# BAB I
# PENDAHULUAN

## A. Latar Belakang

Perkembangan teknologi informasi dan komunikasi telah membawa perubahan signifikan dalam pola interaksi masyarakat, khususnya dalam hal produksi dan distribusi informasi di ruang digital. Salah satu inovasi teknologi yang berkembang pesat adalah teknologi *deepfake*, yaitu teknik berbasis kecerdasan buatan (*artificial intelligence*) yang mampu memanipulasi gambar, suara, dan video sehingga tampak seolah-olah autentik, padahal merupakan hasil rekayasa.[1]

Dalam konteks perkembangan hukum, kemunculan teknologi ini menimbulkan tantangan serius, terutama ketika digunakan sebagai sarana penyebaran hoaks atau informasi bohong yang dapat merugikan individu maupun masyarakat luas. Penelitian terdahulu menunjukkan bahwa penyalahgunaan teknologi deepfake berpotensi menimbulkan berbagai bentuk kejahatan siber, seperti pencemaran nama baik, penipuan, disinformasi, pelanggaran privasi, hingga mengganggu stabilitas sosial dan kepercayaan publik terhadap informasi digital.[2]

---

[1] Happy Sturaya Quratuainniza dan Ema Nurkhaerani, "*Regulasi Kecerdasan Buatan untuk Mengatasi Penyalahgunaan Deepfake di Indonesia*," ALADALAH: Jurnal Politik, Sosial, Hukum dan Humaniora 4, no. 1 (2025).

[2] Jonathan Endro Sumual, Reynold Simandjuntak, dan Marven A. Kasenda, "*Analisis Yuridis Batasan Kebebasan Berekspresi terhadap Penyebaran Informasi Palsu yang Dibuat dari Teknologi Berbasis Kecerdasan Buatan*," Jurnal Legislasi dan Pembentukan Peraturan Perundang-undangan 2, no. 1 (2026).

Di sisi lain, perkembangan regulasi di Indonesia belum secara khusus mengatur pertanggungjawaban hukum terhadap penyalahgunaan teknologi deepfake, sehingga penegakan hukum masih bergantung pada ketentuan umum dalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). Kondisi tersebut menunjukkan adanya kebutuhan mendesak untuk membangun kerangka regulasi yang lebih adaptif terhadap perkembangan teknologi kecerdasan buatan serta memperkuat sistem penegakan hukum di ruang siber.[3]

Penggunaan *deepfake* sebagai alat penyebaran hoaks memiliki dampak yang sangat kompleks. Secara sosial, konten manipulatif tersebut dapat merusak reputasi seseorang, menciptakan kebingungan informasi, serta memicu konflik di tengah masyarakat. Secara politik, *deepfake* berpotensi digunakan untuk menyebarkan disinformasi yang dapat memengaruhi opini publik, terutama menjelang momentum demokrasi seperti pemilihan umum. Sementara itu, dari aspek hukum, penggunaan deepfake dalam penyebaran hoaks menimbulkan persoalan terkait pembuktian, identifikasi pelaku, serta penentuan pertanggungjawaban pidana.[4]

Dalam perspektif hukum positif di Indonesia, pengaturan mengenai penyebaran hoaks diatur dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) yang telah mengalami perubahan

---

[3] Rendi Syaputra Nur Haida dan Eko Nuriyatman, "*Urgensi Pengaturan Perlindungan Hukum terhadap Korban Deepfake melalui Artificial Intelligence (AI) dari Perspektif Hukum Pidana Indonesia*," Jurnal Hukum Respublica 24, no. 1 (2024).

[4] Jan Kietzmann et al., "Deepfakes: Trick or Treat?," *Business Horizons*, Vol. 63, 2020, hlm. 135–146.

melalui Undang-Undang Nomor 19 Tahun 2016 dan terakhir melalui Undang-Undang Nomor 1 Tahun 2024. Perubahan terakhir ini menunjukkan adanya upaya negara dalam menyesuaikan regulasi dengan perkembangan teknologi digital. Namun demikian, secara normatif, pengaturan terkait penggunaan *deepfake* sebagai sarana penyebaran hoaks belum diatur secara eksplisit. Ketentuan seperti Pasal 28 ayat (1) UU ITE yang mengatur penyebaran berita bohong dan menyesatkan masih bersifat umum, sehingga belum sepenuhnya mampu menjangkau kompleksitas kejahatan berbasis *deepfake*.[5]

Kondisi tersebut menimbulkan kesenjangan antara realitas sosial (*das sein*) dan norma hukum (*das sollen*). Dalam praktiknya, penyebaran deepfake sebagai sarana hoaks telah terjadi dan menunjukkan peningkatan, termasuk di wilayah hukum Kepolisian Resor Bireuen. Berdasarkan data empiris, data unit tindak pidana tertentu (tipiter) yang berkaitan dengan kasus *deepfake* di wilayah hukum Polres Bireuen, jumlah kasus yang terungkap menunjukkan adanya peningkatan dari tahun ke tahun. Pada tahun 2023 tercatat sebanyak 1 (satu) kasus, kemudian meningkat menjadi 2 (dua) kasus pada tahun 2024, dan pada tahun 2025 jumlah kasus yang ditangani tetap berada pada angka 2 (dua) kasus.[6] Namun demikian, perkara-perkara tersebut belum mampu diselesaikan hingga tahap persidangan.

---

[5] H. Nasution, *Aspek Hukum Informasi dan Transaksi Elektronik di Indonesia*, Jakarta: Prenadamedia Group, 2021, hlm. 102.

[6] Data Tindak Pidana Tertentu, Kasus *Deepfake* di Wilayah Hukum Kepolisian Resor Bireuen Tahun 2023–2025, diperoleh dari dokumentasi dan data Satreskrim Polres Bireuen, Tahun 2025.

Hal ini menunjukkan adanya permasalahan dalam penegakan hukum, baik pada tahap penyelidikan, penyidikan, maupun pembuktian di pengadilan.[7]

Selain itu, alat bukti elektronik yang dihasilkan dari teknologi manipulatif sering kali sulit diverifikasi keasliannya, sehingga menyulitkan aparat penegak hukum dalam membuktikan unsur tindak pidana. Kondisi ini diperparah dengan belum optimalnya pemahaman aparat terhadap karakteristik kejahatan berbasis kecerdasan buatan, serta terbatasnya sarana dan prasarana pendukung dalam penanganan kejahatan siber.[8]

Dalam konteks ini, pelaku memanfaatkan teknologi *deepfake* sebagai alat untuk melakukan kejahatan, sementara masyarakat sebagai pengguna media sosial menjadi target yang mudah terpengaruh oleh informasi manipulatif. Di sisi lain, lemahnya pengawasan dan keterbatasan regulasi menjadi faktor yang memungkinkan kejahatan tersebut terus berkembang.[9]

Selain itu, teori *deterrence* juga menunjukkan bahwa lemahnya penegakan hukum dapat mengurangi efek jera, sehingga berpotensi meningkatkan angka kejahatan serupa di masa mendatang.[10]

Dengan demikian, persoalan *deepfake* sebagai sarana penyebaran hoaks tidak hanya berkaitan dengan kekurangan norma hukum, tetapi juga menyangkut

---

[7] Data empiris Kepolisian Resor Bireuen,*Kasus deepfake*,2021–2025

[8] Susan W. Brenner, *Cybercrime: Criminal Threats from Cyberspace*, California: Praeger, 2010, hlm. 28.

[9] Lawrence E. Cohen & Marcus Felson, "Social Change and Crime Rate Trends: A Routine Activity Approach," *American Sociological Review*, Vol. 44 No. 4, 1979, hlm. 588–608.

[10] Muladi dan Barda Nawawi Arief, *Teori-Teori dan Kebijakan Pidana*, Bandung: Alumni, 2010, hlm. 52.

efektivitas penegakan hukum itu sendiri. Penegakan hukum yang tidak optimal akan berdampak pada menurunnya kepercayaan masyarakat terhadap hukum serta membuka peluang bagi pelaku kejahatan untuk terus melakukan perbuatannya.

Berdasarkan uraian tersebut, penelitian ini menjadi penting untuk dilakukan guna menganalisis bagaimana penegakan hukum terhadap penggunaan *deepfake* sebagai sarana penyebaran hoaks berdasarkan Undang-Undang Nomor 1 Tahun 2024 tentang perubahan kedua UU ITE, khususnya di wilayah hukum Polres Bireuen. Penelitian ini diharapkan dapat memberikan kontribusi dalam mengidentifikasi kendala penegakan hukum, mengevaluasi efektivitas regulasi yang ada, serta merumuskan rekomendasi kebijakan hukum yang lebih adaptif dan responsif terhadap perkembangan teknologi informasi di era digital.

## B. Rumusan Masalah

Berdasarkan latar belakang yang telah dikemukakan, penelitian ini akan menjawab beberapa pertanyaan utama sebagai berikut:

1. Bagaimanakah penegakan hukum terhadap kejahatan *deepfake* sebagai sarana penyebaran hoaks di wilayah hukum Polres Bireuen?
2. Apa saja hambatan yang dihadapi penyelidik dan penyidik dalam penegakan hukum terhadap kejahatan *deepfake* sebagai sarana penyebaran hoaks di wilayah hukum Polres Bireuen?
3. Bagaimanakah solusi yang dapat dilakukan untuk mengatasi hambatan dalam proses penyelidikan dan penyidikan terhadap kejahatan *deepfake* sebagai sarana penyebaran hoaks agar lebih efektif dan optimal?

## C. Tujuan Penelitian

Adapun tujuan dalam penulisan ini sebagai berikut:

1. Untuk menganalisis dan mengetahui penegakan hukum terhadap kejahatan *deepfake* sebagai sarana penyebaran hoaks di wilayah hukum Polres Bireuen.
2. Untuk mengidentifikasi dan menganalisis hambatan yang dihadapi penyelidik dan penyidik dalam penegakan hukum terhadap kejahatan *deepfake* sebagai sarana penyebaran hoaks di wilayah hukum Polres Bireuen.
3. Solusi yang dapat dilakukan untuk mengatasi hambatan dalam proses penyelidikan dan penyidikan terhadap kejahatan *deepfake* sebagai sarana penyebaran hoaks agar lebih efektif dan optimal.

## D. Manfaat Penelitian

Manfaat penelitian ini terbagi menjadi dua, yaitu:

### 1. Manfaat Teoritis

Penelitian ini diharapkan dapat memberikan kontribusi dalam pengembangan ilmu pengetahuan, khususnya di bidang hukum pidana dan hukum siber (*cyber law*), terutama yang berkaitan dengan penegakan hukum terhadap penggunaan teknologi *deepfake* sebagai sarana penyebaran hoaks.[11]

Selain itu, penelitian ini juga diharapkan dapat memperkaya kajian akademik mengenai penerapan Undang-Undang Nomor 1 Tahun 2024 sebagai perubahan kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi

[11] Muladi dan Barda Nawawi Arief, *Teori-Teori dan Kebijakan Pidana*, Bandung: Alumni, 2010, hlm. 15.

dan Transaksi Elektronik dalam menghadapi perkembangan teknologi digital yang semakin kompleks. Hasil penelitian ini juga dapat menjadi referensi bagi penelitian selanjutnya yang mengkaji kejahatan berbasis kecerdasan buatan (*artificial intelligence*) dalam perspektif hukum.[12]

**2. Manfaat Praktis**

Penelitian ini dapat menjadi pertimbangan bagi:

a. Bagi Penyelidik dan Penyidik (Polres Bireuen)

Penelitian ini diharapkan dapat menjadi bahan masukan bagi aparat penegak hukum, khususnya Polres Bireuen, dalam memahami faktor-faktor penyebab terjadinya tindak pidana *deepfake*, kendala penegakan hukum yang dihadapi, serta merumuskan strategi penanggulangan yang lebih efektif dan adaptif terhadap perkembangan teknologi digital.

b. Bagi Pemerintah dan Pembuat Kebijakan

Hasil penelitian ini dapat digunakan sebagai dasar pertimbangan dalam perumusan dan pembaruan kebijakan hukum, baik di tingkat daerah maupun nasional, terutama dalam rangka memperkuat regulasi dan mekanisme pengawasan terhadap penyalahgunaan teknologi *deepfake* dalam penyebaran informasi palsu (*hoaks*).

[12] H. Nasution, *Aspek Hukum Informasi dan Transaksi Elektronik di Indonesia*, Jakarta: Prenadamedia Group, 2021, hlm. 102.

c. Bagi Masyarakat

Penelitian ini diharapkan dapat meningkatkan kesadaran dan pemahaman masyarakat mengenai bahaya penyalahgunaan teknologi *deepfake* serta dampak hukumnya. Dengan meningkatnya literasi hukum dan literasi digital, masyarakat diharapkan lebih berhati-hati dalam menerima dan menyebarkan informasi di ruang digital.

d. Bagi Akademisi

Penelitian ini dapat menjadi referensi dan bahan perbandingan bagi akademisi dan peneliti lain yang ingin mengkaji isu serupa, khususnya terkait kejahatan *deepfake*, penyebaran hoaks, dan penegakan hukum di bidang teknologi informasi.

## E. Penelitian Terdahulu

Dalam rangka penyusunan penelitian ini, penulis telah melakukan kajian komprehensif terhadap berbagai literatur akademis yang relevan, meliputi tesis, disertasi, jurnal ilmiah, laporan penelitian, dan sumber-sumber sekunder terkait. Tinjauan literatur ini mengungkapkan sejumlah studi terdahulu yang memiliki titik persinggungan dengan fokus penelitian penulis, khususnya mengenai aspek hukum teknologi *deepfake* dalam konteks penyebaran disinformasi dan penerapan regulasi undang-undang informasi dan transaksi elektronik.

Analisis penelitian tesis ini berjudul “Penegakan hukum terhadap kejahatan *deepfake* berdasarkan undang-undang nomor 1 tahun 2024 tentang informasi dan transaksi elektronik (studi penelitian polres bireuen)” belum pernah dilakukan.

Berdasarkan penelusuran literatur yang dilakukan oleh peneliti, terdapat beberapa penelitian yang berkaitan dengan penerapan hukum terhadap *Deepfake* Sebagai Sarana Penyebaran Hoaks, di antaranya adalah:

1. Jurnal penelitian yang dilakukan oleh Meirza Aulia Chairani, Krista Yitawati, dan Angga Pramodya Pradhana pada tahun 2024 dengan judul "*Urgensi Pengaturan Hukum Bagi Penyalahgunaan Aplikasi Deepfake"* yang dipublikasikan dalam Jurnal Rechtens. Penelitian tersebut membahas urgensi pengaturan hukum terhadap penyalahgunaan teknologi *deepfake* di Indonesia yang semakin berkembang seiring kemajuan teknologi kecerdasan buatan (*artificial intelligence*). Hasil penelitian menunjukkan bahwa Indonesia belum memiliki regulasi khusus yang mengatur penyalahgunaan teknologi deepfake, sehingga penegakan hukum masih mengandalkan ketentuan yang tersebar dalam Undang-Undang Informasi dan Transaksi Elektronik, Kitab Undang-Undang Hukum Pidana, Undang-Undang Pornografi, serta Undang-Undang Perlindungan Data Pribadi. Oleh karena itu, peneliti merekomendasikan pembentukan regulasi khusus yang mampu memberikan kepastian hukum terhadap penyalahgunaan teknologi *deepfake*.[13] Perbedaan dengan penelitian ini terletak pada fokus kajian. Penelitian tersebut lebih menitikberatkan pada urgensi pembentukan regulasi, sedangkan penelitian ini mengkaji implementasi penegakan hukum terhadap kejahatan *deepfake*

[13] Meirza Aulia Chairani, Krista Yitawati, dan Angga Pramodya Pradhana, "*Urgensi Pengaturan Hukum Bagi Penyalahgunaan Aplikasi Deepfake*," Jurnal Rechtens, Vol. 13, No. 1, 2024, hlm. 81–96. DOI: 10.56013/rechtens.v13i1.2668.

berdasarkan Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik melalui penelitian empiris di Polres Bireuen.

2. Jurnal penelitian yang dilakukan oleh Hendra Prayoga dan Hadi Tuasikal dengan judul "*Penyebaran Konten Deepfake Sebagai Tindak Pidana: Analisis Kritis Terhadap Penegakan Hukum dan Perlindungan Publik di Indonesia*" mengkaji tentang modus penggunaan *deepfake* untuk pencemaran nama baik, hoaks, dan ancaman terhadap opini publik. Penelitian ini juga mengkritisi kelemahan aparat dalam pembuktian digital, anonimitas pelaku, dan kelangkaan forensik digital.[14] Perbedaan dengan penelitian ini ada pendekatan empiris melalui identifikasi modus operandi penyebaran hoaks deepfake serta memberikan analisa sistematis terhadap efektivitas UU ITE tidak hanya mengkritisi secara retoris.
3. Jurnal penelitian yang dilakukan oleh Rendi Syaputra Nur Haida dan Eko Nuriyatman pada tahun 2024 dengan judul "*Urgensi Pengaturan Perlindungan Hukum terhadap Korban Deepfake melalui Artificial Intelligence (AI) dari Perspektif Hukum Pidana Indonesia"* yang dipublikasikan dalam Jurnal Hukum Respublica. Penelitian tersebut memfokuskan pembahasan pada perlindungan hukum terhadap korban penyalahgunaan teknologi deepfake, khususnya yang berkaitan dengan perlindungan hak privasi, kehormatan, dan data pribadi korban. Hasil

[14] Hendra Prayoga dan Hadi Tuasikal, "*Penyebaran Konten Deepfake Sebagai Tindak Pidana: Analisis Kritis Terhadap Penegakan Hukum dan Perlindungan Publik di Indonesia*," Abdurrauf Law and Sharia, Vol. 2, No. 1, 2025, hlm. 22–38.

penelitian menyimpulkan bahwa diperlukan pembentukan regulasi yang lebih komprehensif guna menjamin perlindungan hukum, mekanisme pemulihan, serta pemberian kompensasi kepada korban penyalahgunaan teknologi *deepfake*.[15] Perbedaan dengan penelitian ini adalah bahwa penelitian tersebut berorientasi pada perlindungan korban, sedangkan penelitian ini lebih memfokuskan kajian pada penegakan hukum terhadap pelaku penyalahgunaan teknologi deepfake sebagai sarana penyebaran hoaks berdasarkan Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik.

4. Jurnal penelitian yang dilakukan oleh Rafly Satria Ramadhan, Yusuf Saefudin, Selamat Widodo, dan Rahtami Susanti pada tahun 2026 dengan judul *Urgensi Pengaturan Khusus Teknologi Deepfake di Indonesia Ditinjau dari Teori Tujuan Hukum Gustav Radbruch* yang diterbitkan dalam Jurnal Yustisi. Penelitian tersebut mengkaji kebutuhan pembentukan regulasi khusus mengenai teknologi *deepfake* berdasarkan teori tujuan hukum Gustav Radbruch yang menekankan pentingnya kepastian hukum, keadilan, dan kemanfaatan. Hasil penelitian menunjukkan bahwa ketentuan dalam Undang-Undang Informasi dan Transaksi Elektronik belum mampu memberikan kepastian hukum terhadap penyalahgunaan teknologi *deepfake*, sehingga diperlukan pengaturan khusus yang lebih adaptif terhadap perkembangan

[15] Rendi Syaputra Nur Haida dan Eko Nuriyatman, "*Urgensi Pengaturan Perlindungan Hukum terhadap Korban Deepfake melalui Artificial Intelligence (AI) dari Perspektif Hukum Pidana Indonesia*," Jurnal Hukum Respublica, Vol. 24, No. 1, 2024.

kecerdasan buatan. [16] Perbedaan dengan penelitian ini terletak pada ruang lingkup kajian. Penelitian tersebut bersifat normatif dan berfokus pada pembentukan regulasi, sedangkan penelitian ini mengkaji implementasi penegakan hukum terhadap kejahatan deepfake berdasarkan Undang-Undang Nomor 1 Tahun 2024 melalui studi empiris di Polres Bireuen dengan menganalisis proses penegakan hukum, hambatan penyidik, serta solusi yang dapat diterapkan untuk meningkatkan efektivitas penanganan perkara *deepfake*.

## F. Kerangka Teori dan Tinjauan Pustaka

### 1. Kerangka Teori

Kerangka teori dalam penelitian ini mencakup beberapa konsep penting yang menjadi dasar analisis, yaitu:

a. Teori penanggulangan Kejahatan

Penanggulangan kejahatan merupakan bagian penting dalam sistem hukum pidana yang bertujuan untuk mengendalikan, mencegah, dan menindak perbuatan yang melanggar hukum demi terciptanya ketertiban dan keamanan masyarakat. Dalam perspektif kriminologi, penanggulangan kejahatan tidak hanya berfokus pada pemberian sanksi terhadap pelaku, tetapi juga mencakup upaya preventif dan rehabilitatif yang bersifat komprehensif.[17]

---

[16] Rafly Satria Ramadhan, Yusuf Saefudin, Selamat Widodo, dan Rahtami Susanti, "Urgensi Pengaturan Khusus Teknologi Deepfake di Indonesia Ditinjau dari Teori Tujuan Hukum Gustav Radbruch," Jurnal Yustisi, Vol. 13, No. 2, 2026.

[17] Muladi dan Barda Nawawi Arief, *Teori-Teori dan Kebijakan Pidana*, Bandung: Alumni, 2010, hlm. 1.

Secara umum, penanggulangan kejahatan dapat dibagi menjadi tiga pendekatan utama, yaitu pendekatan penal, non-penal, dan pendekatan terpadu dengan penjelasan sebagai berikut:

1) Pendekatan Penal (*Represif*)

Pendekatan penal merupakan upaya penanggulangan kejahatan melalui sarana hukum pidana, yaitu dengan menerapkan sanksi pidana terhadap pelaku kejahatan. Pendekatan ini menitikberatkan pada penindakan setelah terjadinya kejahatan (*repressive action*), seperti proses penyelidikan, penyidikan, penuntutan, hingga pemidanaan di pengadilan.[18]

Dalam konteks ini, hukum pidana berfungsi sebagai sarana untuk memberikan efek jera (*deterrent effect*) kepada pelaku serta sebagai bentuk perlindungan terhadap masyarakat. Namun demikian, pendekatan penal sering kali dianggap memiliki keterbatasan karena bersifat reaktif dan tidak mampu sepenuhnya mencegah terjadinya kejahatan di masa depan.

2) Pendekatan Non-Penal (*Preventif*)

Pendekatan non-penal merupakan upaya penanggulangan kejahatan yang dilakukan sebelum terjadinya kejahatan (*preventive action*). Pendekatan ini menitikberatkan pada penghapusan faktor-faktor penyebab kejahatan, seperti

[18] Sudarto, *Hukum dan Hukum Pidana*, Bandung: Alumni, 1986, hlm. 45

kondisi sosial, ekonomi, dan lingkungan yang mendukung terjadinya tindak pidana.[19]

Dalam konteks kejahatan berbasis teknologi seperti *deepfake*, pendekatan non-penal dapat berupa peningkatan literasi digital masyarakat, penguatan sistem keamanan siber, serta edukasi mengenai bahaya penyebaran hoaks. Pendekatan ini dinilai lebih efektif dalam jangka panjang karena berorientasi pada pencegahan.

3) Pendekatan Terpadu (*Integral/Komprehensif*)

Pendekatan terpadu merupakan kombinasi antara pendekatan penal dan non-penal dalam penanggulangan kejahatan. Pendekatan ini menekankan bahwa penanggulangan kejahatan harus dilakukan secara menyeluruh dengan melibatkan berbagai pihak, baik aparat penegak hukum, pemerintah, maupun masyarakat.[20]

Pendekatan ini sejalan dengan pandangan kebijakan kriminal (*criminal policy*) yang menyatakan bahwa penanggulangan kejahatan tidak hanya menjadi tanggung jawab hukum pidana semata, tetapi juga memerlukan dukungan kebijakan sosial (*social policy*). Dengan demikian, upaya penanggulangan kejahatan harus dilakukan secara sistematis dan berkesinambungan.

Dalam kaitannya dengan kejahatan *deepfake* sebagai sarana penyebaran hoaks, teori penanggulangan kejahatan menunjukkan bahwa penanganan tidak cukup hanya melalui penegakan hukum pidana. Diperlukan pula pendekatan

---

[19] Barda Nawawi Arief, *Bunga Rampai Kebijakan Hukum Pidana*, Jakarta: Kencana, 2011, hlm. 77.

[20] Marc Ancel, Social Defence: *A Modern Approach to Criminal Problems*, London: Routledge, 1965, hlm. 23

preventif seperti peningkatan kapasitas aparat penegak hukum dalam bidang teknologi digital, penguatan regulasi yang lebih spesifik, serta peningkatan kesadaran masyarakat terhadap bahaya manipulasi informasi digital.

Dengan demikian, teori penanggulangan kejahatan memberikan kerangka konseptual yang penting dalam menganalisis bagaimana hukum dapat berfungsi secara efektif dalam menghadapi bentuk kejahatan baru yang terus berkembang seiring dengan kemajuan teknologi.

b. Teori Kepastian Hukum

Teori kepastian hukum merupakan salah satu pilar utama dalam negara hukum (*rechtstaat*) yang menekankan bahwa hukum harus memberikan kejelasan, ketegasan, dan dapat diprediksi dalam penerapannya. Kepastian hukum bertujuan untuk melindungi masyarakat dari tindakan sewenang-wenang serta memberikan jaminan bahwa setiap perbuatan hukum akan diperlakukan secara konsisten berdasarkan aturan yang berlaku. Tanpa adanya kepastian hukum, hukum kehilangan fungsi utamanya sebagai pedoman perilaku dalam kehidupan bermasyarakat.[21]

Menurut Gustav Radbruch, kepastian hukum merupakan salah satu nilai fundamental hukum di samping keadilan dan kemanfaatan. Kepastian hukum menuntut agar peraturan perundang-undangan dirumuskan secara jelas (*lex certa*), tidak multitafsir, serta dapat dilaksanakan secara konsisten oleh aparat penegak

[21] Philipus M. Hadjon, *Perlindungan Hukum bagi Rakyat di Indonesia*, Surabaya: Bina Ilmu, 1987, hlm. 25.

hukum.[22] Dalam konteks hukum pidana, kepastian hukum berkaitan erat dengan asas legalitas (*nullum crimen, nulla poena sine lege*), yang mengharuskan bahwa suatu perbuatan hanya dapat dipidana apabila telah diatur secara tegas dalam peraturan perundang-undangan.

Dalam kaitannya dengan tindak pidana *deepfake* dalam penyebaran informasi palsu (*hoaks*), teori kepastian hukum menjadi sangat relevan mengingat pesatnya perkembangan teknologi sering kali tidak diimbangi dengan pembaruan regulasi yang memadai. Ketidakjelasan norma hukum mengenai batasan perbuatan yang dilarang, unsur delik, serta bentuk pertanggungjawaban pidana dapat menimbulkan kesulitan dalam penegakan hukum, baik bagi aparat penegak hukum maupun bagi masyarakat sebagai subjek hukum.[23]

Dengan demikian, teori kepastian hukum berperan penting dalam memastikan bahwa upaya penanggulangan tindak pidana *deepfake* dilakukan secara adil, efektif, dan memberikan perlindungan hukum yang optimal bagi masyarakat, sekaligus menjamin hak asasi manusia dalam era digital.

c. Teori Penegakan Hukum

Teori penegakan hukum merupakan teori yang digunakan untuk menganalisis proses pelaksanaan dan penerapan hukum dalam kehidupan masyarakat. Penegakan hukum pada hakikatnya merupakan suatu proses untuk

---

[22] Gustav Radbruch, *Legal Philosophy*, London: Oxford University Press, 1950, hlm. 107–109.

[23] Barda Nawawi Arief, *Kebijakan Hukum Pidana*, Jakarta: Kencana Prenada Media Group, 2018, hlm. 54–56.

mewujudkan keinginan-keinginan hukum, yaitu pikiran-pikiran badan pembentuk undang-undang yang dituangkan dalam peraturan hukum, agar dapat dilaksanakan dalam kehidupan masyarakat. Dengan demikian, keberadaan suatu peraturan perundang-undangan tidak secara otomatis menjamin tercapainya tujuan hukum apabila tidak didukung oleh proses penegakan hukum yang efektif.[24]

Penegakan hukum dipengaruhi oleh beberapa faktor yang saling berkaitan, yaitu faktor hukum atau peraturan itu sendiri, faktor penegak hukum, faktor sarana atau fasilitas pendukung, faktor masyarakat, dan faktor kebudayaan.[25] Kelima faktor tersebut memiliki kedudukan yang penting karena keberhasilan penegakan hukum tidak hanya ditentukan oleh kualitas norma hukum, tetapi juga oleh kemampuan aparat, ketersediaan sarana, kesadaran masyarakat, serta nilai-nilai yang berkembang dalam kehidupan sosial.

1. Faktor hukum berkaitan dengan substansi atau ketentuan peraturan perundang-undangan yang menjadi dasar dalam melakukan penegakan hukum. Suatu aturan harus memiliki rumusan yang jelas, tidak saling bertentangan, dan mampu memberikan dasar hukum yang memadai bagi aparat penegak hukum dalam menangani suatu tindak pidana. Dalam konteks deepfake, faktor ini menjadi penting karena perkembangan teknologi digital dapat melahirkan bentuk-bentuk perbuatan yang belum secara spesifik diatur dalam peraturan perundang-undangan.

---

[24] Soerjono Soekanto, *Faktor-Faktor yang Mempengaruhi Penegakan Hukum*, Jakarta: Rajawali Pers, 2014, hlm. 7.

[25] *Ibid.* hlm. 8.

2. Faktor penegak hukum berkaitan dengan pihak-pihak yang secara langsung maupun tidak langsung terlibat dalam proses penegakan hukum, seperti kepolisian, kejaksaan, pengadilan, dan lembaga terkait lainnya. Profesionalitas, integritas, kompetensi, serta pemahaman aparat terhadap perkembangan teknologi menjadi faktor penting dalam menentukan efektivitas penegakan hukum terhadap tindak pidana berbasis digital.
3. Faktor sarana dan fasilitas berkaitan dengan ketersediaan perangkat, teknologi, sumber daya manusia, serta dukungan kelembagaan yang diperlukan dalam proses penegakan hukum. Dalam menangani kejahatan deepfake, misalnya, aparat penegak hukum memerlukan kemampuan digital forensics, teknologi untuk mengidentifikasi manipulasi media digital, serta tenaga ahli yang mampu menganalisis bukti elektronik. Tanpa dukungan sarana dan kemampuan teknis yang memadai, proses penyelidikan, penyidikan, pembuktian, dan penuntutan dapat mengalami hambatan.
4. Faktor masyarakat berkaitan dengan tingkat kesadaran dan kepatuhan masyarakat terhadap hukum. Masyarakat memiliki peran penting dalam penegakan hukum karena penegakan hukum pada dasarnya tidak hanya menjadi tanggung jawab aparat, tetapi juga membutuhkan partisipasi masyarakat. Dalam kasus penyebaran deepfake yang mengandung informasi palsu, masyarakat perlu memiliki kemampuan untuk mengenali informasi yang telah dimanipulasi, tidak melakukan penyebaran kembali terhadap

konten yang belum terverifikasi, serta melaporkan konten yang diduga melanggar hukum kepada pihak yang berwenang.

5. Faktor kebudayaan berkaitan dengan nilai-nilai, sikap, dan pola perilaku masyarakat yang memengaruhi bagaimana hukum dipahami dan ditaati. Perkembangan budaya digital yang ditandai dengan tingginya penggunaan media sosial dapat memberikan tantangan tersendiri dalam penegakan hukum. Kebiasaan masyarakat untuk membagikan informasi secara cepat tanpa melakukan verifikasi dapat memperbesar dampak penyebaran deepfake dan informasi palsu.

Dalam konteks tindak pidana deepfake sebagai sarana penyebaran hoaks, teori penegakan hukum Soerjono Soekanto dapat digunakan untuk melihat apakah ketentuan hukum yang tersedia telah dapat diterapkan secara efektif. Analisis tidak hanya diarahkan pada ada atau tidaknya aturan yang dapat digunakan untuk menjerat pelaku, tetapi juga mencakup kemampuan aparat penegak hukum dalam mengidentifikasi pelaku, mengumpulkan dan mengamankan alat bukti elektronik, melakukan pemeriksaan terhadap keaslian suatu konten digital, serta membuktikan hubungan antara pelaku dengan konten deepfake yang disebarluaskan.

Selain itu, teori penegakan hukum juga dapat digunakan untuk mengidentifikasi berbagai hambatan dalam penanganan kejahatan digital. Perkembangan teknologi deepfake yang semakin canggih dapat menyebabkan kesulitan dalam membedakan konten asli dan konten hasil manipulasi. Kondisi

tersebut menuntut adanya peningkatan kompetensi aparat penegak hukum dan penguatan koordinasi antarlembaga dalam menangani kejahatan berbasis teknologi informasi.

Dengan demikian, teori penegakan hukum memberikan kerangka analisis untuk menilai efektivitas penerapan hukum terhadap tindak pidana deepfake dalam penyebaran hoaks. Teori ini juga melengkapi teori penanggulangan kejahatan dan teori kepastian hukum. Teori penanggulangan kejahatan digunakan untuk menganalisis strategi preventif dan represif dalam menghadapi kejahatan deepfake, teori kepastian hukum digunakan untuk menilai kejelasan dan ketegasan norma hukum yang berlaku, sedangkan teori penegakan hukum digunakan untuk menganalisis bagaimana norma tersebut diterapkan oleh aparat penegak hukum dalam praktik.

**2. Tinjauan Pustaka**

a. *Deepfake* dan Teknologi Digital

Perkembangan teknologi *deepfake* merupakan tantangan serius bagi integritas informasi digital di Indonesia. Teknologi ini memanfaatkan kecerdasan buatan khususnya teknik *machine learning* dan *generative adversarial networks* (GANs) untuk memproduksi rekaman audio maupun video yang tampak autentik meskipun sepenuhnya hasil manipulasi. Kemampuan *deepfake* meniru ekspresi wajah, gerak bibir, dan intonasi suara secara presisi menjadikan teknologi ini tidak hanya mengaburkan batas antara realitas dan rekayasa digital, tetapi juga menciptakan potensi penyalahgunaan yang luas. Ketika masyarakat tidak lagi

dapat mempercayai bukti visual dan audio, maka validitas informasi digital berada dalam ancaman serius.[26]

Dalam konteks akademik Indonesia, sejumlah ahli menegaskan bahwa *deepfake* berpotensi mengganggu ruang publik, menurunkan kepercayaan masyarakat terhadap media, serta memperburuk polarisasi sosial.[27] Teknologi ini dapat digunakan untuk menciptakan konten hoaks yang menampilkan figur publik seolah-olah mengucapkan atau melakukan sesuatu yang sebenarnya tidak pernah terjadi. Dampaknya tidak hanya pada reputasi individu, tetapi juga pada stabilitas politik dan proses demokrasi, terutama pada momentum sensitif seperti pemilihan umum. Penelitian lain menyoroti bahwa *deepfake* dapat mendorong meningkatnya disinformasi, yang pada akhirnya melemahkan kualitas partisipasi politik masyarakat.[28]

Ancaman terhadap privasi dan keamanan personal juga sangat signifikan. *Deepfake* dapat dimanfaatkan untuk menghasilkan konten pornografi non-konsensual, pemerasan, atau fitnah digital yang menyerang korban secara psikologis maupun sosial.[29] Pada level kelembagaan, kejahatan berbasis *deepfake* juga dapat diarahkan untuk penipuan korporasi, rekayasa suara pejabat perusahaan

---

[26] Robert Chesney & Danielle Citron, 2019, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, California Law Review, Vol. 107 No. 1, https://doi.org/10.2139/ssrn.3213954

[27] Ahmad, Fadli, 2021, "*Ancaman Deepfake terhadap Keamanan Informasi Digital di Indonesia*", Jurnal Ilmu Komunikasi Universitas Indonesia, Vol. 12 No. 2, hlm. 134–136.

[28] Wijayanto, H. & R. Prasetyo, 2022, *Disinformasi Politik pada Era Digital dan Dampaknya terhadap Demokrasi Indonesia*, Jurnal Politik dan Kebijakan Publik, Vol. 8 No. 1, hlm. 45–48.

[29] Nurhadi, *Keamanan Siber dan Perlindungan Data Pribadi, Jakarta: Prenadamedia Group*, 2020, hlm. 89–92.

dalam penipuan keuangan, hingga manipulasi percakapan dalam transaksi bisnis. Kejahatan semacam ini menuntut sistem hukum Indonesia untuk memperkuat perangkat normatif dan kapasitas penegakan hukum agar mampu mengatasi modus kejahatan yang semakin kompleks.

b. Hoaks dan Penyebaran Informasi Palsu

Hoaks di era digital mengalami transformasi signifikan. Menurut Nasrullah, penyebaran hoaks menjadi lebih cepat dan sulit dikendalikan karena dukungan teknologi informasi seperti media sosial.[30] Hoaks bukan sekadar informasi palsu, melainkan konten yang sengaja diciptakan untuk membentuk opini publik secara menyesatkan, sering kali dengan tujuan politis maupun ekonomi. Hoaks dirancang untuk memanipulasi persepsi masyarakat melalui narasi yang tampak meyakinkan, memanfaatkan emosi publik seperti ketakutan, kemarahan, atau simpati. Dalam konteks digital, hoaks mudah menyebar secara cepat karena didukung oleh algoritma media sosial yang memprioritaskan konten viral tanpa verifikasi kebenaran.[31] Akibatnya, hoaks dapat menciptakan distorsi informasi secara massif yang mengancam kualitas diskursus publik. Lebih jauh, hoaks sering diorganisasi secara sistematis sebagai bagian dari strategi propaganda, kampanye hitam, atau upaya destabilisasi sosial. Dalam ranah politik, hoaks dapat digunakan untuk merusak reputasi lawan, mengarahkan pilihan pemilih, bahkan

[30] Rulli Nasrullah, 2018, *Literasi Digital: Budaya Bermedia di Masyarakat Digital*, Remaja Rosdakarya, Bandung, hlm. 93–97.

[31] Juwita, M. R., Anggraini, N. R., Ulum, M. S., et al., 2024, *Hoaxes in the Digital Era: An Analysis of Social Media Users' Perceptions and Attitudes*, Jurnal Lemhannas RI, Vol. 12 No. 4, hlm. 567–580.

memicu konflik horizontal dengan mengangkat isu-isu sensitif seperti agama, etnis, dan ideologi. Di ranah ekonomi, hoaks mampu mempengaruhi sentimen pasar, menjatuhkan reputasi perusahaan, atau mempengaruhi perilaku konsumen, sehingga menimbulkan kerugian finansial yang signifikan.[32]

c. Penegakan Hukum

Penegakan hukum merupakan proses untuk mewujudkan norma hukum menjadi kenyataan melalui tindakan aparat penegak hukum. Menurut Soerjono Soekanto, penegakan hukum dipengaruhi oleh beberapa faktor, yaitu faktor hukum itu sendiri, aparat penegak hukum, sarana atau fasilitas, masyarakat, serta budaya hukum.[33]

Dalam konteks kejahatan siber seperti *deepfake*, penegakan hukum menghadapi tantangan yang lebih kompleks, seperti anonimitas pelaku, kesulitan pembuktian, serta keterbatasan teknologi yang dimiliki aparat penegak hukum. Oleh karena itu, diperlukan pendekatan yang adaptif dan berbasis teknologi dalam proses penegakan hukum.

d. Hukum Siber (*Cyber Law*)

---

[32] Hidayati, Nurul, 2025,*Hoaks dan Disinformasi: Tantangan Terbesar dalam Membangun Opini Publik yang Sehat*", Jurnal Cakrawala, https://oj.mjukn.org/index.php/jca/article/view/181?utm

[33] Soerjono Soekanto, *Faktor-Faktor yang Mempengaruhi Penegakan Hukum*, Jakarta: Rajawali Pers, 2014, hlm. 8.

Hukum siber atau cyber law merupakan seperangkat aturan hukum yang mengatur aktivitas di dunia maya, termasuk penggunaan teknologi informasi dan komunikasi.[34]

Di Indonesia, hukum siber diatur melalui UU ITE yang telah mengalami beberapa kali perubahan, terakhir melalui Undang-Undang Nomor 1 Tahun 2024. Namun demikian, perkembangan teknologi yang sangat cepat sering kali tidak diimbangi dengan pembaruan regulasi yang memadai. Hal ini menyebabkan adanya kekosongan hukum atau ketidakjelasan norma dalam menangani kejahatan berbasis teknologi baru seperti *deepfake*. Hal ini terlihat dari belum adanya satu pun ketentuan dalam Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik maupun Kitab Undang-Undang Hukum Pidana yang secara eksplisit mendefinisikan, mengkriminalisasi, atau mengatur unsur-unsur tindak pidana yang dilakukan melalui teknologi *deepfake*. Akibatnya, aparat penegak hukum masih menggunakan ketentuan umum, seperti Pasal 27A, Pasal 28, Pasal 45, dan Pasal 45A UU ITE, yang pada dasarnya hanya mengatur akibat dari penyebaran informasi elektronik, bukan karakteristik manipulasi konten berbasis kecerdasan buatan.[35]

---

[34] Edmon Makarim, *Pengantar Hukum Telematika*, Jakarta: RajaGrafindo Persada, 2005, hlm. 12.

[35] Rafly Satria Ramadhan, Yusuf Saefudin, Selamat Widodo, dan Rahtami Susanti, *Urgensi Pengaturan Khusus Teknologi Deepfake di Indonesia Ditinjau dari Teori Tujuan Hukum Gustav Radbruch*, YUSTISI, Vol. 13, No. 2, 2026.