

## **Integrasi Upaya Penal dan Non-Penal oleh Kepolisian dalam Menanggulangi Penipuan Berbasis Deepfake: Studi Kasus di Polres Metro Jakarta Pusat**

**Kayla Azzahra<sup>1</sup> Deni Achmad<sup>2</sup> Muhammad Farid<sup>3</sup> Maya Shafira<sup>4</sup> Refi Meidiantama<sup>5</sup>**  
Program Studi Ilmu Hukum, Fakultas Hukum, Universitas Lampung, Kota Bandar Lampung,  
Provinsi Lampung, Indonesia<sup>1,2,3,4,5</sup>  
Email: [kaylaazzahra3008@gmail.com](mailto:kaylaazzahra3008@gmail.com)<sup>1</sup> [deni.achmad@fh.unila.ac.id](mailto:deni.achmad@fh.unila.ac.id)<sup>2</sup> [farid@unila.ac.id](mailto:farid@unila.ac.id)<sup>3</sup>  
[maya.shafira@unila.ac.id](mailto:maya.shafira@unila.ac.id)<sup>4</sup> [refitama21@gmail.com](mailto:refitama21@gmail.com)<sup>5</sup>

### **Abstrak**

Penipuan melalui modus *deepfake scam* sudah sering terjadi, salah satu kasus penipuan melalui modus *deepfake scam* ini melibatkan kepala negara Republik Indonesia yaitu Prabowo Subianto, pelaku menggunakan wajah Prabowo Subianto untuk mendapat keuntungan materiil. Permasalahan dalam penelitian ini adalah: upaya penanggulangan oleh kepolisian tindak pidana penipuan melalui modus *deepfake* serta faktor yang mempengaruhi kepolisian dalam penanggulangan kejahatan penipuan melalui modus *deepfake*. Hasil penelitian dan pembahasan menunjukkan bahwa penanggulangan kejahatan *deepfake scam* oleh kepolisian melalui pendekatan penal dan non-penal. Secara penal, kepolisian fokus pada penegakan hukum yang tegas mulai dari penyelidikan hingga penerapan sanksi pidana berdasarkan undang-undang untuk menciptakan efek jera bagi pelaku. Sementara secara non-penal, upaya difokuskan pada edukasi dan sosialisasi guna meningkatkan kesadaran hukum masyarakat serta memperkuat kolaborasi dengan berbagai pihak terkait dalam menangani ancaman tersebut. Faktor utama kepolisian dalam memberantas *deepfake scam* terletak pada aspek aparat penegak hukum dan masyarakat. Keterbatasan kualitas serta kuantitas SDM kepolisian dalam menguasai kompetensi teknis menjadi kendala serius, yang diperburuk oleh rendahnya literasi digital dan edukasi hukum masyarakat terhadap modus kejahatan ini.

**Kata Kunci:** Penanggulangan Kejahatan, *Deepfake*, Kepolisian, *Cyber Crime*



This work is licensed under a [Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License](https://creativecommons.org/licenses/by-nc-sa/4.0/).

### **PENDAHULUAN**

Teknologi informasi (TI) menempati posisi strategis di era globalisasi karena kemampuannya menghapus batasan geografis dan waktu, sekaligus meningkatkan produktivitas dan efisiensi. Teknologi informasi telah merubah pola hidup masyarakat secara global dan menyebabkan perubahan sosial budaya, ekonomi, dan kerangka hukum yang berlangsung secara cepat dengan signifikan. Teknologi Informasi bagaikan pedang bermata dua, karena selain memberikan kontribusi bagi peningkatan kesejahteraan, kemajuan, dan peradaban manusia, sekaligus menjadi sarana efektif perbuatan melawan hukum. (Nugraha, 2012) Penggunaan teknologi internet menjadikan banyak masalah kompleks dapat diselesaikan secara efektif dan efisien. Selain itu, kecanggihan teknologi menjadikan Masyarakat memiliki kecenderungan untuk melakukan Tindakan-tindakan yang bertentangan dengan norma-norma sosial yang sudah ada. Dengan pemanfaatan teknologi internet, terciptalah masyarakat dunia baru yang tidak lagi dihalangi oleh batas-batas teritorial suatu negara yang dahulu ditetapkan sangat esensial sekali, yaitu dunia maya dunia yang tanpa batas, realitas virtual (*virtual reality*). Inilah yang sebenarnya dimaksud dengan *Borderless World*. (Pura dalam Rahardjo, 2012 : 5) *Deepfake* adalah karya sintesis yang telah dimanipulasi secara digital untuk menggantikan wajah atau tubuh seseorang dengan sangat meyakinkan sehingga tampak seperti orang lain. (Payne, 2025). *Deep learning*, pada dasarnya, adalah teknik yang digunakan untuk melatih kecerdasan buatan atau AI (*Artificial intelligence*) agar dapat mengeksekusi tugas tertentu. Dalam konteks *deepfake*, *deep learning* memainkan peran penting

dalam menghasilkan manipulasi yang sangat realistis pada gambar dan video. *Deepfake* adalah istilah yang digunakan untuk algoritma teknik pemrosesan video yang memungkinkan pengguna untuk mengganti wajah satu aktor dengan wajah aktor lain dalam video dengan tingkat keaslian gambar yang tinggi yakni meniru objek visual yang nyata. Meskipun tampak nyata, *deepfake* sebenarnya tidak asli. Selain dalam bentuk video, teknologi *deepfake* juga dapat digunakan untuk merekayasa gambar.

Permasalahan yang berkaitan dengan teknologi *deepfake* menjadi semakin serius setelah munculnya aplikasi yang dikenal dengan nama *FakeApp* pada bulan Januari 2018. *FakeApp* merupakan sebuah aplikasi yang dapat diakses oleh siapa saja, yang memungkinkan pengguna untuk menciptakan gambar dan klip video yang tidak asli. Ketakutan akan potensi penyalahgunaan dan dampak negatif dari penggunaan aplikasi ini telah meningkat seiring dengan kemudahan penggunaannya. Penyalahgunaan teknologi *deepfake* ini memunculkan tantangan serius dalam konteks hukum dan etika. Berdasarkan jenis kejahatan tersebut merujuk pada ketentuan dalam Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, atau Pasal 378 Kitab Undang-undang Hukum Pidana (KUHP) tentang Penipuan. Lembaga penegak hukum merupakan Lembaga penegak keadilan dalam suatu masyarakat, Lembaga di mana masyarakat memerlukan dan mencari suatu keadilan. (Rizki H & Fathonah, 2014: 1). Kepolisian Negara Republik Indonesia (POLRI) adalah salah satu lembaga penegak hukum yang bertanggung jawab langsung di bawah Presiden. Tugas pokok Polri diatur dalam Undang-Undang Nomor 2 Tahun 2002 tentang Kepolisian Negara Republik Indonesia antara lain memelihara keamanan dan ketertiban masyarakat, menegakkan hukum, dan memberikan perlindungan, pengayoman, dan pelayanan kepada masyarakat.

Contoh kasus terjadi baru-baru ini pada tahun 2025, Pejabat negara seperti Presiden Prabowo dan Menteri Keuangan Sri Mulyani telah menjadi korban kejahatan *deepfake* yang dilakukan oleh JS berusia 25 Tahun, melalui modus operandinya adalah mengunggah dan menyebarkan video di media sosial menggunakan *deepfake*, dengan foto dan suara yang dibuat seolah-olah pemerintah menawarkan bantuan kepada Masyarakat, dengan mencantumkan nomor WhatsApp tersangka. "Pada tanggal 4 Februari 2025 penyidik berhasil mengamankan tersangka inisial JS, 25 tahun yang bekerja sebagai buruh harian lepas di Kabupaten Pringsewu, Provinsi Lampung," kata Bayu Aji dalam konferensi pers di Polres Metro Jakarta Pusat, Jumat, 7 Februari 2025. Dan saat ini Polri terus mendalami kasus ini. Terutama mengungkapkan sindikat mereka. Kemudian, mencari aktor intelektual di balik kasus penipuan yang meresahkan Masyarakat tersebut. (Hukmana, 2025).

Mengingat kasus-kasus kejahatan siber di Indonesia masih terus ada, maka kepolisian sebagai gerbang keadilan masyarakat yang memiliki tujuan untuk mewujudkan keamanan dalam negeri meliputi terpeliharanya keamanan dan ketertiban masyarakat, tertib dan tegaknya hukum, terselenggaranya perlindungan, pengayoman, dan pelayanan masyarakat, serta terbinanya ketenteraman masyarakat dengan menjunjung tinggi hak asasi manusia diharapkan memiliki terobosan baru dalam menanggulangi kejahatan penipuan melalui modus *deepfake*. Berdasarkan fenomena kasus yang terjadi di Jakarta Pusat dan Kabupaten Pringsewu bahwasanya tindak pidana penipuan Online sudah berada ditingkat yang mengkhawatirkan. Sehingga perlu mengetahui upaya penanggulangan oleh kepolisian dan faktor penghambat upaya penanggulangan agar kejahatan tersebut dapat ditekan dan supaya kejahatan di media sosial yang mengatasnamakan pihak lain tidak terulang kembali. Berdasarkan uraian latar belakang diatas, maka penulis tertarik untuk melakukan penelitian yang berjudul: "Integrasi Upaya Penal dan Non-Penal oleh Kepolisian dalam Menanggulangi Penipuan Berbasis *Deepfake*: Studi Kasus di Polres Metro Jakarta Pusat".

## **HASIL PENELITIAN DAN PEMBAHASAN**

### **Upaya Kepolisian Dalam Penanggulangan Kejahatan Penipuan Melalui Modus *Deepfake Scam***

Hukum adalah aturan-aturan, baik yang tertulis maupun tidak, yang berisi norma-norma dan sanksi-sanksi yang bertujuan untuk mengatur kehidupan masyarakat. Negara hukum wajib menghormati dan menjalankan hukum, agar tercipta rasa aman dan nyaman dalam masyarakat. Dalam hidup bermasyarakat, kita selalu terikat oleh nilai-nilai yang mengatur perilaku kita, salah satunya adalah norma hukum. Selain itu, masalah kriminal seperti penipuan dengan cara *deepfake* juga menjadi perhatian. Hukum positif adalah sejumlah prinsip dan aturan hukum yang berlaku saat ini, berbentuk lisan atau tulisan. Aturan hukum tersebut berlaku secara khusus dan umum serta ditegakkan oleh lembaga peradilan atau pemerintah di dalam suatu negara. Meskipun hukum positif yang dibicarakan ini berlaku pada masa kini, tidak berarti mengabaikan hukum yang berlaku di masa lalu. Setiap negara pasti memiliki hukum yang diharapkan atau digunakan untuk mendukung perkembangan masyarakat. Hukum positif adalah sejumlah prinsip dan aturan hukum yang berlaku saat ini, berbentuk lisan atau tulisan. Aturan hukum tersebut berlaku secara khusus dan umum serta ditegakkan oleh lembaga peradilan atau pemerintah di dalam suatu negara. Meskipun hukum positif yang dibicarakan ini berlaku pada masa kini, tidak berarti mengabaikan hukum yang berlaku di masa lalu. Setiap negara pasti memiliki hukum yang diharapkan atau digunakan untuk mendukung perkembangan masyarakat. (Apeldoorn, 2001: 11)

Hukum yang berlaku terus berubah dan berkembang seiring berjalannya waktu. Perkembangan zaman, yang sering disebut modernisasi, mengubah banyak hal dalam kehidupan masyarakat, terutama nilai-nilai dan budaya yang dimiliki. Seiring dengan berkembangnya masyarakat, jenis tindak kriminal dan kejahatan juga mengalami perubahan. Demikian pula dengan peraturan hukum pidana yang terus diperbarui. Kebijakan atau upaya mengatasi kejahatan sebenarnya merupakan bagian yang tidak terpisahkan dari upaya melindungi masyarakat dan upaya mencapai kesejahteraan bagi masyarakat. (Hamdan, 1999) Kebijakan penanggulangan kejahatan atau disebut juga politik kriminal bertujuan utama untuk melindungi masyarakat agar dapat mencapai kesejahteraan yang lebih baik. (Ucuk, 2020: 169) Kebijakan penanggulangan kejahatan merupakan bagian dari kebijakan penegakan hukum. Kebijakan penegakan hukum termasuk dalam kebijakan sosial dan juga bagian dari kebijakan legislatif. Secara hakikat, politik kriminal adalah bagian yang tidak terpisahkan dari kebijakan sosial, yaitu upaya mencapai kesejahteraan sosial.

Penanggulangan pidana adalah upaya mengatasi kejahatan dengan memberikan sanksi kepada pelaku berupa sarana pidana (penal) atau bukan hukum pidana (non penal), yang bisa digabungkan bersama-sama. Pendekatan penal bertujuan memberi sanksi kepada pelaku melalui cara pidana, sedangkan pendekatan non penal berfokus pada pencegahan sebelum kejahatan terjadi. Kedua cara ini bisa saling melengkapi untuk membuat kebijakan hukum yang sesuai dengan kebutuhan masyarakat dan aturan yang berlaku. Suyudi mengatakan bahwa kebijakan kriminal atau kebijakan penanggulangan kejahatan, jika dilihat dari cakupannya, sangat luas dan memiliki tingkat kompleksitas yang tinggi. Ini wajar karena pada dasarnya kejahatan merupakan masalah kemanusiaan sekaligus masalah sosial yang membutuhkan pemahaman khusus. Kejahatan sebagai masalah sosial adalah gejala yang terus berkembang dan berkaitan dengan berbagai gejala serta struktur masyarakat yang sangat kompleks, sehingga termasuk dalam masalah sosial-politik. Salah satu bentuk perencanaan perlindungan sosial adalah upaya rasional yang dilakukan masyarakat untuk mengatasi kejahatan, yang biasanya disebut dengan politik kriminal. Tujuan akhir dari politik kriminal adalah melindungi masyarakat. Dengan demikian, politik kriminal merupakan bagian dari perencanaan

perlindungan masyarakat, yang merupakan bagian dari kebijakan sosial secara keseluruhan. Penanggulangan kejahatan perlu menggabungkan aspek penal (hukuman) dan non penal (pencegahan) agar bisa mencapai tujuan melindungi masyarakat dan meningkatkan kesejahteraan sosial. Hal ini menunjukkan bahwa tanpa adanya kesejahteraan sosial yang cukup, upaya melindungi masyarakat melalui pendekatan *social defence* tidak akan berhasil. Oleh karena itu, untuk mencapai tujuan akhir kebijakan kriminal yaitu melindungi masyarakat dan meningkatkan kesejahteraan sosial, diperlukan kerja sama antara *social defence* dan *social welfare*. Ini akan menciptakan lingkungan yang tidak hanya melindungi masyarakat dari tindak kejahatan, tetapi juga memberdayakan mereka agar mengurangi kemungkinan terjadinya kejahatan di masa depan. Teknologi kecerdasan buatan atau *artificial intelligence* (AI) sudah digunakan dalam berbagai alat di kehidupan sehari-hari, seperti perangkat rumah tangga virtual, chatbot di smartphone, alat transportasi, serta teknologi *deepfake*. Teknologi *deepfake* adalah suatu metode yang menghasilkan salinan manusia dengan bantuan kecerdasan buatan atau *artificial intelligence* (AI). Teknologi ini digunakan untuk menggabungkan dan memasukkan gambar atau video ke dalam sumber gambar atau video lainnya menggunakan teknik mesin belajar bernama jaringan *generatif adversarial* (*generative adversarial network*) atau GAN. (Khusna & Pangestuti, 2019: 6) Teknologi *deepfake* sebenarnya mulai dikenal pada tahun 2017 lewat pengguna di forum Reddit.

Permasalahan yang berhubungan dengan teknologi *deepfake* semakin mendesak sejak peluncuran aplikasi bernama FakeApp pada Januari 2018. FakeApp adalah aplikasi yang dapat digunakan oleh siapa saja, yang memungkinkan penggunanya untuk membuat gambar dan video yang tidak autentik. Kekhawatiran mengenai kemungkinan penyalahgunaan dan dampak buruk dari penggunaan aplikasi ini semakin meningkat seiring dengan kemudahan aksesnya. Oleh karena itu, penting bagi pengguna untuk selalu berpikir kritis dan bijaksana ketika menggunakan teknologi seperti kecerdasan buatan, untuk mencegah munculnya gangguan dalam masyarakat atau kerusakan dalam hubungan antar orang. Penyalahgunaan teknologi *deepfake* menghadirkan tantangan serius dalam aspek hukum dan etika. Dalam konteks kejahatan ini, dapat merujuk pada ketentuan dalam Undang-Undang Nomor 19 Tahun 2016 yang mengubah Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, atau Pasal 378 KUHP mengenai Penipuan. Kasus penyalahgunaan teknologi *deepfake* semakin marak. Salah satu insiden yang mencuri perhatian publik adalah penipuan yang melibatkan penggunaan *deepfake* wajah Presiden Prabowo Subianto. Pelaku menggunakan teknologi ini untuk membuat video palsu yang menampilkan Presiden Prabowo menawarkan bantuan pemerintah, namun dengan syarat korban harus mentransfer sejumlah uang terlebih dahulu. Kasus ini berhasil diungkap oleh Direktorat Tindak Pidana Siber Bareskrim Polri, dengan pelaku berinisial AMA ditangkap di Lampung Tengah pada Januari 2025.

Modus yang digunakan dalam kasus ini memperlihatkan bagaimana teknologi *deepfake* dapat dimanfaatkan untuk menipu publik dengan cara yang semakin canggih. Pelaku tak hanya memasang wajah Presiden Prabowo, tetapi juga Wakil Presiden Gibran Rakabuming Raka serta Menteri Keuangan Sri Mulyani, untuk meyakinkan korban bahwa tawaran bantuan tersebut benar-benar ada. Akibatnya, lebih dari 100 orang dari 20 provinsi mengalami penipuan dengan total kerugian mencapai Rp 65 juta. Situasi ini menekankan perlunya adanya regulasi hukum yang lebih spesifik terkait penyalahgunaan teknologi *deepfake* di Indonesia. Saat ini, kerangka hukum yang ada belum secara menyeluruh mencakup masalah *deepfake*, sehingga penegakan hukum terhadap pelaku biasanya menghadapi berbagai tantangan. Oleh karena itu, diperlukan revisi terhadap undang-undang yang sudah ada atau bahkan pembentukan peraturan baru yang secara khusus mengatur tentang *deepfake* dan konsekuensinya. Hal ini termasuk dalam

tindakan kriminal, di mana pelakunya melakukan berbagai kejahatan secara bersamaan, seperti mencuri informasi pribadi, menyebarkan hoaks, serta melakukan manipulasi. Menurut Pasal 4 Undang-Undang Nomor 2 Tahun 2002 tentang Kepolisian Negara Republik Indonesia, dijelaskan bahwa tujuan kepolisian adalah untuk mewujudkan keamanan dalam negeri, yang mencakup terjaminnya keamanan dan ketertiban masyarakat, penegakan hukum, penyelenggaraan perlindungan, pengayoman, serta pelayanan kepada masyarakat, dan terwujudnya ketenteraman masyarakat dengan menghormati Hak Asasi Manusia. Oleh karena itu, peran kepolisian dalam menanggulangi kejahatan *deepfake scam* sangat penting untuk menjaga keamanan dan keadilan di masyarakat.

Sebelum melanjutkan pembahasan tentang langkah-langkah yang diambil oleh pihak kepolisian dalam menangani kasus penipuan yang menggunakan teknik *deepfake scam*, ada baiknya kita memahami terlebih dahulu tentang apa yang dimaksud dengan *deepfake scam*. Menurut penyidik Suyudi Kriminal Khusus Polres Metro Jakarta Pusat, *deepfake* adalah sebuah teknologi yang memungkinkan individu untuk mengambil wajah orang lain dan menggunakannya dalam praktik penipuan untuk tujuan tertentu, seperti untuk mendapatkan keuntungan pribadi dengan memanfaatkan wajah seseorang dalam foto dan video yang bersifat menipu, mencemarkan reputasi seseorang melalui video palsu, atau mendapatkan keuntungan dari jual beli video *deepfake* dan lain-lain. Menurut hasil wawancara dengan Suyudi, langkah-langkah dalam penanganan kejahatan penipuan dengan menggunakan metode *deepfake scam*, sebagian besar didasarkan pada model B. Model ini diatur dalam Pasal 5 ayat (1) huruf b Peraturan Kapolri Nomor 14 Tahun 2012 mengenai Manajemen Pendidikan Tindak Pidana, yang menyatakan bahwa laporan polisi dibuat oleh anggota Polri berdasarkan pengaduan dari Masyarakat.

Hasil wawancara dengan Suyudi tidak dapat memberikan penjelasan mengenai cara penangkapan pelaku dalam kasus *Cyber Crime*, khususnya yang berkaitan dengan pencemaran nama baik, karena informasi tersebut bersifat rahasia. Proses penyidikan kasus ini dilakukan sesuai dengan ketentuan yang terdapat dalam UU ITE Pasal 42, yang menyatakan bahwa "penyidikan terhadap tindak pidana yang diatur dalam undang-undang ini dilakukan dengan mengikuti hukum acara pidana dan ketentuan dalam undang-undang ini". Dalam KUHAP, aturan mengenai penyidikan tercantum di BAB penyidikan Pasal 107, dan ini juga dinyatakan dalam Pasal 43 UU ITE, yang menyebutkan bahwa penyidik dari kepolisian Negara Republik Indonesia dapat bekerja sama dengan pejabat pegawai negeri sipil. Setelah penyelidikan selesai dan dituangkan dalam format berkas perkara, masalah yang muncul adalah berkaitan dengan barang bukti akibat perbedaan pemahaman di antara para penegak hukum. Barang bukti digital merupakan bukti dalam kasus kejahatan siber yang masih belum memiliki definisi yang jelas dalam penentuan, karena bukti digital tidak selalu ada dalam wujud fisik yang nyata. Contohnya, dalam kasus pembunuhan, sebuah pisau dianggap sebagai barang bukti utama, sedangkan dalam kasus kejahatan siber, komputer menjadi barang bukti utama, tetapi komputer hanyalah wujud fisiknya saja, sementara yang paling penting adalah data yang tersimpan di dalam hard disk komputer tersebut dalam bentuk file, yang jika dicetak menjadi nyata memerlukan banyak kertas. Pertanyaannya, apakah barang bukti tersebut bisa disajikan hanya dalam bentuk compact disc? Hingga kini, belum terdapat Undang-Undang yang mengatur mengenai bentuk barang bukti digital ketika diajukan sebagai bukti di pengadilan.

Pihak kepolisian menangkap pelaku penipuan dengan modus *deepfake* yang menggunakan wajah Presiden Prabowo Subianto, pelaku menyalin dan mengedit konten dari unggahan orang lain, dan kemudian pelaku memposting di media sosial serta dibubuhi dengan caption yang memancing perhatian beberapa masyarakat sehingga korban tergiur dan menghubungi kontak yang tertera dalam konten tersebut, yang dimana kontak yang terhubung

itu adalah kontak pribadi dari pelaku penipuan. Pasal 28 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik tersebut dibuktikan dengan pelaku yang mengambil video dari media sosial lalu mengeditnya dengan AI serta menyebar luaskan video editannya ke media sosial. Maka pasal tersebut terpenuhi unsur-unsurnya. Penyalahgunaan *deepfake* dengan menggunakan foto atau video salah satunya dapat berupa konten penipuan, yang mana foto atau video milik pribadi di tempel dengan foto atau video milik orang lain yang menjadi korban. demikian juga dengan UU ITE Pasal 28 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik juga mengatur larangan mendistribusikan, mentransmisikan, dan/atau membuat dapat diaksesnya Informasi atau Dokumen Elektronik yang memiliki muatan yang bersifat penipuan.

Uraian di atas menunjukkan bahwa penyalahgunaan aplikasi *deepfake* berpotensi menciptakan peristiwa hukum, sebab teknologi ini mulai dieksploitasi untuk berbagai kepentingan. Sasaran utama penyalahgunaan *deepfake* lazimnya diarahkan kepada individu dengan kedudukan atau tokoh publik, meskipun risiko serupa tetap mengancam masyarakat sipil. Penyalahgunaan *deepfake* ini dapat dikelompokkan sebagai tindak pidana spesifik yang penetapannya bergantung pada korban dan kerugian yang diakibatkannya. Salah satu modus operandi kejahatan yang relevan adalah *deepfake scam*. Kejahatan penipuan yang menggunakan modus *deepfake scam* termasuk kategori delik aduan. Ini berarti bahwa proses hukum hanya dapat dimulai jika korban secara aktif mengajukan pengaduan atau laporan resmi. Dalam kasus delik aduan, penuntutan pidana atas kejahatan tersebut bergantung pada persetujuan dari pihak yang mengalami kerugian. Keistimewaan dari delik aduan adalah korban memiliki hak untuk mencabut laporannya kepada aparat penegak hukum apabila telah tercapai perdamaian atau kesepakatan damai dengan pelaku. Delik aduan ini di atur dalam KUHP seperti pasal 378 tentang penipuan, dan pasal 310 tentang pencemaran nama baik.

Kebijakan non-penal (*non-penal policy*) didefinisikan sebagai strategi penanggulangan kejahatan yang secara eksklusif menggunakan sarana di luar mekanisme hukum pidana. Implementasi kebijakan non-penal mencakup berbagai inisiatif sosial, seperti penyantunan, pendidikan sosial guna mengembangkan tanggung jawab warga, penggarapan kesehatan jiwa melalui pendidikan moral dan agama, peningkatan kesejahteraan anak dan remaja, serta kegiatan pengawasan berkelanjutan seperti patroli oleh aparat keamanan. Meskipun tujuan utama kebijakan ini adalah memperbaiki kondisi-kondisi sosial di berbagai sektor, secara tidak langsung, upaya ini memiliki pengaruh preventif yang signifikan terhadap kriminalitas. Oleh karena itu, kegiatan pencegahan (*preventif*) melalui sarana non-penal menempati kedudukan yang sangat strategis dan memegang posisi kunci yang wajib diintensifkan serta diefektifkan guna merealisasikan tujuan akhir dari politik kriminal negara. (Muladi & Arief, 2010: 159)

Barda Nawawi Arief berpendapat bahwa upaya penanggulangan kejahatan yang menggunakan pendekatan non-penal (*non-penal policy*) merupakan strategi yang dilaksanakan melalui sarana di luar ketentuan hukum pidana. (Arief, 2011: 46) Upaya ini secara fundamental bersifat preventif, yaitu lebih mengedepankan tindakan pencegahan sebelum suatu tindak kejahatan terjadi. Tujuan utama dari pendekatan non-penal adalah mengatasi faktor-faktor kondusif yang menjadi penyebab kriminalitas. Faktor-faktor ini mencakup berbagai masalah atau kondisi sosial yang, baik secara langsung maupun tidak langsung, dapat memicu atau menyuburkan pertumbuhan kejahatan. Pada dasarnya, penjelasan di atas ingin menggarisbawahi bahwa upaya non-penal yang paling strategis adalah menjadikan masyarakat sebagai lingkungan sosial dan lingkungan hidup yang sehat baik secara materiil maupun immateriil dari faktor-faktor kriminogen (penyebab utama terjadinya kejahatan). Dengan demikian, masyarakat harus dioptimalkan dengan segala potensinya untuk bertindak sebagai faktor penangkal kejahatan (*anti-kriminogen*) yang merupakan komponen integral dari

keseluruhan politik kriminal negara. Adapun kebijakan non-penal yang telah diimplementasikan oleh Kepolisian Resor Metropolitan Jakarta Pusat (Polres Metro Jakarta Pusat) dalam rangka menanggulangi tindak kejahatan penipuan dengan modus *deepfake scam* meliputi:

1. Melakukan sosialisasi kepada Masyarakat
  - a. Sosialisasi ke sekolah, pasar, balai warga, dan komunitas lainnya. Dalam rangka rangkaian Pelayanan Bulan Bakti Polri Presisi, pihak Kepolisian telah menyelenggarakan seminar dan workshop yang diberi nama "Jum'at Curhat Plus". Kegiatan sosialisasi ini secara spesifik bertujuan untuk memberikan penjelasan mendalam mengenai teknologi *deepfake*, potensi penyalahgunaannya, serta panduan praktis tentang cara melindungi diri dari penipuan dengan modus tersebut. Lebih dari sekadar edukasi, program ini juga berfungsi sebagai platform untuk menerima dan merespons keluhan yang timbul di tengah masyarakat.
  - b. Kampanye kesadaran. Pihak kepolisian memanfaatkan media sosial dan berbagai platform digital lainnya untuk menjalankan kampanye kesadaran publik yang bertujuan mengedukasi masyarakat mengenai modus-modus kejahatan tersebut.

Berdasarkan teori hukum pidana yang berkaitan dengan upaya penanggulangan, penyebaran informasi secara menyeluruh kepada masyarakat menjadi sangat penting untuk mencegah penipuan yang menggunakan metode penipuan *deepfake*. Strategi yang dilakukan oleh Polres Metro Jakarta Pusat meliputi dua arah: pendekatan spesifik yang fokus pada sekolah dan komunitas, serta pendekatan umum yang mencakup semua warga di daerah hukum mereka. Langkah ini mencerminkan bahwa Polres Metro Jakarta Pusat tidak hanya mengutamakan tindakan hukum yang bersifat menekan, tetapi juga menekankan pendekatan pencegahan untuk mengurangi kejadian penipuan *deepfake*. Dengan meningkatkan pemahaman masyarakat melalui sosialisasi, Polres Metro Jakarta Pusat berusaha membangun kerja sama antara usaha pencegahan dan penanggulangan. Tujuannya adalah untuk menjaga daerah Jakarta Pusat dari risiko kejahatan siber, terutama penipuan *deepfake*, secara berkelanjutan.

2. Berkoordinasi dengan Direktorat Tindak Pidana Siber (Dittipidsiber) Bareskrim Polri. Direktorat Tindak Pidana Siber (Dittipidsiber) memiliki keahlian yang cukup dalam mengatasi kasus-kasus siber yang kompleks, didukung oleh teknologi dan sumber daya modern untuk melaksanakan investigasi dan penyelidikan. Oleh sebab itu, pentingnya kolaborasi yang aktif antara Kepolisian Reserse Metro Jakarta Pusat dan Dittipidsiber sangat diperlukan, baik untuk mencegah (preventif) kejahatan siber maupun untuk mengambil tindakan tegas (represif) terhadap para pelaku. Kerja sama strategis antara kedua lembaga ini dapat dilakukan dalam berbagai cara, seperti:
  - a. Pertukaran Data, harus dilaksanakan supaya kedua belah pihak dapat saling menukarkan informasi dan perkembangan mengenai kasus-kasus siber yang sedang ditangani.
  - b. Bantuan teknis yang diberikan oleh Dittipidsiber kepada Polres Metro Jakarta Pusat, terutama dalam menangani kasus yang memerlukan keahlian teknis khusus yang mendalam.
  - c. Operasi Bersama dilakukan secara terpadu untuk meningkatkan efisiensi dalam membongkar jaringan kejahatan siber yang beroperasi dalam skala yang lebih besar.

Berdasarkan analisis terhadap teori politik hukum pidana mengenai langkah-langkah penanggulangan, kolaborasi antara Polres Metro Jakarta Pusat dan Bareskrim POLRI merupakan langkah yang sangat penting. Kerjasama ini dengan jelas menggambarkan

kesungguhan pihak kepolisian dalam mengatasi kejahatan penipuan yang menggunakan modus *deepfake scam*. Meskipun Polres Metro Jakarta Pusat menghadapi batasan dalam hal sumber daya atau keahlian terkait penanggulangan *deepfake scam*, kolaborasi dengan Bareskrim Polri akan sangat membantu dan memperkuat usaha dalam menanggulangi kejahatan tersebut.

3. Kerja sama dengan Kementerian Komunikasi dan Digital (KOMDIGI). Berdasarkan teori hukum pidana yang berkaitan dengan pencegahan, kolaborasi yang solid antara Polres Metro Jakarta Pusat dan Kementerian Komunikasi dan Digital (KOMDIGI) menjadi sangat penting untuk meningkatkan efektivitas tindakan kepolisian dalam menghadapi kejahatan penipuan yang menggunakan metode *deepfake scam*. Polres Metro Jakarta Pusat berkomitmen untuk memanfaatkan kombinasi teknologi modern, keterampilan petugas, dan kerja sama antar lembaga sebagai pendekatan utama untuk melawan *deepfake scam*. Dengan dukungan teknologi dan sumber daya manusia yang handal, diharapkan tingkat keberhasilan dalam menangani masalah ini dapat meningkat secara signifikan, serta memberikan perlindungan yang maksimal kepada para korbannya.
4. Mengembangkan Kapasitas Sumber Daya Manusia. Pelatihan bagi personel kepolisian tentang penggunaan teknologi *deepfake*, termasuk cara mengidentifikasi dan menangani isu-isu yang berhubungan, telah menjadi fokus utama. Tujuan dari pelatihan ini adalah untuk mempersiapkan para petugas dalam menghadapi tantangan baru yang muncul akibat perkembangan teknologi yang semakin cepat. Untuk meningkatkan kemampuan dalam menangani kasus siber, pelatihan bagi anggota Polri mencakup pemahaman yang mendalam tentang teknologi *deepfake*, analisis dampak sosial yang ditimbulkan, serta cara yang tepat untuk membantu korban. Diharapkan hal ini dapat mempercepat proses penanganan kasus dan memberikan rasa aman yang lebih baik bagi masyarakat. Lebih jauh lagi, dalam wawancara, Suyudi menyatakan bahwa personel Kepolisian Reserse Metro Jakarta Pusat secara aktif berpartisipasi dalam program pendidikan vokasional di Pusat Pendidikan Reserse Kriminal Polri di Megamendung untuk mengembangkan kemampuan dan keterampilan mereka. Menurut Wendy, saat ini ada pertumbuhan yang cepat dalam jenis kejahatan modern yang menggunakan ilmu dan teknologi sebagai alat, termasuk penipuan yang memanfaatkan *deepfake scam*. Kondisi ini mendorong masyarakat dan aparat penegak hukum untuk tetap mengikuti perkembangan teknologi, karena ancaman kriminal di masa depan tidak hanya akan berbentuk *deepfake scam*, tetapi juga akan muncul dalam banyak bentuk lain seiring dengan kemajuan teknologi. Wendy menegaskan bahwa masyarakat serta penegak hukum perlu bersikap proaktif untuk tidak tertinggal. Secara teori, interaksi antara perkembangan kejahatan dan penegakan hukum dapat disamakan dengan deret ukur dan deret hitung, di mana penegakan hukum (deret hitung) akan selalu terbelakang dibandingkan dengan kejahatan yang berkembang. Oleh karena itu, Wendy menekankan pentingnya peningkatan kemampuan polisi secara berkelanjutan agar penegakan hukum bisa sejalan dengan cepatnya laju kejahatan yang muncul. Berdasarkan analisis terhadap teori politik dalam hukum pidana terkait dengan upaya penanggulangan, dapat disimpulkan bahwa pengembangan sumber daya manusia (SDM) di Polres Metro Jakarta Pusat adalah sesuatu yang sangat penting. Tujuan pengembangan ini adalah untuk meningkatkan kemampuan aparat kepolisian agar dapat sejalan dengan perkembangan kejahatan penipuan yang semakin rumit di era digital. Oleh karena itu, peningkatan kualitas SDM di Polres Metro Jakarta Pusat diharapkan dapat meningkatkan efektivitas dalam penanggulangan kejahatan siber secara menyeluruh.
5. Melakukan Patroli Siber. Unit Patroli Siber adalah tim khusus yang dibentuk oleh Kepolisian Republik Indonesia dengan tugas utama untuk melindungi keselamatan pengguna internet

di dunia maya. Unit ini memiliki tiga peran pokok dalam menghadapi kejahatan siber, yaitu melakukan pengawasan, pencegahan, dan penegakan hukum. Selain menjalankan fungsi penegakan hukum, Patroli Siber juga secara aktif mengadakan kegiatan edukasi untuk masyarakat mengenai penerapan Undang-Undang Informasi dan Transaksi Elektronik (ITE). Tujuannya adalah untuk melindungi pengguna internet agar tidak menjadi sasaran dan sekaligus mencegah mereka terlibat sebagai pelaku kejahatan siber. Patroli Siber mengundang pengguna internet untuk bersama-sama berkolaborasi dalam usaha melawan kejahatan siber guna mencapai kedaulatan digital Indonesia, sebuah inisiatif yang didukung lewat situs resmi mereka. Untuk menghadapi kompleksitas kejahatan siber yang terus berubah, unit ini terus mengembangkan metode dan teknologi terbaru. Keberhasilan dalam menciptakan ruang siber yang aman dan nyaman sangat bergantung pada keterlibatan aktif masyarakat. Berdasarkan dasar teoretis dalam politik hukum pidana tentang strategi penanggulangan, dapat diartikan bahwa patroli siber adalah salah satu cara tindakan tegas yang cukup berhasil dalam menangani penipuan yang menggunakan metode *deepfake scam*. Metode ini menunjukkan bahwa Polres Metro Jakarta Pusat tidak hanya bersikap menunggu terjadinya kejahatan, tetapi juga aktif dalam memantau dan melindungi masyarakat dengan melakukan kegiatan patroli di dunia maya.

### **Hambatan yang dihadapi oleh penyidik Polres Metro Jakarta Pusat dalam mengintegrasikan upaya penal dan non-penal terhadap kasus penipuan berbasis *deepfake***

Faktor-faktor yang menjadi penghambat penegakan hukum tidak hanya berasal dari penerapan undang-undang. Terdapat berbagai aspek lain yang berkontribusi terhadap keterlambatan dalam proses hukum. Di samping itu, kompleksitas teknik *deepfake* yang memanfaatkan kemajuan teknologi seringkali membuat aparat penegak hukum membutuhkan waktu lebih lama untuk melakukan identifikasi, verifikasi, dan pembuktian secara digital. Situasi ini semakin diperburuk oleh kekurangan dalam fasilitas, infrastruktur, serta kemampuan sumber daya manusia dalam memahami teknologi baru. Berikut ini adalah hal-hal yang menghambat usaha dalam menangani kejahatan penipuan yang dilakukan dengan metode *deepfake scam*:

1. Faktor Perundang-undangan (Substansi Hukum). Dalam penerapan penegakan hukum di lapangan, seringkali terdapat perbedaan antara kepastian hukum dan keadilan. Keadilan merupakan sebuah ide yang tidak konkrit, sedangkan kepastian hukum adalah norma-norma yang telah ditetapkan. Maka dari itu, sebuah tindakan atau kebijakan yang tidak sepenuhnya sesuai dengan hukum bisa dibenarkan selama tidak bertentangan dengan hukum.
2. Faktor Penegak Hukum. Dalam menjalankan penegakan hukum, keadilan yang tidak disertai dengan kebenaran adalah sesuatu yang tidak baik, sementara kebenaran yang tidak disertai dengan kejujuran merupakan tindakan yang tidak tulus. Setiap lembaga penegak hukum dalam melaksanakan tugasnya perlu menegaskan, merasakan, dan mencerminkan keadilan serta kebenaran. Hal ini membutuhkan integritas dan dedikasi yang tinggi dari para penegak hukum agar mereka tidak hanya sekadar mengikuti prosedur secara formal, tetapi juga memastikan hasil yang diperoleh adil dan selaras dengan nilai-nilai moral dan etika.
3. Faktor Sarana dan Fasilitas yang Mendukung. Sarana serta fasilitas yang mendukung pelaksanaan hukum meliputi sumber daya manusia yang terdidik dan ahli, organisasi yang terstruktur dengan baik, alat yang memadai, dan sumber dana yang cukup. Tanpa dukungan sarana dan fasilitas yang tepat, pelaksanaan penegakan hukum tidak akan berjalan dengan baik, dan petugas penegak hukum tidak dapat menjalankan tugas mereka secara efektif.

4. Faktor Masyarakat. Hal yang paling utama dalam menilai suksesnya penegakan hukum adalah seberapa tinggi tingkat kesadaran hukum di masyarakat. Ketika kesadaran hukum di kalangan masyarakat meningkat, pelaksanaan penegakan hukum akan menjadi lebih mudah. Sebaliknya, jika tingkat kesadaran hukum di masyarakat rendah, maka pelaksanaan penegakan hukum akan semakin sulit.
5. Faktor Budaya. Ketika hukum ditegakkan, kemudahan dalam penerapan aturan hukum akan meningkat jika hukum tersebut selaras dengan budaya masyarakat. Namun, jika hukum tersebut tidak sejalan atau bertentangan dengan budaya masyarakat, maka penegakannya akan menjadi lebih sulit.

Berbagai tantangan dalam penerapan hukum di Indonesia dipengaruhi oleh semua elemen yang telah disebutkan sebelumnya, mulai dari aspek regulasi, aparat penegak hukum, dukungan sarana dan prasarana, hingga keadaan masyarakat dan budaya. Hal ini juga berlaku dalam penanganan kasus penipuan yang menggunakan teknik *deepfake scam*, di mana masih sering ditemukan berbagai kesulitan dalam proses penegakannya. Aparat penegak hukum, yang seharusnya menjadi contoh di masyarakat, diharapkan memiliki kemampuan tertentu yang sejalan dengan ekspektasi publik. Mereka tidak hanya dituntut mampu berkomunikasi dan menjalin pengertian dengan pihak yang dikenakan tindakan hukum, tetapi juga perlu menjalankan peran yang dapat diterima oleh masyarakat. Namun, ada beberapa kendala yang sering muncul dalam pelaksanaan peran tersebut, baik dari masyarakat maupun dari aparat itu sendiri, antara lain:

1. Adanya keterbatasan dalam memahami sudut pandang pihak lain yang berinteraksi dengannya.
2. Tingkat aspirasi dan motivasi yang masih relatif rendah.
3. Minimnya dorongan untuk memikirkan perkembangan jangka panjang, sehingga sulit menyusun perencanaan ke depan.
4. Belum tumbuhnya kemampuan menunda pemenuhan kebutuhan tertentu, khususnya kebutuhan material.
5. Rendahnya kemampuan berinovasi yang seharusnya menjadi penyeimbang sifat konservatif.

Penegak hukum adalah semua pihak yang terlibat, baik secara langsung maupun tidak langsung, dalam penegakan hukum. Ini mencakup polisi, jaksa, hakim, pengacara, serta petugas dari lembaga pemasyarakatan. Setiap profesi memiliki wewenang dan tanggung jawab yang berbeda sesuai dengan fungsi institusional yang dipikul. Hakim memiliki posisi yang sangat penting karena berada pada tahap akhir dalam proses pengambilan keputusan, dan dalam melaksanakan tugasnya, hakim bertindak dengan independensinya. Sedangkan, aparat penegak hukum yang lain memiliki tanggung jawab untuk memberikan informasi dan meyakinkan hakim tentang fakta dan konstruksi hukum yang terkait dengan suatu kasus, sehingga dapat tercapai keyakinan yang objektif demi menghasilkan keputusan yang adil dan bijaksana. Namun, dalam kenyataannya, tidak selalu berjalan seperti yang diharapkan. Penegakan hukum sering kali menyimpang dari prosedur yang benar, sehingga menimbulkan berbagai kesulitan dalam aspek operasional di setiap lembaga penegak hukum. Beberapa faktor utama yang menyebabkan masalah tersebut antara lain:

1. Kualitas sumber daya manusia hakim, jaksa, polisi, dan advokat masih rendah.
2. Diabaikannya prinsip *the right man in the right place*.
3. Minimnya komitmen aparat dalam menjalankan penegakan hukum secara konsisten.
4. Ketiadaan mekanisme penegakan hukum yang terpadu, efektif, dan modern.

5. Adanya pengaruh serta intervensi politik dan kekuasaan yang kuat dalam institusi kepolisian, kejaksaan, dan kehakiman.
6. Maraknya tuduhan mengenai praktik korupsi dan *organized crime* di antara aparat penegak hukum yang sering dikenal dengan mafia peradilan.

Berdasarkan temuan yang penulis peroleh mengenai tantangan yang dihadapi oleh Kepolisian di Polres Metro Jakarta Pusat dalam menangani kejahatan penipuan yang menggunakan modus *deepfake scam*, dapat disampaikan penjelasan sebagai berikut:

1. Faktor Subtansi Hukum. Suyudi menegaskan bahwa salah satu kendala dalam mengatasi kejahatan penipuan yang menggunakan metode *deepfake scam* adalah ketiadaan regulasi tertentu yang mengatur tindakan penipuan tersebut. Untuk memerangi kejahatan penipuan yang menggunakan metode *deepfake scam*, perlu adanya pembentukan undang-undang yang dapat memperkuat ketentuan yang sudah ada, sehingga penipuan melalui metode *deepfake scam* bisa ditangani dengan lebih efektif dan dapat memberikan efek jera kepada para pelaku, agar mereka tidak mengulangi tindakannya. Sejalan dengan pernyataan itu, Wendy menyatakan bahwa laju kemajuan teknologi *deepfake* sangat pesat sehingga banyak regulasi dan tata cara hukum belum secara jelas mengatur atau mengklasifikasikan penggunaan manipulasi audio/video yang berbasis AI sebagai kejahatan tersendiri. Hal ini mengakibatkan pihak penegak hukum sering kali mengandalkan ketentuan umum seperti penipuan, pencemaran nama baik, atau pelanggaran privasi, yang belum tentu sesuai untuk bukti digital yang telah dimodifikasi. Oleh karena itu, proses penyelidikan dan penuntutan menjadi lebih rumit dan kurang efisien. Berdasarkan penjelasan di atas, penyebab utama yang menghambat penanggulangan kejahatan penipuan dengan teknik *deepfake* adalah kurangnya regulasi yang secara spesifik mengatur dan mendefinisikan penggunaan teknologi manipulasi video dan audio berbasis kecerdasan buatan sebagai suatu tindak pidana yang terpisah. Dengan lemahnya basis hukum, penegak hukum terpaksa mengacu pada pasal-pasal umum yang sering kali tidak sesuai dengan sifat bukti digital yang dihasilkan secara artifisial, sehingga membuat proses penyelidikan dan penuntutan menjadi kurang efektif. Oleh sebab itu, sangat penting untuk merumuskan undang-undang khusus yang dapat memberikan kepastian hukum, memperkuat langkah-langkah penegakan hukum, serta menimbulkan efek jera bagi para pelaku, sehingga kejahatan *deepfake* dapat dikendalikan dan ditangani dengan lebih baik.
2. Faktor Penegak Hukum. Berdasarkan hasil wawancara dengan Suyudi, salah satu hambatan dalam usaha menangani kejahatan penipuan dengan metode *deepfake scam* disebabkan oleh penegak hukum, khususnya pihak kepolisian yang masih sedikit tertinggal dibandingkan dengan pelaku penipuan yang menggunakan teknik ini. Ini mencakup minimnya pemahaman mengenai teknologi yang mendasari pembuatan dan penyebaran konten *deepfake*, serta kurangnya fasilitas untuk melacak, menganalisis, dan membuktikan kejahatan siber yang semakin rumit. Selain itu, pihak kepolisian perlu mengejar ketertinggalan ini dengan meningkatkan kualitas Sumber Daya Manusia (SDM) atau merekrut anggota yang memiliki keahlian tinggi dalam bidang informasi dan teknologi (IT). Upaya peningkatan ini harus dilakukan secara berkelanjutan melalui pelatihan spesialis dalam forensik digital dan kejahatan siber agar dapat beradaptasi dengan perkembangan metode operandi pelaku yang selalu berubah. Berdasarkan penjelasan sebelumnya, dapat disimpulkan bahwa peran penegakan hukum berpengaruh besar terhadap keberhasilan atau kegagalan langkah-langkah penanganan kejahatan pelecehan yang menggunakan metode *deepfake scam*. Kemampuan petugas di bidang teknologi informasi menjadi faktor krusial untuk memastikan bahwa proses penegakan hukum berlangsung secara efektif dan

efisien. Ketidakmampuan untuk menyesuaikan diri dengan perkembangan teknologi dapat menyebabkan kesenjangan dalam penegakan hukum, di mana sejumlah kasus kejahatan siber, termasuk *deepfake scam*, tidak mampu ditangani atau dibuktikan dengan baik, sehingga memberikan kebebasan kepada pelaku dan meningkatkan ancaman untuk korban. Dengan demikian, pengembangan kapasitas teknis dan peraturan internal pada kepolisian adalah hal mendasar yang harus dilakukan untuk menciptakan dunia digital yang lebih aman.

3. Sarana Dan Fasilitas Yang Kurang Memadai. Berdasarkan percakapan dengan Gigih, cara untuk mendeteksi *deepfake* terus berevolusi dan para pelaku dapat menggunakan model generatif yang semakin mirip dengan yang asli. Hal ini membuat bukti multimedia menjadi sulit untuk dibedakan dari aslinya melalui pemeriksaan kasat mata maupun metode forensik yang konvensional. Perkembangan yang cepat dalam Jaringan Generatif Adversarial (GAN) dan model difusi telah menghasilkan konten *deepfake* dengan sedikit artefak dan tingkat koherensi visual yang tinggi, sehingga menantang bahkan alat deteksi berbasis pembelajaran mesin yang terbaru. Suyudi menyatakan bahwa institusi penegakan hukum sering kali kekurangan tenaga ahli forensik digital yang terlatih, perangkat lunak deteksi yang terbaru, serta prosedur yang dapat diandalkan dalam rantai bukti digital; hal ini memperpanjang durasi pemeriksaan dan mengurangi peluang keberhasilan dalam penuntutan. Kekurangan sumber daya ini menimbulkan kendala serius dalam proses penyelidikan, di mana perlakuan yang tidak tepat terhadap bukti digital dapat merusak integritas barang bukti dan menjadikannya tidak sah di pengadilan. Berdasarkan penjelasan di atas, Deteksi *deepfake* masih menghadapi banyak hambatan karena teknologi *deepfake* yang kian realistis dan sulit untuk dibedakan dari konten yang asli, bahkan dengan adanya teknik forensik dan machine learning terbaru. Kurangnya jumlah tenaga ahli, perangkat lunak untuk deteksi, dan prosedur yang andal untuk menangani bukti digital di lembaga penegak hukum menghambat kemajuan investigasi dan berisiko terhadap validitas bukti di pengadilan. Oleh karena itu, diperlukan investasi yang signifikan dalam pelatihan bagi ahli forensik digital dan pengembangan infrastruktur teknologi mutakhir, agar penegak hukum dapat berfungsi dengan efektif dalam melawan kejahatan *deepfake* yang semakin kompleks dan melindungi keadilan bagi para korban.
4. Faktor Masyarakat. Faktor sosial juga memainkan peran penting dalam kesuksesan penipuan *deepfake* serta penyebaran luas konten *deepfake*. Rendahnya kemampuan literasi digital di kalangan masyarakat dimanfaatkan oleh pelaku kejahatan, di mana banyak orang mengalami kesulitan dalam membedakan antara konten yang asli dan yang telah dimanipulasi oleh *deepfake* yang semakin mirip dengan kenyataan. Kecenderungan untuk langsung percaya pada informasi atau gambar yang ditemukan di media sosial, ditambah dengan keinginan untuk membagikan konten yang menarik atau menggugah emosi tanpa melakukan pengecekan, mempercepat distribusi konten *deepfake*. Wendy menyatakan bahwa rendahnya pemahaman mengenai bahaya privasi dan keamanan siber, ditambah dengan *reluctance* untuk melaporkan atau meminta bantuan setelah menjadi sasaran penipuan *deepfake* karena rasa malu atau ketidakpercayaan terhadap sistem hukum, semakin menciptakan kondisi yang mendukung pertumbuhan kejahatan ini. Berdasarkan penjelasan di atas, keberhasilan penipuan *deepfake* sangat bergantung pada kerentanan sosial yang ada di masyarakat. Secara keseluruhan, peningkatan pemahaman digital dan kesadaran bersama sangat penting untuk memutus jalur kerentanan yang dimanfaatkan oleh pelaku penipuan *deepfake*.
5. Faktor kebudayaan. Berdasarkan hasil wawancara dengan Suyudi, diketahui bahwa aspek budaya memiliki dampak yang besar terhadap penerapan hukum, terutama dalam usaha

menangani kejahatan penipuan dengan menggunakan metode *deepfake scam*. Aspek budaya menjadi salah satu kendala karena beberapa hal berikut:

- a. Budaya Kepatuhan terhadap Otoritas. Dalam banyak budaya, terdapat rasa hormat dan kepatuhan yang tinggi terhadap figur otoritas, seperti pimpinan perusahaan, tokoh agama, atau pejabat pemerintah. Pelaku *deepfake scam* mengeksploitasi budaya ini dengan memalsukan suara atau citra tokoh otoritas untuk mengeluarkan perintah mendesak (misalnya, transfer dana segera, tawaran bantuan dana), yang membuat korban cenderung patuh tanpa verifikasi kritis.
- b. Budaya Tabu Terhadap Kegagalan atau Kerugian. Topik-topik yang berkaitan dengan kerugian finansial atau menjadi korban penipuan sering kali dianggap tabu atau memalukan. Hal ini dapat menghambat korban *deepfake scam* untuk melapor karena takut akan stigma atau dianggap ceroboh. Stigma ini mempersulit penegak hukum untuk mendapatkan data kasus yang akurat dan melakukan upaya penanggulangan.
- c. Kurangnya Sikap Skeptis Kritis. Dalam beberapa konteks budaya, skeptisisme atau pertanyaan balik yang tajam terhadap informasi yang diterima, terutama dari lingkaran sosial terdekat, dianggap kurang sopan atau tidak berempati. Kurangnya sikap kritis ini dimanfaatkan dalam penipuan yang menargetkan kelompok sosial (misalnya, *deepfake* yang meniru suara kerabat yang sedang dalam kesulitan), di mana korban merasa berkewajiban untuk membantu segera tanpa memverifikasi keasliannya.

Hambatan yang paling menonjol bagi kepolisian dalam menangani kejahatan penipuan dengan modus *deepfake scam* berasal dari masyarakat. Ini terlihat dari rendahnya kesadaran masyarakat mengenai risiko privasi dan keamanan siber, serta kurangnya pemahaman digital yang membuat mereka belum mampu mengenali ciri-ciri manipulasi konten berbasis kecerdasan buatan. Situasi ini menciptakan celah yang mudah dimanfaatkan oleh pelaku untuk melaksanakan aksinya dan meningkatkan tantangan bagi kepolisian dalam mencegah serta menindak. Hambatan kedua yang sangat signifikan dalam upaya memberantas *deepfake scam* adalah masalah sarana dan fasilitas, khususnya kekurangan alat bantu pembuktian dalam bidang forensik digital. Keterbatasan ini menyulitkan proses penyidikan kejahatan *deepfake scam* yang sangat bergantung pada analisis data dan bukti digital. Sarana dan fasilitas yang memadai sangat penting untuk mendukung penegakan hukum dalam mencapai tujuannya. Tanpa adanya perangkat seperti perangkat lunak deteksi *deepfake* terbaru dan infrastruktur untuk penyimpanan bukti digital yang aman, proses penegakan hukum akan terhambat, sehingga penegak hukum tidak dapat mendukung perannya secara optimal dalam melawan kejahatan siber yang kompleks ini.

## **KESIMPULAN**

Berdasarkan temuan dari penelitian dan diskusi yang telah dilakukan, dapat ditarik kesimpulan bahwa Upaya yang dilakukan oleh kepolisian dalam mengatasi kejahatan penipuan dengan menggunakan teknik *deepfake scam* meliputi langkah-langkah penanggulangan melalui hukum pidana dan non-pidana. Dalam memberantas tindak penipuan yang menggunakan metode *deepfake scam*, perlu didukung dengan penyusunan undang-undang serta penerapan hukum yang tegas, termasuk melakukan penyelidikan, pengusutan, tindakan terhadap pelaku, serta pemberian hukuman sesuai dengan ketentuan hukum yang berlaku untuk memberikan efek jera. Selain itu, tindakan non-pidana seperti kampanye informasi dan peningkatan kesadaran hukum di masyarakat mengenai bahaya *deepfake scam*, serta pengembangan kerjasama antara pihak kepolisian dan instansi terkait lainnya juga sangat penting. Faktor penghambat yang paling dominan dalam upaya kepolisian untuk menanggulangi tindak pidana

penipuan bermodus *deepfake scam* terletak pada aspek aparat penegak hukum dan aspek masyarakat. Hambatan tersebut secara spesifik mencakup keterbatasan Sumber Daya Manusia (SDM) kepolisian, baik dari segi kuantitas maupun kualitas kompetensi teknis, serta masih rendahnya tingkat literasi dan edukasi hukum di kalangan masyarakat terkait modus kejahatan *deepfake scam*.

#### **DAFTAR PUSTAKA**

- Adi Nugraha, Radian, (2012) *Analisis Yuridis Mengenai Perlindungan Data Pribadi Dalam Cloud Computing System Ditinjau dari Undang-Undang Informasi dan Transaksi Elektronik*, (Depok: FH, Universitas Indonesia).
- Apeldoorn, Van, *Pengantar Ilmu Hukum*, Jakarta: PT Pradnya Paramitha.
- Arief, Barda Nawawi, *Bunga Rampai Kebijakan Hukum Pidana*, (Semarang: Fajar Interpratama, 2011)
- Budi Rizki H, dan Rini Fathonah, (2014), *Studi Lembaga Penegak Hukum*, Justice Publisher: Bandar Lampung, hlm.1.
- Hamdan, M, "*Politik Hukum Pidana*", (Jakarta: Raja Grafindo Persada, 1999).
- ILaura Payne, *Deepfake AI-Generated Synthetic Media*, Encyclopedia Britannica, <https://www.britannica.com/technology/deepfake>, diakses pada tanggal 21 April 2025.
- Itsna Hidayatul Khusna, Sri Pangestuti, *Deepfake, Tantangan Baru Untuk Netizen*, Promedia Vol 5, No. 2 Tahun 2019.
- M. Ramli, Ahmad, (2004), *Cyberlaw dan HAKI dalam Sistem Hukum di Indonesia*.
- Muladi dan Barda Nawawi Arief, *Teori-Teori dan Kebijakan Pidana*, (Bandung: Alumni, 2010).
- Onno W. Pura dalam Agus Rahardjo, *Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*, (Bandung: Citra Aditya Bhakti).
- Patroli Siber , *Tentang Unit Patroli Siber*, <https://patrolisiber.id/about-us/>, diakses pada tanggal 8 September 2025.
- Siti Yona Hukmana, *Penipu Deepfake AI Presiden Prabowo di Lampung Seorang Buruh Metro TV*, <https://www.metrotvnews.com/read/b7WCgDRLpenipu-deepfake-ai-presiden-prabowo-di-lampung-seorangburuh>, diakses pada tanggal 24 April 2025.
- Ucuk, Yoyok, "*Mediasi Penal Alternatif Penyelesaian Perkara Dalam Hukum Pidana*", (Yogyakarta: Laksbang Justitia, 2020).