

BAB IV

PENUTUP

A. Kesimpulan

Berdasarkan hasil penelitian dan pembahasan yang telah disampaikan, Penulis menarik kesimpulan sebagai berikut:

1. Regulasi khusus mengenai teknologi *voice cloning* dalam konteks peradilan pidana di Indonesia belum tersedia, sehingga penerapannya masih mengacu pada Pasal 35 Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) serta Pasal 4 ayat (2) dan Pasal 65 Undang-Undang Perlindungan Data Pribadi (UU PDP). Meskipun Pasal 235 Kitab Undang-Undang Hukum Acara Pidana (KUHAP) dan Pasal 5 UU ITE mengakui informasi elektronik sebagai alat bukti, ketiadaan standar khusus terkait bukti yang berasal dari kecerdasan buatan mengakibatkan hakim sering menghadapi ketidakpastian hukum. Dalam proses pemeriksaan forensik, Laboratorium Forensik Kepolisian Republik Indonesia (Polri) masih menerapkan metode analisis suara konvensional berdasarkan Peraturan Kepala Kepolisian Nomor 10 Tahun 2009, dan belum sepenuhnya mengadopsi standar internasional seperti ISO/IEC 27037 maupun ISO/IEC 17025, sehingga kemampuan mendeteksi rekaman sintesis berbasis kecerdasan buatan masih terbatas. Pada tahap penyidikan, permintaan data digital diperlakukan sebagaimana penyitaan fisik berdasarkan ketentuan UU ITE dan Peraturan Menteri Komunikasi dan Informatika Nomor 5 Tahun 2020, yang menyebabkan aparat penegak hukum mengalami kesulitan dalam mengakses data dari *platform* AI asing karena harus

melalui prosedur *Mutual Legal Assistance* (MLA) yang memakan waktu cukup lama.

2. Berbeda dengan Indonesia, sistem hukum pidana di Amerika Serikat menyajikan kerangka penanganan yang lebih terstruktur dan responsif dalam menangani tindak kejahatan berbasis kecerdasan buatan. Dari segi aturan substantif, *ELVIS Act* 2024 dan usulan *No AI FRAUD Act* 2024 telah menetapkan perlindungan hukum yang jelas dan tegas terhadap penyalahgunaan *voice cloning*. Dalam proses pembuktian di pengadilan, Amerika Serikat mengatasi kerentanan alat bukti elektronik melalui rancangan *Proposed FRE Rule 901(c)* yang menerapkan mekanisme pembalikan beban pembuktian bagi pihak yang mengajukan alat bukti tersebut. Sistem peradilan ini juga didukung oleh standarisasi forensik yang ketat, di mana laboratorium diwajibkan memenuhi standar akreditasi ISO/IEC 17025 serta mengimplementasikan pedoman teknis *NIST AI 100-4* guna melacak asal-usul data dan mendeteksi konten buatan secara berlapis dan ilmiah. Dalam operasional investigasi, pelacakan terhadap pembuat *voice cloning* dapat berlangsung secara efisien berkat *Stored Communications Act* (18 U.S.C. § 2703). Undang-undang tersebut menerapkan instrumen penyidikan berjenjang yang meliputi *Subpoena*, *Court Order*, dan *Search Warrant*, sehingga penyidik berwenang untuk mengungkap identitas pelaku anonim secara cepat sesuai dengan tingkat sensitivitas privasi data yang bersangkutan.
3. Berdasarkan hasil perbandingan antara kedua negara tersebut, sistem hukum positif di Indonesia terbukti masih tertinggal dalam menanggapi ancaman tindak pidana rekayasa *voice cloning*. Kesenjangan regulasi di Indonesia meliputi empat

kelemahan utama, yaitu ketiadaan definisi normatif yang secara khusus mengatur suara buatan, belum adanya pedoman hukum pembuktian yang sesuai dengan karakteristik kecerdasan buatan, keterbatasan standar forensik kepolisian yang masih bersifat manual, serta prosedur pelacakan data elektronik yang kaku dan lambat akibat aturan yang disamakan dengan prosedur penyitaan benda fisik. Seluruh ketidaksempurnaan struktural dan prosedural tersebut menjadi penyebab utama terjadinya ketidakpastian hukum. Pada akhirnya, kelemahan ini menyebabkan penegakan keadilan terhadap tindak pidana siber yang memanfaatkan teknologi kecerdasan buatan di Indonesia belum dapat direalisasikan secara optimal.

B. Saran

Berdasarkan kesimpulan di atas, penulis mengajukan rekomendasi sebagai berikut:

1. Pemerintah bersama Dewan Perwakilan Rakyat (DPR) dianjurkan untuk segera memperbarui perangkat perundang-undangan yang berlaku dengan menyertakan definisi normatif yang spesifik mengenai *voice cloning*. Suara buatan atau hasil sintesis perlu diakui secara eksplisit sebagai data biometrik yang dilindungi oleh ketentuan hukum. Upaya perlindungan ini dapat diwujudkan melalui revisi Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), revisi Undang-Undang Perlindungan Data Pribadi (UU PDP), atau dengan merancang undang-undang khusus mengenai Kecerdasan Buatan (*AI Act*). Dalam proses penyusunan

regulasi tersebut, regulasi yang lebih maju dari Amerika Serikat, seperti *ELVIS Act* dan usulan *No AI FRAUD Act*, dapat dijadikan sebagai acuan utama.

2. Pihak legislatif perlu melakukan revisi terhadap ketentuan terkait permintaan data elektronik dalam KUHAP dan UU ITE dengan mengadopsi sistem perizinan bertahap, sebagaimana mekanisme *Stored Communications Act* (SCA) di Amerika Serikat. Diperlukan pemisahan prosedur yang jelas antara pencarian identitas dasar pelaku dan penyitaan isi komunikasi, agar proses pelacakan pembuat *voice cloning* dapat dilakukan lebih efisien tanpa terkendala oleh administrasi yang kaku. Selain itu, Mahkamah Agung disarankan untuk menerbitkan Peraturan Mahkamah Agung (PERMA) yang mengatur penerapan mekanisme pembalikan beban pembuktian. Dengan adanya PERMA tersebut, para hakim akan memperoleh pedoman teknis yang seragam dalam menilai keabsahan alat bukti elektronik yang diduga merupakan hasil rekayasa AI.
3. Kepolisian Republik Indonesia, khususnya Pusat Laboratorium Forensik (Puslabfor), sangat dianjurkan untuk segera melakukan modernisasi terhadap Peraturan Kapolri Nomor 10 Tahun 2009. Prosedur pengujian bukti suara hendaknya tidak lagi mengandalkan metode perbandingan pendengaran secara manual, melainkan mulai mengimplementasikan standar internasional seperti *NIST AI 100-4* guna melacak jejak digital (*watermarking*) serta mendeteksi konten yang dihasilkan kecerdasan buatan. Pembaruan regulasi teknis tersebut juga perlu disertai dengan pemenuhan akreditasi laboratorium sesuai standar ISO/IEC 17025, pengadaan perangkat lunak forensik berbasis kecerdasan buatan, pelatihan intensif bagi para penyidik siber, serta peningkatan kerja sama dengan institusi

pendidikan tinggi di bidang hukum dan teknologi guna menghasilkan tenaga ahli forensik digital yang kompeten.

