BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Media massa kian menyebarkan informasi hingga memberikan edukasi terkait kebocoran data pribadi. Jika dicari dengan kata kunci ‘kebocoran data pribadi’ pada *search engine google.com* maka akan menghasilkan sekitar 269,000 lebih berita pada 6 September 2022. Banyaknya berita yang beredar mengenai kebocoran data pribadi masyarakat belum memiliki titik terang dan akan terus merugikan masyarakat.

Indonesia sedang digemparkan dengan berita mengenai kebocoran identitas terkait dengan data SIM prabayar. Kebocoran data mengenai SIM terkuak melalui forum jual beli data yaitu *breached.to*. Di dalamnya terdapat 1,3 miliar data registrasi kartu SIM prabayar berupa nomor induk kependudukan, provider telekomunikasi, nomor telepon seluler, hingga tanggal registrasi (Mediana, 2022). Sebelumnya, kebocoran data pribadi warga juga terjadi pada pelanggan PT Perusahaan Listrik Negara (PLN) yang dijual dalam *breached.to* oleh akun “Loliyta” (Mediana, 2022).

Pada tahun 2021, ramai pemberitaan mengenai kebocoran data *Electronic Health Alert Card* (eHac) yang ditemukan pertama kali oleh *vpnMentor*, ada sekitar 1,3 juta data pengguna eHAC yang ditemukan pertama kali pada sebuah server yang bisa diakses oleh masyarakat. Data yang bocor tersebut antara lain

nama, alamat rumah, nomor KTP, rumah sakit tempat dilakukan tes Covid-19 dan lainnya (Rotem & Locar, 2021).

Dilansir dari Tempo pernah ada insiden kebocoran identitas yang cukup menggemparkan di Indonesia di antaranya kebocoran data BPJS Kesehatan yang terjadi pada Mei 2021. Insiden tersebut menyebabkan data peserta Badan Penyelenggara Jaminan Sosial (BPJS) dijual melalui Raid Forums dengan harga 0,15 *Bitcoin*. Di penghujung 2020, Lazada dan Cermati mengalami pelanggaran data. Kebocoran data, sejumlah data di *Cermati.com* diperdagangkan oleh 2,9 juta pengguna. Sementara itu, 1,1 juta file Lazada terekspos (Akbar, 2021).

Kasus kebocoran selanjutnya adalah penjualan data nasabah BRI Life. Data nasabah BRI Life sebanyak 2 juta data dijual seharga 7.000 USD atau sekitar Rp 101,6 juta. Insiden tersebut viral melalui akun Twitter *@HRock* yang menunjukan tangkapan layar dan pesan berisi 463.000 dokumen yang diperjualbelikan. Dokumen yang tertera dalam tangkapan layar berupa foto KTP elektronik nasabah BRI Life, NPWP, nomor rekening dan rekam (Akbar, 2021). Pada tahun 2020, kasus kebocoran juga terjadi pada perusahaan Tokopedia, jutaan akun pengguna *e-commerce* Tokopedia diduga mengalami kebocoran. Sejumlah 91 juta akun *database* Tokopedia terjual dengan harga sekitar US$ 5.000 di situs ilegal (Jati, 2020). Tidak hanya itu, Indonesia juga sempat mengalami kebocoran data Komisi Pemilihan Umum, peretas mengklaim telah membocorkan data sebanyak 2,3 juta data warga Indonesia dari Komisi Pemilihan Umum (KPU) (R. Setiawan, 2020).

UNIVERSITAS MULTIMEDIA NUSANTARA

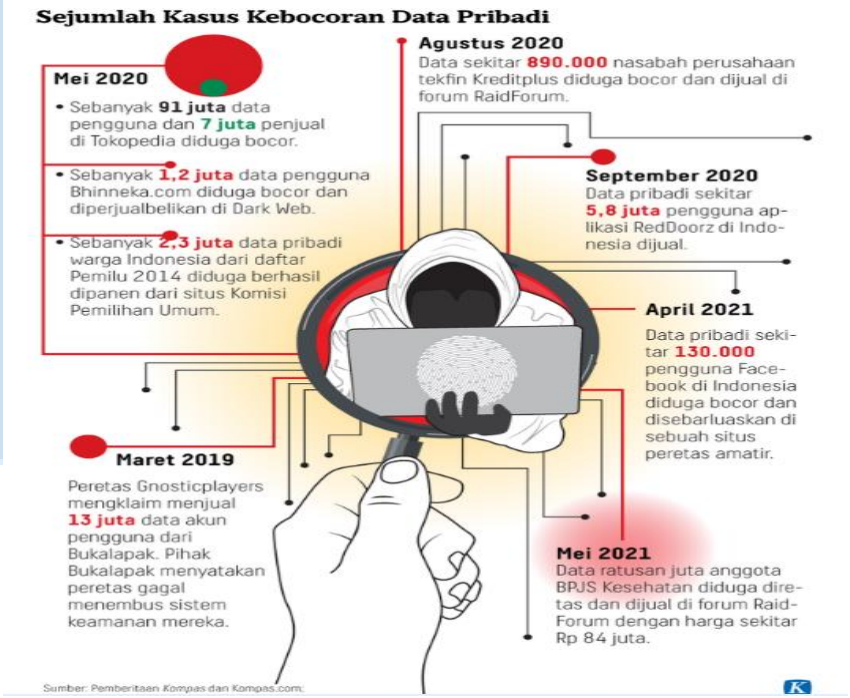
Data reportal memaparkan dari total penduduk Indonesia sebanyak 277,7 juta jiwa terdapat 204,7 juta pengguna internet pada Januari 2022. Situs tersebut memaparkan peningkatan jumlah pengguna internet di Indonesia mencapai 2 juta dalam setahun (Kemp, 2022). Hal tersebut menunjukan lebih dari 50% penduduk di Indonesia menikmati jaringan internet. Di era *Internet of Things* (IoT) saat ini, celah keamanan dan privasi semakin besar saat semua terhubung dengan internet (Revilia & Irwansyah, 2020). Fenomena kebocoran data belakangan ini kerap kali terjadi secara berulang kali di Indonesia. Definisi kebocoran data bisa bervariasi antara organisasi, tergantung pada sensitivitas data untuk dilindungi, tingkat interaksi antara pengguna dan saluran komunikasi yang tersedia (Goel, 2011)

Kemajuan teknologi IoT mengusung pada keamanan siber, berbagai ancaman dan masalah perlindungan data yang berdampak pada keselamatan publik (Setiawan & Najicha, 2022). Menurut data milik Yayasan Lembaga Konsumen Indonesia (YLKI) pada tahun 2020, kasus pencurian data paling banyak terdapat pada sektor belanja online yaitu 54 kasus, disusul dengan telekomunikasi sebanyak 31 kasus, sektor listrik sebanyak 28 kasus, pinjaman online sebanyak 27 kasus hingga kasus terendah yaitu sektor PDAM yaitu 3 kasus (Hidayah & Ezerli, 2020). Pada kuartal kedua 2022, kasus kebocoran data melonjak hingga 143%. Ada sekitar 1,04 juta akun yang bertambah dari kuartal 1 2022 yaitu 430,1 ribu akun yang mengalami kebocoran. Banyaknya kasus kebocoran data yang terjadi membuat Indonesia masuk kedalam urutan 8 dari 10 negara dengan kasus kebocoran data terbanyak (Dihni, 2022). Serta menjadi

UNIVERSITAS MULTIMEDIA NUSANTARA

negara nomor 1 dengan kasus kebocoran data terbanyak di Asia Tenggara (Septiani, 2022).

Gambar 1.1 Sejumlah Kasus Kebocoran Data Pribadi di Indonesia



Sumber: Kompas.id, 2022.

Indonesia dapat dikatakan cukup terlambat dalam hal perlindungan data pribadi. Hal ini dapat dilihat dari perbandingan dengan negara lain seperti misalnya Thailand yang sudah mengesahkan *Personal Data Protection Act* (PDPA) pada Mei 2019 lalu (*Data Protection Laws Of The World*, 2022). Bahkan Malaysia menjadi negara pertama di ASEAN yang mengesahkan undang-undang terkait perlindungan data pribadi pertama di Malaysia pada 2 Juni 2010 dan mulai berlaku pada 15 November 2013 (*Data Protection Laws Of The World*, 2021).

Kementerian Komunikasi dan Informatika Republik Indonesia menyatakan generasi muda perlu memahami jenis data pribadi dan relevansinya.

Hal tersebut termasuk mencermati layanan yang disediakan, jenis produk jasa, hingga memeriksa kebijakan data privasi (Yusuf, 2020). Di sisi lain, perhatian terkait privasi berhubungan lekat dengan isu keamanan dan bebas berekspresi. Sikap tidak peduli terhadap privasi yang dianggap tidak penting dapat didasarkan pada ketidaktahuan atas ancaman dan risiko privasi seseorang (Batmetan, 2018).

Isu mengenai privasi sudah menjadi topik yang tidak asing lagi. Isu privasi menjadi isu yang semakin intens dibicarakan saat ini (Sarikakis & Winter, 2017). Di sisi lain, Saeful menyatakan bahwa privasi saat ini masih menjadi konsep yang asing bagi khalayak teknologi informasi, meskipun saat ini perhatian privasi sering menjadi bahan pembicaraan (Batmetan, 2018). Menurut Henrici, peringatan tentang ancaman privasi seringkali tidak memiliki respon yang baik dalam jangka panjang, peringatan tentang ancaman yang tidak menyebabkan kerugian dalam waktu yang dekat semakin dianggap tidak berdasar (Henrici, 2008).

Privasi menjadi bagian yang utuh dari kemanusiaan, di mana seseorang memiliki batasan akses terhadap diri sendiri, pengendalian dan kerahasiaan atas informasi pribadi miliknya (Fuchs, 2011). Namun, menurut Burrows perkembangan teknologi saat ini semakin memudahkan untuk mengumpulkan, menyimpan, menganalisis, menyalin dan mendistribusikan data pribadi, sehingga semakin sulit untuk menjaga privasi (Dorraji & Barcys, 2014).

Phelps menyatakan bahwa individu lebih cenderung khawatir mengenai privasi mereka ketika informasi digunakan tanpa izin atau sepengetahuan seseorang (Tan *et al*., 2012). Masalah privasi lainnya terkait dengan penggunaan

sekunder informasi pribadi (Tan *et al*., 2012). Sebuah penelitian yang dilakukan oleh Chu *et al.* (2022) menemukan bahwa terpaan media memiliki hubungan positif dengan perhatian terkait penyakit (*disease concern*). Hal ini menjadi gambaran dalam penelitian ini, khususnya terkait dengan perhatian privasi seseorang.

Secara demografis, DKI Jakarta memiliki sekitar 698 ribu mahasiswa baik negeri maupun swasta pada 2021 (Badan Pusat Statistik DKI Jakarta, 2021). Sebagai mahasiswa tentu memiliki latar belakang studi pendidikan yang beragam sehingga diharapkan penelitian ini dapat menggambarkan dalam konteks lebih luas. Sehingga harapannya, penelitian ini dapat menjawab pengaruh terpaan media terkait berita kebocoran data pribadi terhadap perhatian privasi mahasiswa di DKI Jakarta.

1.2 Rumusan Masalah

Latar belakang yang telah dijabarkan di atas, maka rumusan masalah penelitian ini adalah "Apakah Terdapat Pengaruh Berita tentang Kebocoran Data Pribadi di Media Daring terhadap Perhatian Privasi Mahasiswa di DKI Jakarta?".

1.3 Pertanyaan Penelitian

Dari rumusan masalah diatas maka pertanyaan penelitian yang dapat diajukan adalah:

1. Seberapa tinggi terpaan berita kebocoran data di media daring pada mahasiswa DKI Jakarta?

UNIVERSITAS MULTIMEDIA NUSANTARA

2. Seberapa tinggi tingkat perhatian privasi pada mahasiswa DKI Jakarta?
3. Seberapa besar pengaruh terpaan berita tentang kebocoran data pribadi di media daring terhadap perhatian privasi mahasiswa DKI Jakarta ?

1.4 Tujuan Penelitian

Dari pertanyaan diatas maka tujuan diadakannya penelitian ini adalah:

1. Untuk mengetahui seberapa tinggi terpaan berita kebocoran data di media daring pada mahasiswa DKI Jakarta
2. Untuk mengetahui seberapa tinggi tingkat perhatian privasi pada mahasiswa DKI Jakarta
3. Untuk mengetahui seberapa besar pengaruh terpaan berita tentang kebocoran data pribadi di media daring terhadap perhatian privasi mahasiswa DKI Jakarta

1.5 Kegunaan Penelitian

Kegunaan dari penelitian ini terbagi menjadi 3 bagian yaitu:

A. Kegunaan Akademis

Penelitian ini akan menjelaskan bagaimana terpaan media terkait suatu kasus dapat mempengaruhi tingkat perhatian privasi mahasiswa di DKI Jakarta. Dengan menerapkan konsep terpaan media dengan tiga dimensi terpaan media dan empat dimensi perhatian privasi, penelitian ini akan menjabarkan apakah pemberitaan terkait kebocoran data pribadi dapat berpengaruh terhadap perhatian privasi mahasiswa di DKI Jakarta.

UNIVERSITAS MULTIMEDIA NUSANTARA

Penelitian ini juga diharapkan dapat menjadi referensi bagi penelitian yang relevan.

B. Kegunaan Praktis

Kegunaan praktis dalam penelitian ini diharapkan bisa menjadi acuan bagi media yang menyebarkan informasi mengenai kebocoran identitas. Dengan begitu, media dapat lebih meningkatkan informasi terkait kebocoran data pribadi agar dapat memberikan pemahaman terhadap khalayak yang mengkonsumsi berita serta mencegah adanya pihak masyarakat yang dirugikan.

C. Kegunaan Sosial

Penelitian ini diharapkan dapat menambah pengetahuan bagi masyarakat, terutama kaum pengguna internet mengenai perhatian privasi. Selain itu penelitian ini juga diharapkan dapat memberikan informasi kepada media dalam membangun persepsi privasi masyarakat terkait berita kebocoran data pribadi.

1.6 Kelemahan Penelitian

Kelemahan penelitian sebagai berikut:

A. Penelitian ini menggunakan teknik quota sampling yang termasuk dalam *non-probability sampling*. Sehingga penelitian ini tidak memberikan kesempatan yang sama bagi seluruh responden.

UNIVERSITAS MULTIMEDIA NUSANTARA

B. Penyebaran kuesioner tidak merata dikarenakan ada beberapa universitas tidak ikut andil dalam penelitian.

UNIVERSITAS
MULTIMEDIA
NUSANTARA