BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Perkembangan teknologi informasi dan komunikasi telah membawa perubahan signifikan dalam pola interaksi sosial, ekonomi dan hukum di tingkat global. Digitalisasi yang semakin masif melalui media sosial, aplikasi pesan instan, serta sistem keuangan digital telah menciptakan ruang interaksi lintas negara yang tidak lagi dibatasi oleh batas teritorial. Transformasi ini kemudian memberikan berbagai macam manfaat, seperti efisiensi komunikasi, kemudahan transaksi ekonomi dan percepatan arus informasi. Namun, di sisi lain, perkembangan tersebut juga memunculkan bentuk-bentuk ancaman baru yang bersifat non-tradisional, salah satunya adalah kejahatan siber atau *cybercrime* yang semakin kompleks, anonim, dan bersifat transnasional (United Nations Office on Drugs and Crime, 2022).

Salah satu bentuk kejahatan siber yang menunjukkan eskalasi signifikan dewasa ini adalah *love scamming*, yaitu modus penipuan daring yang memanfaatkan hubungan emosional dan kepercayaan korban untuk memperoleh keuntungan finansial. Kejahatan ini umumnya dilakukan melalui media sosial, aplikasi pencari jodoh daring, dan platform komunikasi digital lainnya. Pelaku kemudian membangun relasi secara bertahap, dimulai dari menciptakan emosional semu, sebelum melakukan manipulasi dan eksploitasi ekonomi terhadap korban. Karakteristik tersebut menjadikan *love scamming* menjadi sulit terdeteksi sejak awal dan sering kali baru disadari setelah korban mengalami kerugian finansial dan psikologis yang signifikan. Selain kerugian material, kejahatan ini juga berdampak pada aspek keamanan manusia atau *human security*. Khususnya pada keamanan ekonomi dan kesehatan individu bagi korban (Erikha & Saptomo, 2024 p. 500-504). Dampak finansial yang besar, rasa trauma, serta hilangnya kepercayaan korban terhadap ruang digital yang kemudian menunjukkan bahwa kejahatan ini memiliki implikasi sosial yang luas. Oleh karena itu, negara tidak hanya dituntut untuk memiliki kerangka hukum formal,

tetapi juga kapasitas institusional dan tata kelola keamanan siber yang mampu merespons ancaman tersebut secara adaptif dan terkoordinasi (Krahmann, 2003; Salifu & Hafeez-Baig, 2021).

Periode tahun 2020 hingga 2025 merupakan fase krusial dalam eskalasi kasus *love scamming*. Pandemi COVID-19 yang dimulai pada tahun 2020 meningkatkan ketergantungan masyarakat terhadap ruang digital untuk berinteraksi, bekerja, serta melakukan aktivitas ekonomi. Kondisi ini secara pararel membuka peluang yang besar bagi pelaku kejahatan siber untuk mengeksploitasi relasi daring. Secara global, fenomena ini juga tercermin dalam laporan *Federal Trade Commision* (FTC) Amerika Serikat yang berhasil mencatat kerugian finansial pada tahun 2020 akibat *romance scam* yang mencapai USD 304 juta. Kerugian tersebut meningkat sekitar 50 persen dibandingkan tahun sebelumnya, dengan total kerugian kumulatif mencapai 1,3 miliar dalam rentang lima tahun (Federal Trade Commission, 2021).

Di tingkat nasional, tren peningkatan kejahatan penipuan berbasis digital juga terlihat secara signifikan di Indonesia. Otoritas Jasa Keuangan (OJK) mencatat bahwa hingga tahun 2025 terdapat sekitar 297.000 laporan tentang kasus penipuan daring dengan total kerugian masyarakat mencapai Rp 7 triliun. Data ini menunjukkan tingginya tingkat kerentanan masyarakat terhadap penipuan digital serta menegaskan adanya tantangan yang serius dalam sistem keamanan siber nasional (Otoritas Jasa Keuangan, 2025). Tingginya angka tersebut juga mengindikasikan bahwa penipuan berbasis relasi daring, termasuk *love scamming*, menjadi bagian penting dari penipuan digital yang lebih luas.

Lebih lanjut, laporan Otoritas Jasa Keuangan melalui Indonesia Anti Scam Center (IASC) menunjukkan bahwa hingga akhir Mei 2023 tercatat sebanyak 135.397 laporan kasus penipuan keuangan digital yang melibatkan lebih dari 219.168 rekening. Total kerugian dari akibat penipuan daring hingga pertengahan 2025 mencapai Rp 2,6 triliun. Sebagian besar laporan tersebut berkaitan dengan penipuan finansial yang berawal dari interaksi digital, termasuk modus yang

memiliki kemiripan kuat dengan *love scamming* (Meilina, 2025). Data ini memperlihatkan bahwa ancaman *love scamming* tidak dapat dipisahkan dari meningkatnya skala penipuan online secara umum.

Selain itu, laporan media nasional menunjukkan bahwa Indonesia mencatat sejumlah laporan penipuan daring yang sangat tinggi dibandingkam dengan negara lain di kawasan. Pada tahun 2025, jumlah laporan penipuan digital di Indonesia bahkan jauh lebih tinggi dibandingkan dengan Singapura dan Hong Kong, yang masing-masing mencatat ratusan laporan kasus (Romualdus, 2025). Kondisi ini kembali menegaskan bahwa permasalahan penipuan digital di Indonesia termasuk berskala besar.

Sementara itu, data lain juga menunjukkan adanya dimensi sosial yang mengkhawatirkan dari kejahatan siber. Sejak 2020 hingga 2024, lebih dari 5.000 warga negara Indonesia tercatat dalam kasus *online scam*, baik sebagai korban maupun pelaku. Fenomena ini menandai pergeseran berbahaya dalam dinamika *cybercrime*, di mana penipuan daring mulai dipersepsikan oleh sebagian individu sebagai sumber penghasilan, sehingga berpotensi memperluas ekosistem kejahatan siber dan meningkatkan jumlah korban di masa depan (Kompas Nasional, 2024).

Otoritas Jasa Keuangan (OJK) melalui IASC juga mencatat telah menerima 3.494 laporan terkait modus penipuan asmara atau *love scam* sepanjang 2025, dengan kerugian finansial yang signifikan di kalangan masyarakat Indonesia. Laporan ini menunjukkan bahwa *love scamming* bukan lagi merupakan fenomena sporadis, tetapi telah berkembang menjadi bagian dari tren kejahatan siber yang merugikan banyak warga negara secara ekonomi dan psikologis (Tempo.co, 2026). Data ini kemudian diperkuat oleh catatan lain dari IASC yang menunjukkan bahwa dalam periode sebelumnya lembaga ini telah menerima puluhan ribu laporan scam digital dengan nilai total kerugian masyarakat mencapai triliunan rupiah, didominasi oleh berbagai modus penipuan online yang saling terkait, termasuk *love scamming* (InvestorTrust.id, 2025).

Kondisi tersebut diatas menunjukkan bahwa *love scamming* merupakan bagian dari fenomena yang lebih luas, yaitu peningkatan kejahatan siber yang memiliki dampak serius pada aspek ekonomi dan psikologis korban (United Nations Office on Drugs and Crime, 2022). Dampak finansial dari penipuan yang semacam ini tidak hanya bersifat individual, tetapi juga mengancam kepercayaan publik terhadap ekosistem digital, selain itu dampak psikologis yang ditimbulkan oleh manipulasi emosional dapat menyebabkan trauma jangka panjang bagi korban, sehingga menjadikan *love scamming* sebagai ancaman terhadap *human security* (Erikha & Saptomo, 2024 p. 500-504).

Tingginya kasus *love scamming* di Indonesia juga menyoroti keterbatasan kerangka hukum dan kapasitas institusional negara. Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) sebagai payung hukum utama dalam penanganan kejahatan siber dinilai belum sepenuhnya adapif terhadap perkembangan modus kejahatan digital yang semakin canggih, termasuk pemanfaatan media sosial, kecerdasan buatan, dan aset kripto. Selain itu, penanganan kasus *love scamming* masih menghadapi kendala berupa lemahnya koordinasi antarlembaga, fragmentasi kewenangan, dan belum optimalnya mekanisme perlindungan komprehensif bagi korban (Erikha & Saptomo, 2024 p. 500-506).

Situasi serupa juga terjadi di Singapura, di mana *love scamming* termasuk dalam salah satu jenis kejahatan siber yang sering dihadapi oleh penegak hukum. Laporan *Mid-Year Scams and Cybercrime Brief* 2024 yang diterbitkan oleh *Singapore Police Force (SPF)* menunjukkan bahwa diantara berbagai jenis scam yang dilaporkan, *Internet Love Scams* tercatat sebagai salah satu kategori yang signifikan dalam jumlah kasus, dengan ratusan kasus dilaporkan dalam satu semester pertama tahun 2024 (Singapore Policy Force, 2024). Dalam konteks kawasan Asia Tenggara, ancaman *love scamming* tidak hanya dihadapi oleh Indonesia dan Singapura saja, tetapi juga oleh negara-negara anggota ASEAN lainnya. Sebagai sesama anggota ASEAN, Indonesia dan Singapura juga berada di bawah payung kerja sama regional ASEAN *Plan of Action to Combat*

Transnational Crime, yang menempatkan kejahatan siber dan penipuan lintas batas sebagai agenda prioritas. Kerangka ASEAN *Plan of Action to Combat Transnational Crime* secara normatif mendorong harmonisasi kebijakan, pertukaran informasi, serta penguatan kerja sama antarnegara dalam menangani kejahatan transnasional, termasuk penipuan dan kejahatan siber (ASEAN Senior Officials Meeting on Transnational Crime, 2022).

Dalam konteks kawasan Asia Tenggara, penanganan kejahatan siber dan penipuan lintas batas telah menjadi agenda kolektif negara-negara anggota ASEAN melalui ASEAN *Plan of Action to Combat Transnational Crime*. Dokumen tersebut menempatkan kejahatan siber sebagai salah satu bentuk ancaman transnasional prioritas yang memerlukan harmonisasi kebijakan, penguatan kapasitas nasional, serta peningkatan kerja sama lintas negara (ASEAN Senior Officials Meeting on Transnational Crime, 2022). Melalui rencana aksi tersebut, negara anggota ASEAN didorong untuk mengintegrasikan komitmen regional ke dalam kebijakan nasional masing-masing, termasuk dalam aspek pencegahan, penegakan hukum, serta perlindungan terhadap korban kejahatan digital.

ASEAN Plan tersebut tidak hanya bersifat deklaratif, tetapi berfungsi sebagai kerangka normatif yang mengarahkan strategi nasional dalam menghadapi ancaman lintas batas. Dalam dokumen tersebut ditegaskan pentingnya koordinasi antarlembaga, pertukaran informasi, serta penguatan sistem regulasi domestik guna merespons dinamika kejahatan transnasional yang semakin kompleks (ASEAN Senior Officials Meeting on Transnational Crime, 2022). Dengan demikian, penanganan *love scamming* oleh Indonesia dan Singapura tidak dapat dipahami semata-mata sebagai kebijakan domestik, melainkan sebagai bagian dari implementasi komitmen regional ASEAN dalam memerangi kejahatan transnasional.

Namun, meskipun berada di bawah payung komitmen regional yang sama, implementasi dan efektivitas respons antarnegara ASEAN menunjukkan variasi

yang signifikan. Kesamaan norma dan kerangka kebijakan regional tidak secara otomatis menghasilkan kesamaan kapasitas institusional maupun efektivitas penanganan di tingkat nasional. Variasi ini menimbulkan pertanyaan analitis mengenai bagaimana komitmen regional tersebut diterjemahkan ke dalam desain institusi, kebijakan, dan praktik nasional yang berbeda-beda (ASEAN Senior Officials Meeting on Transnational Crime, 2022).

Indonesia dan Singapura dipilih sebagai kasus pembanding dalam penelitian ini karena keduanya sama-sama merupakan anggota ASEAN yang terikat pada ASEAN *Plan of Action to Combat Transnational Crime* serta menghadapi ancaman *love scamming* yang bersifat lintas batas dan memanfaatkan ekosistem digital modern. Kesamaan posisi dalam kerangka regional tersebut menjadikan keduanya relevan untuk dibandingkan dalam pendekatan *Most Similar System Design* (Przeworski & Teune, 1970). Dengan dasar normatif yang sama, perbandingan ini bertujuan untuk mengidentifikasi faktor-faktor domestik yang menjelaskan perbedaan dalam efektivitas respons kebijakan.

Meskipun demikian, data empiris yang sudah disebutkan sebelumnya menunjukkan adanya perbedaan dalam skala kasus dan respons kebijakan antara kedua negara. Indonesia mencatat ratusan ribu laporan penipuan daring dengan kerugian mencapai triliunan rupiah, termasuk ribuan kasus *love scamming* (Meilina, 2025). Sementara itu, Singapura juga menghadapi kasus Internet *Love Scams* dalam jumlah signifikan, namun menunjukkan sistem pelaporan terpadu dan mekanisme pembekuan dana yang relatif lebih cepat melalui koordinasi antarlembaga (Singapore Police Force, 2024). Perbedaan ini menjadi menarik untuk dianalisis karena muncul dalam konteks komitmen regional yang sama sebagaimana tertuang dalam ASEAN *Plan of Action to Combat Transnational Crime* (ASEAN Senior Officials Meeting on Transnational Crime, 2022).

Dengan demikian, urgensi penelitian ini tidak hanya terletak pada tingginya angka kasus *love scamming*, tetapi juga pada kebutuhan untuk memahami bagaimana kesepakatan regional ASEAN diterjemahkan ke dalam kebijakan dan

transformasi institusional di tingkat nasional. Studi perbandingan Indonesia dan Singapura menjadi penting untuk mengkaji variasi implementasi kebijakan dalam kerangka normatif yang sama, serta untuk menjelaskan faktor-faktor yang memengaruhi efektivitas respons negara terhadap ancaman kejahatan siber lintas batas (ASEAN Senior Officials Meeting on Transnational Crime, 2022).

1.2 Permasalahan Penelitian

Bagaimana perbedaan respons antara Indonesia dan Singapura sebagai institusi negara dalam menangani ancaman kejahatan siber *love scamming*?

1.3 Tujuan Penelitian

- Menjelaskan perbedaan respons negara Indonesia dan Singapura dalam menangani kejahatan siber *love scamming*.
- Untuk menganalisis peran dan kapasitas institusi negara dalam menangani *love scamming*
- Melihat tanggung jawab dan *awareness* negara Indonesia dan Singapura dalam menangani kejahatan siber *love scamming*.
- Untuk menganalisis seberapa serius negara Indonesia dan Singapura dalam menjalankan komitmen regional ASEAN diterjemahkan ke dalam kebijakan dan praktik nasional.
- Menilai implikasi respons yang dilakukan oleh negara Indonesia dan Singapura dalam menangani kejahatan siber *love scamming*.

1.4 Manfaat Penelitian

- Memberikan kontribusi terhadap pengembangan kajian Hubungan Internasional, khususnya pada pengayaan studi keamanan non-tradisional dan keamanan siber melalui analisis perbandingan kebijakan negara dalam menghadapi kejahatan transnasional.
- Memperkaya literatur akademik mengenai kejahatan siber berbasis relasi emosional (*love scamming*) dengan menekankan pada pentingnya peran keamanan manusia *(human security)* dan kebijakan domestik dalam

kerangka studi perbandingan antarnegara.

- Memberikan kontribusi terhadap pengembangan penggunaan teori transformasi negara atau *state transformation* dalam konteks Asia Tenggara. Dengan mengkaji peran negara, institusi penegak hukum, dan kerangka kerja sama regional (ASEAN SOMTC), penelitian ini menunjukkan bahwa tata kelola keamanan siber tidak hanya ditentukan oleh kekuatan negara semata, tetapi juga oleh koordinasi lintas institusi dan tingkat implementasi kebijakan.
- Memberikan contoh penerapan studi perbandingan dengan desain *Most Similar System Design (MSSD)* dalam kajian keamanan siber. Pendekatan ini memperkuat tradisi metodologis dalam studi Hubungan Internasional dengan menunjukkan bagaimana perbedaan hasil kebijakan dapat dianalisis diantara negara-negara yang memiliki karakteristik regional dan komitmen internasional yang relatif serupa.
- Menjadi bahan evaluasi kebijakan bagi institusi terkait di Indonesia seperti Kepolisian Republik Indonesia (Polri), Otoritas Jasa Keuangan (OJK), dan lembaga keamanan siber, dalam memperkuat mekanisme penanganan kasus *love scamming*. Hasil dari penelitian ini dapat membantu mengidentifikasi kelemahan koordinasi antarlembaga serta celah dalam implementasi kebijakan yang selama ini menghambat perlindungan korban.

1.5 Sistematika penulisan

Penulis menyusun skripsi ini dalam lima bab dengan sistematika penulisan sebagai berikut:

BAB I Pendahuluan

Bab ini menguraikan latar belakang masalah yang melandasi penelitian, rumusan masalah, tujuan penelitian, manfaat penelitian, serta sistematika penulisan. Bab ini bertujuan untuk memberikan gambaran umum mengenai urgensi penelitian dan posisi kajian dalam konteks keamanan siber dan Hubungan Internasional.

BAB II Tinjauan Pustaka

Bab ini membahas teori dan konsep yang digunakan sebagai dasar analisis

penelitian. Teori utama yang digunakan adalah teori *state transformation* atau transformasi negara. Pemilihan teori ini didasarkan pada asumsi bahwa respons negara terhadap ancaman keamanan non-tradisional tidak semata-mata ditentukan oleh kapasitas teknis, tetapi oleh konfigurasi kekuasaan, relasi sosial-politik, serta arah perubahan institusional negara dalam konteks globalisasi dan kapitalisme digital. Selain itu, bab ini juga menguraikan konsep keamanan non-tradisional, *human security*, serta memaparkan penelitian terdahulu yang relevan guna menunjukkan posisi dan kontribusi penelitian ini dalam literatur akademik.

BAB III Metodologi Penelitian

Bab ini menjelaskan metode penelitian yang digunakan oleh penulis, yaitu metode penelitian kualitatif dengan pendekatan studi perbandingan. Desain penelitian yang digunakan adalah *Most Similar System Design (MSSD)*, dengan Indonesia dan Singapura sebagai objek perbandingan. Teknik pengumpulan data dilakukan melalui studi kepustakaan yang meliputi, dokumen kebijakan, laporan resmi institusi dan literatur akademik.

BAB IV Analisis dan Pembahasan

Bab ini menyajikan hasil analisis penelitian dengan menggunakan teknik analisis kualitatif-komparatif dan menggunakan desain penelitian MSSD. Analisis dilakukan dengan membandingkan respons di Indonesia dan Singapura dalam menangani kasus *love scamming*. Bab ini juga membahas bagaimana penanganan kasus *love scamming* di Indonesia dan Singapura, perbedaan implementasi kebijakan di Indonesia dan Singapura, mengaitkan kebijakan nasional dengan kerangka kerja regional ASEAN *Plan of Action to Combat Transnational Crime*, serta implikasinya terhadap perlindungan korban dan keamanan siber nasional.

BAB V Penutup

Bab ini berisi kesimpulan dari hasil penelitian serta rekomendasi kebijakan dan saran untuk penelitian selanjutnya.