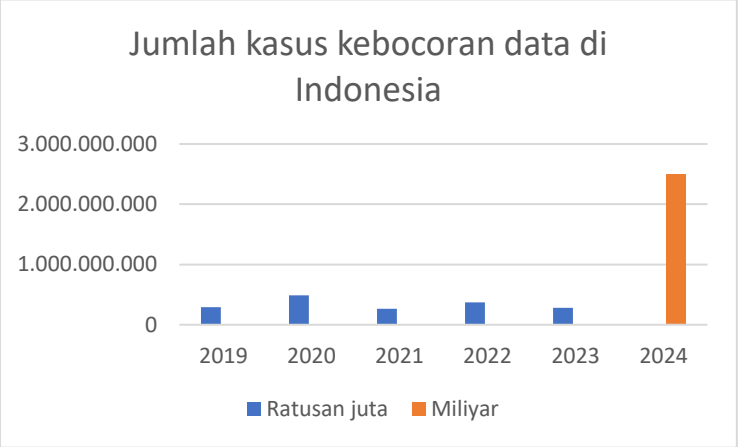
BAB I
PENDAHULUAN

1.1 Latar Belakang

Dinamika kemajuan teknologi komunikasi dan informasi dalam berbagai aspek kehidupan manusia sekarang ini tidak hanya memberikan dampak positif tetapi juga terdapat dampak negatif (Utin Indah, 2021). Perkembangan teknologi telah menyeluruh di kehidupan manusia, hampir keseluruhan aspek saat ini menyangkut pada teknologi digital, dari mulai pemerintahan, bisnis sampai aktivias pribadi. Hal ini ditandai dari munculnya ciptaan-ciptaam baru berbasis teknologi seperti *smartphone, laptop,* televesi, *personal computer (PC), air conditioner,* gelombang radio, dan sebagainya. Tetapi bersamaan dengan kemajuan teknologi ini, ancaman terhadap data dan informasi menjadi semakin meningkat. Dampak negatif yang muncul dari perkembngan teknologi dan ketidaksesuaian penggunaan ini menimbulkan suatu kejahatan yang dikenal dengan istilah kejahatan siber *(cyber crime)* (Arief, 2012).

Kejahatan siber atau *cyber crime* merupakan tindakan kriminal yang terjadi melalui pemanfaatan perangkat komputer, jaringan internet, atau teknologi informasi dan komunikasi lainnya sebagai sarana utama (McGuire, Mike, and Samantha Dowling, 2013). *Cyber crime* membuka peluang besar untuk pelaku melewati berbagai ruang dan waktu dengan jangkauan global. Kejahatam di dunia maya dapat dilakukan dimanapun dan kapanpun dengan mengandalkan jaringan internet dan peralatan yang memadai. Berkembangnya kejahatan dunia maya atau *cyber crime* dapat ditandai dari munculnya berbagai istilah *seperti online business crime, high tech white collar crime, cyber money laundering,* dan sebagainya. Bahkan dalam dokumen PBB, *cyber crime* mempunyai istilah baru yakni, *Dogpiling, Dixing, Doxware*, kejahatan seputar identitas, pelecehan seksual bermotif gambar, *online impersonation, roasting, pharming, sextortion, dan Zero day.*

Gambar 1 Jumlah kasus kebocoran data 5 tahun terakhir (2019-2024)



sumber: Tempo.co

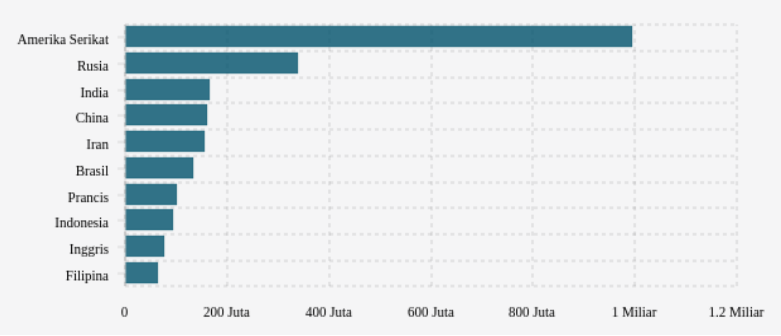
Berdasarkan data grafik di atas, kasus *cyber crime* di Indonesia tahun 2024 mengalami kenaikan drastis hingga enam kali lipat dibanding tahun sebelumnya. Tingginya angka kasus *cyber crime* ini menuntut masyarakat agar memahami keamanan dalam menggunakan internet, yang dikenal dengan istilah keamanan siber (*cyber security).* Pemahaman *cyber security* sangat penting untuk mengetahui berbagai ancaman yang dapat muncul dan cara mengatasi ancamannya (Wahyu, et.al, 2021). *Cyber security* adalah sekumpulan alat, kebijakan, prinsip perlindungan, perlindungan keselamatan, pedoman, strategi pengendalian peluang, strategi manajemen risiko, pelatihan, langkah-langkah, praktik unggulan, perlindungan, serta pemanfaatan teknologi yang bertujuan untuk menjaga keamanan lingkungan siber, organisasi, dan aset milik pengguna.. Keamanan siber diartikan juga sebagai segala Upaya dan proses yang dilakukan untuk mempertahankan serta mengurangi masalah privasi, keintegritasan dan melindungi data yang ada (Ardiyanti, 2016).

Sistem keamanan informasi *(information security)* mempunyai empat tujuan yang sangat mendasar yakni: a). Kerahasiaan *(confidentiality)* yakni informasi yang terdapat pada sistem akan tetap terjaga, sehingga tindakan untuk mencuri informasi tersebut akan gagal. b). Ketersediaan

(availability) mengacu pada upaya untuk memastikan bahwa pengguna yang berwenang selalu dapat mengakses informasi dan sumber daya yang diperlukan, serta menjamin bahwa akses tersebut hanya diberikan kepada individu yang benar-benar sah. c). Integritas *(integrity)* bertujuan untuk menjaga konsistensi data dan memastikan bahwa data tetap sesuai dengan kondisi aslinya. Dengan demikian, setiap upaya perubahan yang dilakukan oleh pihak yang tidak berwenang dapat terdeteksi. d). Penggunaan yang sah *(legitimate use)* merujuk pada jaminan bahwa data dan sumber daya hanya digunakan oleh pihak yang memiliki hak akses, sehingga mencegah penyalahgunaan oleh pihak yang tidak berwenang. (Wahyu, et.al, 2021).

Berdasarkan grafik kebocoran data di bawah ini, Indonesia menempati peringkat kedelapan sebagai negara dengan jumlah insiden kebocoran data tertinggi di dunia. Diperkirakan sebanyak 94,22 juta akun telah terdampak. Estimasi ini berasal dari riset yang dilakukan oleh Surfshark, sebuah perusahaan penyedia layanan *Virtual Private Network* (VPN) yang berbasis di Belanda. Penelitian tersebut mencakup periode Januari 2020 hingga Januari 2024, dan mencatat bahwa secara global terdapat sekitar 3,96 miliar akun digital yang mengalami kebocoran data selama kurun waktu tersebut (Adi ahdiat, 2024).

Gambar 2 Indonesia masuk 10 negara dengan kebocoran data terbesar



sumber: databoks.katadata.co.id

Pada lima tahun terakhir (2020-2024) terjadi kasus-kasus kebocoran data. Pada tahun 2020 bulan Mei terjadi dua kasus secara langsung yakni

kebocoran data pribadi pasien terinfeksi virus corona dijual di forum dark web RaidForums sebanyak 230 ribu data dan terjadi peretasan data pribadi di situs web Komisi Pemilihan Umum sebanyak 2,3 juta. Pada bulan November di tahun yang sama terjadi kebocoran data pengguna di Aplikasi fintech diretas dan dijual bebas pada forum peretas sebanyak 2,9 juta. Lalu pada tahun 2021 di bulan Mei sebanyak 279 juta data BPJS Kesehatan bocor, kemudian sebanyak 1,3 juta data Kartu Kewaspadaan Kesehatan (Electronic Healt Alert Card/eHAC) dari platform verivikasi penumpang selama covid-19 bocor pada bulan Agustus. Selanjutnya pada bulan Oktober terjadi kebocoran data Komisi Perlindungan Anak Indonesia, kemudian pada bulan November 2021 data polri diretas oleh peretas asal Brasil, dengan membocorkan data pribadi. Selanjutnya pada tahun 2023 terjadi Kebocoran data pengguna BPJS Ketenagakerjaan oleh hacker Bjorka sebanyak 19,5 juta. Lalu pada bulan Mei terjadi kebocoran data sebanyak 15 juta melalui LockBit yang menyebarkan data nasabah yang telah dienkripsi dari dark web milik Bank Syariah Indonesia. Kemudian sebanyak 1,64 terabita dokumen di situs resmi milik Kementerian Pertahanan dibobol pada November 2023. (Hendrik Yaputra, 2024).

Kasus kebocoran data di Indonesia paling dominan adalah kebocoran data pribadi. Sepanjang tahun 2024, berbagai insiden kebocoran data tercatat terjadi di berbagai sektor. Kasus yang menonjol terjadi pada bulan Juni, ketika serangan siber oleh kelompok ransomware LockBit 3.0 berhasil melumpuhkan server Pusat Data Nasional sementara. Dampak dari serangan siber ini mengangggu sejumlah layananan publik. Selanjutnya pada Agustus 2024 terjadi kebocoran data NIP dan NIK milik aparatur sipil negara dari Satu Data ASN yang dikelola Badan Kepegawaian Negara. sebesar 4,7 juta data. Kemudian pada bulan September 2024 terjadi kasus kebocoran data Nomor Pokok Wajib Pajak (NPWP) sebanyak 6 juta data, bahkan milik presiden Joko Widodo. (Hendrik Yaputra, 2024).

Gambar 3 Rangkuman kasus kebocoran data 5 tahun terakhir

Fenomena kebocoran data NPWP hingga melibatkan milik presiden menggambarkan rentannya keamanan data pribadi di dunia digital, terutama untuk generasi yang tumbuh bersamaan dengan pesatnya perkembangan internet dan teknologi. Munculnya internet tahun 2000-an menjadikan kelompok Generasi Z yang lahir antara 1997 hingga 2012 adalah generasi yang terhubung dengan dunia digital sejak usia dini. Generasi Z menjadi kelompok yang paling terdampak dan rentan oleh berbagai kebocoran data. Termasuk generasi Z di Kabupaten Tulungagung dengan karakteristik demografis yang dimiliki menggambarkan generasi muda di Indonesia dengan wilayah semi perkotaan. Generasi Z ini artinya hidup dalam linngkungan yang melek akan teknologi digital tetapi tetap erat dengan nilai-nilai budaya lokal. Hal ini tidak terlepas dari Undang-Undang yang telah berlaku untuk menangani berbagai kejahatan di dunia maya. Pemerintah Indonesia telah membentuk undang-undang cyber dalam

rancangan Undang-Undang Informasi dan Transaksi Elektronik (ITE) Nomor 11 Tahun 2008 (Hermawan, 2019). Pengesahan UU ITE ini bertujuan untuk mengurangi, mengatasi, dan menghentikan pelaku kejahatan di dunia maya yang dikenal dengan cyber law Indonesia. Cyber law adalah suatu aspek hukum yang mencakup penerapan yang berkaitan dengan individu atau badan hukum yang menggunakan dan memanfaatkan teknologi internet untuk berinteraksi di dunia maya (Makun, et al., 2024).

Upaya untuk memperkuat strategi regulasi keamanan siber saat ini telah dilakukan melalui Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) beserta ruang lingkupnya, serta Peraturan Pemerintah (PP) tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Melalui ini terbentuk kerangka kerja yang melahirkan sejumlah kebijakan keamanan siber, di antaranya adalah Peraturan Presiden Nomor 82 Tahun 2022 mengenai Perlindungan Infrastruktur Informasi Vital dan Peraturan Presiden Nomor 17 Tahun 2023 mengenai Strategi Nasional Keamanan Siber dan Penanganan Krisis Siber (NeZar Patria, et al., 2024). Berdasarkan pemaparan yang ada, peneliti memiliki ketertarikan untuk meneliti persepsi generasi Z setelah adanya fenomena kebocoran data di Indonesia ini.

1.2 Rumusan Masalah

Berdasarkan pemaparan judul dan latar belakang di atas, maka rumusan masalah dalam penelitian ini sebagai berikut:b

1. Bagaimana persepsi generasi Z pada fanomena kebocoran data di Indonesia?
2. Bagaimana generasi Z menilai kebijakan privasi pada aplikasi yang digunakan?

1.3 Tujuan Penelitian

Berdasarkan rumusan masalah yang sudah dipaparkan peneliti di atas, maka tujuan dari penelitian ini yakni:

1. Untuk mengetahui persepsi generasi Z pada fanomena kebocoran data di Indonesia
2. Untuk mengetahui penilaian generasi Z pada kebijakan privasi di aplikasi yang digunakan

1.4 Manfaat Penelitian

Adapun manfaat dari penelitian ini yaitu sebagai berikut:

a. Secara Teoritis
   1. Hasil penelitian ini diharapkan dapat menjadi referensi bagi perkembangan ilmu komunikasi khususnya menambah kajian mengenai persepsi masyarkat
   2. Memberikan sumbangsih sumber referensi perpustakaan Universitas Islam Negeri Sayyid Ali Rahmatullah Tulungagung.

b. Secara Praktis
   1. Hasil penelitian ini diharapkan dapat menjadi pertimbangan untuk para praktisi dalam menyikapi fenomena kebocoran data yang terjadi di Indonesia saat ini.
   2. Peneltian ini diharapkan bisa bermanfaat untuk memperluas dan menambah ilmu pengetahuan dalam menibgkatkan kesadaran tentang pentingnya perlindungan data dan informasi pribadi, serta menciptakan lingkungan daring yang aman dan terpercaya bagi pengguna internet, serta mengurangi kerentanan terhadap serangan siber dan memberikan edukasi tentang resiko kejahatan dunia maya.

1.5 Metode Penelitian

1.5.1 Desain Penelitian

Metode penelitian menggunakan *mixed methods* adalah metode campuran, yang mengintegrasikan pendekatan kuantitatif dan kualitatif, seperti yang dijelaskan oleh (John W. Creswell, 2010). Kemudian Sugiyono (2012) menjabarkan campuran metode penelitian kuantitatif dan kualitatif adalah sebuah metode penelitian yang menggabungkan dua metode untuk digabungkan bersama-

sama dalam sebuah penelitian, penggabungan antara kedua pendekatan ini dalam satu penelitian akan menghasilkan data yang lebih komprehensif, valid, reliabel, dan objektif.

Strategi-strategi dalam *mixed methods* meliputi,

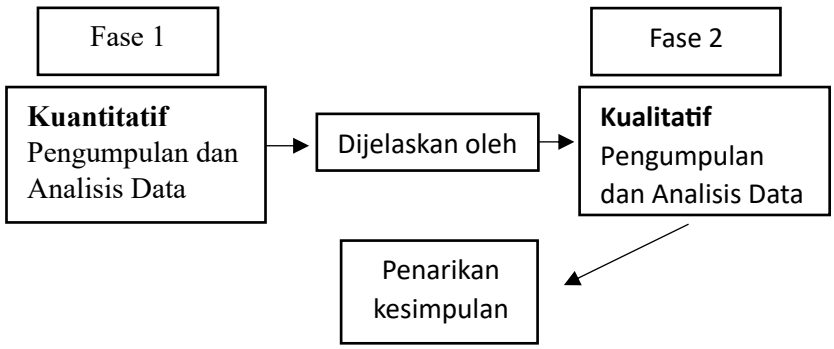
1. Strategi metode kombinasi sekuensial atau bertahap (*sequential mixed methods*) adalah strategi untuk peneliti dapat menggabungkan data yang didapatkan dari satu metode dengan metode lainnya. Strategi pertama ini dibagi menjadi tiga bagian yakni,
   a) Strategi eksplanatoris sekuensial
   b) Strategi eksploratoris sekuensial
   c) Strategi transformative sekuensial
2. Strategi metode kombinasi konkuren atau sewaktu-waktu (*concuren mixed method*) adalah penelitian yang menggabungkan antara data kuantitatif dan data kualitatif dalam satu waktu. Pada strategi ini terdapat 3 strategi metode campuran konkuren, yaitu:
   a) Strategi triangulasi konkuren
   b) Strategi embedded konkuren
   c) Strategi transformative konkuren
3. Prosedur metode campuran tranformatif (*transformative mixed methods*) adalah suatu metode penelitian yang mengintegrasikan perspektif overaching meliputi baik data kualitatif maupun kuantitatif.

Penelitian ini menggunakan metode strategi kombinasi (campuran) sekuensial atau bertahap *(sequential mixed methods)* dengan menggunakan strategi eksplanatoris sekuensial. Pada tahap pertama, peneliti melakukan pengumpulan dan analisis data kuantitatif, sebelum melanjutkan dengan pengumpulan dan analisis data kualitatif yang dibangun berdasarkan temuan kuantitatif yang

telah ada. Dalam proses ini, data kuantitatif diberikan prioritas atau pembobotan yang lebih besar.

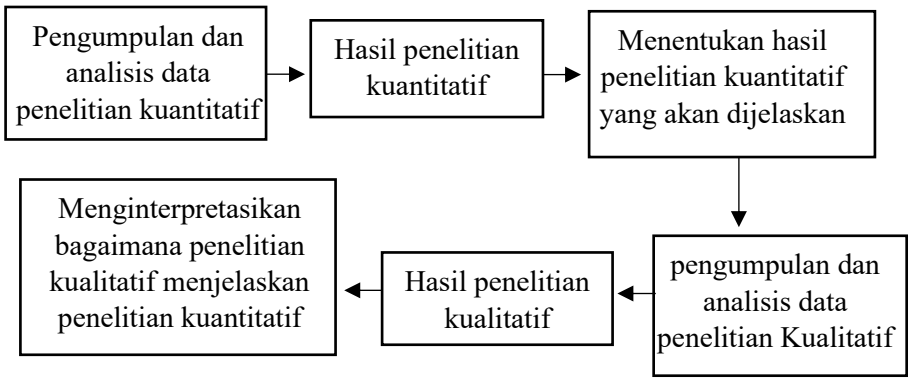
Pada penelitian ini dalam pertama mengumpulkan dan menganalisis data kuantitatif untuk mengumpulkan persepsi generasi Z terkait dengan kasus kebocoran data di Indonesia. Pengumpulan data kuantitatif ini dengan menggunakan metode survey dengan menyebarkan kuesioner. Metode survey adalah langkah untuk mengumpulkan data tentang populasi yang berjumlah besar, pengambilan sampelnya relatif kecil, dan menggunakan kuesioner sebagai alat untuk menerima data primer. Survey adalah metode riset yang menggunakan kuesioner untuk instrument pengumpulan data yang didapatkan. Tujuan dari metode ini adalah untuk mendapatkan informasi dari sampel responden yang dianggap mampu mewakili populasi yang ada. Dalam survei, proses analisis dan pengumpulan data sosial dilakukan secara rinci dan terstruktur, dengan kuesioner sebagai alat utama dalam mengumpulkan informasi dari sampel yang dipilih untuk secara khusus mewakili populasi tersebut (Rachmat Kriyantono, 2014).

Kemudian tahap kedua adalah mengumpulkan data dan menganalisis data kualitatif yang dalam hal ini untuk menjabarkan persepsi generasi Z terkait dengan kasus kebocoran data di Indonesia secara deskriptif. Penggabungan data kuantitatif dan data kuantitatif ini didasarkan pada hasil-hasil yang sebelumnya sudah diperoleh dari tahap pertama. Prioritas utama pada tahap ini lebih diprioritaskan pada tahap pertama, dan proses penggabungan diantara kedua metode penelitian ini terjadi saat peneliti menghubungkan antara pengumpulan dari data kuantitatif dengan anlisis data kualitatif. Dalam penelitian ini, data kualitatif digunakan guna menjelaskan data kuantitatif.



Sumber: pengantar penelitian mixed methods, John w. creswell

1.5.2 Prosedur Penelitian



Sumber: pengantar penelitian mixed methods, John W. Creswell

1.5.3 Populasi dan Sampel

Populasi

Populasi adalah kumpulan abstraksi yang terdiri dari objek-objek yang memiliki jumlah dan karakteristik tertentu, sesuai dengan tujuan penelitian yang ditetapkan (Rachmat Kriyantono, 2014). Populasi dalam penelitian ini adalah jumlah keseluruhan generasi Z di Kabupaten Tulungagung dengan rentan usia 28 – 13 tahun. Kabupaten Tulungagung dipilih menjadi populasi penelitian dikarenakan karakteristik demografis yang dimiliki menggambarkan generasi muda di Indonesia dengan wilayah semi perkotaan. Generasi Z ini artinya hidup dalam linngkungan yang melek akan teknologi digital tetapi tetap erat dengan nilai-nilai budaya lokal. Hal ini menjadi alasan peneliti untuk menggali

persepsi generasi Z terhadap isu kebocoran data. Dari data yang didapatkan peneliti melalui Badan Pusat Statistik Tulungagung, jumlah penduduk kelahiran 1997 – 2012 yakni rentan usia 28 – 13 tahun berjumlah 306 ribu jiwa (Badapn Pusat Statistik Kabupaten Tulungagung, 2024).

Sampel

Bagian dari keseluruhan jumla fenomena atau objek yang sedang diamati disebut dengan sampel (Rachmat Kriyantono, 2014). Pengambilan sampel dilakukan dengan menggunakan metode *simple random sampling*, yang berarti setiap individu dalam populasi memiliki kesempatan yang sama untuk berpartisispasi sebagai responden dalam penelitian ini. Perhitungan sampel menggunakan rumus Slovin dengan *margin error* 10%..

$$n = \frac{N}{1 + Ne^2}$$

$$= \frac{306.000}{1 + 306.000\ (0{,}10)^2}$$

$$= \frac{306.000}{1 + 306.000\ \times 0{,}1}$$

$$= \frac{306.000}{1 + 306.000\ (0{,}01)}$$

$$= \frac{306.000}{1 + 3.060}$$

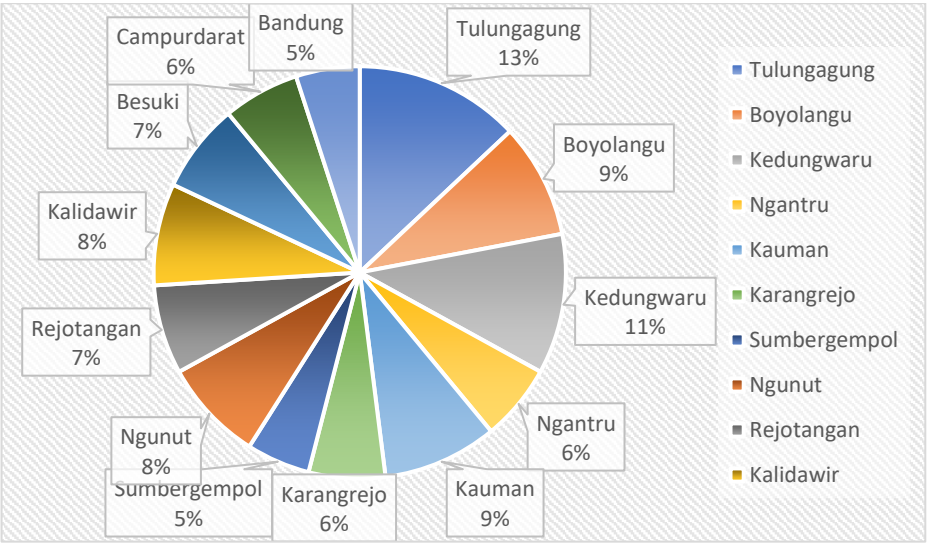
$$= \frac{306.000}{3.061}$$

$$= 100$$

Didapatkan jumlah sampel pada penelitian ini adalah 100 sampel. Selanjutnya berdasarkan hasil penyebaran kuesioner, responden yang berpartisipasi didapatkan berasal dari 10 Kecamatan di Kabupaten Tulungagung, yaitu Kecamatan Tulungagung,

Boyolangu, Kedungwaru, Ngantru, Kauman, Karangrejo, Sumbergempol, Ngunut, Rejotaangan, Kalidawir. Hal ini mencerminkan keterwakilan wilayah dalam kabupaten, meskipun tidak mencakup seluruh kecamatan yang ada. Hasil dari pengelompokkan jumlah responden berdasarkan Kecamatan dapat dilihat di diagram berikut ini:

Gambar 4. Hasil reponden berdasarkan Kecamatan



Sumber: hasil pengolahan data primer 2025

1.5.4 Identifikasi Variabel Penelitian

Menurut Hatch & Farhady (1981) variabel dapat didefinisikan sebagai karakteristik yang menunjukkan perbedaan antara individu satu dengan yang lain, maupun antara objek yang satu dengan objek yang lainnya. Berat badan, tinggi badan, sikap, kepemimpinan, motivasi, kepemimpinan, kedisiplinan, sifat, menjadi bagian dari atribut setiap orang (Bambang & Ricky, 2022). Pada penelitian ini variabel yang digunakan adalah variabel mandiri. Variabel mandiri atau yang biasa disebut variabel tunggal merupakan variabel yang berdiri sendiri tanpa mempengaruhi

variabel lainnya. Variabel mandiri bukan termasuk dalam variabel independent ataupun dependen (Sugiyono, 2013). Variabel mandiri pada penelitian ini adalah persepsi generasi Z.

1.5.5 Definisi Operasional

Definisi operasional merupakan definisi yang didasarkan atas sifat-sifat hal yang didefinisikan sehingga bisa diamati. Bentuk bilangan dapat diamati ini menjadi hal yang penting, karena hal yang dapat diamati ini membuka kemungkinanan untuk orang lain selain peneliti untuk dapat melakukan hal yang sama, sehingga apa dilakukan oleh peneliti terbuka untuk diuji kembali oleh orang lain (Adhi Kusumastuti, 2020). Dikarenakan penelitian ini menggunakan variabel mandiri yakni hanya satu variabel sehingga tidak terdapat pengaruh atau korelasi antar variabel. Penjelasan definisi operasional untuk variabel persepsi dapat dilihat di tabel bawah ini.

Tabel 1 Definisi Operasional

Variabel	Definisi operasional	Skala pengukuran
Persepsi	Stimulus merupakan bentuk rangsangan dari informasi yang diterima oleh individu dari sekitar lingkungannya, dapat melalui indra (pendengaran, pengelihatan, sentuhan) termassuk pikiran	Individu mengalami rangsangan dari indra melihat, mendengar, mengenai isu kebocoran data dari media sosial, berita, atau mendengar cerita di sekelilingnya.

	Respons mengarah pada reaksi atau tindakan yang muncul dari individu terhadap stimulus yang diterima. Respons dapat berbentuk jawaban, gerekan fisik, atau respons mental yang timbul dari reaksi terhadap rangsangan eksternal yang didapa	Individu tergerak untuk mencari informasi kebocoran data, memastikan kebenaran dari setiap informasi yang diterima,
	Seleksi berbentuk proses pemilihan informasi yang di anggap relevan, penting dari berbagai sumber yang ada, termasuk mengabaikan informasi yang kurang relevan	Individu cenderung memilih sumber berita guna mendapat informasi yang akurat, memilih menggunakan data pribadi untuk beberapa kebutuhan.
	Pengorganisasian yakni proses mengatur dan mengkategorikan informasi yang didapat dan sudah dipilih agar mudah dipahami dan diingat.	Dari cara Individu mengelompokkan aplikasi atau platform yang dipastikan aman guna mencantumkan data pribadi,

	Pengorganisasian membantu individu untuk menyusun informasi ke bentuk struktur yang sistematis	
	Memori merupakan kapasitas dan kemempuan untuk menyimpan, mempertahankan, dan mengingat informasi yang sudah diterima dan diproses sebelumnya.	Dari sejauh mana individu mengingat fenomena kebocoran dara dari yang pernah dialami, didengar, atau dibaca.
	Recall bentuk kemampuan untuk mengingat dan menarik kembali informasi yang disimpan dalam memori.	Individu mampu mengingat kembali fenomena kebocoran dara dari yang pernah dialami, didengar, atau dibaca. Sehingga dapat memunculkan Keputusan tindakan setelahnya dari ingatan tersebut.
	Interpretasi adalah proses menyimpulkan makna atau pemahaman terhadap informasi yang diterima dan diingat.	Dari munculnya tindakan, penilaian, dan kesimpulan pemaknaan terkait dengan fenomena kebocoran data

	Interpretasi melibatkan penilaian, analisis, dan pemrosesan kognitif untuk memahami konteks atau implikasi dari informasi tersebut, dan mengaitkannya dengan pengalaman dan pengetahuan sebelumnya.	

1.5.6 Teknik Pengumpulan Data

Pengumpulan data dilakukan melalui penyebaran kuesioner kepada para responden. Kuesioner ini dirancang untuk mengukur variabel-variabel yang diteliti dengan menyediakan pilihan jawaban yang dapat dipilih oleh responden. Metode ini merupakan teknik pengumpulan data yang paling umum digunakan dalam penelitian sosial. Dalam kuesioner, peneliti mengimplementasikan dua jenis jawaban, yaitu jawaban terbuka dan jawaban tertutup. Pada jawaban tertutup, responden diminta untuk memilih salah satu jawaban yang telah disediakan tanpa kesempatan untuk memperluas atau menjelaskan jawabannya. Sementara itu, pada jawaban terbuka, responden memiliki kebebasan untuk menyampaikan pendapat dan pandangan mereka secara lebih luas (Adhi Kusumastuti, 2020).

1.5.7 Uji Instrumen

a. Uji Validitas

Uji Validitas merupakan aspek kualitas dari sebuah instrument yang menggambarkan sejauh mana atau seberapa andall

instrument pengukuran yang sudah dibuat berhasil mengukur apa yang sehrausnya diukur. Dalam penelitian kuantitatif ayng dimaksud "apa yang seharusnya diukur" adalah variabel dalam penelitian sesuai dengan konsep (konstruk) atau definsi operasional variabel yang bersangkutan sehingga data yang didapatkan tidak sepenuhnya mencerminkan nilai variabel sesuai dengan konsep atau definsi operasional dari variabel tersebut maka dikatakan jika instrument tersebut "tidak valid." Sebaliknya jika instrument tersebut mampu mengukur apa yang seharusnya diukur maka apat dikatakan instrument "valid." Untuk mengetahui seberapa jauh validitas dari sebuah instrument penelitian diperlukan melakukan pengujjianp ada aspek validitas instrument tersebut (Bambang & Ricky, 2022).

Untuk menguji kesahihan (valid) dari sebuah instrument diperlukan kriteria yang wajib terpenuhi, yakni:

c. Apabila r hitung > r tabel, maka pernyataan/pertanyaan dari kuesioner sudah dianggap valid.

d. Apabila r hitung <r tabel, maka pernyataan/pertanyaan dari kuesioner dianggap tidak valid.

Rumus kolerasi Pearson Product Moment sebagai berikut:

$$r_{xy} = \frac{N\sum XY - (\sum X)(\sum Y)}{\sqrt{A = \pi r^2\{N\sum X^2 - (\sum X)^2\}\{N\sum Y^2 - (\sum Y)^2\}}}$$

Keterangan:

Rxy: koofisien variabel

X: skor item

N: Jumlah subjek

Y: Skor total.

b. Uji Reliabilitas

Reliabilitas instrumen merupakan sejauh mana konsistensi sebuah instrument pengkuran untuk instrument penelitian dalam mengukur variable yang diteliti. Dalam penelitian sebuah instrument pengukuran dapat dikatakan reliabel jika instrument tersebut dipakai berulang untuk mengukur variable yang sama dan membuahkan hasil sama atau juga instrument tersebut digunakan oleh orang lain untuk mengukur cariabel yang sama dan hasilnya akan sama. Reliabilitas adalah salah satu aspek keandalan atau kualitas instrument yang penting untuk memastikan data nilai variable yang didapatkan benar-benar mempresentasikan variable yang diteliti sesuai dengan konstruk atau definisi operasionalnya (Bambang & Ricky, 2022).

Untuk menguji reliabilitas instrument penelitian, peneliti menerapkan uji statistik Cronbach Alpha. Uji ini mengikuti koefisien Cronbach Alpha yang dijelaskan oleh Sugiyono, di mana instrument dianggap reliabel apabila nilai Cronbach Alpha lebih besar dari 0,60 (Sugiyono, 2013). Dalam nilai Cronbach Alpha tingkat reliabilitas diukur menggunakan pembagian tingkatan reliabel menurut (Sugiyono, 2007:365) sebagai berikut:

1) Nilai Alpha 0.00 - 0.20 berarti reliabel sangat rendah
2) Nilai Alpha > 0.20 – 0.40 berarti reliabel rendah
3) Nilai Alpha > 0.40 – 0.60 berarti reliabel cukup
4) Nilai Alpha > 0.60 – 0.80 berarti reliabel tinggi
   Nilai Alpha > 0.80 – 1.00 berarti reliabel sangat tinggi

1.5.8 Teknik Analisis Data

Pada sebuah penelitian kuantitatif, data yang didapatkan melalui kuesioner selanjutnya akan diolah menggunakan uji-uji sesuai dengan model penelitian dan uji atau analisis yang dibutuhkan. Pada penelitian ini, hasil data kuantitatif diolah

menggunakan teknik analisis deskriptif statistik. Pengolahan data menggunakan teknik ini bertujuan untuk mengetahui gambaran persepsi yang terbentuk pada responden pada fenomena kebocoran data di Indonesia.

Analisis deskriptif statistik digunakan untuk menyajikan dalam bentuk yang lebih sederhana dan mudah dipahami, seperti distribusi frekuensi, persentase, dan rata-rata. Melalui analisis ini, peneliti dapat melihat jawaban umum atau kecenderungan persepsi yang terbentuk pada responden berdasarkan jawaban yang telah diberikan. Pengolahan data dilakukan menggunakan IBM SPSS versi 27. Setiap butir pertanyaan dalam kuesioner dianalisis untuk melihat frekuensi dan persentase serta rata-rata jawaban dari responden. Selanjutnya, data dihitung skor totalnya dan dibandingkan dengan kategori klasifikasi persepsi untuk mengetahui apakah persepsi guna mengetahui apakah persepsi yang terbentuk dari jawaban responden berada dalam kategori tinggi, sedang, atau rendah.

Adapun rumus rumus yang digunakan guna menghitung persentase dari masing-masing jawaban responden sebagai berikut:

$$P = \frac{f}{n} \times 100$$

Keterangan:

P = persentase

F = frekuensi jawaban tertentu

N = jumlah total responden

Penggunaan teknik analisis ini karena disesuaikan dengan tujuan penelitian untuk mendeskripsikan persepsi generasi Z secara kuantitatif tanpa melakukan pengujian hipotesis lebih lanjut.