BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan layanan digital di Indonesia dalam beberapa tahun terakhir meningkat secara signifikan, ditandai dengan penggunaan sistem digital dalam hampir seluruh aktivitas masyarakat, mulai dari registrasi akun, transaksi keuangan, layanan kesehatan, hingga verifikasi identitas berbasis biometrik. Setiap interaksi tersebut menghasilkan beragam data pribadi, termasuk data sensitif seperti biometrik, lokasi dan riwayat perilaku pengguna. Lonjakan volume dan keragaman data ini menjadikan pengelolaan data pribadi sebagai kebutuhan yang semakin penting dalam ekosistem digital modern.

Namun, pertumbuhan digitalisasi tersebut tidak diimbangi dengan kesiapan keamanan dan tata kelola data yang memadai. Laporan resmi BSSN menunjukkan bahwa sepanjang 2024 terdapat 241 dugaan insiden kebocoran data di Indonesia, serta lebih dari 56 juta data terekspos di *darkweb* [1]. Temuan tersebut mengindikasikan bahwa banyak organisasi masih memiliki kelemahan fundamental dalam melindungi data pribadi. Kebocoran informasi seperti identitas pengguna, data biometrik, hingga riwayat aktivitas aplikasi menimbulkan risiko signifikan terhadap keamanan individu serta menurunkan tingkat kepercayaan masyarakat terhadap layanan digital.

Meskipun risiko privasi semakin tinggi, sebagian besar platform digital belum memiliki mekanisme penilaian risiko yang terstruktur dan terstandarisasi. Banyak metode penilaian risiko saat ini masih bersifat manual yang subjektif, atau hanya berfokus pada aspek keamanan infrastruktur (*security*) tanpa mempertimbangkan dimensi privasi (*privacy*) secara khusus. Pendekatan tersebut menghasilkan evaluasi yang tidak konsisten, sulit direplikasi dan tidak mampu mengikuti dinamika pemrosesan data yang sangat cepat dalam lingkungan digital. Hal ini menciptakan kesenjangan antara kebutuhan penilaian risiko privasi dan alat bantu yang tersedia.

Indonesia telah memiliki Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP 2022) sebagai landasan hukum utama, serta standar internasional seperti kerangka kerja NIST Cybersecurity *Framework* 2.0 yang memberikan panduan tata kelola risiko. Namun, terdapat kesenjangan teknis dan operasional karena regulasi tersebut masih bersifat kompleks dan belum menyediakan

instrumen penilaian mandiri (*self-assessment*) yang bersifat kuantitatif, otomatis dan berbiaya rendah bagi organisasi. Ketiadaan alat bantu yang dapat menerjemahkan standar kepatuhan ke dalam metrik risiko yang terukur secara objektif menciptakan celah dalam tata kelola keamanan informasi pada platform digital. Berdasarkan celah dan urgensi tersebut, maka diperlukan perumusan masalah yang spesifik untuk membedah bagaimana pendekatan kuantitatif dan aturan hukum dapat diintegrasikan guna menghasilkan sistem analisis risiko privasi yang komprehensif.

1.2 Rumusan Masalah

Berdasarkan latar belakang di atas, maka rumusan masalah penelitian ini adalah sebagai berikut:

1. Bagaimana merancang *framework* analisis risiko privasi yang mengintegrasikan model *Likelihood–Impact* dengan UU PDP 2022 dan *NIST CSF 2.0*?
2. Bagaimana mengimplementasikan *framework* tersebut menjadi sistem web statis untuk penilaian risiko otomatis berbasis parameter teknis?
3. Bagaimana sistem menghasilkan penilaian risiko, status kepatuhan dan rekomendasi mitigasi yang konsisten dan terstandarisasi?

1.3 Batasan Masalah

Pada penelitian ini terdapat batasan-batasan masalah yang bertujuan agar pembahasan terfokus dan terarah. Batasan-batasan tersebut antara lain sebagai berikut:

1. Analisis risiko menggunakan model *Likelihood–Impact* di mana penilaian parameter menggunakan skala input 1–5 untuk menghasilkan matriks risiko.
2. Evaluasi kepatuhan dibatasi pada regulasi UU PDP 2022 dan kerangka kerja *NIST Cybersecurity Framework 2.0*, tanpa membahas regulasi spesifik sektor lain.
3. Sistem mengevaluasi risiko berdasarkan parameter teknis pemrosesan data dan logika privasi, bukan melakukan pengujian keamanan infrastruktur secara aktif.
4. Aplikasi dibangun berbasis web statis yang pengolahan datanya berjalan sepenuhnya di sisi klien (*client-side*) demi menjaga privasi data input, di mana validasi legalitas menggunakan basis data internal (statis/*whitelist*) dan belum terhubung secara *real-time* dengan API regulator eksternal.
5. Penelitian fokus pada perancangan logika dan akurasi *rule-engine*, tidak mengevaluasi performa beban aplikasi (*load testing*) dalam skala besar.

6. Rekomendasi mitigasi yang dihasilkan bersifat umum (*best practice*) berdasarkan aturan yang ditanamkan, bukan rekomendasi spesifik yang disesuaikan dengan konteks bisnis unik setiap organisasi.

1.4 Tujuan Penelitian

Tujuan dari penelitian ini adalah untuk:

1. Menghasilkan *framework* analisis risiko privasi yang mengintegrasikan model kuantitatif *Likelihood–Impact* dengan aturan berbasis regulasi UU PDP 2022 dan *NIST CSF 2.0*.
2. Mengimplementasikan *framework* tersebut ke dalam sistem web statis berbasis *client-side* yang mampu melakukan kalkulasi dan visualisasi risiko privasi secara otomatis tanpa memerlukan infrastruktur *backend* yang kompleks.
3. Menyediakan alat bantu (*tool*) yang mampu menghasilkan laporan terstandarisasi berupa tingkat risiko, status kepatuhan, serta rekomendasi mitigasi yang konsisten untuk membantu organisasi melakukan *self-assessment*.

1.5 Manfaat Penelitian

Penelitian ini diharapkan memberikan manfaat baik secara teoritis maupun praktis sebagai berikut:

1. Manfaat Teoritis
    1) Memberikan kontribusi ilmiah terkait integrasi model kuantitatif (*Likelihood–Impact*) dengan pendekatan kualitatif berbasis regulasi (*rule-based*) dalam konteks manajemen risiko privasi.
    2) Menjadi landasan akademis bagi penelitian lanjutan mengenai teknik *privacy by design* dan pemodelan risiko yang menjembatani aspek teknis dengan aspek hukum (UU PDP 2022).

2. Manfaat Praktis

   a. Menyediakan alat bantu otomatis yang mengurangi subjektivitas dan waktu yang dibutuhkan dalam penilaian risiko privasi, mengatasi kelemahan metode manual yang ada saat ini.

   b. Memberikan solusi penilaian risiko yang aman bagi organisasi, di mana proses kalkulasi berjalan sepenuhnya di sisi pengguna (*client-side*) sehingga data sensitif terkait sistem yang dinilai tidak terekspos ke pihak ketiga.

   c. Membantu masyarakat, organisasi, pengembang dan auditor internal untuk mengukur tingkat kepatuhan awal terhadap UU PDP 2022 dan *NIST CSF 2.0* secara mandiri (*self-assessment*) dengan biaya yang terjangkau (*low-cost*).

   d. Mempermudah pemangku kepentingan dalam mengidentifikasi celah privasi spesifik dan mendapatkan rekomendasi teknis yang dapat langsung ditindaklanjuti (*actionable insights*).

1.6 Sistematika Penulisan

Penulisan laporan skripsi ini disusun secara sistematis agar memudahkan dalam penyampaian informasi dan mempermudah pembaca dalam memahami alur penelitian. Adapun susunan bab dalam laporan ini adalah sebagai berikut:

1. BAB I PENDAHULUAN

   Berisi gambaran umum mengenai penelitian, meliputi latar belakang, rumusan masalah, tujuan penelitian, batasan masalah, manfaat penelitian, serta sistematika penulisan. Bab ini menjadi dasar dalam memahami urgensi dan arah penelitian yang dilakukan.

2. BAB II TINJAUAN PUSTAKA

   Bab ini memuat studi literatur yang relevan dengan topik penelitian, yang disusun dari konsep umum hingga konsep khusus. Pembahasan meliputi teori dasar mengenai privasi data, risiko privasi, model *Likelihood–Impact*, *rule-based system*, serta kerangka regulasi dan standar keamanan informasi seperti Undang-Undang Perlindungan Data Pribadi (UU PDP 2022) 2022 dan *NIST Cybersecurity Framework 2.0*. Bab ini juga menyajikan penelitian terdahulu sebagai dasar penyusunan *framework* analisis risiko yang dikembangkan.

3. BAB III METODE PENELITIAN

Bab ini menjelaskan metode dan pendekatan penelitian yang digunakan, termasuk objek penelitian, alur penelitian, metode pengembangan sistem, perancangan *framework* analisis risiko, serta rancangan aplikasi yang diimplementasikan. Bab ini juga memuat alur penelitian, perancangan arsitektur, perancangan *rule-engine* dan instrumen yang digunakan dalam pengembangan sistem analisis risiko privasi berbasis web statis. Penelitian ini berfokus pada analisis parameter teknis dan pengembangan artefak sistem berbasis web.

4. BAB IV HASIL DAN PEMBAHASAN

Bab ini menyajikan hasil implementasi sistem dan pembahasan terkait kinerja *framework* analisis risiko privasi yang telah dikembangkan. Hasil ditampilkan dalam bentuk dashboard yang memuat nilai risiko (*Likelihood–Impact*), kategori risiko, matriks risiko, evaluasi kepatuhan terhadap UU PDP 2022 dan *NIST CSF 2.0*, serta rekomendasi mitigasi otomatis. Pembahasan difokuskan pada analisis hasil untuk berbagai skenario pemrosesan data pribadi dan bagaimana *framework* ini dapat digunakan untuk mendukung penilaian risiko yang lebih objektif dan terstruktur.

5. BAB V PENUTUP

Bab ini berisi kesimpulan dari penelitian yang telah dilakukan serta saran yang dapat dijadikan acuan untuk pengembangan penelitian selanjutnya. Kesimpulan merangkum kontribusi penelitian dalam membangun *framework* dan sistem analisis risiko privasi, sedangkan saran mencakup peluang pengembangan lanjutan baik dari sisi teknis maupun penerapan di dunia nyata.