BAB IV

KESIMPULAN DAN SARAN

A. Kesimpulan

Berdasarkan hasil penelitian dan pembahasan yang telah dibahas, penulis menarik dapat kesimpulan sebagai berikut:

1. GDPR dan AI Act sama-sama mengatur penggunaan FRT, akan tetapi dengan pendekatan yang berbeda. GDPR menggunakan *rights-based approach* dengan berfokus pada perlindungan data pribadi melalui pembatasan pemrosesan data biometrik, penerapan prinsip-prinsip perlindungan data, dasar hukum pemrosesan, hak-hak subjek data, serta kewajiban *Data Protection Impact Assessment* (DPIA). Sementara itu, AI Act menggunakan *risk-based approach* dengan mengklasifikasikan FRT sebagai sistem AI berisiko tinggi, melarang praktik *untargeted scraping* dan penggunaan *real-time remote biometric identification* dalam kondisi tertentu, serta mewajibkan penerapan manajemen risiko, tata kelola data, transparansi, pengawasan manusia, dan *Fundamental Rights Impact Assessment* (FRIA).
2. Dalam kasus Clearview AI Inc., GDPR memberikan perlindungan melalui larangan pemrosesan data biometrik tanpa dasar hukum, penerapan prinsip perlindungan data, penegakan hak-hak subjek data, serta kewenangan otoritas perlindungan data untuk menjatuhkan sanksi dan menerapkan prinsip ekstrateritorialitas. Meskipun AI Act belum berlaku saat putusan dijatuhkan, ketentuannya menunjukkan perlindungan yang lebih preventif dengan melarang *untargeted scraping*, membatasi penggunaan *real-time remote biometric identification*, mengklasifikasikan FRT sebagai sistem AI berisiko

tinggi, serta menetapkan kewajiban kepatuhan dan sanksi yang tegas. Dengan demikian, GDPR melindungi dari aspek pemrosesan data pribadi, sedangkan AI Act melindungi dari aspek pengaturan sistem AI yang digunakan dalam FRT.

B. Saran

1. Uni Eropa perlu memastikan implementasi GDPR dan AI Act dilakukan secara konsisten dalam setiap penggunaan FRT. *Data controller*, *provider, dan deployer* harus memenuhi seluruh kewajiban yang diatur dalam kedua regulasi, seperti memiliki dasar hukum pemrosesan data biometrik, menerapkan prinsip-prinsip perlindungan data, melaksanakan *Data Protection Impact Assessment* (DPIA) dan *Fundamental Rights Impact Assessment* (FRIA), serta menerapkan manajemen risiko, transparansi, dan pengawasan manusia sesuai dengan tingkat risiko sistem AI. Di samping itu, EU perlu segera menerbitkan panduan teknis yang lebih rinci mengenai batas penggunaan FRT di ruang publik maupun di ruang digital. Tanpa pedoman operasional yang jelas, larangan *real-time remote biometric identification* dan *untargeted scraping* berisiko dapat disalahgunakan.
2. Bagi negara-negara di luar EU, yang sedang mengembangkan regulasi perlindungan data pribadi dan kecerdasan buatan, disarankan untuk mengadopsi pendekatan berbasis risiko dan konsep *extraterritorial effect* seperti dalam GDPR dan AI Act. Regulasi yang dibuat harus secara eksplisit melarang praktik *untargeted scraping* untuk membangun *database* wajah tanpa persertujuan, serta membatasi penggunaan FRT jenis *Real time remote biometric identification* di ruang publik. Selain itu, perlu dibentuk otoritas pengawas independen yang memiliki jangkauan ekstrateritorial dan memiliki

UNIVERSITAS ANDALAS
UNTUK KEDJAJAAN BANGSA

kewenangan untuk menjatuhkan sanksi dan penegakan hukum yang mampu memberikan efek jera terhadap para pihak yang melakukan pelanggaran data pribadi, serta dapat mengaudit kepatuhan terhadap perlindungan data pribadi. Langkah ini penting mengingat kasus Clearview AI Inc., dimana perusahaan berkedudukan di Amerika Serikat. Kasus ini menunjukkan perusahaan asing dapat memproses data wajah warga negara lain tanpa dasar hukum yang sah dan tanpa memandang wilayah yurisdiksi suatu negara.

UNIVERSITAS ANDALAS
UNTUK KEDJAJAAN BANGSA