

BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi pada struktur masyarakat telah mengalami transformasi signifikan karena kemajuan teknologi yang pesat. Internet adalah salah satu perangkat teknologi yang telah mempercepat perubahan ini. Tindakan manusia kini lebih cepat dan sederhana berkat perkembangan teknologi internet. (Mahendra et al., 2024). Menurut survei yang dilakukan oleh Asosiasi Penyedia Layanan Internet Indonesia (APJII), terdapat 215,63 juta pengguna internet di Indonesia pada tahun 2022–2023. Dibandingkan dengan periode sebelumnya, ketika tercatat 210,03 juta pengguna, angka ini meningkat sebesar 2,67%. (Hanum, 2024). Teknologi *deepfake* adalah salah satu dari sekian banyak inovasi dalam kehidupan manusia yang dihasilkan oleh kemajuan teknologi kecerdasan buatan (*AI*). (Eriana & Zein, 2023). *Deepfake* merupakan bentuk manipulasi konten digital baik gambar, suara, maupun video yang menggunakan algoritma berbasis AI untuk mengubah atau merekayasa wajah dan suara seseorang secara sangat realistis, sehingga tampak seperti nyata yang sebenarnya tidak pernah terjadi sebelumnya. Meskipun teknologi ini memiliki potensi positif dalam dunia perfilman, pendidikan, hingga hiburan, pemanfaatannya dalam konteks negatif justru lebih mendominasi. Salah satu bentuk penyalahgunaan teknologi *deepfake* yang paling meresahkan adalah pembuatan dan penyebaran konten pornografi yang mencatut wajah seseorang tanpa persetujuan. Fenomena ini bukan hanya merusak reputasi korban, tetapi juga mencederai martabat dan privasi individu.

Menurut *Internet Governance Forum* (IGF), Kekerasan Berbasis Gender Online (KBGO) mencakup berbagai bentuk tindakan, mulai dari penguntitan, intimidasi, pelecehan seksual, pencemaran nama baik, ujaran kebencian, hingga eksploitasi. Data menunjukkan bahwa pada tahun 2020, masa ketika pandemi, jumlah laporan kasus KBGO yang diterima Komnas Perempuan meningkat hingga 300% dibandingkan tahun sebelumnya, yakni dari 218 kasus pada 2019 menjadi 940 kasus pada 2020 (Hanum, 2024).

Tabel 1. Kasus Kekerasan Berbasis Gender Online (KBGO)

No	Sumber Data	Periode	Jumlah Kasus/Pengguna	Keterangan
1.	APJII	2022–2023	215,63 juta pengguna	Meningkat 2,67% dari periode sebelumnya (210,03 juta pengguna)
2.	Komnas Perempuan	2019	218 Kasus KBGO	Data sebelum pandemi COVID-19
3.	Komnas Perempuan	2020	940 kasus KBGO	Meningkat sekitar 300% selama pandemi
4.	LBH APIK Jakarta	2018–2021	83 kasus KBGO	Kasus pendampingan hukum
5.	SAFEnet	2019–2021	1.357 aduan KBGO	Aduan terkait pelanggaran hak digital
6.	Komnas Perempuan	2017–2020	2.625 kasus KBGO	Data kumulatif nasional
7.	KPAI	2018–202	679 kasus KBGO (anak	Kasus yang melibatkan anak sebagai korban

Selain itu, Yayasan LBH APIK Jakarta yang berfokus pada pendampingan hukum dengan perspektif keadilan bagi perempuan, mencatat telah menangani 83 kasus KBGO sepanjang periode 2018–2021. Sementara itu, SAFEnet (*Southeast Asia Freedom of Expression Network*), sebagai lembaga yang bergerak dalam advokasi hak-hak digital di Asia Tenggara, melaporkan sebanyak 1.357 aduan kasus

KBGO dalam rentang waktu 2019–2021. Sejalan dengan itu, Komnas Perempuan juga mencatat adanya 2.625 kasus KBGO dari 2017–2020. Sedangkan Komisi Perlindungan Anak Indonesia (KPAI) mencatat 679 kasus KBGO yang melibatkan anak-anak pada periode 2018–2020 (Hanum, 2024).

Kejahatan selalu berkembang mengikuti peradaban manusia dan bahkan dianggap sebagai sesuatu yang melekat pada dinamika kehidupan masyarakat. Kini, umat manusia telah memasuki era revolusi industri 4.0 yang ditandai dengan integrasi teknologi otomatisasi dan digitalisasi yang masif. Teknologi seperti *Internet of Things (IoT)*, *big data*, *augmented reality*, hingga *artificial intelligence (AI)* telah menjadi bagian tak terpisahkan dari kehidupan sehari-hari (Hindarto et al., 2022). Namun, perkembangan ini juga membawa dampak negatif berupa kemunculan bentuk-bentuk kejahatan baru yang memanfaatkan celah dari teknologi yang ada. Kejahatan yang sebelumnya bersifat konvensional kini berevolusi menjadi kejahatan siber (*cybercrime*), termasuk kejahatan yang memanfaatkan teknologi AI seperti *deepfake*. *Cybercrime* mencakup berbagai bentuk pelanggaran hukum, mulai dari perjudian daring, ujaran kebencian, pencurian data, hingga penyebaran konten pornografi (Amanda dkk., 2024).

AI yang awalnya merupakan inovasi ilmiah oleh John McCarthy pada tahun 1955, kini telah menjangkau seluruh aspek kehidupan, dari fitur pengenalan wajah di media sosial, layanan terjemahan otomatis, hingga kendaraan otonom (Zebua et al., 2023). Salah satu turunan AI yang kini mendapat sorotan luas adalah teknologi *deepfake*, yang memungkinkan manipulasi wajah dan suara manusia dengan sangat realistis (Aziz Apriadi et al., 2025). Teknologi ini awalnya digunakan untuk tujuan hiburan, seperti aplikasi "*My Heritage*" yang menghidupkan foto lama menjadi

animasi. Namun, kemudahan akses terhadap aplikasi *deepfake* ini justru membuka peluang besar penyalahgunaan, seperti penipuan, penyebaran hoaks, bahkan manipulasi konten pornografi. kenyataan bahwa jutaan orang dengan mudah mengakses situs “pornografi deepfake” dan aplikasi nudify, yang difasilitasi oleh media sosial serta platform mesin pencari, menciptakan iklim yang menormalisasi dan meremehkan aktivitas seksual tanpa persetujuan. Budaya semacam ini pada akhirnya turut mendukung terjadinya berbagai bentuk kekerasan seksual lainnya. Rasa ancaman dan kerugian tersebut meluas ke seluruh ruang digital, mengganggu kebebasan sipil perempuan seperti kebebasan berekspresi dan hak privasi, serta menghambat partisipasi mereka dalam kehidupan publik (McGlynn & Toparlak, 2025).

Konten pornografi berbasis *deepfake* banyak digunakan untuk merendahkan, memperlakukan, dan menyerang martabat seseorang terutama perempuan melalui penyebaran konten seksual yang tidak pernah mereka lakukan. Dalam banyak kasus, korban tidak mengetahui bahwa wajah atau tubuh mereka telah dimanipulasi menjadi bagian dari konten pornografi. Tindakan ini masuk dalam kategori Kekerasan Berbasis Gender Online (KBGO), yaitu kekerasan yang terjadi di ranah digital dengan korban yang umumnya adalah perempuan dan pelaku menggunakan internet atau teknologi untuk mengintimidasi, memperlakukan, mengancam, atau mengeksploitasi secara seksual (Rohmawati et al., 2024).

Kasus penyebaran konten pornografi bermuatan *deepfake* yang melibatkan seorang mahasiswa Universitas Udayana (UNUD) berinisial SLKDP pada tahun 2025 menjadi bukti konkret bahwa teknologi *deepfake* disalahgunakan untuk hal-hal yang merugikan dan berdampak serius terhadap korban. SLKDP diduga telah

memanfaatkan aplikasi BOT berbasis kecerdasan buatan melalui platform Telegram untuk mengedit foto-foto teman kuliahnya menjadi konten tidak senonoh. Salah satu korban, berinisial KB, menyebutkan bahwa pelaku mengambil tangkapan layar dari akun Instagram para korban tanpa izin, lalu mengubahnya menjadi gambar vulgar. Beberapa korban bahkan pernah mengikuti perkuliahan yang sama dengan pelaku, dan hingga kini jumlah korban masih dalam penyelidikan. Fakta ini menunjukkan bahwa KBGO melalui teknologi *deepfake* bukan sekadar isu global, melainkan telah nyata terjadi di lingkungan akademik dan sosial terdekat, dengan dampak psikologis dan sosial yang mendalam bagi para korban.

KBGO yang dilakukan melalui konten *deepfake* pornografi merupakan bentuk kekerasan seksual digital yang semakin marak, namun belum mendapatkan perhatian serius dari sistem hukum Indonesia. Padahal, korban KBGO mengalami trauma psikologis yang serius, tekanan sosial, dan kerusakan reputasi yang sulit dipulihkan. Sayangnya, hingga saat ini belum terdapat peraturan perundang-undangan di Indonesia yang secara spesifik mengatur perihal kejahatan ini, baik dari sisi tindakan pembuatannya maupun dari perlindungan terhadap korban.

Kejahatan pornografi sebenarnya bukan hal baru di Indonesia dan telah lama menjadi perhatian hukum. Beberapa regulasi seperti Kitab Undang-Undang Hukum Pidana (KUHP), Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), serta Undang-Undang Nomor 44 Tahun 2008 tentang Pornografi telah memberikan dasar hukum dalam memberantas pornografi. Namun, kehadiran teknologi *deepfake* memperumit pemberantasan kejahatan ini karena konten yang dihasilkan sangat realistis dan sulit dibedakan dari yang asli. Konten *deepfake* dapat mencatut wajah orang yang tidak bersalah dan

menyematkannya dalam adegan-adegan seksual, yang secara drastis merusak nama baik dan integritas korban. Studi menunjukkan bahwa 96% dari konten *deepfake* global adalah konten pornografi, dengan peningkatan drastis dari tahun ke tahun (Christella Seveney dkk., 2025).

Secara normatif, Indonesia memiliki beberapa instrumen hukum yang mengatur tindak pidana kesusilaan dan perlindungan terhadap hak privasi. Yaitu Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana (KUHP) baru, Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), serta Undang-Undang Nomor 44 Tahun 2008 tentang Pornografi telah menyediakan norma hukum yang relevan, tetapi belum mampu menjangkau modus operandi kejahatan digital modern seperti *deepfake*. Pertama, pada UU No 1 Tahun 2023 atau KUHP baru, terdapat 2 pasal yang mengatur terkait pengaturan pornografi yaitu pada pasal 172 yang berbunyi “Pornografi adalah gambar, sketsa, ilustrasi, foto, suara, bunyi, gambar bergerak, animasi, kartun, percakapan, gerak tubuh, atau bunyi pesan lainnya melalui berbagai bentuk media komunikasi dan/atau pertunjukan Di Muka Umum, yang memuat kecabulan atau eksploitasi seksual yang melanggar norma kesusilaan dalam masyarakat”, pada pasal ini dinilai kurang relevan untuk menangani pornografi berbasis AI karena pasal ini hanya berfokus pada bentuk *konten cabul* tanpa mempertimbangkan proses pembuatannya melalui teknologi *deepfake*. Dalam kasus pornografi AI, inti persoalan bukan sekadar adanya konten cabul, tetapi pemalsuan identitas seseorang melalui manipulasi wajah yang dibuat tanpa persetujuan korban. Pasal ini tidak membedakan antara konten asli dan konten hasil rekayasa AI, sehingga aspek “non-konsensual” yang sangat penting dalam *deepfake porn* tidak tercakup.

Selain itu, Pasal 172 tidak mengatur tindakan pembuatan deepfake itu sendiri, padahal dalam konteks AI, proses pembuatan sudah merupakan pelanggaran serius terhadap integritas citra seseorang walaupun belum disebar. Pasal ini juga tidak menyentuh tanggung jawab teknologi dan platform yang memfasilitasi pembuatan atau penyebaran deepfake, sehingga tidak sesuai dengan karakter kejahatan digital modern yang melibatkan algoritma, aplikasi, dan distribusi otomatis. Karena itu, meskipun bisa digunakan sebagai dasar umum, Pasal 172 belum cukup untuk menjawab kompleksitas pornografi berbasis AI dan memperjelas perlunya regulasi khusus yang lebih sesuai dengan perkembangan teknologi. Lalu pada pasal kedua yaitu pasal 407 yang berbunyi “(1) Setiap Orang yang memproduksi, membuat, memperbanyak, menggandakan, menyebarkan, menyiarkan, mengimpor, mengekspor, menawarkan, memperjualbelikan, menyewakan, atau menyediakan Pornografi, dipidana dengan pidana penjara paling singkat 6 (enam) bulan dan pidana penjara paling lama 10 (sepuluh) tahun atau pidana denda paling sedikit kategori IV dan pidana denda paling banyak kategori VI.” Pada pasal ini Pasal 407 KUHP baru memang mengatur larangan memproduksi atau menyebarkan pornografi, tetapi pasal ini kurang relevan untuk menangani pornografi deepfake berbasis AI.

Pasal ini masih menggunakan pemahaman tradisional tentang pornografi sebagai hasil tindakan nyata atau rekaman asli, sehingga tidak membedakan antara pornografi yang melibatkan tubuh sebenarnya dan konten sintesis hasil manipulasi AI. Padahal, dalam kasus deepfake porn, inti persoalannya bukan hanya pada konten cabulnya, tetapi pada pemalsuan identitas dan penggunaan wajah korban tanpa persetujuan.

Selain itu, definisi “memproduksi” dalam pasal ini masih terlalu umum dan tidak secara eksplisit mencakup proses teknis pembuatan deepfake menggunakan algoritma AI. Hal ini berpotensi menimbulkan celah hukum karena pelaku dapat berdalih bahwa konten yang dibuat tidak menampilkan tubuh asli siapa pun. Pasal ini juga tidak memasukkan unsur penting berupa *non-konsensual*, yang merupakan karakter utama dari deepfake porn. Terakhir, pasal ini tidak mengatur peran platform atau teknologi yang memfasilitasi produksi dan penyebaran deepfake, sehingga tidak cukup efektif menghadapi kecepatan penyebaran konten digital modern. Dengan demikian, meskipun berguna untuk pornografi konvensional, Pasal 407 tetap belum memadai untuk menangani kompleksitas pornografi berbasis AI dan memerlukan regulasi tambahan yang lebih spesifik

Kedua Dalam UU ITE baru atau UU No 1 Tahun 2024 yang dimana terdapat beberapa revisi dari tahun 2008 dan 2016, terdapat beberapa pasal yang mengatur terkait penyebaran, manipulasi dan pencemaran yaitu pada pasal 27 ayat 1, pasal 27A UU No 1 Tahun 2024 UU No 1 Tahun 2024, lalu Pasal 35 UU No 11 Tahun 2008.

Pada pasal 27 ayat 1 berbunyi “(1) Setiap Orang dengan sengaja dan tanpa hak menyiarkan, mempertunjukkan, mendistribusikan, mentransmisikan, dan/atau membuat dapat diaksesnya Informasi Elektronik dan/ atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan untuk diketahui umum”, pada pasal Pasal 27A berbunyi “Setiap Orang dengan sengaja menyerang kehormatan atau nama baik orang lain dengan cara menuduhkan suatu hal, dengan maksud supaya hal tersebut diketahui umum dalam bentuk Informasi Elektronik dan/ atau Dokumen Elektronik yang dilakukan melalui Sistem Elektronik” lalu yang terakhir

pada pasal 35 uu No 11 Tahun 2008 yang berbunyi “Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik.”

Pada pasal pasal diatas UU ITE sebenarnya hanya mengatur akibat hukumnya, yaitu konten elektronik yang melanggar kesusilaan, tetapi tidak mengatur teknologi deepfake itu sendiri. Ini membuat munculnya beberapa celah penting. Pertama, UU ITE tidak mengatur tindakan membuat deepfake, padahal penyalahgunaan sudah terjadi sejak identitas korban dimanipulasi, bukan hanya ketika disebar, pelaku yang hanya memproduksi konten tetapi belum menyebarkannya berada dalam wilayah abu-abu hukum. Kedua, UU ITE tidak mewajibkan pelabelan atau watermark pada konten yang dihasilkan oleh AI, sehingga masyarakat sulit membedakan mana konten asli dan mana yang manipulasi. Ketiga, UU ini tidak memiliki definisi hukum mengenai deepfake, membuat proses penegakan hukum sangat bergantung pada interpretasi aparat dan berpotensi menimbulkan ketidakpastian. Keempat, tidak ada ketentuan terkait tanggung jawab platform, seperti kewajiban menghapus konten deepfake dalam waktu tertentu atau menyediakan sistem deteksi otomatis, padahal platform memegang peran besar dalam penyebaran konten. Terakhir, UU ITE tidak membedakan antara deepfake yang bersifat kriminal dan deepfake yang bersifat kreatif, sehingga regulasi menjadi terlalu umum dan tidak cukup sensitif terhadap konteks kejahatan seperti pornografi non-konsensual. Karena celah-celah inilah,

UU ITE masih belum memadai dan perlu didukung oleh regulasi khusus yang dirancang untuk menghadapi teknologi AI secara lebih spesifik.

Pasal 14 UU TPKS yang mengatur mengenai Kekerasan Seksual Berbasis Elektronik (KSBE) pada dasarnya dapat digunakan untuk menjerat pelaku penyebaran konten seksual tanpa persetujuan korban melalui media elektronik. Dalam konteks perkembangan teknologi, ketentuan ini secara konseptual dapat dikaitkan dengan fenomena deepfake pornografi, yaitu manipulasi wajah atau identitas seseorang pada konten seksual menggunakan teknologi kecerdasan buatan (Artificial Intelligence). Apabila seseorang dengan sengaja membuat dan menyebarkan gambar atau video pornografi hasil manipulasi yang menampilkan identitas korban tanpa persetujuannya, maka tindakan tersebut berpotensi memenuhi unsur kekerasan seksual berbasis elektronik sebagaimana dimaksud dalam Pasal 14 UU TPKS, karena korban mengalami kerugian berupa pelanggaran martabat, reputasi, serta integritas seksualnya.

Namun demikian, ketentuan dalam Pasal 14 UU TPKS masih memiliki keterbatasan dalam menjangkau kompleksitas kejahatan deepfake. Pasal tersebut pada dasarnya lebih menitikberatkan pada perbuatan perekaman, pengambilan gambar, atau penyebaran konten seksual yang sudah ada, sementara dalam kasus deepfake konten tersebut sering kali merupakan hasil rekayasa teknologi yang menciptakan representasi visual baru yang tidak pernah benar-benar dilakukan oleh korban. Selain itu, UU TPKS juga belum secara eksplisit mengatur penggunaan teknologi kecerdasan buatan dalam manipulasi identitas digital, sehingga penegakan hukum terhadap kasus deepfake masih sangat bergantung pada penafsiran aparat penegak hukum. Kondisi ini menunjukkan bahwa meskipun UU

TPKS dapat digunakan sebagai dasar hukum dalam menindak dampak dari deepfake pornografi, regulasi tersebut belum sepenuhnya mampu mengantisipasi perkembangan teknologi manipulasi digital yang semakin canggih. Oleh karena itu, diperlukan pengaturan hukum yang lebih spesifik terkait penggunaan teknologi kecerdasan buatan, khususnya dalam konteks perlindungan terhadap penyalahgunaan identitas digital dan pencegahan konten deepfake yang bersifat pornografis.

Perkembangan kecerdasan buatan (*Artificial Intelligence/AI*), khususnya AI generatif, telah membawa perubahan signifikan dalam cara data pribadi dikumpulkan, dianalisis, dan digunakan (Putri et al., 2024). Teknologi seperti *large language models*, *image generators*, serta sistem berbasis pembelajaran mendalam membutuhkan data dalam jumlah besar, termasuk data yang bersifat sensitif (Jumrawati et al., 2025). Kondisi ini menimbulkan risiko baru terhadap perlindungan data pribadi, seperti praktik *data scraping*, kurangnya transparansi pemrosesan, serta potensi kebocoran data (*data leakage*) melalui output model. Sejumlah kajian internasional menunjukkan bahwa perkembangan teknologi AI sering kali berjalan lebih cepat dibandingkan dengan kemampuan regulasi dalam meresponsnya, sehingga menciptakan celah hukum terkait akuntabilitas dan transparansi (Aiman et al., 2025).

Dalam praktiknya, pengembangan AI generatif sering dilakukan dengan mengumpulkan data publik secara masif tanpa persetujuan eksplisit dari pemilik data. Data yang dikumpulkan dari internet tidak jarang mengandung informasi sensitif, bias, bahkan konten ilegal (Manoppo, 2025). Hal ini menunjukkan bahwa meskipun regulasi seperti UU No. 27 Tahun 2022 tentang Perlindungan Data

Pribadi (UU PDP) telah bersifat progresif, masih terdapat keterbatasan dalam mengantisipasi risiko teknologi AI yang berbasis pada pemrosesan data skala besar. Bahkan, dalam perspektif global seperti General Data Protection Regulation (GDPR), prinsip-prinsip seperti *lawfulness*, *purpose limitation*, dan *data minimization* pun sering kali sulit diterapkan dalam konteks AI generatif yang membutuhkan data luas dan beragam untuk pelatihan model (Aiman et al., 2025).

Di Indonesia, praktik penggunaan data untuk AI juga menunjukkan permasalahan nyata. Data pribadi seperti foto, suara, dan teks yang diunggah di media sosial sering digunakan tanpa persetujuan yang jelas untuk melatih sistem AI. Selain itu, UU PDP belum memiliki ketentuan teknis yang secara spesifik mengatur bagaimana data pelatihan AI harus diproses, disimpan, atau diaudit. Risiko seperti *model memorization* yang memungkinkan AI mengeluarkan kembali data sensitif dari dataset pelatihan semakin memperkuat bahwa perlindungan hukum yang ada belum sepenuhnya mampu menjangkau kompleksitas teknologi ini (Aiman et al., 2025).

Dalam konteks tersebut, kasus deepfake pornografi menjadi salah satu bentuk nyata dari penyalahgunaan AI yang berdampak serius terhadap data pribadi dan integritas individu. Deepfake memungkinkan manipulasi wajah, suara, atau identitas visual seseorang menjadi konten seksual tanpa persetujuan, sehingga menimbulkan kerugian baik secara psikologis, sosial, maupun reputasional.

Jika dikaitkan dengan Pasal 4 ayat (1) huruf b UU PDP, yang mengkategorikan data biometrik sebagai data pribadi spesifik, secara normatif wajah yang digunakan dalam deepfake termasuk objek yang dilindungi. Namun

demikian, ketentuan ini masih memiliki keterbatasan karena UU PDP hanya mengatur data biometrik yang bersifat asli, sedangkan dalam deepfake, yang digunakan adalah representasi sintetis hasil rekayasa AI. Hal ini menimbulkan celah hukum mengenai apakah konten hasil manipulasi tersebut tetap dikategorikan sebagai data pribadi, sehingga perlindungan hukum menjadi tidak optimal.

Selanjutnya, dalam Pasal 65 UU PDP, yang melarang perolehan, pengungkapan, dan penggunaan data pribadi secara melawan hukum, secara teoritis dapat digunakan untuk menjerat pelaku deepfake. Misalnya, penggunaan foto seseorang dari media sosial tanpa izin untuk dijadikan bahan deepfake dapat dianggap sebagai penggunaan data pribadi tanpa hak. Namun, dalam praktiknya, pembuktian pelanggaran pasal ini menjadi sulit karena pelaku sering kali tidak menyimpan data secara permanen, melainkan hanya menggunakan data secara sementara dalam proses AI. Selain itu, pasal ini belum secara spesifik mengatur bentuk penyalahgunaan data dalam konteks manipulasi visual dan konten sintetis.

Sementara itu, Pasal 66 UU PDP yang melarang pembuatan atau pemalsuan data pribadi dengan tujuan menguntungkan diri sendiri atau orang lain juga tampak relevan terhadap deepfake. Namun, terdapat keterbatasan dalam penerapannya karena deepfake tidak selalu bertujuan untuk keuntungan ekonomi, melainkan sering kali didorong oleh motif pelecehan, balas dendam, atau eksploitasi seksual. Selain itu, deepfake tidak secara langsung memalsukan data pribadi dalam arti administratif, melainkan menciptakan konten baru yang menyerupai identitas seseorang, sehingga interpretasi terhadap “pemalsuan data pribadi” dalam pasal ini masih bersifat ambigu.

Dengan demikian, meskipun Pasal 4, Pasal 65, dan Pasal 66 UU PDP dapat dikaitkan dengan kasus deepfake pornografi, ketentuan-ketentuan tersebut masih belum mampu menjangkau secara komprehensif karakteristik kejahatan berbasis AI. UU PDP belum mengatur secara spesifik mengenai manipulasi biometrik, konten sintetis, tanggung jawab platform AI, maupun mekanisme pencegahan seperti pelabelan konten dan deteksi otomatis. Oleh karena itu, diperlukan pengembangan regulasi yang lebih khusus dan adaptif terhadap teknologi AI guna memberikan perlindungan hukum yang efektif terhadap korban deepfake pornografi

Berdasarkan catatan LBH APIK Jakarta, dari sembilan bentuk KBGO yang pernah ditangani, masih terdapat tujuh bentuk yang belum terakomodasi dalam UU TPKS, yaitu pembuatan konten yang berbasis digital bernuansa seksual tanpa sebuah persetujuan, modifikasi konten seksual, perdagangan konten seksual berbasis elektronik, pelecehan seksual, eksploitasi seksual, serta perundungan seksual yang dilakukan melalui media digital (Bestiara Hanum, 2024).

kekosongan norma ini menimbulkan berbagai dampak, antara lain ketidakpastian hukum karena pasal-pasal yang ada masih kurang relevan terkait isu permasalahan tersebut, potensi kriminalisasi korban ketika korban justru dilaporkan karena dianggap ikut menyebarkan konten, kendala penegakan hukum akibat aparat penegak hukum kesulitan menentukan pasal yang paling tepat, serta celah hukum yang dimanfaatkan pelaku dengan dalih bahwa *deepfake* hanyalah karya digital yang belum diatur secara spesifik. Akibatnya, terjadi kesenjangan perlindungan hukum, di mana regulasi yang ada masih menitikberatkan pada pornografi

konvensional dan belum mampu mengantisipasi perkembangan teknologi kecerdasan buatan yang semakin kompleks.

kekosongan pengaturan hukum yang secara khusus dan tegas mengatur konten pornografi berbasis teknologi *deepfake* dalam konteks KBGO menimbulkan kekosongan norma hukum pidana. Kekosongan ini menciptakan ketidakpastian hukum dalam hal pertanggungjawaban pidana terhadap pelaku, serta memperlemah perlindungan hukum terhadap korban. Dalam kerangka negara hukum, prinsip legalitas mensyaratkan bahwa suatu perbuatan tidak dapat dipidana kecuali berdasarkan peraturan perundang-undangan yang telah ada sebelumnya (*nullum crimen, nulla poena sine lege*). Dengan demikian, korban KBGO melalui konten *deepfake* tidak mendapatkan kepastian hukum dan keadilan yang semestinya.

Studi yuridis normatif menjadi penting dilakukan untuk menelaah sejauh mana kekosongan norma hukum pidana dalam konteks kejahatan ini, serta bagaimana seharusnya hukum pidana Indonesia merespons perkembangan teknologi dan bentuk-bentuk kejahatan baru yang muncul (Cahyani, 2026). Pendekatan ini akan menganalisis peraturan perundang-undangan yang ada, mengidentifikasi celah hukum, dan merumuskan urgensi pembentukan norma baru yang mampu melindungi korban KBGO berbasis *deepfake* secara komprehensif.

Latar belakang penelitian ini mengacu pada realitas sosial yang terjadi akibat keterlambatan regulasi dalam merespons perkembangan teknologi. Negara, sebagai penyelenggara kekuasaan hukum, memiliki tanggung jawab untuk memastikan bahwa setiap warganya terlindungi dari bentuk kejahatan baru, termasuk kejahatan digital yang menyerang martabat dan integritas personal. Oleh karena itu, penting

untuk mengkaji dan mendorong lahirnya regulasi pidana yang spesifik, adaptif, dan progresif dalam menghadapi tantangan kejahatan berbasis teknologi (Kristanto & Baihaki, 2025).

Selaras dengan itu, penting pula untuk memahami bahwa karakteristik KBGO yang dilakukan melalui teknologi *deepfake* sangat berbeda dengan kejahatan konvensional lainnya. KBGO cenderung menyerang secara tidak langsung, melalui ranah maya, tanpa keterlibatan fisik pelaku terhadap korban. Meski demikian, dampaknya terhadap korban tidak kalah serius dibanding kekerasan seksual langsung. Rasa malu, depresi, hilangnya rasa aman di ruang digital, hingga keinginan untuk menarik diri dari lingkungan sosial adalah dampak nyata yang dialami korban. Oleh karena itu, pendekatan hukum terhadap bentuk kekerasan ini tidak bisa lagi bergantung pada kerangka hukum konvensional.

Di berbagai negara, tantangan serupa juga mulai direspons dengan berbagai upaya legislasi. Uni Eropa misalnya, dalam kerangka General Data Protection Regulation (GDPR), menekankan pentingnya perlindungan data pribadi dan pengendalian terhadap konten digital yang melibatkan identitas individu (Mangku et al., 2021). Sementara itu, Amerika Serikat telah memulai pembahasan hukum federal yang secara khusus menasar penyalahgunaan teknologi *deepfake*, termasuk dalam konteks kekerasan seksual. Indonesia sebagai bagian dari masyarakat global dituntut untuk bergerak ke arah serupa, mengingat ancaman kejahatan digital bersifat lintas batas dan terus berkembang (Simanjuntak, 2024).

Penelitian ini tidak hanya penting dalam aspek teoritis, tetapi juga mendesak dari segi praktis. Dengan meningkatnya jumlah kasus KBGO melalui *deepfake*,

korban tidak bisa menunggu lebih lama hingga negara menyediakan perlindungan yang layak. Hukum harus segera hadir untuk memberikan jaminan perlindungan dan pemulihan bagi korban, sekaligus memberikan efek jera bagi pelaku. Dalam konteks ini, hukum pidana yang adaptif terhadap perkembangan teknologi merupakan keniscayaan.

Dengan menelaah norma hukum pidana terhadap Kekerasan Berbasis Gender Online (KBGO) melalui konten pornografi berteknologi *deepfake*, diharapkan penelitian ini dapat memberikan sumbangan pemikiran yang konstruktif bagi pembaruan hukum pidana di Indonesia. Pembaruan tersebut bukan hanya sekadar menambah pasal-pasal dalam perundang-undangan, tetapi menyusun sistem hukum yang lebih inklusif, adil, dan berorientasi pada korban.

Penulis penelitian ini mengutip sejumlah studi sebelumnya yang relevan dengan isu pemeriksaan kekerasan berbasis gender online dari perspektif hukum yang menguntungkan di Indonesia, khususnya studi-studi berikut, untuk perbandingan dan pertimbangan.

Analisis Kekerasan Berbasis Gender online dari Perspektif Hukum Positif di Indonesia oleh Bestiara Hanum (2024). Bestiara Hanum sebelumnya telah mempelajari kekerasan berbasis gender online (KBGO). Penelitian tersebut menggunakan pendekatan yuridis normatif dengan menganalisis berbagai regulasi nasional yang berkaitan dengan KBGO, seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), Undang-Undang Tindak Pidana Kekerasan Seksual (UU TPKS), serta peraturan perundang-undangan lain yang relevan. Fokus utama penelitian Bestiara Hanum adalah bagaimana regulasi hukum yang ada mampu

memberikan perlindungan bagi korban KBGO serta hambatan-hambatan yang dihadapi dalam implementasinya.

Berdasarkan temuan penelitian, perlindungan hukum bagi korban kekerasan berbasis online (KBGO) masih belum memadai meskipun sudah ada undang-undang seperti UU ITE dan UU TPKS. Hal ini karena hanya sedikit standar hukum yang secara spesifik melarang berbagai jenis kekerasan yang dilakukan secara daring. Misalnya, hanya teridentifikasi dari sembilan jenis agresi daring yang ditangani oleh LBH APIK Jakarta., sebagian besar belum terakomodasi secara jelas dalam UU TPKS. Akibatnya, korban seringkali mengalami kesulitan dalam memperoleh kepastian hukum maupun pemulihan hak-haknya.

Kaitan penelitian Bestiara Hanum dengan penelitian ini terletak pada fokus permasalahan yang sama-sama membahas tentang lemahnya perlindungan hukum terhadap korban KBGO. Namun, penelitian ini memiliki perbedaan dalam hal objek kajian. Jika penelitian Bestiara Hanum lebih menyoroti perlindungan korban KBGO secara umum, penelitian ini akan lebih spesifik menelaah analisis hukum pidana terhadap Kekerasan Berbasis Gender Online berteknologi *deepfake*. Dengan demikian, penelitian ini diharapkan dapat memperluas kajian mengenai KBGO dengan memberikan perspektif yang lebih khusus terkait tantangan hukum dalam menghadapi kejahatan digital berbasis teknologi kecerdasan buatan.

Penelitian ini bertujuan untuk mengidentifikasi norma hukum pidana dalam kasus KBGO yang menggunakan teknologi *deepfake*, mengkaji perlindungan hukum yang tersedia bagi korban, dan merumuskan kebutuhan akan regulasi baru yang mampu menjawab tantangan zaman. Kajian ini bersifat yuridis normatif

dengan pendekatan perundang-undangan, konsep hukum pidana modern, serta teori perlindungan hukum dan hak asasi manusia (Sinaulan, 2021). Kekerasan berbasis gender online telah menjadi masalah serius seiring dengan perkembangan teknologi kontemporer, yang menuntut perhatian khusus dari perspektif hukum yang positif di Indonesia. Oleh karena itu, berdasarkan topik ini, penulis tertarik untuk menghasilkan penelitian berjudul "Analisis Yuridis Hukum Pidana Terhadap Penyalahgunaan *Artificial Intelligence (AI)* Berkenaan Dengan Konten *Deepfake* Pornografi."

1.2 Identifikasi Masalah

Berdasarkan latar belakang yang telah diuraikan, dapat diidentifikasi beberapa permasalahan hukum sebagai berikut:

- 1) Perkembangan teknologi kecerdasan buatan (*Artificial Intelligence/AI*), khususnya *deepfake*, telah disalahgunakan untuk membuat dan menyebarkan konten pornografi yang mencatut wajah seseorang tanpa persetujuan, sehingga menimbulkan bentuk Kekerasan Berbasis Gender Online (KBGO).
- 2) Fenomena KBGO berbasis *deepfake* telah terjadi secara nyata di Indonesia, bahkan dalam lingkungan akademik, yang menimbulkan kerugian psikologis, sosial, dan reputasi bagi korban.
- 3) Instrumen hukum positif di Indonesia seperti KUHP, UU ITE, UU Pornografi, dan UU TPKS memang mengatur tindak pidana kesusilaan dan kekerasan seksual digital, namun belum secara tegas mengatur mengenai penggunaan teknologi AI (*deepfake*) dalam pembuatan maupun penyebaran konten asusila.

- 4) Terdapat kekosongan norma dalam regulasi yang berlaku, Hal ini menimbulkan ketidakpastian hukum, serta memperlemah perlindungan korban.
- 5) Belum adanya regulasi yang spesifik dan adaptif menyebabkan keterlambatan negara dalam memberikan perlindungan hukum yang memadai terhadap korban KBGO berbasis *deepfake*.
- 6) Perlunya studi yuridis normatif untuk menelaah kekosongan norma hukum pidana terkait fenomena KBGO berbasis *deepfake*, sekaligus merumuskan urgensi pembentukan regulasi baru yang lebih responsif.

1.3 Pembatasan Masalah

Dalam penelitian ini, pembahasan dibatasi pada:

- 1) Penelitian ini hanya membahas Kekerasan Berbasis Gender Online (KBGO) dalam bentuk konten pornografi yang dimanipulasi dengan teknologi *deepfake*.
- 2) Analisis hukum dibatasi pada instrumen hukum pidana Indonesia, yakni KUHP, UU ITE, UU Pornografi, dan UU TPKS, UU Perlindungan data Pribadi.
- 3) Fokus kajian terletak pada adanya kekosongan norma hukum pidana dalam mengatur penyalahgunaan AI berbasis *deepfake*.
- 4) Penelitian ini menggunakan pendekatan yuridis normatif, sehingga pembahasan terbatas pada analisis peraturan perundang-undangan, doktrin hukum, serta literatur akademik, tanpa melakukan penelitian lapangan.

- 5) Ruang lingkup penelitian difokuskan pada perlindungan hukum bagi korban dan pertanggungjawaban pidana pelaku, serta urgensi pembaruan hukum pidana Indonesia dalam menghadapi kejahatan digital berbasis AI.

1.4 Rumusan Masalah

Adapun rumusan masalah yang diambil dalam penelitian ini, yaitu sebagai berikut.

- 1) Bagaimana pengaturan hukum pidana di Indonesia terkait dengan penyalahgunaan Artificial Intelligence (AI) melalui konten pornografi berteknologi *deepfake*?
- 2) Bagaimana upaya yang dapat dilakukan untuk memberikan perlindungan hukum terhadap korban serta menjamin kepastian hukum terkait fenomena KBGO berbasis *deepfake*?

1.5 Tujuan Masalah

Adapun tujuan masalah yang hendak dicapai dalam penelitian ini, sebagai berikut.

- 1) Menganalisis pengaturan hukum pidana di Indonesia terkait penyalahgunaan Artificial Intelligence (AI) melalui konten pornografi berteknologi *deepfake*.
- 2) Merumuskan upaya yang dapat dilakukan untuk memberikan perlindungan hukum yang efektif bagi korban serta menjamin kepastian hukum dalam menghadapi fenomena KBGO berbasis *deepfake*.

1.6 Manfaat Penelitian

Melalui dilaksanakannya kajian studi ini, diharapkan mampu memberikan manfaat berikut:

1) Manfaat Teoritis

Dengan memperkaya literatur tentang norma dan kebutuhan akan pembaruan hukum terkait kejahatan digital kontemporer, seperti keterlibatan *AI* dalam KBGO berbasis *deepfake*, penelitian ini diharapkan dapat memberikan panduan atau berkontribusi pada pengembangan ilmu hukum, khususnya di bidang Hukum Pidana dan ITE.

2) Manfaat Praktis

- a. Memberikan masukan kepada pembentuk kebijakan dan legislator mengenai pentingnya merumuskan regulasi pidana yang tegas dan jelas dalam menanggulangi penyalahgunaan teknologi *deepfake* untuk tujuan pornografi.
- b. Memberikan pemahaman kepada aparat penegak hukum, akademisi, dan masyarakat mengenai bentuk-bentuk kejahatan baru di era digital serta perlunya pendekatan hukum yang adaptif.
- c. Meningkatkan kesadaran publik akan bahaya *AI (Deepfake)* dan pentingnya perlindungan hukum terhadap korban KBGO kejahatan digital yang berbasis pada pelanggaran privasi dan manipulasi visual.