

BAB I PENDAHULUAN

1.1 Latar Belakang Masalah

Pertumbuhan dan penggunaan media sosial kini menjadi semakin *massive* dan meningkat (Budi, 2019). Keadaan di Indonesia sendiri dibuktikan dengan adanya riset yang dilakukan oleh *We Are Social* yang bekerjasama dengan *Hootsuite* pada Januari 2021 dengan judul “*Digital In Indonesia*” yang menyatakan bahwa penggunaan media sosial mengalami kenaikan sebesar lebih dari 6,3% atau sekitar 10 juta pengguna dari tahun sebelumnya yakni mencapai 170 juta pengguna aktif atau mencapai sekitar 61,8% dari jumlah total populasi penduduk di Indonesia yang berjumlah 274,9 juta penduduk. Dengan rata-rata intensitas waktu yang dihabiskan sekitar 3 jam 14 menit dalam setiap harinya. Hasil riset ini pun diprediksi akan terus mengalami peningkatan dalam setiap tahunnya (Data Reportal, 2021). Berdasarkan penelitian yang telah dilakukan oleh Valkenburg dan Peter dalam Sari (2018) mengungkapkan bahwa generasi yang paling sering menggunakan media sosial yakni generasi *digital native*. Pernyataan tersebut ditunjang oleh data hasil penelitian dari *Google Consumer Behaviour* dalam Kemp (2021) yang mengungkapkan bahwa dari total populasi penduduk Indonesia yang berjumlah 275 juta, 50% tersebut merupakan generasi *digital native* yang memiliki hubungan yang sangat erat dengan perangkat digital seperti media sosial (Supratman, 2018). Selain itu *digital native* ini merupakan generasi yang sudah terbiasa dalam menemukan dan menerima informasi secara sangat cepat, menyukai proses yang berkelanjutan atau parallel, menyukai dan cenderung untuk memilih suatu hal yang berupa foto, atau grafik dan video dengan representasi visual dibandingkan dengan sesuatu yang berupa teks. Mereka juga sudah terbiasa untuk melakukan beberapa hal sekaligus dalam waktu yang bersamaan yakni *multitasking*. Di samping beberapa hal di atas, ditemukan juga bahwa *digital native* ini gemar untuk berjejaring dengan orang lain. Dan lebih menyukai hal yang berupa atau sejenis dengan “*game*” dibandingkan dengan

sesuatu yang lebih mengarah pada hal atau pekerjaan yang “serius” (Prensky, 2001).

Media sosial yang ada saat ini memang sangatlah luas cakupannya yang dapat membuka berbagai peluang untuk mempermudah segala aktivitas yang ada, bahkan tak ayal sering juga digunakan untuk hal yang kurang tepat seperti mempresentasikan atau melakukan pengungkapan diri (*self-disclosure*) yang terlalu berlebihan dengan membagikan aktivitas mereka dengan orang lain yang dapat berupa pemikiran yakni terkait dengan apa yang sedang mereka pikirkan, perasaan mengenai apa yang sedang mereka rasakan, baik tentang hal yang mereka suka atau yang tidak suka, setuju atau tidak setuju dan informasi yang bersifat penting atau tidak penting yang bahkan merujuk pada data, informasi atau identitas yang bersifat pribadi (*personal*) melalui beragam fitur yang disediakan oleh media sosial seperti berbagi foto, video, tulisan-status, dan *chatting* di ruang obrolan (Kaplan & Haenlin, 2010). Hal tersebut lah yang menimbulkan suatu kekhawatiran oleh berbagai kalangan atau pihak tentunya termasuk para *digital native* sendiri, karena akan rentan terhadap kejahatan di dunia *online*. Adanya pengungkapan diri tersebut dalam waktu yang bersamaan, tanpa disadari membuat data pribadi yang seharusnya hanya menjadi konsumsi pribadi kini menjadi konsumsi publik, yang membuat para pengguna media sosial menjadi lebih rentan mengenai bahaya risiko yang ada mengenai *privacy violation* seperti hilangnya privasi, *online sexual harassment*, *doxing*, pencurian dan penyalahgunaan identitas atau data pribadi, pencemaran nama baik, perundungan melalui siber (*cyberbullying*) serta berbagai macam tindak kejahatan melalui siber (*cybercrime*) (Xiao Ma, Hancock, & Naaman, 2016).

APJII dalam (Pertiwi & Manalu, 2018) juga mengemukakan bahwa sebesar 58,6% pengguna media sosial tidak merasa khawatir atas ancaman keamanan dari media sosial mereka. Yang berarti bahwa sekitar 77,7 juta pengguna media sosial yang merasa “aman” tersebut kemungkinan tidak mengoptimalkan pengaturan atau perlindungan privasi media sosial mereka dan membuat mereka merasa nyaman untuk membagikan informasi atau data pribadi mereka di media sosial. Selaras dengan apa yang dilaporkan oleh APJII, Rafique

(2017) menyatakan bahwa sebagian besar generasi secara sadar membagikan informasi pribadi di media sosial tanpa mengkhawatirkan masalah mengenai privasi mereka. Melihat beberapa pernyataan yang ada tersebut membuktikan bahwasannya generasi *digital native* ini terbilang masih belum memiliki pengetahuan dan kemampuan dalam mengoptimalkan atau melindungi privasi atau data pribadi mereka di media sosial atau dengan kata lain masih belum memiliki kesadaran dan kekhawatiran terkait masalah privasi.

Berdasarkan penelitian yang telah dikaji sebelumnya yang mana gencar menekankan bahwa pengguna media sosial dewasa kini harus dibekali oleh pengetahuan dan kemampuan yang nantinya akan membantu para pengguna media sosial agar lebih sadar dan *concern* atau memperhatikan informasi pribadi mereka terkait dengan akses, *sharing* dan publikasinya di media sosial serta sebagai suatu upaya preventif guna mencegah adanya *privacy violation*. Salah satu kemampuan yang harus dimiliki yakni kemampuan literasi privasi *online*. Literasi privasi *online* ini dapat ditinjau melalui beberapa teori seperti teori dari Trepte et al. (2015) yang lebih berfokus untuk menjabarkan mengenai peran dari literasi privasi terhadap perilaku atau sikap seseorang mengenai privasi. Sebelumnya juga terdapat penelitian yang dilakukan oleh Rundhovde (2013) yang mengungkapkan bahwa literasi privasi ini dapat ditinjau melalui tiga sudut pandang yaitu, sudut pandang rasional pengguna dan pengetahuan mereka yang berdasar atas fakta terkait dengan apa yang mereka ketahui mengenai privasi. Kedua sudut pandang adanya pengungkapan informasi pribadi atau perilaku yang berdasar atas keputusan privasi dari pengguna itu sendiri. Ketiga yakni sudut pandang pengalaman umum terkait privasi para pengguna dalam interaksinya dengan media. Selanjutnya mengenai teori literasi privasi *online* yang paling terbaru yakni milik Masur (2020), di mana dalam penelitiannya ia meneliti dan mengembangkan skala literasi privasi *online* yang mencakup empat aspek yakni *factual privacy knowledge* yang dibagi kembali dalam dua tingkatan yakni verikal dan horizontal, lalu *privacy-related reflection ability*, *privacy and data protection skills*, serta *critical privacy violation*. Masur (2020) juga menyoroti bahwa hal yang perlu untuk diperhatikan yakni terkait dengan pengetahuan, kemampuan dan

keterampilan seorang pengguna untuk melindungi informasi pribadi mereka. Hal ini berarti bahwa ketika ketiga hal tersebut dan empat aspek yang ada menunjukkan atau terkategori sangat tinggi maka akan membuat mereka juga menjadi lebih mendukung dan *concern* atas perlindungan data pribadi milik mereka.

Wacana dan teori mengenai privasi umumnya memiliki fokus dan tujuan yang sama yakni berfokus terhadap perlindungan akan identifikasi akses dan kebutuhan privasi individu mengenai pengaturan dan perlindungan data pribadi. Penelitian-penelitian yang telah dilakukan sebelumnya juga seringkali memberikan atau mengusulkan beberapa solusi atas permasalahan dan risiko terkait privasi, serta pengimplementasian dari peraturan, undang-undang hingga kebijakan mengenai perlindungan data pribadi untuk menghindari dari segala ancaman dan risiko mengenai *privacy violation* (Trepte et al., 2015)

Dilihat dari kenyataan yang ada kasus *privacy violation* ini marak terjadi dan beberapa kasus yang telah terjadi di media sosial yakni seringkali berhubungan dengan pencurian dan penyalahgunaan foto ataupun video. Hal ini didukung penelitian yang dilakukan oleh *Pew Research Center* dalam (Pertwi & Manalu, 2018) yang mengungkapkan bahwasanya risiko dari adanya data atau informasi pribadi yang dibagikan di media sosial dapat menimbulkan beberapa tindakan *privacy violation* salah satu di antaranya yakni seperti pencurian identitas pribadi. Mereka menyatakan bahwa pengguna media sosial yang berumur 18 hingga 29 tahun yang masuk dalam kategori *digital native* merupakan kelompok yang paling sering mengalami kasus tersebut yakni seperti pengambilan atau pengalihan data pada akun email atau akun media sosial lainnya, mengalami tindak kekerasan secara *online* atau suatu hal yang dapat menimbulkan risiko yang sangat besar seperti terjadinya kasus pembunuhan. Beberapa contoh kasusnya yakni yang di alami oleh seorang remaja perempuan, di mana salah satu foto yang ia unggah di akun media sosial Instagram miliknya telah dicuri oleh oknum yang tidak bertanggung jawab dan diedit menjadi foto yang tidak pantas atau tidak senonoh yang meranah ke arah pornografi dan dijual ke pihak lain dengan kisaran harga 90 ribu rupiah per buah foto. Adapun kasus lain yang serupa

yakni melanda seorang remaja perempuan juga yang foto-fotonya diambil tanpa seizin pemilik lalu dipajang dan dipromosikan pada sebuah portal *web* prostitusi *online*. Ada juga kasus data-data informasi pribadi miliknya turut dicuri dan dicantumkan pada deskripsi prostitusi *online* tersebut (Widiyaningsih, 2018). Kasus lainnya yang berkaitan dengan pelecehan seksual secara *online* yakni dilakukan dengan bentuk mengirimkan pesan atau *chat* yang mengganggu dengan kata-kata yang kurang sopan dan terkesan “menggoda”, atau dengan *catcalling*, namun dilakukan pada dunia maya. Hal ini juga diperkuat oleh penelitian yang dilakukan oleh Aprillia dalam Rosyidah & Nurdin (2018), di mana 76% dari keseluruhan jumlah 1.000 responden perempuan yang berusia di bawah 30 tahun mengakui pernah mengalami tindak pelecehan seksual melalui *online*.

Penelitian yang dilakukan oleh Zarkasih & Nugroho (2019) di mana pelecehan seksual secara *cyber* menunjukkan terdapat 97 pengaduan terkait masalah *sex harassment* dan terjadi pada 125 kasus tindakan. Jadi dalam hal ini berarti bahwa satu kasus yang ada dalam hal *sex harassment* dapat melingkupi atau mencakup beberapa macam kekerasan seksual terutama terhadap para wanita dengan uraian dalam hal *revenge porn* sebesar 33%, yakni bentuk kekerasan seksual yang secara khusus dilakukan oleh para pelaku dalam ranah pornografi dengan menggunakan atau melibatkan kontan atau unggahan dari para korban yang didasari atas balas dendam. Lalu terdapat *cyber harassment* sebesar 15%, yakni menggunakan teknologi yang ada seperti melalui media sosial untuk melakukan tindakan pelecehan seperti menghubungi dengan melakukan panggilan, mengganggu, bahkan sampai dalam hal mengancam dan melakukan teror pada korban untuk menakut-nakuti. Berikutnya *sexting* sebesar 3%, yakni kependekan dari istilah *sex texting* di mana pelaku akan mengirimkan sesuatu baik berupa foto atau gambar sampai video mengenai pornografi kepada para korban. dan *cyber stalking* sebesar 7%. yakni pada umumnya dilakukan dengan cara menguntit dan mengawasi setiap gerak-gerik atau segala perilaku dari korban menggunakan pengamatan melalui media *online* dan melibatkan segala macam produk teknologi untuk melancarkan aksinya.

Di samping itu pencurian data pribadi untuk keperluan *trading* atau bisnis di dunia ekonomi juga pernah terjadi, *privacy violation* ini disebut dengan *Dataveillance*, yakni informasi milik pribadi akan didistribusikan dan dibagikan pada beberapa organisasi selain dari pihak pertama. Baran dalam Pertiwi & Manalu (2018) memaparkan *Dataveillance* disini yakni suatu pelacakan jejak elektronik suatu pengguna media sosial mengenai pilihan-pilihan atau preferensi terkait sesuatu saat sedang mengakses media sosial. Hal ini biasanya sering terjadi dalam dunia marketing atau ekonomi, karena pada umumnya pengguna media sosial tersebut acapkali tidak menyadari bahwa jejak elektronik aktivitas mereka di *internet* maupun pembelian suatu produk secara *online* tersimpan secara otomatis oleh sistem (Acquisti, Brandimarte, & Loewenstein, 2015).

Secara umum atau general *privacy violation* ini pun dikelompokkan ke dalam empat hal yang terdiri dari *intrusion* yakni jenis pelanggaran privasi yang terjadi dikarenakan adanya hambatan dalam wilayah kepemilikan individu yang bersangkutan dengan fisik milik individu tersebut yang secara hukum dilindungi. Selanjutnya yakni *disclosure of private facts* yakni suatu pelanggaran privasi yang diakibatkan atau terjai karena adanya bentuk suatu pengungkapan atau keterbukaan diri yang terlalu berlebihan atau tidak sesuai dengan porsinya. Lalu terdapat *appropriation* yakni suatu pelanggaran privasi yang terjadi mengenai penyalahgunaan data informasi pribadi dalam beragam bentuk atau rupa, mulai dari nama, foto, video atau bentuk informasi pribadi lainnya untuk suatu kepentingan, dan *false light* yakni penaggran privasi yang terjadi disebabkan oleh adanya publikasi akan suatu hal tertentu yang nyatanya tidak benar atau tidak sesuai dengan fakta atau realita yang ada (Seiren, 2020)

Dapat disimpulkan tujuan penelitian ini dilakukan untuk melihat sejauh mana atau seberapa tinggi tingkat kemampuan literasi privasi *online* para *digital native* Kota Surabaya pada media sosial Instagram menggunakan model literasi privasi *online* yang dikembangkan oleh Masur (2020). Park & Jang dalam Sari (2019) menyatakan bahwa literasi privasi *online* dapat dipengaruhi oleh berbagai faktor di antaranya seperti karakteristik para pengguna (dalam penelitian ini yakni *digital native*) seperti demografi yakni usia, dan *gender* serta karakteristik

penggunaan *gadget* maka selain hal tersebut dalam penelitian ini juga akan meneliti mengenai karakteristik para pengguna yakni *digital native* sebagai pengguna media sosial (Prensky, 2001). Serta akan meneliti terkait pemahaman dan pengalaman mengenai *privacy violation* (Seiren, 2020). Urgensi dari penelitian ini yakni berdasar atas adanya kekhawatiran mengenai masalah *privacy violation* yang ada di media sosial Instagram yang membawa individu dalam tersebut harus melek akan literasi privasi *online* yang akan menjadikan mereka untuk lebih memperhatikan dan melindungi informasi pribadi atau privasi mereka. Selain itu karena teori yang digunakan terbilang cukup baru (Masur, 2020), dan masih sedikit penelitian terkait, oleh karenanya peneliti memilih untuk meneliti topik ini menggunakan teori tersebut. Alasan peneliti memilih *digital native* sebagai subjek penelitian yakni dikarenakan masih sedikitnya penelitian mengenai *digital native* yang berkaitan dengan literasi privasi *online*.

1.2 Rumusan Masalah

Dari adanya pemaparan latar belakang masalah di atas maka dapat dirumuskan beberapa rumusan masalah di antaranya, yakni:

1. Bagaimana gambaran karakteristik masyarakat *digital native* kota Surabaya sebagai pengguna media sosial Instagram?
2. Sejauhmana tingkat kemampuan literasi privasi *online* masyarakat *digital native* kota Surabaya di media sosial Instagram?
3. Bagaimana gambaran pemahaman *privacy violation* para *digital native* Kota Surabaya dan pengalaman *privacy violation* yang pernah dialami?

1.3 Tujuan Penelitian

Secara umum tujuan dari penelitian ini yakni:

1. Untuk mengetahui gambaran karakteristik masyarakat *digital native* kota Surabaya sebagai pengguna media sosial Instagram.
2. Untuk mengetahui sejauhmana tingkat kemampuan literasi privasi *online* masyarakat *digital native* kota Surabaya di media sosial Instagram.

3. Untuk mengetahui tingkat pemahaman *privacy violation* para *digital native* Kota Surabaya dan pengalaman *privacy violation* yang pernah dialami.

1.4 Manfaat Penelitian

Adapun manfaat yang dapat diperoleh dari penelitian ini yakni:

1. Manfaat Akademis

Dapat memberikan sumbangsih atau kontribusi dalam memperluas wawasan dan kajian di bidang Ilmu Informasi dan Perpustakaan terkait dengan literasi privasi *online* di kalangan masyarakat *digital native*. Di mana yang dimaksudkan disini berkaitan dengan media sosial Instagram dan keterkaitannya dengan bentuk *privacy violation*. Serta dapat menjadi bahan referensi atau rujukan bagi penelitian-penelitian terkait berikutnya.

2. Manfaat Praktis

- a. Memberikan kontribusi pemikiran bagi seseorang atau sekelompok orang untuk mampu berpikir kritis sehingga dapat menciptakan suatu model baru mengenai literasi privasi *online*.
- b. Memberikan pengetahuan dan informasi untuk meningkatkan kesadaran mengenai pentingnya literasi privasi *online* di era *digital* seperti saat ini. Atau dapat digunakan sebagai bahan masukan atau evaluasi dari penelitian yang sejenis.
- c. Menambah wawasan pengetahuan dan pengalaman bagi peneliti atau pembaca mengenai perkembangan penelitian di bidang Ilmu Informasi dan Perpustakaan mengenai literasi privasi *online*.

1.5 Kerangka Teori dan Tinjauan Literatur

1.5.1 Karakteristik *Digital Native Sebagai Pengguna Media Sosial*

Dalam Aunul (2019) dipaparkan bahwa istilah dari *digital native* ini pertama kali diperkenalkan oleh Marc Prensky. Yang mana kelompok *digital*

native ini merupakan generasi yang lahir di era digital. Yang sudah tidak asing lagi dengan penggunaan perangkat teknologi *digital* seperti komputer, laptop, *smartphone*, *playstation*, *video games* dan sejenisnya. Di karenakan telah akrab dengan yang dinamakan teknologi tentunya *digital native* ini mengenal yang dinamakan media sosial. Para *digital native* ini menggunakan media sosial untuk berkomunikasi, menelusuri suatu informasi, mengembangkan hobi atau bakat pribadi, mencari suatu hiburan, bahkan mengekspresikan atau melakukan perilaku keterbukaan diri seperti yang telah dipaparkan sebelumnya.

Dan dalam menggunakan media sosial tentunya pengguna harus memiliki suatu kemampuan untuk mengatur dan melindungi privasi mereka. Kemampuan yang dimiliki seorang pengguna pun tentunya berbeda satu sama lain di mana sesuai dengan karakteristik masing-masing. Yang dimaksudkan karakteristik disini yakni mengenai karakteristik *digital native* sebagai pengguna media sosial diantaranya seperti karakteristik sosial yang mencakup usia, *gender*, pendidikan, dan pola penggunaan *gadget*. Serta karakteristik *digital native* seperti preferensi bentuk unggahan atau postingan, dan pola perilaku *multitasking*. Karakteristik yang ada dalam penelitian ini berdasarkan dari penelitian yang telah dilakukan oleh Park (2014) yang menyatakan bahwa unsur sosio-demografi seseorang dapat memberikan pengaruh atas tingkat kemampuan dalam mengatur dan melindungi privasi mereka. Dan juga dari Prensky (2001) yang menjelaskan bagaimana *digital native* ini cenderung memilih preferensi unggahan yang berupa grafik atau gambar dibandingkan dengan teks. Dan mereka merasa nyaman dan terbiasa dengan yang dinamakan *multitasking* yakni suatu kemampuan untuk melakukan beberapa kegiatan atau pekerjaan dalam waktu yang bersamaan, atau penggunaan media sosial ini tidak lagi terbatas pada satu media sosial, akan tetapi pada media sosial lainnya sekaligus. Misalnya mereka dapat berkomunikasi melalui media sosial *Instagram* sembari menonton video dari *YouTube*. Selain itu, penentuan karakteristik penggunaan *gadget* juga akan diteliti, seperti intensitas mengakses internet, lama waktu menjadi pengguna *Instagram*, dan intensitas mengakses *Instagram* selama sehari.

1.5.2 Literasi Privasi *Online*

Privasi merupakan suatu konsep yang bersifat sangat kompleks dan *universal*. Konsep privasi pertama kali diperkenalkan oleh penulis yang bernama Warren dan juga rekannya yang bernama Brandeis dalam buku yang mereka tulis dengan judul “*The Right to Privacy*”. Mereka mengatakan bahwa privasi merupakan suatu hak individu mengenai pemikiran, dan perasaan mereka yang berhak untuk dihargai (Wulandari, 2019).

Nippert-Eng dalam Blank (2014) mendefinisikan privasi sebagai suatu kemampuan yang dimiliki oleh seorang individu untuk memutuskan mana sesuatu yang perlu diketahui oleh orang lain dan mana yang tidak, sesuai dengan yang mereka kehendaki. Sejenis dengan pernyataan tersebut Altman dalam Blank (2014) mendeskripsikan privasi sebagai suatu pengendalian terkait dengan akses pada diri seorang individu.

Seiring semakin majunya perkembangan zaman, kini sudah tak asing lagi di telinga ketika mendengar kata privasi *online*. Sebenarnya definisi dari privasi *online* sendiri tidak jauh berbeda dengan definisi dari privasi pada umumnya. Hanya saja privasi *online* ini lebih merujuk pada suatu proses dari pengendalian akses pribadi ketika menggunakan layanan *internet*, seperti media sosial (Trepte et.al., 2015).

Park (2013) mendefinisikan literasi privasi *online* sebagai suatu prinsip untuk mendukung, mendorong, dan memberdayakan seseorang untuk melakukan pengendalian atau kontrol atas informasi identitas pribadi *digital* mereka. Di mana merujuk pada pengetahuan terkait perlindungan data dan strategi perlindungan data. Lebih lanjut, literasi privasi *online* didefinisikan sebagai suatu kombinasi dari pengetahuan fakta atau deklaratif (*knowing that*) serta prosedural (*knowing how*) mengenai privasi *online*. Dalam hal ini pengetahuan fakta atau deklaratif merujuk pada pengetahuan seseorang terkait aspek teknis perlindungan data secara *online* dan undang-undang serta arahan dari praktisi institusi. Sedangkan, dalam hal prosedural merujuk pada kemampuan seseorang untuk mengimplementasikan strategi terkait dengan regulasi dari privasi individu dan

perlindungan data. Adapun definisi lain dari literasi privasi *online* yakni suatu tingkat pemahaman dan kesadaran seseorang mengenai bagaimana informasi dapat dilacak dan digunakan secara *online* serta bagaimana informasi tersebut dapat dipertahankan atau justru kehilangan sifat asli (kerahasiannya). Literasi privasi *online* merupakan suatu konsep baru yang bertujuan untuk mengukur dan memberikan penjelasan mengenai sikap atau tindakan atau perilaku yang berkaitan dengan pengumpulan, pemrosesan dan pengendalian dari informasi atau data pribadi seseorang (Veghes, et.al., 2012).

Konsep literasi privasi *online* ini tentunya berbeda dengan literasi *digital*. Menurut ALA (*American Library Association*) dalam Visser (2013) literasi *digital* merupakan kemampuan untuk menggunakan informasi dan teknologi komunikasi untuk menemukan, mengevaluasi, menciptakan, dan mengkomunikasikan informasi, di mana mencakup kognitif dan juga kemampuan teknis. Sedangkan literasi privasi *online* sendiri berfokus pada pemahaman mengenai tanggung jawab dan risiko yang terkait dengan berbagi informasi secara *online*.

Jika di tarik mundur kembali penelitian terkait dengan literasi privasi ini awalnya berkaitan dengan perspektif strategi pemasaran, lalu diikuti oleh pengetahuan pengguna *internet* terkait dengan arus data dalam dunia *internet*. Di mana beberapa studi menyoroti bahwa pengguna secara umum atau pengguna dari *website* tertentu menunjukkan pengetahuan yang rendah mengenai risiko privasi, yakni terkait dengan bagaimana *website* tersebut menggunakan data mereka, dan bagaimana kemampuan mereka untuk mengendalikan informasi mereka.

Literasi privasi *online* ini dapat diukur menggunakan beberapa teori. Di antaranya seperti teori dari Park (2011) yang menilai bahwa literasi privasi *online* ini dapat dilihat atau diukur dari literasi digital dan bagaimana seseorang berperilaku mengenai privasi mereka di dunia internet. Selanjutnya Rundhovde (2013) melakukan penelitian lebih lanjut mengenai literasi privasi *online* di mana ia menjelaskan bahwa literasi privasi *online* ini dapat dipahami dan ditelusuri lebih lanjut menggunakan tiga perspektif yang saling berkaitan yakni, 1) dilihat dari rasional pengguna dan pengetahuan mereka yang berdasarkan fakta mengenai privasi, 2) dilihat dari perilaku pengungkapan data informasi pribadi pengguna

yang berdasar pada keputusan privasi mereka, 3) dilihat dari pengalaman yang pernah mereka alami sebelumnya yang berkaitan dengan privasi di media digital. Dua tahun setelahnya terdapat pengembangan literasi privasi *online* yang dilakukan oleh Trepte dan rekan-rekannya (2015) dengan menciptakan skala untuk mengukur literasi privasi *online* yang terdiri dari beberapa dimensi. Mulai dari pengetahuan pengguna mengenai pengaturan privasi, pengimplementasian pengaturan terkait data identitas pengguna, dan perlindungan data informasi pribadi di media digital. Dan hingga kini literasi privasi *online* terus mengalami pembaharuan dan perkembangan. Lalu di susul oleh penelitian yang dilakukan oleh Acquisti & Gross, 2006 dalam Sari (2018) di mana literasi privasi *online* dapat ditinjau melalui aspek pengetahuan yang dapat mempengaruhi rasa percaya dan kesadaran diri seseorang.

Yang terbaru yakni penelitian oleh Masur (2020) yang akan menjadi dasar teori dalam penelitian ini. Di mana dalam penelitian tersebut menggambarkan bagaimana literasi privasi *online* dapat mendukung perlindungan data pribadi dan *self determination* di era informasi. Di mana dengan mengkombinasikan atau menggabungkan beragam dimensi pengetahuan dan kemampuan prosedural dengan refleksi dan kemampuan berpikir kritis. Dalam model literasi privasi *online* ini terdapat empat aspek utama. Yakni aspek *factual privacy knowledge*, aspek *privacy-related (self-) reflection ability*, dan aspek *privacy and data protection skills*, yang tercakup dalam lingkup *Individual Privacy*. Dan satu aspek lainnya yakni *critical privacy literacy* yang termasuk dalam *Collective Privacy*.

1. Factual Privacy Knowledge

Literasi privasi *online* pada dasarnya mencakup pengetahuan faktual mengenai beberapa aspek seperti sosial, ekonomi, kelembagaan, teknis, dan hukum dari privasi *online* dan perlindungan data. Dalam aspek ini pengetahuan faktual dibagi ke dalam dua tingkatan, yakni tingkatan vertikal dan tingkatan horizontal. Pada tingkat vertikal mencakup mengenai 4 hal yakni, 1). Kesadaran dan pemahaman arus informasi di *internet*, model ekonomi penyedia layanan *online* serta kesadaran akan pengumpulan, dan analisis data; 2). Kesadaran dan

pengetahuan terkait praktik pemantauan dan pengawasan oleh pemerintahan dan institusi; 3). Pengetahuan terkait aspek teknis perlindungan data dan privasi di *internet*; 4). Pengetahuan terkait hukum perlindungan data nasional dan internasional. Pada tingkat horizontal yakni mencakup kesadaran dan pemahaman mengenai dinamika sosial baru yang terbentuk dan dibentuk oleh lingkungan berjejaring seperti situs jejaring sosial, pesan instan, *platform* belanja *online* dan meningkatkan risiko gangguan dan *privacy violation* oleh pengguna lain seperti adanya kemampuan untuk mengedit suatu informasi, menggabungkan beberapa konten dan kaburnya batasan antara ruang publik dan privasi.

2. Privacy-Related (Self-) Reflection Ability

Dalam aspek ini menggambarkan kemampuan untuk merefleksikan pengetahuan dalam kaitanya dengan penggunaan medianya sendiri. Yang mencakup 1). Kemampuan untuk mengidentifikasi risiko privasi tertentu yang berkaitan dengan diri sendiri dan untuk mengevaluasi tingkat privasi aktual dalam berbagai konteks dan lingkungan media. Selain itu individu juga perlu untuk memiliki 2). Kemampuan untuk mengidentifikasi kebutuhan privasinya dalam berbagai konteks dan lingkungan media di mana dinamika privasi horizontal dan vertikal terjadi. Dan yang terakhir 3). Kemampuan untuk mencerminkan perilaku seseorang dan bagaimana hal tersebut dapat meningkatkan risiko *privacy violation*.

3. Privacy and Data Protection Skills

Aspek ini yang bertindak sebagai aspek kunci atau yang mewakili semua kemampuan yang diperlukan untuk mengimplementasikan strategi perlindungan data dan pengaturan privasi yang efektif yang dapat melindungi dari berbagai risiko di lingkungan *online*. Dalam aspek ini yang perlu dikembangkan yakni 1). Pemahaman dan kesadaran akan kesederhanaan data seperti mengungkapkan informasi pribadi merupakan langkah mendasar menuju lebih banyak privasi *online*. Dan kemampuan yang lebih lanjut yakni termasuk pengetahuan prosedural 2). Bagaimana menerapkan strategi perlindungan data yang mencegah akses dan identifikasi pada tingkat vertikal seperti menggunakan perangkat lunak

anonimisasi seperti TOR, menginstal plugin anti pelacakan, atau mengenkripsi komunikasi. 3). Bagaimana memilih *platform* dan layanan secara selektif yang dapat menjamin tingkat privasi yang lebih tinggi atau dapat menarik diri dari suatu produk yang melanggar privasi. Dan 4). Kemampuan yang diperlukan untuk menggunakan pengaturan privasi khusus dari suatu *platform* untuk meminimalkan risiko privasi seperti membatasi akses ke postingan, lingkup pertemanan dan menggunakan nama samaran atau anonim.

4. Critical Privacy Literacy

Tiga aspek di atas yakni berperan sebagai dasar dari literasi privasi *online* untuk memberdayakan individu agar lebih memperhatikan batasan akses pada diri mereka, untuk mencegah adanya hal-hal yang tidak diinginkan terkait dengan privasi dan untuk memastikan perlindungan data. Sedangkan aspek *critical privacy literacy* ini didefinisikan sebagai suatu kemampuan untuk mengkritisi, mempertanyakan dan menantang asumsi yang ada mengenai sosial, ekonomi dan praktik kelembagaan yang mengarah pada status quo. Di mana individu harus dapat membela kebebasan dirinya untuk melawan ketidakmerataan ekonomi dan pengaruh institutional.

Dalam aspek ini mencakup beberapa hal yang perlu diperhatikan yakni, 1) Mengidentifikasi dan menganalisis masalah struktur sosial, norma, dan praktik yang dapat memengaruhi privasi individu sebagai bagian dari masyarakat luas. Pada aspek ini, fokus yang sebelumnya lebih tertuju pada individu, kini beralih ke lingkup kolektif atau masyarakat. Dan hal ini juga melibatkan pemahaman terkait dengan ekonomi dan kepentingan pemerintah dalam pengumpulan dan pemrosesan data. Ketika individu menjadi jauh lebih kritis maka mereka akan semakin merasa memiliki 2) Tanggung jawab untuk mengubah struktur, norma, dan praktik yang bermasalah. Tanggung jawab yang dimaksudkan dapat berbentuk seperti mengambil bagian dalam mendukung gerakan terkait privasi atau berpartisipasi dalam masyarakat demokratis seperti pada umumnya.

Singkatnya, individu dengan *critical privacy literacy* yang tinggi lebih termotivasi dan lebih berkompeten di kehidupan sosial dibandingkan dengan

individu yang lain karena mereka tahu dan paham bagaimana menggunakan pengetahuan dan keterampilan mereka terkait dengan privasi sebagai suatu instrument dari komunikasi dan perubahan sosial.

1.5.3 *Privacy Violation*

Privacy violation didefinisikan sebagai suatu bentuk pelanggaran dalam hal atau yang berkaitan dengan privasi. Atau dapat digambarkan ketika suatu data, informasi atau identitas pribadi seseorang diambil, dicuri, disalahgunakan, dan berbagai hal yang bersifat negatif lainnya yang dilakukan oleh seseorang atau oknum yang tidak bertanggung jawab baik digunakan untuk mencari keuntungan baik pribadi atau kelompok atau untuk mencapai suatu tujuan tertentu, maka hal tersebut dapat dikatakan sebagai *privacy violation*. Strahilivetz dalam (Houghton&Joinson, 2010). Bentuk dari *privacy violation* di media sosial sendiri beragam, mulai dari pencurian data atau informasi pribadi, yang dapat berupa foto atau video. Penyalahgunaan dan penyebaran informasi pribadi oleh pihak lain tanpa seizin atau tanpa sepengetahuan dari pihak pertama atau pemilik.

Dalam hal ini *privacy violation* dikelompokkan ke dalam empat hal yakni yang pertama, *intrusion* di mana pelanggaran mengenai privasi disebabkan oleh adanya hambatan dalam wilayah kepemilikan dalam bentuk fisik seseorang yang dilindungi secara hukum. Dalam hal ini lebih merujuk pada pelanggaran privasi dalam dunia nyata (*non-online*) seperti adanya tindak pelecehan seksual dalam hal fisik. Yang kedua, yakni *disclosure of private facts* yakni pelanggaran terhadap privasi yang terjadi sebagai akibat dari bentuk pengungkapan atau keterbukaan diri yang terlalu berlebihan. Contohnya yakni dengan adanya foto atau video atau informasi yang berkaitan dengan identitas pribadi yang dibagikan atau dipublikasikan di media sosial. Di mana dalam hal ini seseorang yang melakukan hal tersebut harus siap menanggung risiko yang ditimbulkan salah satunya bahkan harus siap menanggung “malu” meskipun informasi tersebut benar adanya dan bukan rekaan. Yang ketiga, yakni *appropriation*, yakni pelanggaran privasi seperti penyalahgunaan dalam berbagai bentuk, baik nama, foto, video, atau informasi pribadi lainnya dan kemiripan suatu individu untuk kepentingan atau tujuan

tertentu terutama menyangkut komersial. Dan yang keempat, yakni *false light*, pelanggaran terhadap privasi yang disebabkan oleh adanya publikasi terkait hal tertentu yang tidak benar atau tidak sesuai dengan realita. Sari dalam (Seiren, 2020).

1.5.4 Tinjauan Literatur atau Penelitian yang Relevan

1. Penelitian yang dilakukan oleh Philipp K. Masur (2020) yang berjudul “How Online Privacy Literacy Supports Self-Data Protection and Self-Determination in The Age of Information”. Dalam penelitian tersebut terdapat suatu model literasi privasi *online* yang terdiri dari 4 dimensi yakni pengetahuan privasi faktual, kemampuan privasi terkait dengan refleksi diri, keterampilan perlindungan privasi dan data serta literasi privasi kritis.
2. Penelitian yang dilakukan oleh Trepte at. al (2015) yang berjudul “Do People Know about Privacy and Data Protection Strategies? Towards The “Online Privacy Literacy Scale” (OPLIS)”. Di mana ia dan rekan-rekannya menyarankan sebuah skala pengukuran literasi privasi menggunakan enam dimensi. Pertama, pengetahuan praktik organisasi, institusi, dan penyedia layanan *online*. Kedua, pengetahuan aspek teknik perlindungan data dan privasi *online*. Ketiga, pengetahuan potensi risiko dan ancaman privasi. Keempat, pengetahuan aspek hukum dan aspek legal perlindungan data di Jerman dan Persatuan Eropa. Kelima, pengetahuan strategi pengaturan privasi *online* individu. Keenam, pengetahuan mengenai bagaimana menghadapi ancaman privasi.
3. Penelitian yang dilakukan oleh Masur & Trepte (2021) yang berjudul “Transformative or Not? How Privacy Violation Experiences Influence Online Privacy Concerns and Online Information Disclosure”. Di mana dalam penelitian ini mencoba untuk membuktikan beberapa hipotesis yang ada terkait dengan pengalaman *privacy violation* dengan *privacy concerns* dan *information disclosure* menggunakan data dari *five-wave panel study* dan menggunakan pendekatan Bayesian.

4. Penelitian dalam bentuk skripsi yang dilakukan oleh Zunita Ayu Eka Sari (2019) yang berjudul “Literasi Privasi Pada Media Sosial Instagram di Kalangan Mahasiswa Strata 1 Universitas Airlangga Surabaya”. Penelitian ini meneliti terkait dengan literasi privasi di kalangan mahasiswa Universitas Airlangga di media sosial Instagram ditinjau dari teori literasi privasi Rundhovde (2013) yakni melihat seberapa besar tingkat literasi privasi berdasarkan 3 aspek yakni, pengetahuan, perilaku dan pengalaman seseorang dalam melakukan perlindungan informasi. Dan berdasarkan hasil menyatakan bahwa literasi privasi mahasiswa dapat dikategorikan sedang atau cukup.

1.6 Variabel Penelitian

1.6.1 Definisi Konseptual

1. *Digital Native*

Pada era ini sudah tidak asing lagi dengan yang dinamakan generasi *digital native*, yakni generasi yang ketika lahir telah dikelilingi dengan penggunaan internet yang sudah cukup merebak luas. Generasi ini pun berbeda dengan generasi yang ada sebelumnya. Di mana pada generasi ini mereka telah mahir untuk menggunakan segala perangkat teknologi yang ada atau dapat dikatakan telah melek teknologi sejak lahir. Mereka memiliki pengetahuan atau wawasan yang luas mengenai teknologi. Banyak juga dari generasi ini menjadi pencipta produk teknologi yang ada dan telah banyak digunakan pada saat ini.

2. *Literasi Privasi Online*

Literasi privasi *online* yakni suatu kemampuan kritis atas penggunaan media sosial, yang tidak semata-mata sebatas menggunakan akan tetapi juga mampu untuk menganalisis, mengkritisi, menginterpretasikan, dan mengkomunikasikan hingga melakukan perlindungan data atau privasi secara *online*. Atau dapat dipahami bahwa privasi merupakan suatu kemampuan individu untuk mengatur akses mengenai informasi atau data pribadi mereka yang ditujukan untuk siapa, dan pada waktu serta kondisi yang seperti apa. Maka dapat

disimpulkan bahwa privasi *online* ini erat kaitannya dengan kerahasiaan informasi pribadi seorang individu. Di mana ketika informasi pribadi milik seseorang telah dibagikan atau disebarluaskan maka informasi tersebut telah menjadi informasi publik dan ketika disalah gunakan oleh oknum yang tidak bertanggung jawab atau tanpa seizin dari individu tersebut maka tentunya akan merugikan individu tersebut dan menimbulkan beragam risiko mengenai *privacy violation*. Adapun aspek-aspek literasi provasi *online* yang ada dalam penelitian ini yakni, *factual privacy knowledge*, aspek *privacy-related (self-) reflection ability*, dan aspek *privacy and data protection skills*, dan *critical privacy literacy*.

Seseorang dapat dikatakan ia telah terliterasi dengan baik ketika mereka mampu untuk memahami arus informasi yang ada di media sosial, berpengetahuan dan memiliki kemampuan untuk menganalisis akan risiko dan kebutuhan privasi yang ada dan paham bagaimana cara menerapkan strategi perlindungan privasi, memilih layanan yang lebih selektif, serta mengidentifikasi masalah struktur sosial yang berkaitan dengan privasi juga mengambil peranan untuk berpartisipasi dalam gerakan literasi privasi *online*.

3. Privacy Violation

Dengan adanya beragam alat dan fitur yang semakin canggih di era digital seperti saat ini menjadikan seseorang lebih mudah untuk menjadi korban atau bahkan pelaku dari tindakan *privacy violation*. *Privacy violation* kini pun telah banyak terjadi, terutama dalam dunia media sosial. Seseorang dapat dengan mudah melakukan pencurian atau pengambilan data, informasi atau identitas pribadi milik seseorang lalu disalahgunakan dan disebar dengan begitu mudah dengan beragam tujuan tertentu baik yang bersangkutan dengan kepentingan pribadi atau kelompok.

1.6.2 Definisi Operasional

Dalam penelitian ini yang menjadi definisi operasional variabel tingkat literasi privasi *online* yakni total skor yang diperoleh ketika para responden telah

mengisi angket atau kuesioner penelitian. Beberapa variabel yang digunakan yakni sebagai berikut:

Variabel : Karakteristik *digital native* sebagai pengguna media sosial Instagram

1. Indikator : Sosio-demografi

1. Usia
2. Gender
3. Pendidikan formal yang sedang ditempuh
4. Pekerjaan yang sedang dilakukan

2. Indikator : Penggunaan *gadget* dan media sosial Instagram

1. Intensitas akses internet
2. Lama waktu menggunakan Instagram
3. Intensitas akses Instagram
4. Preferensi bentuk unggahan
5. *Multitasking* dalam menggunakan Instagram

Variabel :Tingkat literasi privasi *online*

3. Indikator : *Factual Privacy Knowledge*

Tingkat vertikal

1. Pegetahuan terkait kekhawatiran dan pemahaman arus informasi di *internet*, model ekonomi dari penyedia layanan online
2. Pengetahuan terkait pengumpulan data dan pengawasan privasi oleh institusi dan pemerintah di media sosial
3. Pengetahuan aspek teknis perlindungan data dan privasi di media sosial
4. Pengetahuan atas pemahaman hukum perlindungan data privasi

Tingkat horizontal

1. Terbentuknya dinamika sosial baru dalam situs jejaring sosial
2. Risiko *privacy violation* dalam jejaring sosial oleh pengguna lain

4. Indikator : *Privacy-Related Reflection Ability*
 1. Kemampuan pengidentifikasian risiko privasi
 2. Kemampuan mengidentifikasi dan merefleksikan kebutuhan privasi
 3. Kemampuan merefleksikan dan mengevaluasi perilaku kebutuhan privasi dengan risiko *privacy violation*
5. Indikator : *Privacy and Data Protection Skills*
 1. Pemahaman dan kesadaran mengenai pengungkapan atau berbagi informasi pribadi
 2. Pengetahuan mengenai pengimplementasian strategi preventif perlindungan data pribadi
 3. Kemampuan memilih *platform* dan layanan secara selektif sesuai dengan kebutuhan privasi
 4. Pengetahuan mengenai menerapkan strategi privasi dan perlindungan data dalam media sosial
6. Indikator : *Critical Privacy Literacy*
 1. Kemampuan pengidentifikasian pertanyaan, pengkritikan struktur sosial, proses dan norma yang mempengaruhi privasi individu di tingkat masyarakat
 2. Pengembangan tanggung jawab dan motivasi sosial untuk menjadi agen perubahan

Variabel : *Privacy Violation*

7. Indikator : a. Pemahaman terkait *Privacy Violation*
 1. Sumber informasi *privacy violation*
 2. Pengetahuan mengenai *privacy violation*
 3. Upaya pencegahan *privacy violation*
- b. Pengalaman *Privacy Violation*
 1. Kejadian *privacy violation* yang dialami
 2. Jenis *privacy violation* yang dialami
 3. Jenis tindakan setelah mengalami *privacy violation*

1.7 Metode dan Prosedur Penelitian

1.7.1 Pendekatan Penelitian

Dalam penelitian ini peneliti menggunakan pendekatan kuantitatif. Yakni pendekatan penelitian yang akan memberikan gambaran atau pemaparan mengenai suatu masalah, yang nantinya hasil dalam penelitian dapat digeneralisasi (Kriyantoro, 2006). Selain itu, penelitian dengan pendekatan kuantitatif ini membutuhkan serangkaian proses analisis dari data-data yang berupa angka untuk dilakukan suatu kajian penelitian, khususnya mengenai apa yang telah diteliti (Kasiram, 2008). Dan metode yang digunakan dalam penelitian ini yakni metode deskriptif. Yakni penelitian yang bertujuan untuk mendeskripsikan suatu gejala, peristiwa dan kejadian yang terjadi pada saat ini (Sudjana & Ibrahim, 1989). Di mana peneliti disini akan memotret peristiwa atau yang sedang terjadi menjadi suatu fenomena yang kemudian akan dideskripsikan secara fakta dan sesuai dengan realita yang ada di lapangan. Dalam metode deskriptif, metode survei digunakan yang mana dilakukan dengan menggunakan instrumen penelitian kuesioner, sebagai suatu alat penelitian untuk mendapatkan data dari responden yang mewakili populasi (Kriyantono, 2006). Oleh karena itu dalam penelitian ini akan diberikan gambaran dan penjelasan mengenai seberapa tinggi tingkat kemampuan literasi privasi *online* para masyarakat *digital native* Kota Surabaya serta bagaimana gambaran keterkaitan *digital native* sebagai pengguna media sosial Instagram serta gambaran dari pemahaman mengenai *privacy violation* dan pengalaman mengenai hal tersebut dalam media sosial Instagram.

1.7.2 Lokasi Penelitian

Penelitian ini dilakukan di wilayah Kota Surabaya, Provinsi Jawa Timur, di mana Kota Surabaya ini merupakan kota terbesar kedua se-Indonesia setelah Jakarta. Dapat dilihat sendiri bahwasannya Kota Surabaya ini merupakan kota metropolitan. Di mana mayoritas penduduknya memiliki gaya hidup yang sangat

modern dan sudah berpikiran maju dan rata-rata telah memiliki *gadget* dan mampu untuk menggunakan atau mengoperasikan *gadget* tersebut. Dan rata-rata mengakses *internet* pun sudah terbilang cukup tinggi yakni sekitar lebih dari lima jam per harinya (Pranata, 2014). Dan mayoritas penggunanya yakni didominasi oleh kalangan remaja dan dewasa yang telah mampu untuk mengoperasikan *smartphone*, *internet* dan media sosial. Sedangkan serangkaian aktifitas yang dilakukan di media sosial Instagram yakni 81.8% melihat berita atau mencari informasi apa yang sedang terjadi, lalu 76.6% mengunggah foto ataupun video, 68.5% memberikan komentar, 66.2% mengupdate status, dan sebagainya. Peneliti memilih Kota Surabaya selain beberapa hal di atas juga karena ingin membuktikan dan mengetahui apakah benar meskipun mereka sudah memiliki pengetahuan yang lebih maju dibandingkan dengan kota-kota yang tertinggal lainnya, benarkah mereka juga memiliki kemampuan yang baik mengenai literasi privasi *online*?

1.7.3 Penentuan Populasi Penelitian

Populasi merupakan wilayah yang terdiri atas objek atau subjek yang memiliki kualitas atau karakteristik khusus yang ditetapkan peneliti yang kemudian akan dianalisis dan kemudian diberikan penjelasan (Sugiyono, 2010). Dan populasi yang dimaksudkan dalam penelitian ini yakni seluruh masyarakat kota Surabaya yang merupakan generasi *digital native* dan menggunakan media sosial Instagram.

1.7.4 Penentuan Metode Pengambilan Sampel

Sampel merupakan sebagian dari populasi yang dapat mempresentasikan sifat dan karakteristik yang sama dari suatu populasi dalam suatu penelitian (Sugiyono, 2010). Dalam menentukan ukuran sampel peneliti mengacu pada teori Frankel dan Wallen (1993) di mana ia menyarankan bahwa untuk penelitian yang bersifat deskriptif besar sampel yang dapat diambil yakni sebesar 100. Dan teknik pengambilan sampel yang digunakan dalam penelitian ini yakni teknik *purposive*

sampling. Yakni metode pengambilan sampel yang berdasarkan pada pertimbangan dengan kriteria tertentu sehingga dapat memperoleh sampel yang tepat (Sekaran, 2006).

Adapun kriteria dari sampel dalam penelitian ini yakni sebagai berikut:

1. Masyarakat *digital native* Kota Surabaya dengan rentang umur 18-29 tahun. (Pertiwi & Manalu, 2018).
2. Memiliki akun media sosial Instagram dan menjadi pengguna aktif dengan waktu kunjungan secara intens atau setiap hari dengan minimal intensitas waktu yang dihabiskan yakni 1-3 jam dalam sehari.
3. Mengetahui atau pernah mengalami *privacy violation* (baik yang dialami oleh diri sendiri, atau orang lain seperti teman, maupun responden sendiri).

Penentuan berdasarkan kriteria tersebut didasarkan karena kalangan *digital native* sendiri cakupannya sangat luas, maka peneliti mengkhususkan penelitian ini untuk para *digital native* di Kota Surabaya dengan rentang umur yang tertera. Selanjutnya populasi yang ada pun dikecilkan kembali cakupannya dengan persyaratan memiliki akun media sosial instagram dan menjadi pengguna aktif dengan mengakses Instagram secara intens setidaknya masuk dalam *range* waktu yang tertera. Hal ini karena harus sesuai dengan karakteristik dari *digital native* sendiri yakni sudah terbiasa dan mahir dalam mengoperasikan *gadget* yang rata-rata telah memiliki media sosial, salah satunya yakni Instagram.

1.7.5 Metode Pengumpulan Data

Metode pengumpulan data merupakan tahap yang paling strategis dalam suatu penelitian, karena tujuan utama dari dilakukannya suatu penelitian yakni untuk memperoleh data. Dalam penelitian ini metode pengumpulan data yang digunakan yakni angket atau kuesioner yang dibagikan baik secara langsung maupun tidak langsung atau secara *online* kepada responden. Selain kuesioner, peneliti melakukan pengumpulan data melalui studi kepustakaan, pengamatan atau observasi yang mendalam di lapangan dan melakukan wawancara dengan beberapa informan untuk memperoleh data tambahan.

Pengumpulan data secara rinci dilakukan dengan langkah awal yakni melakukan *pre-test* yang berupa kuesioner singkat serta wawancara singkat yang dilakukan pada lingkungan sekitar masyarakat umum yang telah terkategori sebagai *digital native*. Hasil yang ada menunjukkan bahwa rata-rata mereka sudah mengerti apa yang dimaksud dengan literasi privasi dan *privacy violation*. Selanjutnya dengan melakukan tahap penyebaran dan pembagian kuesioner melalui *online* di mana ketika terdapat beberapa data yang masuk, peneliti segera melakukan pengecekan mengenai responden mana sajakah yang pernah mengalami (diri sendiri) atau pernah mengetahui bahwa terdapat teman, keluarga atau rekan mereka yang pernah mengalami *privacy violation*. Setelah itu peneliti akan mencoba menelusuri dan menghubungi orang yang pernah mengalami *privacy violation* tersebut yang memenuhi kriteria untuk menjadi responden penelitian yang selanjutnya akan dilakukan wawancara singkat terkait beberapa hal yang menyangkut *privacy violation*.

1.7.6 Metode Analisis Data

Teknik analisis data dalam penelitian ini menggunakan metode deskriptif. Yakni dengan memberikan deskripsi dan penjelasan berdasarkan data yang diperoleh di lapangan atau melalui kuesioner yang telah dibagikan. Di mana dalam penelitian ini analisa pertama akan mendeskripsikan mengenai tingkat kemampuan literasi privasi *online* di kalangan masyarakat *digital native* di kota Surabaya dalam menilai *privacy violation* di media sosial Instagram. Dan yang kedua yakni memberikan gambaran mengenai karaktersistik masyarakat *digital native* di kota Surabaya dengan literasi privasi *online*. Dalam penelitian ini tabel skor digunakan untuk menggambarkan seberapa besar tingkat literasi privasi *online* berdasarkan pilihan jawaban dari responden pada kuesioner. Yakni pemberian skor 4 untuk jawaban yang sangat setuju, selanjutnya skor 3 untuk setuju, skor 2 untuk jawaban tidak setuju, yang terakhir yakni skor 1 untuk jawaban sangat tidak setuju. Seperti tabel di berikut ini:

Skala Likert	Keterangan
Sangat Setuju	4
Setuju	3
Tidak Setuju	2
Sangat Tidak Setuju	1

Sumber: Hasil pengolahan data peneliti

Setelah penentuan skor dari masing- masing skala, selanjutnya yakni menghitung rata-rata variabel untuk menghitung dan menentukan kategori dari jawaban yang ada tergolong tinggi atau rendah. Cara menentukannya yakni dengan berdasarkan pada kelas intervalnya. Dengan demikian dengan perhitungan sebagai berikut:

$$\frac{\text{Nilai tertinggi} - \text{Nilai terendah}}{\text{Jumlah Kelas}} = \frac{4 - 1}{4} = 0,75$$

Berdasarkan dari perhitungan di atas maka dapat diketahui kelas interval dari masing-masing kategori yakni:

Interval	Kategori
3,26 – 4,00	Sangat Tinggi
2,51 – 3,25	Tinggi
1,76 – 2,50	Rendah
1,00 – 1,75	Sangat Rendah

Sumber: Hasil pengolahan data peneliti