BAB VI

PENUTUP

A. Kesimpulan

1. Pengaturan kejahatan siber belum sepenuhnya memadai karena masih mengacu pada berbagai undang-undang yang tidak terintegrasi, seperti KUHP dan UU ITE, yang kadang-kadang tumpang tindih dalam menangani kasus-kasus kejahatan siber. Ada berbagai bentuk kejahatan siber yang diatur dalam undang-undang tersebut, seperti pencurian data, penggelapan, pemerasan, dan penggunaan konten ilegal. Dalam konteks global, termasuk di Indonesia, penegakan hukum atas kejahatan siber menjadi tantangan yang semakin signifikan, terutama terkait dengan perlindungan data pribadi dan privasi pengguna internet. Perlunya pengawasan dan regulasi yang lebih spesifik untuk mengatasi tantangan kejahatan yang melibatkan kecerdasan buatan juga diakui dalam bab ini, mengingat *AI* telah mulai digunakan dalam kejahatan siber. Oleh karena itu, perlu adanya pembaruan hukum yang lebih komprehensif dan terintegrasi, terutama yang mencakup penggunaan *AI* dalam kejahatan siber.
2. Era Revolusi Industri 5.0 *Society*, *AI* telah menjadi ancaman yang signifikan dalam kejahatan siber, terutama karena kompleksitasnya dan potensi penggunaannya untuk tujuan melanggar hukum. Meskipun *AI* dapat dioperasikan secara semi-otonom, teknologi ini belum memenuhi

kriteria untuk dianggap sebagai subjek hukum yang dapat bertanggung jawab secara pidana. Oleh karena itu, tanggung jawab hukum masih dibebankan kepada manusia, baik sebagai pengembang, pengguna, maupun pengawas *AI*. Urgensi dalam pembentukan sebuah wadah yang mampu menangani permasalahan *AI* di Indonesia sangat penting, penulis menggagas pembentukan sebuah Badan yang mampu mengawasi karena pengaturan hukum yang komprehensif mengenai kejahatan siber berbasis *AI* menjadi sangat mendesak agar mampu memberikan kepastian hukum dan melindungi masyarakat dari potensi penyalahgunaan teknologi ini.

3. Formulasi pertanggungjawaban pidana terkait kejahatan siber yang melibatkan kecerdasan buatan yang dalam hal ini, konsep pertanggungjawaban pengganti *(vicarious liability)* menjadi pusat pembahasan. Tanggung jawab pengganti diterapkan tanpa mempersyaratkan adanya unsur kesalahan subyektif seperti niat jahat *(mens rea)* atau kelalaian *(culpa)* dari pihak yang dimintai pertanggungjawaban *AI* yang bertindak secara otonom atas perintah atau program dari pengembang atau pengguna, menimbulkan pertanyaan siapa yang harus bertanggung jawab atas kejahatan yang terjadi. Dalam konteks ini, *vicarious liability* menjadi pendekatan penting untuk mengisi kekosongan normatif mengenai siapa yang harus menanggung risiko pidana dari tindakan sistem cerdas non-manusia. Sebgai contoh penerapan *vicarious liability*, sebuah perusahaan mengembangkan chatbot berbasis *AI* untuk melayani pelanggan. Namun, *AI* tersebut tanpa sengaja memproduksi

dan menyebarkan konten ujaran kebencian karena kurangnya filter etika dan pengawasan dari pengembangnya. Meskipun *AI* tidak memiliki niat atau mens rea, pengembang atau perusahaan dapat dimintai pertanggungjawaban pidana secara pengganti jika terbukti, tidak ada kontrol keamanan terhadap perilaku *AI*, pengembang mengabaikan potensi bahaya dari output system, perusahaan menggunakan *AI* secara publik tanpa pengujian yang memadai. dalam hal ini, pertanggungjawaban pengganti digunakan untuk menjembatani kesenjangan tanggung jawab antara tindakan sistem *AI* dan tanggung jawab manusia di baliknya Oleh karena itu, penting untuk memastikan adanya mekanisme pengawasan dan regulasi yang jelas untuk memantau penggunaan *AI*. Selanjutnya, perlunya pembentukan Badan Pengawas AI, yang berperan dalam memantau dan mengatur penggunaan *AI* untuk mencegah penyalahgunaan. Dengan demikian, pelaku kejahatan siber yang memanfaatkan *AI* dapat lebih mudah diidentifikasi dan dituntut secara pidana.

B. Saran

1. Regulasi kejahatan siber di Indonesia perlu diperbarui dan diintegrasikan secara komprehensif, mencakup teknologi baru seperti kecerdasan buatan. Saat ini, hukum yang ada sering kali tumpang tindih dan tidak mencakup secara spesifik *AI* dalam kejahatan siber. Pemerintah harus segera mengadopsi kerangka hukum yang jelas dan eksplisit terkait penggunaan *AI*, mengingat peningkatan kejahatan yang menggunakan teknologi ini, agar memberikan kepastian hukum.

2. Untuk mengatasi ancaman kejahatan siber berbasis *AI*, pembentukan Badan Pengawas AI menjadi sangat penting. Badan ini berfungsi untuk memantau, mengatur, dan menegakkan aturan terkait penggunaan *AI*, baik dalam sektor sipil maupun kriminal. Dengan demikian, pelaku kejahatan yang memanfaatkan *AI* dapat diidentifikasi dan diproses secara hukum dengan lebih efektif
3. Perlu segera dirumuskan mekanisme pertanggungjawaban pidana berbasis "*vicarious liability*" bagi pihak yang menggunakan atau mengembangkan *AI* yang menyebabkan kerugian. Dalam hal ini, pertanggungjawaban pengganti digunakan untuk menjembatani kesenjangan tanggung jawab antara tindakan sistem *AI* dan tanggung jawab manusia di baliknya.