Remaja Rosda Karya.

Natalia, Cindy. 2024. *Perlindungan Hukum Bagi Korban Pornografi Deepfake dalam Konteks Hukum Indonesia*. Jurnal Kertha Desa, Vol. 12 No. 5 tahun 2024, hlm 4462-4473. Bali: Universitas Udayana.

Rahardjo, Satjipto. (2000). *Ilmu Hukum*. Bandung: PT Citra Aditya Bakti.

Rahardjo, Satjipto. (2021). *Ilmu Hukum*. Bandung: PT Citra Aditya Bakti.

Renata, Bela. 2022. *Aspek Hukum Perlindungan Data Pribadi Source Subject Terhadap Penggunaan Teknik Deepfake dalam Perspektif Perbuatan Melanggar Hukum*. Sumatera Selatan: Universitas Sriwijaya.

Simorangkir, A. (2023). *Urgensi Regulasi Deepfake di Indonesia: Tinjauan terhadap UU PDP dan UU ITE*. Jurnal Hukum Digital, Vol. 4 No. 2, hlm 55–67.

Syarifudin, M. (2023). *Perlindungan Hukum terhadap Korban Deepfake dalam Perspektif Hukum Siber di Indonesia*. Jurnal Hukum & Teknologi, Vol. 5 No. 1, hlm 88–104.

Wachid, Muhammad Rohman. 2023. *Perlindungan Hukum Atas Data Pribadi dalam Penerapan Artificial Intelligence pada Sistem Perbankan*. Surakarta: Universitas Muhammadiyah Surakarta.