BAB I

PENDAHULUAN

1.1. Latar Belakang

Jumlah pengguna *smartphone* secara global terus meningkat dari tahun ke tahun. Pada 2019, setidaknya terdapat 3,2 miliar pengguna, naik 5,6% dari tahun sebelumnya. Sementara jumlah smartphone yang digunakan mencapai 3,8 miliar unit. Pengguna *smartphone* Indonesia juga bertumbuh dengan pesat. Lembaga riset *digital marketing* Emarker memperkirakan pada tahun 2019 jumlah pengguna aktif *smartphone* di Indonesia kurang lebih ada 92 juta orang. *Smartphone* memenuhi banyak kebutuhan seperti menggunakan *internet banking*, media sosial, bermain game, memesan alat transportasi online seperti Grab, membeli tiket, memesan makanan, ngobrol dengan teman melalui pesan, telepon dan *video call*, bahkan tak sedikit yang mengedit video di *smartphone* (website databoks, 2019)

Meskipun *smartphone* memberikan kemudahan terhadap berbagai kebutuhan di satu sisi, akan tetapi di sisi lain, penggunaannya akan menjadi hal yang merugikan apabila tidak berhati-hati terhadap keamanan data pribadi. Seperti yang disampaikan oleh Xu et.al. (2012), bahwa akses data yang digunakan oleh pengembang aplikasi *mobile* dan sistem operasi telah memperburuk masalah privasi para pengguna smartphone. Privasi adalah hak individu untuk menentukan apakah data pribadi akan dikomunikasikan atau tidak kepada pihak lain. (RUU PDP, 2014). Kekhawatiran ini terkait dengan pengumpulan secara otomatis dari pengguna perangkat *smartphone* seperti informasi keberadaan secara *real-time*, kerahasiaan data yang dikumpulkan seperti lokasi, identitas pribadi, dan perilaku sehari-hari. Berbeda dengan internet konvensional, *platform mobile* memungkinkan untuk *real-time* serta komunikasi data, transmisi yang selalu menyala sehingga menimbulkan ancaman terhadap privasi.

Salah satu contoh kasus terjadi pada tahun 2019, yaitu terjadinya kasus kebocoran data pribadi dari perusahaan *marketplace* Tokopedia. Hal ini bermula dari sebuah akun twitter @penjagakijang mem-posting sebuah gambar tangkapan layar yang melihatkan adanya penjualan 4 juta data pribadi pengguna Tokopedia pada tanggal 21 Februari 2019 (Ecular *et al.*, 2020). Di situs selly.id dijelaskan, ada pembagian paket penjualan, di antaranya data

pengguna Tokopedia yang berupa alamat email, nomor telepon, dan alamat tempat tinggal dijual dengan harga 234 dolar AS. Sementara untuk daftar email saja dijual terpisah dengan harga 10 dolar AS untuk 300 ribu alamat email. Masih pada tahun yang sama, tepatnya bulan Maret 2019 juga terjadi kebocoran data pribadi oleh perusahaan Marketplace Bukalapak. Sebanyak 13.369.666 data pengguna telah dicuri oleh seorang *hacker* profesional asal Pakistan dengan julukan Gnostic Players. Data yang dimaksud terdiri dari email, username, nama, rincian pembelanjaan, alamat IP, serta kata sandi akun 5 yang diperjual belikan pada situs "Dream Market", situs jual beli di Dark Web. Bukalapak telah mengonfirmasi bahwa memang ada upaya peretasan. (Ecular et al., 2020).

Kasus pembobolan dan kebocoran data dan informasi juga merupakan problematika yang sedang terjadi di Indonesia, berikut beberapa contoh kasusnya dalam penelitian Aswandi (2018) :

Tabel 1. Beberapa Kasus Pencurian Data Pribadi Dan Penjualan Data Pribadi

Kasus	**Jumlah penyalahgunaan data pribadi**	**Tahun**
Kasus pembobolan Sony Corp.	Kelompok *hacker* membobol jaringan playstation Sony dan mencuri data lebih dari 77 juta *account*.	2011
Kasus pembobolan data pribadi Telkomsel.	Diperkirakan 25 juta data pribadi pelanggan Telkomsel.	2011
Lion group.	Diperkirakan 7,8 juta data penumpang.	2018
Data dan informasi seseorang diperjualbelikan melalui group media sosial facebook "Dream Market Official".	Diketahui menyimpan jutaan data pribadi warga negara Indonesia yang terdiri dari 761.435 nomor ponsel, 129.421 kartu kredit.	2019
Melalui akun twitter @hendralm. Data pribadi yang diperjualbelikan berupa NIK dan KK hingga foto selfie.	Data (Kartu Keluarga) dan Data NIK (Nomor Induk Kependudukan).	2019
Penjualan data ditemukan di aplikasi belanja online besar yakni Tokopedia dan Bukalapak.	Data terbagi atas 75.824 data nasabah deposito, dan 64.769 data nasabah kartu kredit.	2019

(Aswandi, 2018)

Semakin maju teknologi semakin banyak pula tindak pencurian yang dilakukan, mengambil sesuatu dari orang tanpa sepengetahuan orang tersebut adalah tindakan pencurian. Mencuri adalah perbuatan dosa dan akan mendapatkan balasan yang setimpal. Berikut ini ayat yang membahas tentang pencurian dan kejahatan:

وَٱلسَّارِقُ وَٱلسَّارِقَةُ فَٱقْطَعُوٓاْ أَيْدِيَهُمَا جَزَآءًۢ بِمَا كَسَبَا نَكَٰلًا مِّنَ ٱللَّهِ ۗ وَٱللَّهُ عَزِيزٌ حَكِيمٌ

“Laki-laki yang mencuri dan perempuan yang mencuri, potonglah tangan keduanya (sebagai) pembalasan bagi apa yang mereka kerjakan dan sebagai siksaan dari Allah. Dan Allah Maha Perkasa lagi Maha Bijaksana” (QS. al-maidah: 38) :

لَّيْسَ بِأَمَانِيِّكُمْ وَلَآ أَمَانِيِّ أَهْلِ ٱلْكِتَٰبِ ۗ مَن يَعْمَلْ سُوٓءًا يُجْزَ بِهِۦ وَلَا يَجِدْ لَهُۥ مِن دُونِ ٱللَّهِ وَلِيًّا وَلَا نَصِيرًا

“(Pahala dari Allah) bukanlah (menurut) angan-anganmu 168) dan bukan (pula menurut) angan-angan Ahli Kitab. Siapa yang mengerjakan kejahatan niscaya akan dibalas sesuai dengan (kejahatan itu) dan dia tidak akan menemukan untuknya pelindung serta penolong selain Allah" (QS. An-Nisa’: 123)

Dengan semakin banyaknya kasus kebocoran keamanan informasi dan semakin banyaknya berbagai aplikasi pada *smartphone* yang memungkinkan data pribadi tersimpan dalam sistem aplikasi tersebut baik secara disengaja atau tidak, maka masyarakat perlu waspada atau “*aware*” dengan keamanan data pribadinya. Sehingga dapat mencegah terjadinya kemungkinan kerugian baik secara material maupun moril dengan tersebarnya informasi data pribadinya. Untuk mengetahui tingkat kesadaran keamanan informasi pada masyarakat, maka perlu dilakukan sebuah survei mengenai bagaimana sebetulnya tingkat kesadaran keamanan informasi mengenai data pribadi pada para pengguna *smartphone*.

Berdasarkan latar belakang di atas, maka penulis tertarik untuk mengambil topik tentang “TINGKAT KESADARAN KEAMANAN DATA PRIBADI PENGGUNA *SMARTPHONE* DAN TINJAUANNYA MENURUT ISLAM”

1.2. Rumusan Masalah

Berdasarkan latar belakang yang telah dikemukakan, maka dirumuskan masalah sebagai berikut:

a. Bagaimana tingkat kesadaran keamanan data pribadi pada pengguna *smartphone*.
b. Bagaimana tinjauan Islam terhadap tingkat kesadaran keamanan data pribadi pada pengguna *smartphone*.

1.3. Tujuan Penelitian

Tujuan penelitian ini adalah:

a. Untuk mengetahui tingkat kesadaran keamanan data pribadi pada pengguna *smartphone*.
b. Untuk mengetahui tinjauan Islam terhadap tingkat kesadaran keamanan data pribadi pada pengguna *smartphone*.

1.4. Manfaat Penelitian

Adapun manfaat dari penelitian ini adalah:

a. Mengetahui gambaran mengenai tingkat kesadaran keamanan data pribadi pengguna *smartphone.*
b. Dapat memberikan referensi mengenai keamanan data pribadi.

1.5. Batasan Penelitian

Untuk lebih terarah dalam penelitian ini maka diberikan pembatasan masalah yaitu penelitian ini hanya membahas mengenai kesadaran keamanan data pribadi pada pengguna *smartphone* di Indonesia menggunakan Model Kruger dan Kearney dan berfokus pada 3 area keamanan privasi dari Xu et.al (2012).