BAB IV

PENUTUP

A. Kesimpulan

Dari penjelasan pada bab sebelumnya dapat ditarik kesimpulan yaitu sebagai berikut:

1. Salah satu hal penting bagi negara untuk melindungi aset digital dari ancaman *cyber crime* adalah *cyber security*. *Budapest Convention on Cybercrime* 2001 merupakan awal dari munculnya pengaturan terkait *cyber security* di Uni Eropa. Konvensi ini adalah hasil dari kerjasama multilateral yang diadakan guna menanggulangi penyebaran aktivitas kriminal melalui internet dan jaringan computer lainnya. Kemudian, pengaturan *cyber security* yang baru yakninya *The NIS Directive* 2016 yang menekankan setiap Negara anggota membentuk kerangka kerja nasional yang perlu diadopsi oleh setiap Negara anggota terkait keamanan jaringan dan sistem informasi. Uni Eropa memperkenalkan Undang-Undang *cyber security* yang baru yang disebut *EU Cybersecurity Act* 2019 (EUCA). Regulasi ini memperkuat mandat *European Union Agency for Cybersecurity* (ENISA) sebagai badan *cyber security* di Uni Eropa dan juga mengatur pembentukan Kerangka Sertifikasi Keamanan Siber (*Cybersecurity Certification Framework)*. Pengaturan *cyber security* yang terbaru yakninya *proposal Cyber Resilience Act* yang berfokus pada keamanan perangkat keras dan perangkat lunak yang dijual di pasar Uni Eropa, terutama perangkat yang terhubung ke internet seperti *Internet of Things* (IoT).

2. Regulasi untuk melindungi data pribadi dari penyalahgunaan data yang dilakukan oleh perusahaan-perusahaan baik yang berada di Uni Eropa maupun perusahaan asing yang menggunakan data dari warga Uni Eropa diatur di dalam *General Data Protection Regulation* (GDPR). Pelanggaran data pribadi dapat dibagi menjadi beberapa kategori berdasarkan sifat pelanggarannya, yakninya, Pelanggaran Pelaporan (*Breach of Confidentiality*) Pelanggaran Integritas (*Breach of Integrity*) Pelanggaran Ketersediaan (*Breach of Availability)*. Dari segi regulasi, Uni Eropa dapat memperkuat poin terkait perlindungan data pribadi pada Undang-Undang *cyber* yang baru yakninya *EU Cyber Resilience Act* (CRA) atau Undang-Undang Ketahanan Siber Uni Eropa. Kemudian Uni Eropa telah menyiapkan langkah pencegahan untuk menghindari terjadinya pelanggaran data pribadi dengan memberlakukan *Blockchain Strategy*. *Blockchain* dapat mencegah terjadinya pelanggaran data pribadi karena mekanisme transaksi antara konsumen dan produsen dilakukan secara pribadi dan melalui jaringan dengan tingkat keamanan yang tinggi. Selanjutnya ENISA sebagai badan yang berwenang dalam mengatur *cyber security* bisa melakukan tidakan untuk mengatasi pelanggaran data pribadi dengan cara menunjang implementasi dari GDPR dan berbagai inisiatif terkait *cyber security*.

B. Saran

Berdasarkan penelitian yang penulis lakukan, maka ada beberapa saran yang dapat disampaikan:

1. Diperlukan harmonisasi lebih lanjut dalam pelaksanaan Undang-Undang tentang *cyber security* agar ada keselarasan standar keamanan di seluruh negara anggota. Uni Eropa harus memperkuat pengawasan melalui lembaga yang berwenang dalam hal ini ENISA sebagai badan *cyber security* Uni Eropa dalam menunjang implementasi terhadap regulasi yang telah ada. Dalam proposal regulasi yang mengatur keamanan siber yang baru yakninya *Cyber Resilience Act* seharusnya mencantumkan poin-poin yang kurang pada regulasi sebelumnya seperti memperkuat pengaturan data pribadi.
2. Uni Eropa perlu menyegerakan tindakan pencegahan terhadap pelanggaran data pribadi dengan cara menyegerakan diberlakukannya Undang-Undamg Ketahanan Siber atau *Cyber Resilience Act* karena regulasi ini memasukan *data protection* sebagai indikator penting. Kemudian penerapan dari *Blockchain* harus segera di segerakan, untuk mencegah terjadinya kasus pelanggaran data pribadi yang terjadi pada kegiatan transaksional. ENISA sebagai badan keamanan siber Uni Eropa seharusnya berperan lebih dalam implementasi GDPR untuk mencegah dan mengatasi pelanggaran data pribadi.