SKRIPSI

ANALISIS *CYBER SECURITY* TERHADAP PELANGGARAN DATA PRIBADI DALAM HUKUM UNI EROPA

Diajukan Guna Memenuhi Persyaratan Untuk
Memperoleh Gelar Sarjana Hukum

Oleh:

MUHAMMAD ZAQI YAFI
2010111136

PROGRAM KEKHUSUSAN: HUKUM INTERNASIONAL (PK VI)

Pembimbing :

Dr. Jean Elvardi, S.H., M.H.
Sri Oktavia, S.H., M.Sc., Ph.D.

FAKULTAS HUKUM

UNIVERSITAS ANDALAS

PADANG

2025

No.Reg : 5/PK-VI/I/2025

ABSTRAK

Cyber space adalah yurisdiksi baru yang sampai sekarang belum dicapai konsensus secara internasional mengenai negara manakah yang berhak untuk memutuskan atau melaksanakan yurisidiksi di *cyber space* karena tidak berlakunya batasan geografis sehingga hal tersebut menyebabkan adanya ketidakpastian hukum. Akibat dari hal tersebut adalah munculnya *cyber crime*, seperti kasus pelanggaran data pribadi berupa penyalahgunaan data oleh pihak ketiga, sehingga perlu ada regulasi yang mengatur terkait keamanan ruang siber atau *cyber security* yang mengatasi kasus pelanggaran data pribadi. Oleh karena itu, penelitian ini berfokus pada dua hal. *Pertama*, bagaimana pengaturan *cyber security* dalam hukum Uni Eropa? *Kedua*, bagaimana *cyber security* mengatasi kasus pelanggaran data pribadi di Uni Eropa? Penelitian dilakukan menggunakan metode penelitian hukum normatif yaitu jenis penelitian hukum yang dilakukan dengan meneliti bahan pustaka atau data sekunder. Hasil dari penelitian ini menunjukan bahwa Uni Eropa mengharuskan Negara anggota membentuk kerangka kerja nasional yang perlu diadopsi oleh setiap Negara anggota terkait keamanan jaringan dan sistem informasi yang diatur dalam *Directive on Security of Network and Information Systems (NIS Directive 2016)*, kemudian secara signifikan memperkuat yurisdiksi dan peran *European Union Agency for Cybersecurity* (ENISA) dengan memberlakukan *European Union Cybersecurity Act 2019*. Uni Eropa berfokus pada keamanan perangkat keras dan perangkat lunak sehingga dapat memperkuat *cyber security* produk dengan elemen digital (*digital product*) yang ada yang diatur dalam proposal *Cyber Resilience Act*. Kebijakan *Blockchain* dapat mencegah terjadinya penyalahgunaan data oleh pihak ketiga karena data atau aset digital yang dipertukarkan, diverifikasi, dan disimpan dalam sebuah jaringan desentralisasi secara aman, transparan, dan tidak dapat diubah. ENISA sebagai badan yang mengatur *cyber security* harus berperan aktif dengan memberi respon terhadap insiden seperti adanya serangan siber atau ancaman siber seperti pelanggaran data pribadi seperti yang mana wewenang tersebut secara tegas dinyatakan dalam pasal 11 huruf (a) *EU Cybersecurity Act* 2019 serta melakukan tidakan untuk menunjang implementasi dari *General Data Protection Regulation* (GDPR) dan berbagai inisiatif terkait *cyber security*.

Kata Kunci: *Cyber space*, *Cyber crime*, Pelanggaran Data Pribadi, *Cyber Security*, *Cyber Resilience Act*, Uni Eropa