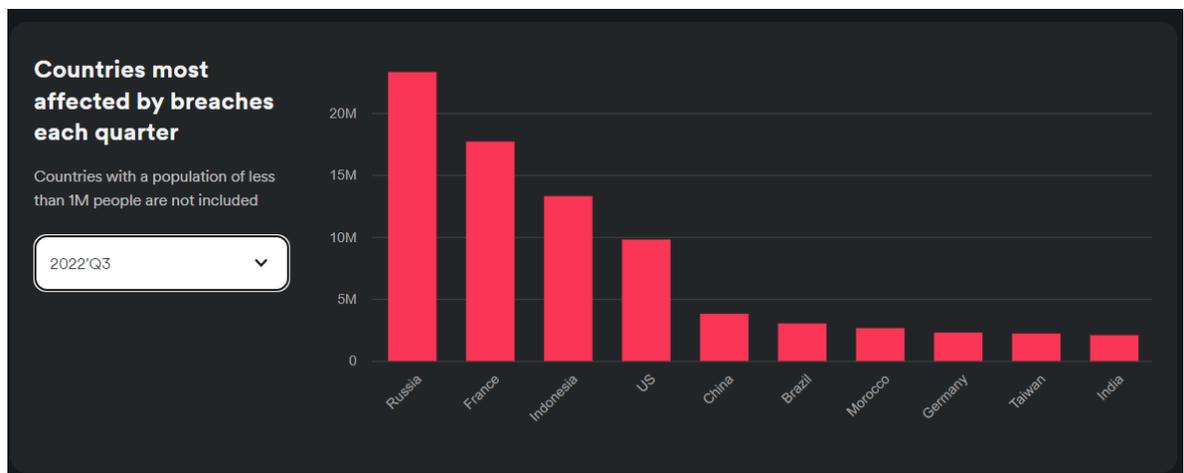


# BAB I

## PENDAHULUAN

### 1.1. Latar Belakang Masalah

Pada Januari 2024, Surfshark sebagai layanan VPN internasional melaporkan *recap* 2023 tentang kebocoran data digital yang terjadi di dunia mencapai 299.8 juta akun (Surfshark, 2024). Amerika Serikat menjadi negara dengan kebocoran data terbanyak sebesar 96,7 juta akun, diikuti oleh Rusia dengan 78,4 juta akun. Padahal pada tahun 2022, Biztech Academy menyebutkan bahwa Amerika Serikat mendapatkan skor sempurna 100 dalam Global Security Indeks (GCI) dan menduduki peringkat pertama dalam kekuatan siber global (Biztech Academy, 2024). Sedangkan pada kuartal pertama tahun 2024, Surfshark menunjukkan bahwa kebocoran data digital yang terjadi di Amerika Serikat meningkat menjadi 102 juta akun. Sementara posisi Rusia digantikan oleh China dengan kebocoran data 70 juta akun. Data ini mengindikasikan bahwa meskipun negara maju dengan tingkat keamanan data yang tinggi telah membuat kemajuan dalam perlindungan data, ancaman kebocoran tetap tinggi. Fenomena kebocoran data digital menjadi masalah global yang perlu diwaspadai.

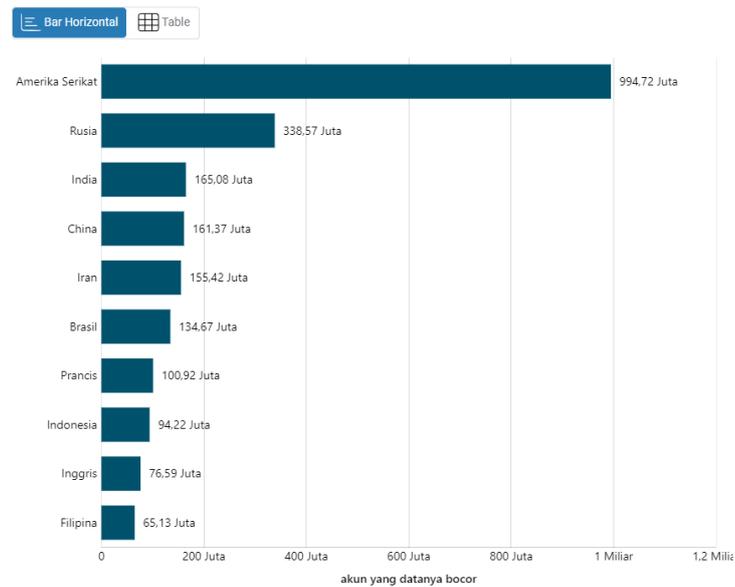


Gambar 1. 1 Countries Most Affected by Breaches Each Quarter

(Sumber: surfshark.com)

10 Negara dengan Kebocoran Data Terbesar (Januari 2020-Januari 2024)\*

databoks



Gambar 1. 2 10 Negara dengan Kebocoran Data Terbesar

(Sumber: databoks.katadata.co.id)

Indonesia juga menghadapi ancaman yang serupa. Menurut Surfshark pada kuartal ketiga 2022, Indonesia menduduki posisi ke-3 dengan 13 juta akun yang mengalami kebocoran data digital di dunia (Surfshark, 2024). Laporan Databoks pada Juli 2024 menyebutkan bahwa Indonesia menempati peringkat ke-8 secara global, dengan total kebocoran 94 juta akun selama periode 2020 hingga 2024 (Ahdiat, 2024). Ancaman terhadap kebocoran data digital menjadi salah satu masalah yang serius terutama di negara-negara berkembang seperti Indonesia yang masih rentan terhadap serangan siber.

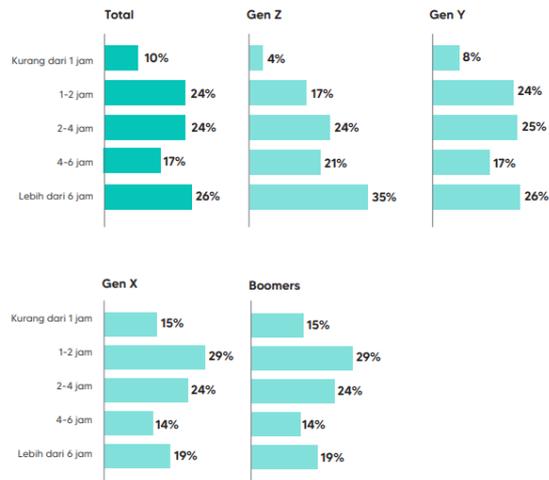
Pada 20 Juni 2024, Indonesia mengalami salah satu insiden kebocoran data besar yang melibatkan Pusat Data Nasional. CNN Indonesia (2024) melaporkan bahwa kebocoran tersebut disebabkan oleh serangan siber berupa *ransomware*, yang dilakukan oleh kelompok peretas Lockbit 3.0 dengan modus pemerasan. Dampaknya, sejumlah layanan publik, salah satunya imigrasi, mengalami gangguan yang cukup lama. Selain itu, sekitar 210 instansi lainnya juga terdampak oleh kebocoran ini. Insiden ini menegaskan pentingnya peningkatan perlindungan dan keamanan data digital di Indonesia, yang masih membutuhkan perhatian lebih serius.

Ancaman kebocoran data digital tidak hanya menasar skala internasional dan nasional, tetapi juga masyarakat luas. Menurut Bisnis.com, tingkat kesadaran masyarakat terhadap keamanan data pribadi mereka masih rendah (Rahardyan, 2021). Salah satu contoh kasus yang terjadi adalah serangan *phishing* yang menimpa pengguna Kredivo pada tahun

2021. Dalam kasus ini, pengguna dihubungi oleh peretas yang menyamar sebagai pihak Kredivo melalui telepon, menawarkan promo, bonus, atau hadiah. Banyak pengguna yang kurang waspada akhirnya menyerahkan data pribadi mereka dengan mudah. Akibatnya, para korban menerima tagihan atas barang yang tidak mereka beli. Serangan *phishing* ini tidak hanya dilakukan melalui telepon, tetapi juga melalui pesan *WhatsApp* hingga tautan-tautan di internet. Kasus ini hanyalah salah satu dari banyak insiden kebocoran data pribadi yang terus mengancam masyarakat.

Selain itu, sejumlah kasus kebocoran data pribadi pada platform layanan publik dan *e-commerce* telah mengakibatkan jutaan data pengguna terancam. Dalam empat tahun terakhir, Medcom.id mencatat bahwa Indonesia telah mengalami setidaknya 10 insiden kebocoran data pribadi (Firdaus, 2024). Data pribadi seseorang mudah terekspos dan dipindahtangankan secara ilegal, tanpa kontrol dari pemiliknya (Yuniarti, 2019). Kondisi ini membuka peluang bagi penyalahgunaan data untuk berbagai tindak kejahatan, seperti penipuan, *phishing*, hingga pencurian identitas.

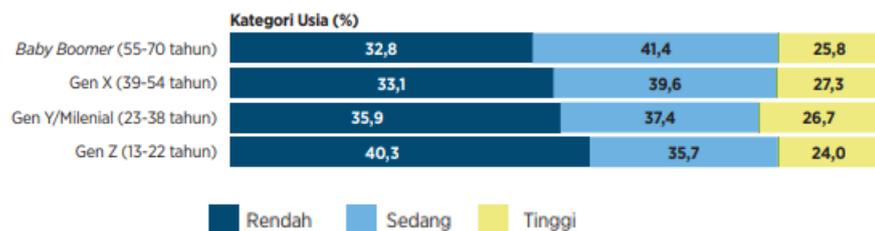
Pada 2024, survei dari Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) mencatat bahwa pengguna internet di Indonesia telah mencapai 214 juta jiwa (APJII, 2024). Penggunaan internet kini tidak lagi terbatas pada komunikasi dan hiburan, tetapi juga mencakup transaksi finansial, penyimpanan informasi pribadi, serta interaksi di berbagai platform media sosial. Menurut Muin (2023), kemajuan teknologi juga membawa tantangan baru, termasuk pengumpulan dan transfer data pribadi tanpa sepengetahuan atau persetujuan pemilik data. Kondisi ini semakin memperkuat urgensi akan pentingnya perlindungan data pribadi, guna menghindari risiko penyalahgunaan dan ancaman keamanan siber.



Gambar 1. 3 Durasi Mengakses Internet

(Sumber: Survei Status Literasi Digital Indonesia 2022)

Menurut data dari KOMINFO dan Katadata Insight Center (2022, hal. 22) dalam Survei Status Literasi Digital Indonesia 2022, remaja di bawah usia 24 tahun merupakan kelompok pengguna internet dengan akses tertinggi, di mana sebanyak 21% dari mereka menghabiskan 4-6 jam, sementara 35% lainnya menghabiskan lebih dari 6 jam per hari di internet. Dari survei yang melibatkan 127 responden, Sebanyak 54% remaja usia 19-24 tahun dilaporkan menggunakan internet selama 5-8 jam per hari, sementara 41% lainnya menghabiskan waktu lebih dari 8 jam per hari. Tingginya durasi penggunaan internet pada kelompok usia ini sejalan dengan meningkatnya risiko kebocoran data pribadi yang semakin sering terjadi di dunia maya.



Gambar 1. 4 Tingkat Pengetahuan Data Pribadi berdasarkan Demograf

(Sumber: Persepsi Masyarakat atas Pelindungan Data Pribadi 2021)

Remaja dengan kategori generasi Z pada Survei Persepsi Masyarakat atas pelindungan data pribadi juga tercatat memiliki tingkat pengetahuan terendah terkait data pribadi, dengan 40,3% memiliki pemahaman rendah dan 35,7% memiliki pemahaman sedang (Kominfo RI, 2021, hal. 27). Dari survei yang melibatkan 127 responden, sebanyak 72% remaja usia 19-24 tahun belum sepenuhnya memahami tentang data pribadi yang mereka miliki, 92% belum mengetahui jenis data pribadi yang mereka miliki, 78% belum

sepenuhnya menyadari tentang keamanan data pribadi mereka di internet, dan 56% belum mengetahui tindakan apa yang harus dilakukan ketika mengalami kebocoran data pribadi di internet. Data tersebut menunjukkan rendahnya tingkat kesadaran remaja usia 19-24 tahun terkait perlindungan data pribadi di internet.

Menurut Syafuddin, Jamalullail, & Rafi'i (2023), kedekatan mereka dengan teknologi membuat kelompok ini rentan terhadap jebakan kejahatan digital. Diananda (2019) menambahkan bahwa pada usia ini, remaja tengah berusaha memantapkan identitas diri, mencapai kemandirian emosional, serta mulai berpikir lebih logis, abstrak, dan idealis. Kondisi psikologis ini membuat mereka lebih aktif dalam menggunakan teknologi, tetapi sekaligus meningkatkan risiko mereka menjadi korban pelanggaran privasi. Dalam kesehariannya remaja tak lepas dari media sosial dan internet yang berfungsi sebagai sumber informasi, media hiburan dan media untuk berkomunikasi dengan teman sebaya melalui media sosial (Pratiwi, Nisa, & Yani, 2021). Oleh karena itu, perhatian khusus perlu diberikan kepada remaja usia 19-24 tahun tentang pentingnya perlindungan data pribadi, mengingat rendahnya kesadaran mereka terhadap ancaman kebocoran data pribadi yang semakin sering terjadi.



Gambar 1. 5 Logo KOMINFO Jawa Timur

(Sumber: [kominfo.jatimprov.go.id](http://kominfo.jatimprov.go.id))

Pemerintah, perusahaan, dan individu perlu meningkatkan kesadaran tentang keamanan data dan mengambil langkah-langkah pencegahan yang tepat untuk melindungi data pribadi (Anggen Suari & Sarjana, 2023). KOMINFO memiliki peran yang sangat penting dan berhak dalam menyebarkan pesan edukasi tentang perlindungan data pribadi, mengingat posisinya sebagai lembaga pemerintah yang berfokus pada regulasi dan pengelolaan komunikasi serta informasi di Indonesia. Dengan pengaruh dan jangkauannya yang luas, KOMINFO dapat memastikan pesan mengenai pentingnya perlindungan data pribadi tersebar secara efektif ke seluruh lapisan masyarakat. Dalam perancangan ini, KOMINFO Jawa Timur akan diusulkan sebagai *stakeholder* yang berperan dalam

memberikan arahan serta mendukung proses publikasi agar pesan dapat tersampaikan secara luas, terutama kepada remaja usia 19-24 tahun. Kerja sama ini menjadi langkah strategis untuk mengedukasi publik mengenai risiko kebocoran data dan urgensi menjaga keamanan data pribadi di era digital.

Media visual, khususnya animasi, telah terbukti menjadi sarana yang efektif dalam menyampaikan pesan kompleks dengan cara yang menarik dan mudah dipahami. Dari survei yang melibatkan 127 responden, menunjukkan bahwa 86% lebih tertarik pada media animasi berupa infografis yang informatif dan jelas. Ardiansyah, Aninditya, & Nisa (2022) menyebutkan bahwa warga Indonesia memiliki minat besar terhadap animasi, yang telah lama menjadi bagian dari keseharian mereka melalui tayangan televisi. Dengan menggunakan media animasi dapat mempermudah menyajikan informasi mengenai proses yang kompleks (Pratama, Widyasari, & Nisa, 2022). Gaya ilustrasi dan animasi yang cocok juga dapat lebih menarik perhatian remaja dalam memahami isi konten yang disajikan. Gaya visual yang digemari para remaja memiliki karakteristik penggambaran anak muda seperti cerita masa sekolah, karakter remaja, dan penggambaran visual yang terbilang cukup sederhana (Nugraha & Nisa, 2023). Dengan demikian, video animasi dinilai sebagai media yang tepat untuk menyampaikan pesan tentang pentingnya menjaga privasi dan keamanan data pribadi terkait perlindungan data pribadi di internet.

Sesuai dengan perkembangan zaman, dirancanglah sebuah perancangan berjudul “Perancangan Video Animasi tentang Pentingnya Pelindungan Data Pribadi di Internet untuk Remaja Usia 19-24 Tahun”. Perancangan ini dibuat sebagai respons terhadap meningkatnya fenomena kebocoran data pribadi digital, baik di Indonesia maupun dunia, yang memicu kekhawatiran akan keamanan data pribadi masyarakat. Target utama dari perancangan ini adalah remaja usia 19-24 tahun yang masih memiliki tingkat pemahaman yang rendah terkait perlindungan data pribadi. Melalui video animasi ini, diharapkan mereka dapat lebih memahami pentingnya menjaga keamanan data pribadi mereka di internet serta mengetahui langkah-langkah yang perlu diambil ketika mengalami kebocoran data. Video animasi ini dirancang untuk menarik perhatian remaja dan menyampaikan pesan dengan cara yang lebih mudah dipahami, sehingga dapat mengedukasi mereka akan pentingnya perlindungan data pribadi di era digital.

## **1.2. Identifikasi Masalah**

- a. Dari data kuesioner yang disebar pada 127 responden, sebesar 72% remaja usia 19-24 tahun belum sepenuhnya paham tentang data pribadi yang mereka miliki. Hal ini diperkuat oleh hasil wawancara dengan KOMINFO Jawa Timur, dosen ahli data digital, serta tanggapan dari audiens.
- b. Dari data kuesioner yang disebar pada 127 responden, sebesar 92% remaja usia 19-24 tahun belum bisa mengidentifikasi data pribadi mereka, khususnya data pribadi umum dan spesifik. Hal ini diperkuat oleh hasil wawancara dengan audiens.
- c. Dari data kuesioner yang disebar pada 127 responden, sebesar 78% remaja usia 19-24 tahun belum sepenuhnya sadar tentang pentingnya perlindungan data pribadi mereka di internet. Hal ini diperkuat oleh hasil wawancara dengan audiens.
- d. Dari data kuesioner yang disebar pada 127 responden, sebesar 56% remaja usia 19-24 tahun belum mengetahui tindakan apa yang harus dilakukan ketika mengalami kebocoran data pribadi mereka di internet. Hal ini diperkuat oleh hasil wawancara dengan KOMINFO Jawa Timur.
- e. Wawancara dengan audiens, stakeholder, dan narasumber ahli menunjukkan bahwa video animasi adalah media terbaik untuk mengedukasi remaja 19–24 tahun tentang perlindungan data pribadi. Hal ini diperkuat oleh kuesioner, di mana 86% dari 127 responden mendukung animasi infografis sebagai media edukasi yang menarik dan informatif.

## **1.3. Rumusan Masalah**

Rumusan masalah pada perancangan kali ini adalah “Bagaimana merancang video animasi yang informatif dan menarik kepada remaja usia 19-24 tahun tentang perlindungan data pribadi?”

## **1.4. Batasan Masalah**

- a. Target audiens yang difokuskan pada perancangan ini adalah remaja usia 19-24 tahun yang memiliki tingkat pemahaman tentang perlindungan data pribadi yang masih rendah
- b. Konten edukasi dalam perancangan ini hanya akan mencakup dasar-dasar perlindungan data pribadi, seperti jenis-jenis data pribadi, pentingnya menjaga keamanan data pribadi, risiko kebocoran data pribadi, dan langkah-langkah yang harus diambil ketika data pribadi bocor. Topik yang lebih teknis dan mendalam, seperti enkripsi atau kebijakan privasi spesifik, tidak akan dibahas secara rinci.

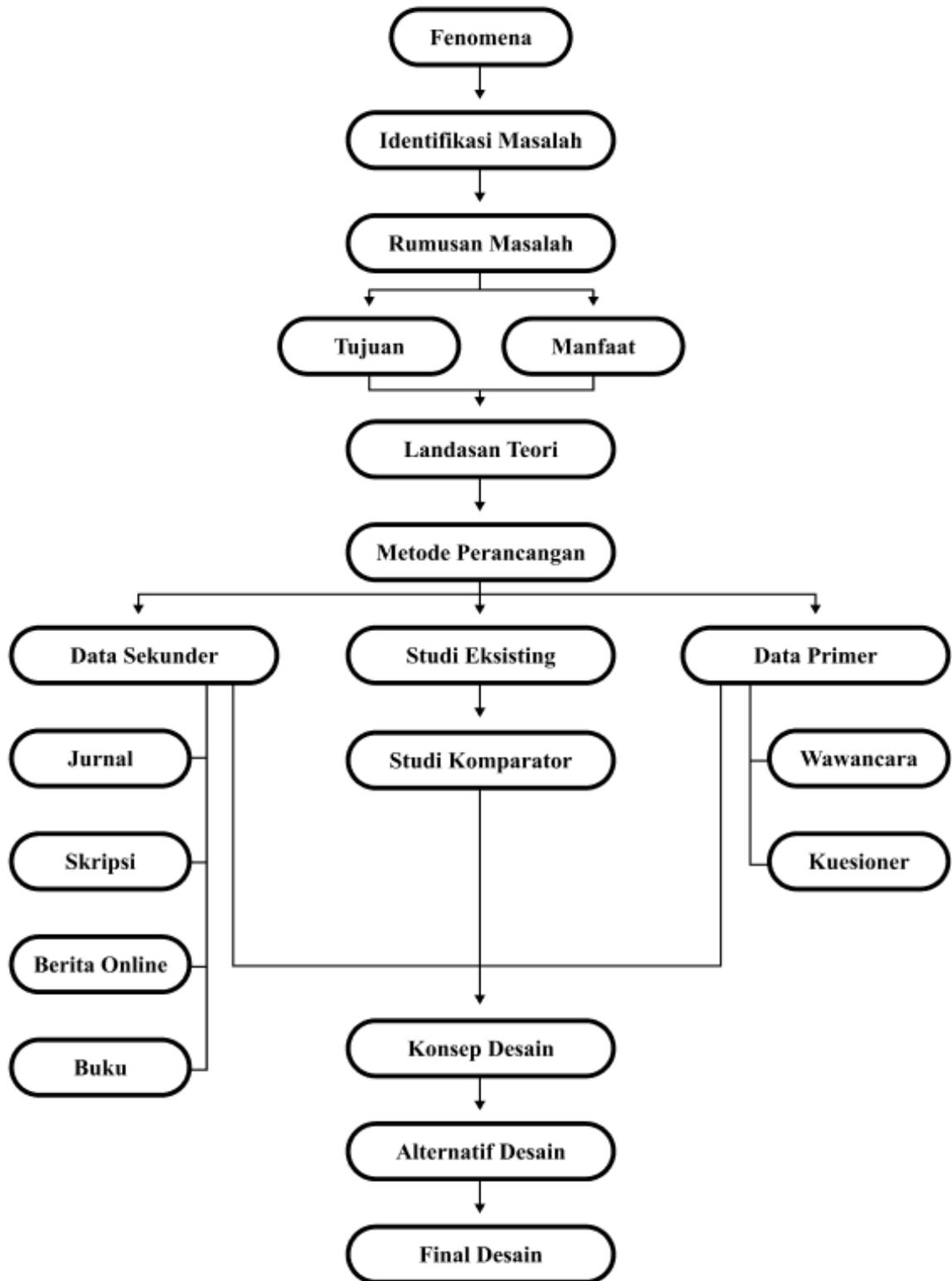
### **1.5. Tujuan Perancangan**

- a. Mengedukasi kalangan remaja usia 19-24 tahun mengenai pentingnya perlindungan data pribadi.
- b. Memberikan pemahaman tentang definisi, jenis-jenis, dan cara mengidentifikasi data pribadi.
- c. Mengedukasi potensi risiko kebocoran data pribadi serta langkah-langkah pencegahannya.
- d. Menyediakan panduan mengenai tindakan yang perlu diambil apabila menjadi korban kebocoran data pribadi.

### **1.6. Manfaat Hasil Perancangan**

- a. Mengedukasi remaja usia 19-24 tahun tentang pemahaman dan kesadaran mengenai pentingnya perlindungan data pribadi di internet, sehingga dapat meminimalkan risiko kebocoran data.
- b. Memberikan pengetahuan yang lebih jelas tentang definisi, jenis-jenis, dan cara mengidentifikasi data pribadi, untuk membantu remaja memahami informasi yang perlu dilindungi.
- c. Memberikan wawasan tentang potensi risiko kebocoran data pribadi dan memberikan langkah-langkah pencegahan yang dapat diambil untuk menghindari pelanggaran privasi.
- d. Menyediakan informasi dan panduan yang tepat mengenai tindakan yang harus diambil oleh remaja jika mereka menjadi korban kebocoran data pribadi, guna meminimalisir dampak negatif yang dapat ditimbulkan.

### 1.7. Kerangka Perancangan



Gambar 1. 6 Kerangka Perancangan  
(Sumber: Dokumentasi Pribadi)