PENEGAKAN HUKUM *DEEPFAKE* DI POLDA JAWA TIMUR SEBAGAI BENTUK KEJAHATAN SIBER

Yani Heskia Putri1 dan Pudji Astuti2

1Fakultas Hukum, Universitas Negeri Surabaya, Surabaya, Indonesia,yaniheskia.22033@unesa.ac.id , https://orcid.org/0000-0001-9744-588X 2Fakultas Hukum, Universitas Airlangga, Surabaya, Indonesia,pudjiastuti@unesa.ac.id,https://orcid.org/0000-0001-9744-588X

Abstrak

The rapid development of Artificial Intelligence has introduced new threats of deepfake technology, which utilizes machine learning to realistically manipulate audio, images, and video content. The misuse of deepfake in Indonesia has led to various cybercrimes, including fraud, sexual harassment, defamation, violation of privacy and dissemination of hoaxes. This study aims to analyze legal basis employed by investigators at East Java Regional Police in enforcing criminal law against deepfake-related offenses and to identify countermeasures undertaken. The research adopts an empirical legal method with a descriptive qualitative approach. Primary data were obtained through interviews with investigators from the Cybercrime Directorate and victims, while secondary data were collected through a literature review. The findings reveal that the East Java Regional Police apply several legal frameworks, including the Law on Sexual Violence Crimes, the Law on Electronic Information and Transactions, the Indonesian Penal Code (KUHP), and potentially the Law on Personal Data Protection. Countermeasures, preventive efforts such as cyber patrols, public education, and complaint channels, and repressive measures including investigation, prosecution, arrest of perpetrators, and submission of case files to the public prosecutor. Nevertheless, law enforcement face challenges, including absence of specific regulations, difficulties in digital evidence collection, limited facilities and infrastructure, and low public awareness. This study recommends establishment of specific regulations on deepfake, capacity building for investigators, strengthening of digital forensic infrastructure.

Keywords: *Deepfake, Cybercrime, East Java Regional Police Cyber Investigation Directorate.*

A. PENDAHULUAN

Perkembangan Artificial Intelligence (AI) berdampak besar pada kehidupan manusia, termasuk komunikasi, hiburan, dan media digital. Salah satu inovasinya, Deepfake, memanfaatkan machine learning dan GAN untuk membuat konten audio, gambar, dan video yang realistis. Kata Deepfake berasal dari kombinasi istilah deep learning dan fake, yang memiliki arti palsu. Awal mula kemunculan Deepfake ini dikembangkan untuk keperluan hiburan dan riset teknologi.(Geby 2023)

Seiring berjalannya waktu, AI memberikan ancaman yang besar dengan model baru AI yang dapat berpotensi melanggar etika. Keberadaan AI saat ini bebas untuk digunakan yang membuat adanya disinformasi yang meyakinkan, memproduksi lebih banyak konten palsu. Penggunaan *Deepfake* bisa memberikan manfaat dalam industri

film dan hiburan, tetapi juga berpotensi disalahgunakan untuk informasi palsu atau manipulasi. Dengan kondisi seperti ini dapat memicu terjadinya tindak pidana seperti penipuan, pelecehan, pencemaran nama baik, pelanggaran privasi dan penyebaran informasi hoaks.(Dahlan 2025)

Deepfake dapat diakses dengan mudah saat ini melalui berbagai platform, siapapun saat ini dapat mengakses dan membuat video editan sesuai yang mereka inginkan. Video foto tersebut dapat berupa hoaks atau hal yang tidak senonoh, teknologi *Deepfake* ini banyak disalahgunakan untuk tujuan yang merugikan, khususnya dalam bentuk pelecehan seksual dan serangan reputasi seseorang.

Deepfake dapat dikualifikasikan sebagai kejahatan siber, karena *Deepfake* merupakan tindakan melanggar hukum yang dilakukan melalui komputer, jaringan internet, atau sistem elektronik sebagai sarana kejahatan. Dan *Deepfake* merupakan perbuatan mengubah, memalsukan, atau merekayasa informasi elektronik tanpa hak , yang merupakan karakteristik utama dari tindak pidana berbasis teknologi informasi.(Kewarganegaraan et al. 2022)

Adanya kejahatan siber menjadi ancaman bagi stabilitas negara, sehingga pemerintah sulit untuk mengimbangi teknik kejahatan yang dilakukan menggunkan teknologi Deepfake ini. Perkembangan teknologi informasi menyebabkan dunia menjadi tanpa batas yang menyebabkan adanya perubahan sosial yang sangat cepat pada masyarakat. Beberapa kasus Deepfake yang menjadi sorotan adalah kasus penipuan Gubernur Jawa Timur dengan memanipulasi video yang tampak seolah-olah seperti Gubernur menawarkan program pembelian sepeda motor murah seharga Rp500.000 untuk warga Jawa Timur. Video tersebut disebarkanluaskan melalui tiktok, sehingga beberapa masyarakat yang tertarik diarahkan untuk mentransfer sejumlah uang ke rekening yang sudah disiapkan oleh para pelaku. (Syahril, 2025) Dan terdapat kasus pelecehan Deepfake dengan merekayasa foto dengan menggunakan AI dengan foto biasa menjadi foto vulgar, kejadian ini berasal dari remaja berumur 18 tahun di Gresik Jawa Timur. (Habib 2024)

Kejahatan penipuan *Deepfake* menimbulkan berbagai dampak yang cukup besar, dari aspek ekonomi, korban dapat mengalami kerugian finansial karena pelaku melakukan penipuan untuk mendapatkan uang dengan transaksi fiktif. Dari sisi psikologis, korban sering mengalami stress berat, kebingungan dan rasa takut hingga ada rasa trauma. Dan yang paling merusak adalah pembuatan dan penyebaran konten seksual non-konsensual atau pelecehan Deepfake yang mayoritas menargetkan perempuan, yang berpotensi menimbulkan stigma sosial, trauma psikologis, ancaman keselamatan pribadi dan kerusakan reputasi jangka panjang.(Puspoayu et al. 2022)

Hal ini memberikan rasa tidak aman untuk bersosial media dimana cukup banyak media sosial yang bisa diakses tanpa menyertakan data diri. Pelaku dapat mengakses foto video seseorang terutama perempuan tanpa harus mendapatkan izin dari korban, dan pelaku tersebut adalah oknum-oknum yang sulit untuk dilacak. Kasus Deepfake yang telah direkayasa ini menjadi bentuk contoh realistis ancaman bagi keselamatan dan harga diri perempuan di ruang digital. (UINSSC 2025)

Di banyak negara, termasuk di Indonesia, kemajuan teknologi bergerak lebih cepat daripada pembentukan norma hukum khusus. Persoalan regulasi hukum di Indonesia

mengenai Deepfake semakin kompleks karena belum dibentuknya regulasi yang secara khusus mengatur fenomena ini. Penegakan hukum terhadap kasus pelecehan Deepfake masih mengandalkan ketentuan-ketentuan dalam berbagai perundang-undangan. (Medgo 2025)

Ada beberapa undang-undang yang bisa menjadi payung hukum dalam menjerat pelaku *Deepfake* pelecehan dan penipuan, yakni dengan Undang-Undang Informasi dan Transaksi Elektronik pada Pasal 27 ayat (1) bahwa "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." Dan berkaitan dengan Kitab Undang-Undang Hukum Pidana pada pasal 378 tentang tindak pidana penipuan bahhwa "Barang siapa dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum, dengan memakai nama palsu atau martabat palsu, dengan tipu muslihat, ataupun rangkaian kebohongan, menggerakkan orang lain untuk menyerahkan barang sesuatu kepadanya, atau supaya memberi hutang maupun menghapuskan piutang, diancam karena penipuan dengan pidana penjara paling lama 4 tahun."

Di banyak yurisdiksi, hukum yang ada belum sepenuhnya mampu untuk menangani permasalahan ini, karena tidak ada regulasi spesifik yang mengatur penggunaan teknologi tersebut. Perlindungan hukum bagi korban Deepfake perlu diperkuat melalui undang-undang yang jelas dan tegas, serta mekanisme penegakan hukum yang efektif. Namun demikian, penerapan pasal-pasal tersebut masih menghadapi kendala yang signifikan karena tidak secara eksplisit menyebutkan teknologi Deepfake sebagai objek pengaturan, sehingga menyebabkan ketidakpastian hukum dalam penegakan dan perlindungan korban. Hal ini membentuk celah hukum yang signifikan, terutama dalam soal pembuktian, pertanggungjawaban, maupun mekanisme penghapusan konten yang disebarluaskan di berbagai platform digital.(siplawfirm 2025)

Karena pengaturan tersebut masih terdapat celah, maka pemerintah diharapkan dapat mengupayakan untuk mengadopsi peraturan yang terlahir dinegara-negara yang telah mengatur secara eksplisit terkait Deepfake. Dampak dari penerapan hukum seringkali bergantung pada pandangan aparat penegak hukum, yang dapat menimbulkan ketidakpastian dan kesenjangan dalam perlindungan terhadap korban. Karena itu, penelitian ini dilakukan untuk menilai sejauh mana aturan yang ada efektif sebagai instrumen hukum dalam memberikan perlindungan nyata bagi korban pelecehan serta penipuan berbasis teknologi artifisial, serta untuk mengidentifikasi kekurangan dan kebutuhan pembaruan regulasi di era digital saat ini. Peran dan kewenangan Polda Jawa Timur dalam menegakan kejahatan siber berupa teknologi *Deepfake* ini sangat strategis dan komprehensif. Sebagai institusi penegak hukum di Jawa Timur, Polda Jawa Timur memiliki peran utama dalam melakukan penyelidikan dan penyidikan terhadap kasus-kasus *Deepfake*. Unit Cyber Crime berada di bawah (Ditressiber) Reserse Siber Polda Jawa Timur Polda Jawa Timur menjadi garda terdepan dalam mengidentifikasi pelaku, mengumpulkan bukti digital, dan melakukan penyidikan sesuai dengan ketentuan KUHP dan UU ITE. (Melati 2022)

Meskipun memiliki peran dan kewenangan yang kuat, Polda Jawa Timur menghadapi berbagai tantangan dalam penegakan hukum kejahatan *Deepfake*. Tantangan teknis muncul karena dibutuhkan keahlian khusus untuk mendeteksi dan menganalisis konten *Deepfake* yang semakin canggih. Masalah yurisdiksi juga menjadi kendala ketika pelaku berada di luar wilayah Jawa Timur atau bahkan di luar negeri.

Perkembangan teknologi *Deepfake* yang sangat cepat membuat aparat harus terus meningkatkan kapasitas dan kemampuannya. Selain itu, proses pembuktian dalam kasus *Deepfake* cukup kompleks karena harus membuktikan niat pelaku dan keaslian atau manipulasi konten. Masyarakat yang menjadi korban atau mengetahui adanya kejahatan *Deepfake* dapat melaporkannya ke Polsek atau Polres setempat di Jawa Timur, langsung ke Ditressiber Polda Jawa Timur, melalui kanal online Polri, atau langsung menghubungi Unit Cyber Crime Polda Jawa Timur. Dengan kewenangan penuh di wilayah hukum Jawa Timur, Polda Jawa Timur siap menindak tegas pelaku kejahatan siber *Deepfake* sambil terus berkoordinasi dengan berbagai instansi terkait untuk penanganan kasus yang lebih kompleks. (Putih 2024)

Hasil dari kajian ini diharapkan dapat menjadi dasar penguatan kebijakan hukum nasional yang lebih adaptif, responsif terhadap kemajuan teknologi, dan berpihak pada korban kekerasan berbasis gender online.

Atas dasar itu, maka topik yang akan ditelaah pada penulisan ini mengenai Penegakan Hukum Deepfake di Polda Jawa Timur Sebagai Bentuk Kejahatan Siber.

Penelitian ini akan menggunakan metode penelitian empiris, yakni dengan menganalisis sistem hukum yang sudah berjalan, dan menelaah bagaimana praktik yang diterapkan oleh aparat penegak hukum, khususnya di Polda Jawa Timur dalam menangani kasus kejahatan Deepfake. Dengan metode penelitian ini penulis bisa menentukan data untuk dinalisis, dan data diperoleh melalui wawancara dengan penyidik di Subdit Siber Ditressiber Polda Jawa Timur, serta dari dokumen laporan kasus dan wawancara dengan korban atau lembaga pendamping korban.
Sumber data yang digunakan dalam penelitian hukum empiris ada dua jenis yaitu data primer dan data sekunder, yaitu:

a. Data Primer

Sumber data primer untuk penelitian ini diperoleh secara langsung dari individu yang mempunyai hubungan dan keahlian terhadap isu yang sedang diteliti., yaitu mengenai Penegakan Hukum *Deepfake* di Polda Jawa Timur Sebagai Bentuk Kejahatan Siber. Adapun sumber data primer dalam penelitian ini meliputi:

1. Wawancara dengan Aparat Kepolisian
2. Wawancara dengan Korban atau Pendamping korban

b. Data Sekunder

Data sekunder menggunakan teknik mengumpulkan bahan seperti buku, jurnal, karya ilmiah, dan dokumen lain yang relevan dengan topik yang dibahas.

Data sekunder dalam penelitian ini antara lain :

a. Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik
b. Kitab Undang-Undang Hukum Pidana;
c. Undang-undang (UU) Nomor 12 Tahun 2022 Tindak Pidana Kekerasan Seksual
d. Kitab Undang-Undang Hukum Acara Pidana
e. Undang-Undang (UU) Nomor 2 Tahun 2002 tentang Kepolisian Negara Republik Indonesia
f. Lembaran Negara Republik Indonesia, Undang-Undang No. 13 Tahun 2022 Tentang Perubahan Kedua atas Undang-Undang Pembentukan Peraturan Perundang-Undangan

Data yang diambil berasal dari sampel salah satu dari mereka yang akan dijadikan responden oleh peneliti dengan bahan wawancara yang telah dipersiapkan oleh peneliti. Sampel yang akan dijadikan responden yaitu :

a. Reserse Siber Polda Jawa Timur Polda Jawa Timur (Ditressiber)

   Penelitian ini fokus pada Bidang siber di Polda Jawa Timur karena institusi ini memiliki peran yang cukup besar dalam penegakan hukum terkait kejahatan berbasis teknologi, termasuk tindak pidana penipuan dan pelecehan melalui teknologi Deepfake. Polda Jawa Timur merupakan salah satu institusi kepolisian yang memiliki struktur dan unit khusus dalam menangani kasus siber.

b. Korban kejahatan *Deepfake*

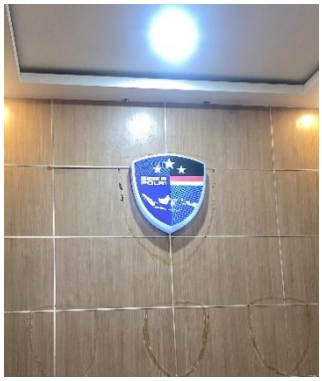
   Korban kejahatan Deepfake dapat memberikan gambaran langsung mengenai pengalaman mereka mulai dari bagaimana kasus tersebut terjadi, langkah yang diambil setelah kejadian, hingga bentuk perlindungan hukum dan psikologis yang mereka peroleh atau justru tidak peroleh.

Pengumpulan data dalam penelitian ini dilakukan melalui wawancara. Wawancara akan dilaksanakan dengan menggunakan pertanyaan yang telah disusun sebelumnya berdasarkan instrumen yang dipersiapkan oleh peneliti. Penelitian ini menggunakan studi kepustakaan dengan menganalisis berbagai sumber yang relevan dengan objek penelitian, meliputi buku-buku hukum, peraturan perundang-perundangan, jurnal ilmiah, hasil penelitian terdahulu, artikel ilmiah, dan bahan hukum lainnya.

B. HASIL DAN PEMBAHASAN

1. Gambaran Umum Tentang Kepolisian Daerah Jawa Timur

Profil Kepolisian Daerah Jawa Timur

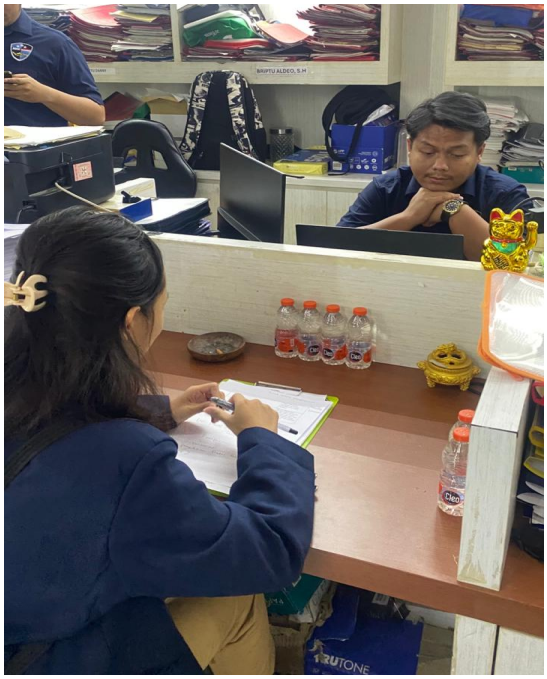


Gambar 1. 1 Kantor Diretsiber Polda Jawa Timur

Kepolisian Daerah Jawa Timur (Polda Jawa Timur) merupakan salah satu institusi kepolisian tingkat provinsi di Indonesia yang memiliki peran strategis dalam menjaga keamanan dan ketertiban masyarakat di wilayah Jawa Timur. Sebagai bagian dari Kepolisian Negara Republik Indonesia (Polri), Polda Jawa Timur memiliki tanggung jawab yang sangat besar mengingat Jawa Timur adalah provinsi dengan populasi terbesar kedua di Indonesia setelah Jawa Barat. Wilayah jurisdiksi Polda Jawa Timur mencakup seluruh Provinsi Jawa Timur yang terdiri dari 29 kabupaten dan 9 kota dengan luas wilayah sekitar 47.800 kilometer persegi dan populasi lebih dari 40 juta jiwa. Kompleksitas wilayah yang luas dan jumlah penduduk yang sangat besar ini menjadikan Polda Jawa Timur sebagai salah satu kepolisian daerah dengan tingkat kesulitan operasional yang tinggi.

Tugas dan fungsi utama Polda Jawa Timur mencakup pemeliharaan keamanan dan ketertiban masyarakat, penegakan hukum, perlindungan dan pelayanan masyarakat, serta pembinaan masyarakat. Dalam menjalankan fungsi penegakan hukum, Polda Jawa Timur melakukan penyelidikan dan penyidikan terhadap berbagai tindak pidana mulai dari kejahatan konvensional hingga kasus-kasus khusus seperti narkoba, korupsi, terorisme, dan kejahatan siber. Direktorat Siber Polda Jawa Timur (Diretsiber Polda Jawa Timur) merupakan salah satu satuan kerja khusus di lingkungan Kepolisian Daerah Jawa Timur yang memiliki tugas dan fungsi utama dalam pencegahan, penindakan, dan penyidikan tindak pidana yang berkaitan dengan teknologi informasi dan transaksi elektronik atau yang lebih dikenal dengan kejahatan siber (cyber crime).

2. Hasil Wawancara Dengan Penyidik Diretsiber Polda Jawa Timur



Gambar 1. 2 Wawancara dengan Bapak Briptu Aldeo, S.H selaku penyidik di Direktorat Reserse Siber Polda Jawa Timur

Berdasarkan hasil wawancara yang telah dilakukan pada tanggal 27 November 2025 pada hari kamis dengan Bapak Deo sebagai Penyidik Diretsiber di ruang Bantek Diretsiber. Dari hasil yang saya dapatkan dari wawancara dengan penyidik dijelaskan terdapat 3 kasus yang telah dan sedang ditangani.

Pertama, kasus pelecehan melalui *Deepfake* Nimas Sabella yang diteror selama 10 tahun oleh Adi Pradita yang terosebsi dengan Nimas. Komisioner Komisi Nasional Antikekerasan terhadap Perempuan atau Komnas Perempuan, Andy Yentriyani menyebutkan kasus ini sebagai Kekerasan Berbasis Gender Online atau KBGO. Adi Pradita melakukan pelecehan terhadapa nimas melalui teknologi *Deepfake* dengan mengubah foto nimas menjadi bugil dan dikirim Adi kepada Nimas. Karena itu, yang dilakukan Adi dapat dikualifikasikan dengan Undang-Undang Tindak Pidana Kekerasan Seksual Pasal 14 ayat (1) huruf b yakni,

"Setiap Orang yang tanpa hak: Mentransmisikan informasi elektronik dan/atau dokumen elektronik yang bermuatan seksual di luar kehendak penerima yang ditujukan terhadap keinginan seksual, dan/atau" Dan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE), Pasal 45 ayat (1) Jo Pasal 27 Ayat (1) "Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan."

Kedua, kasus penipuan *Deepfake* Gubernur Jawa Timur. Kasus ini terungkap setelah adanya laporan dari pegawai Dinas Komunikasi Informatika Provinsi Jawa Timur pada tanggal 15 April 2025. Kemudian Diretsiber Polda Jawa Timur mengambil langkah patroli siber dan behasil mengungkap kasus kejahatan siber yang melibatkan teknologi *Deepfake* AI untuk menipu masyarakat. Penipuan ini dilakukan dengan sejumlah akun palsu yang menyerupai Gubernur Jawa Timur Khofifah Indar Parawansa, dengan memanfaatkan teknologi *Deepfake* untuk memanipulasi video yang kemudian disebarkan melalui media sosial. Teknologi AI digunakan untuk memodifikasi suara dan ekspresi wajah Gubernur agar terlihat autentik.

Dalam video manipulatif tersebut, para tersangka menawarkan sepeda motor dengan harga murah, yakni Rp500.000, seolah-olah merupakan program khusus dari Gubernur Jatim bagi warga Jawa Timur, lengkap dengan surat-surat resmi tanpa proses pembayaran di tempat (COD). Video-video tersebut diunggah ke platform media sosial TikTok. Polda Jawa Timur berhasil mengamankan tiga tersangka berinisial HMP (32 tahun), UP (24 tahun), dan AH (34 tahun), yang ketiganya merupakan warga Kabupaten Pangandaran, Jawa Barat . Selain mencatut nama Gubernur Jawa Timur, para pelaku juga menggunakan modus serupa untuk mencatut nama Gubernur Jawa Barat dan Gubernur Jawa Tengah . Kasus ini menjaring sekitar 100 orang korban yang tersebar di Jawa Timur, Jawa Barat, Jawa Tengah, dan Maluku Utara. Para pelaku menjalankan aksinya selama tiga bulan dan berhasil mengantongi keuntungan sebesar Rp87.600.000 Motif dari ketiga pelaku adalah murni untuk mendapatkan keuntungan pribadi. Ketiga pelaku tersebut diancam dengan : Kesatu, diancam pidana dalam Pasal 51 ayat (1) jo Pasal 35 Undang-Undang Nomor 11 tahun 2008 tentang informasi dan transaksi elektronik sebagaimana terakhir diubah dengan Undang-Undang Nomor 1 tahun 2024 tentang perubahan kedua atas Undang-Undang Nomor 11 tahun 2008 tentang informasi dan transaksi elektronik jo pasal 55 ayat (1) ke-1 KUHP. Kedua, Pasal 45A ayat (1) Jo Pasal 28 Ayat (1) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana terakhir diubah dengan Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik jo pasal 55 ayat (1) ke-1 KUHP. Ketiga, Sebagaimana diatur dan diancam pidana dalam Pasal 378 KUHP jo pasal 55 ayat (1) ke 1 KUHP.

Ketiga, kasus Dokter Tony yang menjadi korban *Deepfake* dalam iklan obat *Glucoformiin.* Iklan dilakukan dalam bentuk video dengan menggunakan wajah dr. Tony Setiobudi secara ilegal melalui teknologi *Deepfake* tanpa persetujuan dr.Tony, dengan seolah-olah dr.Tony memberikan testimoni medis. Pihak dr. Tony melalui kuasa hukumnya melaporkann kasus ini ke Diretsiber. Kasus ini sedang dalam tahap

penyidikan. Tindakan ini merupakan pelanggaran serius terhadap etika digital, reputasi profesional, serta ancaman terhadap kepercayaan publik.

Hambatan dalam kasus kejahatan teknologi *Deepfake* ini yakni karena sulitnya melacak pelaku, serta tidak dan dengan berkembangnya teknologi yang semakin canggih memberikan dampak pada keamanan data diri. Penyidikan kasus kejahatan *Deepfake* menghadapi berbagai hambatan kompleks yang bersumber dari keterbatasan teknis, regulasi. Salah satu hambatan utama adalah kesulitan dalam mengidentifikasi dan membuktikan keaslian atau manipulasi konten digital. Disisi lain, Diretsiber Polda Jawa Timur juga melakukan patroli siber. Yakni dengan memantau dan menindak terhadap kejahatan siber.

2. Hasil Wawancara dengan Korban Kejahatan *Deepfake*

a. Wawancara dengan Korban *Deepfake* Penipuan

Gambar 1.3 Wawancara dengan Korban Deepfake penipuan

Selain wawancara dengan penyidik Diretsiber, peneliti juga melakukan wawancara dengan salah satu korban penipuan *Deepfake* yakni ibu LDP (nama disamarkan) . Ibu LDP bertempat tinggal di Surabaya. Pada tahun 2025 ibu LDP mengalami penipuan melalui teknologi *Deepfake* dan menjadi salah satu saksi dalam kasus penipuan *Deepfake* bu Khofifah.

Kronologi terjadinya penipuan konten *Deepfake* bu Khofifah oleh ibu LDP ini diawali dari ibu LDP yang sering menonton video tiktok promosi menawarkan sepeda motor dengan harga murah, yakni Rp.500.000. Ibu LDP tergiur oleh video promosi yang isi komentarnya banyak membuktikan video promosi ini real dan banyak yang sudah mendapatkan motor dari pembelian tersebut. Sehingga ibu LDP mulai melakukan transaksi melalui link yang tertera di akun tiktok yang mempromosikan, dan tertera no rekening pelaku, kemudian setelah transfer ibu LDP diarahkan ke whatsap pelaku dan diminta untuk menyerahkan bukti transfer, kemudian ibu LDP mendapatkan pesan whatsap bahwa untuk pembelian motor tersebut dikenai pajak sebesar Rp.1.000.000.

Kemudian ibu LDP tetap membayar pajak tersebut dan konfirmasi ke whatsap sebelumnya. Namun setelah konfirmasi ke whatsap tersebut ibu LDP tidak menerima balasan apapun dari pelaku. Dari situ ibu LDP menyadari bahwa ia telah ditipu, dan ia mengiklaskan uang sebesar Rp.1.500.000. Namun pada sekitar bulan april ibu LDP mendapatkan pesan dari Polda Jawa Timur namun ibu LDP menghiraukan karena takut bahwa itu adalah salah satu trik pelaku penipuan. Sampai akhirnya ibu LDP mendapatkan pesan dari Polrestabes Surabaya menjelaskan perkara penipuan yang menimpa Ibu LDP. Dan Polrestabes Surabaya meminta Ibu LDP untuk berkenan diperiksa sebagai saksi. Dan ibu LDP juga dimintai keterangan pada saat persidangan. Namun hingga sekarang belum ada kabar terkait ganti rugi dari penipuan yang dialami oleh ibu LDP.

b. Wawancara dengan Korban Pelecehan *Deepfake*

Gambar 1.4 Wawancara dengan Korban Deepfake pelecehan

Peneliti juga melakukan wawancara kepada korban pelecehan *Deepfake*. Kejadian ini terjadi pada sekitar bulan Maret 2024. Korban berinisial GTA ini mengetahui foto nya menjadi kurang sopan melalui DM instagram yang dikirimkan oleh akun anonim. Namun, GTA bingung karena foto tersebut awalnya foto biasa namun dikirim oleh akun anonim tersebut menjadi foto seksi. GTA berusaha untuk bertanya kepada pelaku tersebut apa maunya sampai buat foto tidak senonoh itu. Namun, akun tersebut tidak membalas chat yang dikirimkan oleh GTA.

Pada saat itu GTA shock dan malu, tapi bingung harus melakukan apa. GTA takut foto tersebut tersebar ke media sosial. Namun, GTA memutuskan untuk tidak melaporkan kejadian ini ke pihak berwenang. GTA takut apabila polisi tidak percaya dengan kejadian yang menimpanya. Dan GTA juga dengar cerita kalau hal seperti ini dianggap sepele, dan GTA takut apabila pelaku balas dendam apabila dia melapor. GTA berharap ada tempat pengaduan khusus untuk perempuan yang benar-benar aman tanpa ada tekanan. Dan proses yang tidak menyudutkan korban.

1. Apakah dasar hukum yang digunakan penyidik di Polda Jawa Timur dalam menegakkan Tindak Pidana *Deepfake*?

Kemajuan teknologi di era digital saat ini berkembang dengan kecepatan yang pesat, sementara regulasi dan kerangka hukum yang mengaturnya bergerak jauh lebih lambat, menciptakan kesenjangan yang semakin lebar antara inovasi dan pengawasan. Fenomena ini terlihat jelas dalam berbagai sektor, mulai dari kecerdasan buatan yang mampu menghasilkan konten kreatif namun belum ada kepastian hukum mengenai hak cipta dan tanggung jawab atas kesalahan yang dibuatnya, hingga platform media sosial yang telah mengubah lanskap komunikasi global tetapi regulasi tentang penyebaran informasi palsu dan perlindungan data pengguna masih terus diperdebatkan. Ketimpangan ini menciptakan zona abu-abu yang berisiko, di mana perusahaan teknologi dapat beroperasi dengan pengawasan minimal hingga terjadi masalah serius yang merugikan masyarakat, baru kemudian pemerintah bereaksi dengan membuat aturan yang seringkali sudah terlambat. Akibatnya, masyarakat menjadi pihak yang paling rentan, terpapar berbagai risiko mulai dari pelanggaran privasi, manipulasi informasi, hingga dampak sosial-ekonomi yang belum terlindungi secara memadai oleh hukum yang ada.

Kemajuan teknologi juga di ikuti dengan kejahatan siber. Hal ini membuka peluang bagi berbagai modus kejahatan, mulai dari penipuan finansial dengan meniru suara seseorang untuk memerintahkan transfer dana, dan pencemaran nama baik tokoh publik melalui video palsu yang viral, hingga pornografi non-konsensual yang menempatkan wajah seseorang pada konten eksplisit tanpa izin. Dalam perspektif pertanggungjawaban pidana, penyebaran konten Deepfake mengandung unsur kesengajaan dan niat jahat (mens rea) apabila dilakukan untuk mencemarkan nama baik, menyebarkan pornografi, atau menipu orang lain.

Kerentanan ini semakin diperparah oleh minimnya regulasi khusus yang mengatur *Deepfake*, keterbatasan regulasi serta rendahnya kesadaran masyarakat akan eksistensi dan bahaya teknologi ini, sehingga banyak korban yang tidak menyadari dirinya telah menjadi sasaran manipulasi digital hingga dampaknya menyebar luas dan sulit untuk dikendalikan. Polda Jawa Timur memberikan ruang untuk pengaduan masyarakat atas kejahatan siber Menurut laporan pengaduan dari masyarakat terdapat data pengaduan tindak pidana siber sebagai berikut:

Tabel 1. 1 Data Jumlah Pengaduan Kejahatan Siber di Polda Jawa Timur

No.	Kejahatan Siber	Jumlah
1.	Penipuan Online (Penipuan Investasi, Penipuan Lotere, dan Hadiah)	14496

2.	Ancaman Kekerasan (Pemerasan Online)	8614
3.	Pencemaran Nama Baik	6556
4.	Ancaman Pencemaran (Doxxing, Pemerasan (mempermalukan)	3675
5.	Berita Bohong (Disinformasi, Misinformasi)	778
6.	Manipulasi Data Yang Tidak Sah	597
7.	Judi Online	220

Sumber : https;//patrolisiber.id

Dari data diatas, penyidik Polda Jawa Timur mengkasifikasikan *Deepfake* sebagai kejahatan manipulasi data. Dari kasus kejahatan siber ini penyidik di Polda Jawa Timur menggunakan beberapa dasar hukum dalam menegakkan tindak pidana *Deepfake*, meskipun Indonesia belum memiliki regulasi khusus yang mengatur teknologi kecerdasan buatan (AI) secara komprehensif. Dasar hukum yang digunakan penyidik dalam penegakan kasus kejahatan *Deepfake* adalah sebagai berikut:

1. Kasus pelecehan melalui *Deepfake* Nimas Sabella oleh Adi Pradita

Dalam kasus ini Adi Pradita dijerat dengan :

Undang-Undang Tindak Pidana Kekerasan Seksual Pasal 14 ayat (1) huruf b yakni, "Setiap Orang yang tanpa hak: Mentransmisikan informasi elektronik dan/atau dokumen elektronik yang bermuatan seksual di luar kehendak penerima yang ditujukan terhadap keinginan seksual, dan/atau"

a. Unsur Subjektif :

- Dengan sengaja : Pelaku secara sadar dan berulang kali mengirim konten seksual, membuat ribuan akun untuk menghindari pemblokiran menunjukkan niat yang jelas, teror selama 10 tahun menunjukkan kesengajaan sistematis dan terencana, pelaku mengakui mencintai korban dan melakukan perbuatan tersebut karena obsesinya.
- Tanpa hak : Tidak ada persetujuan atau consent dari korban,

b. Unsur Obyektif

- Setiap Orang : Adi adalah subjek hukum
- Mentransmisikan informasi elektronik dan/atau dokumen elektronik : Adi mengedit foto Nimas dengan menggabungkan wajah nimas dengan foto pornografi (*Deepfake* pelecehan), adi mengirimkan foto alat kelaminnya sendiri kepada Nimas, mengirim pesan-pesan bermuatan seksual melalui media sosial (X/Twitter, Instagram, WhatsApp).
- Yang Bermuatan Seksual : Foto editan vulgar (wajah korban di atas, foto pornografi di bawah), pesan-pesan yang berisi fantasi seksual terhadap tubuh korban, foto organ intim/kelamin pelaku

- Yang ditujukan terhadap keinginan seksual : Adi mengirim konten seksual dengan tujuan memuaskan hasrat seksualnya.

Undang-undang (UU) Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik (ITE), Pasal 45 ayat (1) Jo Pasal 28 Ayat (1) yakni, "Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan."

a. Unsur Subyektif
- Dengan sengaja : Pelaku sadar sepenuhnya atas perbuatannya, mengulangi perbuatan selama 10 tahun menunjukkan kesengajaan berkelanjutan, tidak ada unsur kealpaan atau ketidaksengajaan
- Tanpa hak : Bertentangan dengan kehendak korban yang sudah menolak berkali-kali

b. Unsur Obyektif
- Setiap orang : Adi Pradita adalah subjek hukum
- Mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik : Mengirim langsung foto kelamin dan pesan seksual ke Nimas, Menyebarkan melalui berbagai platform (X, Instagram, WhatsApp)
- Yang memiliki muatan yang melanggar kesusilaan : Foto editan wajah korban dengan konten pornografi
- Untuk diketahui umum : Meskipun foto dikirim pribadi, namun ada juga postingan publik tentang obsesinya

2. Kasus penipuan konten *Deepfake* Gubernur Jawa Timur

Dalam hal ini pelaku dijerat dengan :

Kesatu, Pasal 51 ayat (1) jo Pasal 35 UU ITE jo Pasal 55 ayat (1) ke-1 KUHP yakni "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." ancaman pidana: penjara paling lama 12 tahun dan/atau denda paling banyak Rp 12 miliar.

a. Unsur Subjektif
- Dengan Sengaja : Pelaku menghendaki dan mengetahui bahwa ia sedang melakukan manipulasi informasi elektronik, Ada kesadaran penuh bahwa perbuatannya melawan hukum
- Dengan Tujuan Tertentu : Pelaku memiliki tujuan spesifik agar informasi/dokumen elektronik yang dimanipulasi dianggap seolah-olah data yang autentik, Niat agar orang lain percaya bahwa konten *Deepfake* tersebut adalah asli, Kehendak untuk menyesatkan publik

b. Unsur Objektif

- Setiap Orang (Subjek Hukum) : Pelaku adalah orang/badan hukum yang dapat dimintai pertanggungjawaban pidana
- Manipulasi, Penciptaan,Perubahan,Penghilangan,Pemindahan : Membuat video/foto dengan teknologi AI/*Deepfake*, Mengambil wajah Ibu Khofifah dan menempatkannya pada tubuh/situasi lain, Menggunakan software/aplikasi manipulasi gambar/video.
- Seolah-olah data yang otentik : Informasi/dokumen elektronik tersebut seolah-olah menjadi data yang autentik, Orang lain terkecoh dan menganggap konten *Deepfake* sebagai konten asli, Tercipta persepsi keliru di masyarakat.

Pasal 55 ayat (1) ke-1 KUHP yakni "Mereka yang melakukan, menyuruh melakukan, dan turut serta melakukan perbuatan."

a. Unsur-Unsur

- Mereka yang melakukan : pelaku utama yang langsung membuat *deepfake* (Hendrik Miftah Parid mengajarkan untuk membuat edit video *deepfake)*
- Yang Menyuruh melakukan : Bahwa terdakwa Hendrik Miftah Parid bekerjasama dengan Saksi Agus Herawan yang mempunyai tugas mengelola akun whatsapp yang di upload di bio tiktok
- Turut serta melakukan perbuatan : 3 pelaku tersebut bersama-sama melakukan penipuan dengan tugas yang sudah mereka bagi masing-masing.

Kedua, Pasal 45A ayat (1) Jo Pasal 28 Ayat (1) " Setiap Orang dengan sengaja mendistribusikan dan/atau mentransmisikan Informasi Elektronikdan/ atau Dokumen Elektronik yang berisi pemberitahuan bohong atau informasi menyesatkan yang mengakibatkan kerugian materiel bagi konsumen dalam Transaksi Elektronik. "

a. Unsur Subjektif

- Dengan Sengaja : Pelaku dengan sengaja membuat dan menyebarkan video *deepfake* tersebut

b. Unsur Obyektif

- Mendistribusikan dan/atau Mentransmisikan Informasi Elektronik dan/atau Dokumen Elektronik : Pelaku menyebarkan video *deepfake* tersebut di sosial media
- Berisi Pemberitahuan Bohong atau Informasi Menyesatkan: Video tersebut berisi informasi palsu/bohong seolah-olah Gubernur Khofifah memberikan pernyataan atau instruksi tertentu
- Mengakibatkan Kerugian Materiel bagi Konsumen dalam Transaksi Elektronik : Korban sebagai konsumen dalam transaksi elektronik percaya pada konten deepfake, korban mengalami kerugian finansial

Ketiga, Pasal 378 KUHP jo Pasal 55 ayat (1)) ke 1 KUHP yakni "Barang siapa dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum, dengan memakai nama palsu atau martabat

palsu, dengan tipu muslihat, ataupun rangkaian kebohongan, menggerakkan orang lain untuk menyerahkan barang sesuatu kepadanya, atau supaya memberi hutang maupun menghapuskan piutang, diancam karena penipuan dengan pidana penjara paling lama 4 tahun." Dan Pasal 55 ayat (1) ke 1 KUHP yakni "Mereka yang melakukan, menyuruh melakukan, dan turut serta melakukan perbuatan"

a. Unsur Subjektif Pasal 378 KUHP

- Dengan Maksud : Pelaku memiliki maksud untuk menguntungkan diri sendiri atau orang lain ,Niat untuk memperoleh keuntungan secara melawan hukum (tidak sah)
- Kesengajaan : Pelaku sengaja menggunakan tipu muslihat/rangkaian kebohongan, Menghendaki agar korban tergerak untuk menyerahkan sesuatu (uang, barang, atau memberikan utang)

b. Unsur Objektif

- Barang Siapa (Setiap Orang) : Pelaku sebagai subjek hukum
- Memakai nama palsu/martabat palsu/tipu muslihat/rangkaian kebohongan : Menyamar sebagai Gubernur Jawa Timur melalui konten *Deepfake*, Menempatkan diri seolah-olah memiliki kedudukan/jabatan tertentu

a. Unsur Subyektif pasal 55 ayat (1) ke-1 KUHP

- Kesengajaan: Menyadari bahwa perbuatan tersebut merupakan rangkaian tipu muslihat, kebohongan, atau rangkaian perbuatan yang menyesatkan korban

b. Unsur Obyektif pasal 55 ayat (1) ke-1 KUHP

- Mereka yang melakukan : pelaku utama yang langsung membuat rencana untuk melakukan penipuan melalui video deepfake gubernur khofifah
- Yang Menyuruh melakukan : Bahwa pelaku memerintahkan rekannya yang lain untuk membantu dalam melakukan penipuan
- Turut serta melakukan perbuatan : 3 pelaku tersebut bersama-sama melakukan penipuan dengan tugas yang sudah mereka bagi masing-masing.

Penerapan berbagai peraturan perundang-undangan oleh Polda Jawa Timur merupakan langkah progresif dalam memberantas kejahatan deepfake, dan diharapkan dapat menjadi model penegakan hukum yang efektif sekaligus mendorong lahirnya regulasi yang lebih adaptif terhadap dinamika kejahatan siber di masa mendatang.

Akan tetapi, peneliti bertanggapan bahwa Undang-undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi juga dapat digunakan dalam menjerat pelaku, terlebih pada Pasal 66 Jo Pasal 68 Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi " 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. ” paling tama 6 (enam) tahun dan/atau pidana denda paling banyak Rp6.000. 000.000,00 (enam miliar rupiah). Pasal ini dapat digunakan untuk tindak pidana kejahatan *deepfake.* Maka peneliti akan menguraikan sedikit dari unsur subyektif dan obyektif pasal 66 UU PDP dari dua kasus yang telah disebutkan diatas sebagai berikut:

Dalam kasus pelecehan Nimas Sabela jika dikaitkan dengan pasal 66 UU PDP adalah sebagai berikut :

a. Unsur Subyektif
- Dengan Maksud untuk Menguntungkan Diri Sendiri atau Orang Lain : Adi Pradita dengan sadar menjadikan korban sebagai objek pelecehan dengan mengedit foto korban menjadi tidak senonoh.

b. Unsur Obyektif
- Setiap Orang : Adi Pradita merupakan (Subjek Hukum)
- Membuat Data Pribadi Palsu atau Memalsukan Data Pribadi : Mengedit foto korban tanpa seizin korban, untuk memuaskan nafsu pelaku
- Yang Dapat Mengakibatkan Kerugian bagi Orang Lain : Korban mengalami teror dari Adi Pradita dan mengalami rasa malu, serta merasa tidak aman atas privasoi korban.

Dalam kasus penipuan deepfake Gubernur Khofifah jika dikaitkan dengan pasal 66 UU PDP adalah sebagai berikut :

a. Unsur Subyektif :
- Dengan Maksud untuk Menguntungkan Diri Sendiri atau Orang Lain : Pelaku secara sadar membuat atau memalsukan data pribadi Gubernur Khofifah berupa wajah, suara, identitas, atau citra diri melalui teknologi deepfake, bertujuan memperoleh keuntungan finansial.

b. Unsur Obyektif :
- Setiap Orang : Pelaku merupakan Subjek Hukum
- Membuat Data Pribadi Palsu atau Memalsukan Data Pribadi : Rekayasa wajah dan suara Gubernur Khofifah sehingga seolah-olah menyampaikan pernyataan, memanipulasi data pribadi sehingga menimbulkan kesan bahwa informasi atau instruksi tersebut benar-benar berasal dari yang bersangkutan
- Yang Dapat Mengakibatkan Kerugian bagi Orang Lain : Korban yang telah menjadi korban penipuan ini mengalami kerugian materil, dan Gubernur Khofifah mengalami kerugian berupa pencemaran nama baik, rusaknya reputasi, dan terganggunya hak atas perlindungan data pribadinya

Diatas adalah unsur-unsur yang dapat terpenuhi apabila menggunakan Undang-Undang Perlindungan Data Pribadi jika digunakan untuk menjerat

pelaku dengan ancaman pidana penjara paling tama 6 (enam) tahun dan/atau pidana denda paling banyak Rp6.000. 000.000,00 (enam miliar rupiah).

Keefektifan suatu penegak hukum bergantung pada keberhasilan dalam pelaksanaanya dan memastikan fungsi hukum berjalan optimal bagi masyarakat, serta aparat penegak hukum dapat memberikan sanksi yang sesuai dengan peraturan. Menurut Soerjono Soekanto, terdapat berbagai faktor yang menjadi penentu efektivitas hukum, meliputi:

a.Faktor Hukum

Dalam praktiknya, Polda Jawa Timur masih menghadapi benturan antara kepastian hukum dan keadilan. Kepastian hukum bersifat nyata dan terukur, sedangkan keadilan bersifat ideal serta bergantung pada penilaian moral. Kelemahan regulasi yang mengatur *Deepfake* di Indonesia masih terdapat kekosongan hukum yang dapat menghambat penegakan hukum.

b. Faktor Penegak Hukum

Kapasitas dan komptensi personil Polda Jawa Timur sudah mencakup pemahaman teknis tentang teknologi AI, kemampuan digital forensik dalam menangani kejahatan siber berbasis *Deepfake.*

c. Faktor sarana atau Fasilitas Hukum

Ketersediaan infrastruktur teknologi software deteksi *Deepfake*, perangkat keras yang memadai, sistem database kejahatan siber untuk menangani kasus *Deepfake* serta anggaran biaya yang cukup mahal untuk proses pelacakan yang jauh diluar jawa. Polda Jawa Timur berusaha untuk terus meningkatkan teknologi yang dapat digunakan untuk pembuktian.

d. Faktor Masyarakat

Tingkat kesadaran masyarakat yang masih minim akan kejahatan siber ini yang menjadi fokus utama.

e. Faktor Kebudayaan

Persepsi masyarakat terhadap kejahatan *Deepfake* apakah *Deepfake* dianggap sebagai kejahatan serius. Dan stigma terhadap korban *Deepfake* yang dapat mempengaruhi pelaporan kasus.

Polda Jawa Timur masih menghadapi beberapa tantangan meliputi pembuktian dalam kejahatan siber skala transnasional (antar negara). Walaupun penyidik sudah memiliki payung hukum untuk menjerat pelaku kejahatan *Deepfake*, namun di sisi lain penyidik masih kesulitan dalam mengkualifikasikan kejahatan ini kedalam undang-undang yang telah ada, karena instrumen hukum yang tersedia belum cukup akomodatif. Penyidik masih gamang dalam menentukan pasal yang tepat untuk menjerat pelaku penyebaran *Deepfake.* Dan Penyidik harus membuktikan secara kompleks dalam membuktikan Niat pelaku (mens rea), keaslian atau manipulasi

konten menggunakan teknologi digital forensik, dampak kerugian materil, dan immateril. Hal ini menyebabkan banyak kasus yang tidak sampai pada tahap peradilan atau dihentikan di tahap penyelidikan karena kesulitan dalam pembuktian. Sebagai responns terhadap tantangan tersebut, maka dibutuhkan pengaturan khusus dalam hukum pidana Indonesia yang tidak hanya bersifat reaktif tetapi juga preventif.

2. Bagaimana upaya Polda Jawa Timur dalam menanggulangi tindak pidana *Deepfake*?

Perlindungan hukum bagi masyarakat sebagai bentuk tindakan pemerintah dibedakan menjadi dua bentuk, yakni: perlindungan hukum preventif, dan perlindungan hukum represif.

Polda Jawa Timur menjalankan kedua fungsi perlindungan hukum tersebut, baik melalui upaya pencegahan dengan melakukan edukasi dan sosialisasi kepada masyarakat tentang bahaya Deepfake, maupun melalui upaya penindakan dengan melakukan penyidikan dan penangkapan terhadap pelaku kejahatan Deepfake.

Upaya Preventif yang dilakukan oleh Polda Jawa Timur dalam menanggulangi tindak pidana *Deepfake* ini dengan membentuk unit khusus *cyber crime*. Polri membentuk Ditressiber yang kini telah ada di Polda Jawa Timur, ini merupakan langkah strategis untuk menanggulangi kejahatan siber di tengah perkembangan teknologi yang cepat.

Dalam menjalankan tugasnya, unit khusus cyber crime membentuk program yang disebut Patroli Siber. Patroli Siber bertugas untuk memelihara keamanan warganet di ruang siber. Patroli siber melakukan pengawasan, penecegahan dan penindakan segala bentuk kejahatan siber. Patroli siber juga melakukan edukasi masyarakat terkait macam-macam kejahatan siber, seperti seminar, workshop, dan kampanye informasi agar warganet tidak menjadi korban apalagi terjerumus menjadi pelaku kejahatan siber.

Dan Polda Jawa Timur selalu melakukan upaya terhadap pencegahan kejahatan siber dengan memanfaatkan kemajuan teknologi untuk memberikan edukasi melalui beberapa platform yakni instagram Polda Jawa Timur, dan tiktok Siber Polda Jawa Timur & Humas Polda Jawa Timur. Dan Polda Jawa Timur memberikan pelatihan cyber forensic dan cyber investigation dan membentuk tim-tim khusus yang dapat menangani masalah transaksi elektronik dan kejahatan siber. Dan tim-tim ini bekerja sama dengan Dinas Kominfo dan lembaga terkait lainnya untuk memantau dan menganalisis aktivitas kejahatan digital. Polda Jawa Timur juga menggunakan teknologi modern dengan menggunakan perangkat lunak analisis data, forensic digital, dan jaringan intelijen untuk melacak dan menangkap pelaku kejahatan. Dengan teknologi ini memungkinkan untuk mendeteksi pola kejahatan dan mengambil tindakan cepat.

Dan pengaduan tentang kejahatan siber bisa dilakukan melalui website patrolisiber.id dengan memberikan informasi yang komprehensif untuk penyelidikan menyeluruh dengan menyertakan detail seperti: Kronologi Kejadian, Detil Pelaku, serta Bukti Digital seperti layar tangkap, dokumen ataupun buktu transaksi dan file apapun yang relevan.

Upaya represif yang dilakukan Polda Jawa Timur melalui beberapa tahapan yakni, dimulai dari proses penyelidikan untuk mengumpulkan bukti-bukti, kemudian dilanjutkan dengan penyidikan untuk mengungkapkan modus operandi pelaku dalam membuat dan menyebarkan konten deepfake. Dalam pelaksanaannya, penyidik menerapkan ketentuan hukum yang telah dijabarkan sebelumnya, dengan menyesuaikan pasal-pasal yang relevan beradasarkan modus dan dampak kejahatan yang dilakukan. Kemudian, proses ini dilanjutkan dengan penangkapan pelaku, pengumpulan alat bukti digital melalui digital forensik, hingga penyerahan berkas perkara kepada kejaksan.

C. KESIMPULAN

Berdasarkan hasil penelitian dan pembahasan, maka dapat disimpulkan sebagai berikut:

1. Dasar hukum yang digunakan penyidik di Polda Jawa Timur dalam menegakkan Tindak Pidana *Deepfake* yakni:
    1. Undang-Undang Tindak Pidana Kekerasan Seksual Pasal 14 ayat (1) huruf b
    2. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE), Pasal 45 ayat (1) Jo Pasal 27 Ayat (1)
    3. Pasal 51 ayat (1) jo Pasal 35 Undang-Undang Nomor 11 tahun 2008 tentang informasi dan transaksi elektronik jo pasal 55 ayat (1) ke-1 KUHP
    4. Pasal 45A ayat (1) Jo Pasal 28 Ayat (1) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik jo pasal 55 ayat (1) ke-1 KUHP
    5. Pasal 378 KUHP jo pasal 55 ayat (1) ke 1 KUHP

    Namun menurut peneliti, dari dasar hukum yang telah digunakan bisa ditambahkan dengan Pasal 66 Jo Pasal 68 Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.
2. Upaya Polda Jawa Timur dalam menanggulangi tindak pidana *Deepfake* dengan dua cara yakni upaya preventif dan upaya represif. Upaya preventif berupa sosialisasi dan edukasi, serta memberikan ruang kepada masyarakat untuk melakukan pengaduan melalui patrolisiber.id. Kemudian upaya represif Polda Jawa Timur memproses pelaku tindak pidana secara profesional dan prosedural sesuai dengan ketentuan KUHAP, mulai dari tahap penyelidikan, penyidikan, penangkapan, hingga penyerahan berkas perkara kepada kejaksaan.

D. SARAN

Berdasarkan hasil penelitian dan pembahasan, maka saran yang diberikan oleh peneliti sebagaiberikut:

1. Perlu segera dibentuk regulasi khusus atau peraturan turunan yang secara eksplisit mengatur tentang teknologi *Deepfake* dan kejahatan siber berbasis kecerdasan buatan (AI). Regulasi yang memuat tentang definisi *Deepfake*, unsur unsur tindak pidana, mekanisme pembuktian digital forensik, serta sanksi yang tegas dan proposional.
2. Meningkatkan kapasitas dan kompetensi penyidik melalui pelatihan berkala mengenai teknologi *Deepfake*, digital forensik, dan teknik investigasi cyber crime yang mutakhir. Pelatihan ini dapat dilakukan melalui kerja sama dengan lembaga riset, universitas, atau institusi internasional yang memiliki keahlian di bidang keamanan siber. Melengkapi sarana dan prasarana penunjang investigasi *Deepfake*, seperti pengadaan software deteksi *Deepfake* yang canggih, peningkatan kapasitas laboratorium forensik digital, serta alokasi anggaran memadai untuk operasional unit cyber crime. Memperkuat koordinasi dan sinergi dengan instansi terkait seperti Kementerian Komunikasi dan Informatika, Badan Siber dan Sandi Negara (BSSN), kejaksaan, dan lembaga penegak hukum lainnya dalam penanganan kasus *Deepfake*, terutama untuk kasus yang bersifat lintas wilayah atau lintas negara.
3. Membangun kesadaran untuk tidak turut menyebarkan konten *Deepfake* yang diterima melalui media sosial atau platform digital lainnya, serta melakukan verifikasi terlebih dahulu sebelum membagikan informasi atau konten visual yang meragukan.

REFERENSI

Dahlan, Universitas Ahmad. 2025. "Disinformasi Dan Deepfake Dalam Konteks Artificial Intelligence." *Https://Lldikti5.Kemdikbud.Go.Id/*. Retrieved (https://lldikti5.kemdikbud.go.id/home/detailpost/dikabarin-bem-fh-uad-disinformasi-dan-deepfake-dalam-konteks-artificial-intelligence).

Geby, Noviana. 2023. "Masyarakat Diminta Sikapi Ancaman Deepfake Image Secara Bijak." *Rri.Co.Id*. Retrieved (https://rri.co.id/nasional/332374/masyarakat-diminta-sikapi-ancaman-deepfake-image-secara-bijak).

Habib, M. 2024. "Remaja Di Gresik Yang Edit Foto Temannya Jadi Telanjang Pakai AI Terancam Pidana 6 Tahun Penjara." *Tvonenews.Com*. Retrieved (https://www.tvonenews.com/daerah/jatim/227903-remaja-di-gresik-yang-edit-foto-temannya-jadi-telanjang-pakai-ai-terancam-pidana-6-tahun-penjara).

Kewarganegaraan, Jurnal, Muhammad Anthony Aldriano, Mas Agus Priyambodo, and Jakarta Pusat. 2022. "Cyber Crime Dalam Sudut Pandang Hukum Pidana." 6(1):2169–75.

Medgo. 2025. "Wajah Dipalsukan AI: Siapa Yang Bertanggung Jawab Secara Hukum?" *Https://Medgo.Id/*. Retrieved (https://medgo.id/wajah-dipalsukan-ai-siapa-yang-bertanggung-jawab-secara-hukum/).

Melati, Dwi Putri. 2022. "CYBER TERORGANISIR." 01(1):94–100.

Puspoayu, Elisabeth Septin, Dian Ayu Larasati, Iman Pasu Marganda H. P., Graciela Natasha Tessalonica Lektonpessy, and Laily Wahyuningtyas Putri Hariono. 2022. "The Understanding of Universitas Negeri Surabaya Students of Sexual Violence on Campus." *Proceedings of the International Joint Conference on Arts and Humanities 2021 (IJCAH 2021)* 618(Ijcah):516–19. doi: 10.2991/assehr.k.211223.090.

Putih, Forum Merah. 2024. "Dirreskrimsus Polda Jatim Siap Perangi Cybercrime!" *Kompasiana.Com*. Retrieved (https://www.kompasiana.com/forummerahputih/671a030434777c69ff3fe532/dirreskrimsus-polda-jatim-siap-perangi-cybercrime).

siplawfirm. 2025. "Pidana Atas Konten Deepfake, Tantangan Baru Penegakan Hukum Di Era AI." *Https://Siplawfirm.Id/*. Retrieved (https://siplawfirm.id/konten-deepfake/?lang=id).

UINSSC, Siti Aisyah Zulfa –. Relawan PKBH. 2025. "Wajahku, Suaraku, Tapi Bukan Aku? Tantangan Hukum Terhadap Deepfake Dan Manipulasi Identitas Digital." *Https://Pkbh.Uinssc.Ac.Id/*. Retrieved (https://pkbh.uinssc.ac.id/wajahku-suaraku-tapi-bukan-aku-tantangan-hukum-terhadap-deepfake-dan-manipulasi-identitas-digital/).