BAB I

PENDAHULUAN

1.1 Latar Belakang

Di masa pandemi Covid-19 hampir dua tahun terakhir, telah terjadi perubahan besar pada komunikasi antar sesama manusia. Interaksi dari luring ke daring mengalami peningkatan yang signifikan berkat adanya pembatasan-pembatasan skala besar yang melarang untuk melaukan pertemuan secara fisik untuk menghindari terpapar virus yang saat ini tegah merebak. Pergeseran cara berkomunikasi ini telah mengubah paradigmasosial di seluruh penjuru dunia, khususnya di Indonesia (Ariansyah, 2015; Fauzi, Harly, dan Hs, 2012; Wardiana, 2004). Hal ini mempercepat masa baru yang diketahui dengan istilah digitalization dan telah merubah banyak perihal dalam seni berbicara dan interaksi sosial kemasyarakatan.

Interaksi sosial dan komunikasi yang bergeser ke dunia maya dengan intensitas yang meningkat telah memaparkan berbagai resiko. Kecanggihan teknologi saat ini banyak memunculkan perilaku kejahatan yang menjadi rekayasa sosial yang digunakan sebagai modus yang dipergunakan di era digitalisasi. Cara atau metode yang digunakan biasanya tidak memerlukan banyak alat ataupun perangkat lunak canggih. Biasanya pelaku kejahatan memanfaatkan situasi kondisi psikologis korban untuk melakukan manipulasi. Seperti dipaparkan oleh Goel, Williams dan Dincelli (2017) bahwa sumber terbesar dari kejahatan siber adalah kelemahan dasar manusiayaitu kerentanan kita untuk ditipu.

Situasi seperti ini juga kian meningkat di masa pandemi Covid-19. Dimasa pandemi, dalam rangka mempercepat penanganan *corona disease* 19 (covid-19), Pemerintah Indonesia menjalankan rencana untuk mengimplementasikan skenario *new normal* dengan mempertimbangkan studi epidemiologis dan kesiapan regional. Pembatasan skala besar tidak memperbolehkan masyarakat untuk membuka usaha mereka sehingga kondisi ekonomi masyarakat yang rata-rata mengalami penurunan. Hal ini memicu beberapa perilaku kejahatan yang berkembang, salah satunya kerentanan sosial dalam tindak kejahatan digitalisasi (*cyber crime*).

Dari laman https://www.patrolisiber.id/home selama setahun terakhir, jumlah laporan polisi yang dibuat masyarakat terdapat total aduan 2.259 aduan dan total kerugian triliunan rupiah, berikut data penyerangan siber per platform yang terjadi di Indonesia.

Tabel 1. 1 Jumlah Laporan Polisi yang Dibuat Masyarakat

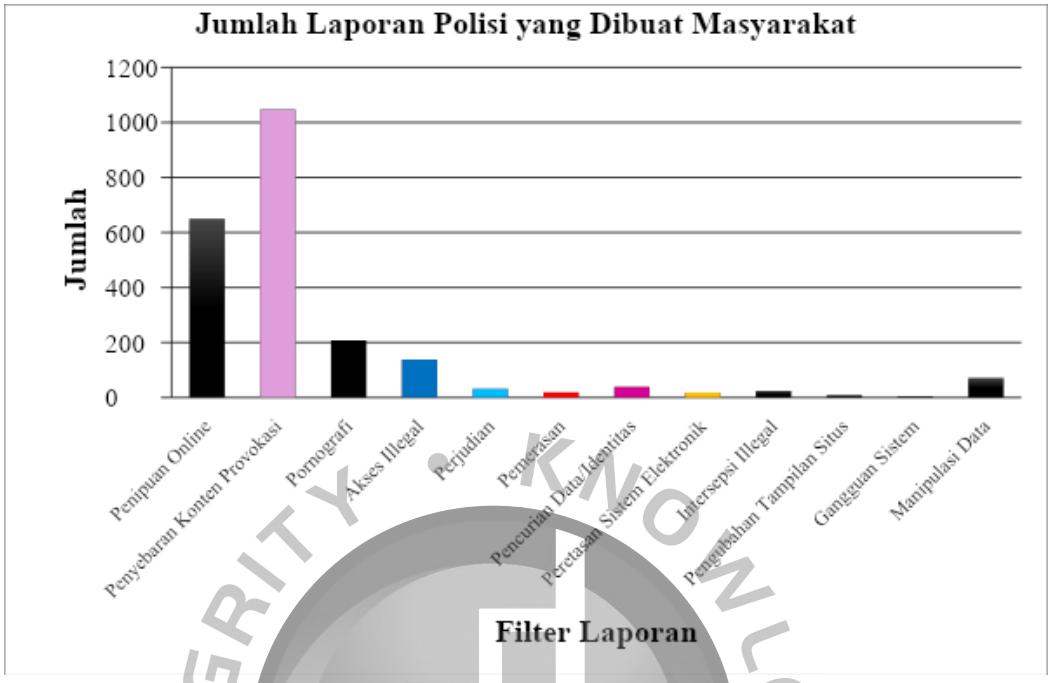
No	Jenis Kejahatan	Jumlah
1	Penyebaran Konten Provokasi	1048
2	Penipuan Online	649
3	Pornografi	208
4	Akses Illegal	138
5	Perjudian	32

6	Pemerasan	19
7	Pencurian Data/Identitas	39
8	Peretasan Sistem Elektronik	18
9	Intersepsi Illegal	24
10	Pengubahan Tampilan Situs	9
11	Gangguan Sistem	4
12	Manipulasi Data	71
Total Jumlah		2259

Sumber : https://www.patrolisiber.id/home

Laporan di atas diketahui bahwa Penipuan Online menjadirangking kedua jumlah aduan yang dilaporkan masyarakat kepada Polisi pada tahun 2020. Selain itu Penyebaran Konten Provokasi juga memiliki aduan tertinggi dengan 1048

aduan.



Sumber: https://www.patrolisiber.id/statistic

Gambar 1. 1 Jumlah Laporan Polisi yang dibuat Masyarakat

1.2 Penggunaan Media Sosial Dalam Kejahatan Siber

Whatsapp (WA) adalah satu dari sebagian opsi aplikasi chat yang sangat terkenal untuk golongan pengguna *smartphone*. Banyaknya fitur yang disediakan WhatsApp dan mudahnya pengoperasian aplikasi ini buatnya kilat merebut hati pengguna *smartphone*. Tetapi sangat di sayangkan terdapat oknum–oknum yang menggunakan kecanggihan teknologi yang terdapat saat ini untuk berbuat jahat.

Dalam kasus McAfee, 46% warga Inggris diretas oleh penjahat dunia maya kaitannya dengan peretasan akun, dan akibatnya mereka kehabisan uang. Di negara

Inggris, penipuan ini menelan biaya rata-rata £725 per orang.. Whatsapp merupakan target *scammers* untuk saaat ini.

Masalah WhatsApp inilah yang paling diharapkan *hacker* untuk menyasar salah satu teman target pengguna. *hacker* bertindak sebagai "teman palsu". Awal mulanya hendak berpura- pura mengubah nomor, merasa kenal, kemudian mempunyai tujuan akhir memohon kode verifikasi selaku pengingat, kode verifikasi ini ialah suatu aspek krusial di WhatsApp. Kalian umumnya hendak menerima kode itu kala mendaftar di WhatsApp. Kode ini sendiri bertugas memverifikasi pengguna nomor telepon sebagai pemegang akun legal. Bila penipu telah mempunyai kode verifikasi, mereka hendak mengambil alih akun WhatsApp tersebut serta setelah itu berpura- pura menjadi sang pengguna yang asli buat melaksanakan kejahatan. Ini yang biasa diketahui dengan akun kena hack ataupun dibajak. Bagi Straits Times, 10 orang di Singapore telah terserang tipuan dengan modus semacam ini. Selaku pengguna WhatsApp, pastinya kita juga mesti mengenali metode supaya bebas dari modus penipuan berbagai ini, jangan sempat sekali- kali memberitahukan kode verifikasi WhatsApp ke orang lain. Tidak terdapat alibi orang lain memerlukan kode tersebut. Tanpa kode verifikasi, pengguna yang lagi melaksanakan verifikasi nomor takkan dapat menyelesaikan proses tersebut, ataupun memakai WhatsApp dengan nomor bersangkutan.

Melihat fenomena berubahnya pola komunikasi masyarakat setelahpandemi menjadi online dan banyaknya kejahatan yang meningkat setelah adanya pergeseran tersebut, mendorong diperlukannya penelitian mengenai kerentanan

seseorang dalam menghadapi ancaman keamanan siber. Namun sayangnya penelitian mengenai konteks ini di Indonesiamasih sangat jarang. Dari telusuran yang dilakukan pada Google Scholar dengan keyword kerentanan dan internet, kebanyakan hasil mengacu pada pengujian teknis informatika dan hampir tidak ada yang mengacu pada kerentanan dalam aspek manusia yang disebabkan oleh rekayasa sosial terutama pada social media chat. Salah satu penelitian yang ditemukan mengenai topic yang serupa adalah milik Albladi dan George (2020) yang meneliti tentang kerentanan di media social facebook. Dalam penelitian tersebut, Albladi dan George mengungkapkan beberapa factor yang bias menjadi indicator dari pada kerentanan seseorang terhadap rekayasa social dalam social media. Salah satunya adalah perspektif Sosio Emosional seseorang seperti antara lain Motivasi dan Kepercayaan.

1.3 Ruang Lingkup Masalah

Adapun ruang lingkup dalam penelitian ini adalah sebagai berikut:

1. Penelitian ini merupakan replikasi dari penelitian sebelumnya yang diteliti oleh (Albladi and George 2020) “Predicting individuals’ vulnerability to social engineering in social networks” Ruang lingkup yang diteliti terbatas pada perspektf Socio Emotional yaitu motivasi*(motivation),* kepercayaan *(trust), dan pengalaman masa lalu(past experience).*
2. Ruang lingkup penelitian hanya akan focus pada social media whatsapp sebagai media rekaya social yang digunakan dan tidak melakukan

investigasi pada media social lain seperti instagram, facebook dan lainnya.

1.4 Identifikasi Masalah

Berdasarkan pengamatan latar belakang diatas bahwa banyak aduan mengenai penipuan online dalam kurun waktu setahun belakangan. Adapun penipuan online tersebut kerap terjadi karena adanya kerentanan serangan siber dengan cara rekayasa sosial pada pengguna internet dan sosial media pada khususnya. Peristiwa yang kerap terjadi menimbulkan *Susceptibility* pada aplikasi sosial media *WhatsApp*. Diduga bahwa kerentanan terhadap serangan siber berbasis rekayasa ini dapat diprediksi dari motivasi *(motivation),* kepercayaan *(trust) dan pengalaman masa lalu(past experience).* sehingga dapat diketahui seberapa pentingnya literasi mengenai kerentanan sosial (*susceptibility)* untuk dipelajari lebih lanjut.

1.5 Perumusan Masalah

Dari kesenjangan penelitian terkait tentang fenomena aduan penipuan online yang meningkat dan juga telusuran literatur mengenai kerentanan terhadap serangan siber, diduga bahwa ada keterkaitan antara motivasi, kepercayaan dan pengalaman masa lalu terhadap kerentanan serangan siber seseorang saat berinteraksi di media sosial studi penelitian yang dilakukan mereplikasi dari penelitian sebelumnya.

Adapun perumusan masalah penelitian ini antara lain :

1. Apakah terdapat pengaruh dari antara motivasi (motivation) terhadap kerentanan serangan siber berbasis rekayasa social ?

a) Apakah terdapat pengaruh antara motivasi yang bersifat hedonisterhadap kerentanan siber berbasis rekaya social ?

b) Apakah terdapat pengaruh antara motivasi yang bersifat socialterhadap kerentanan siber berbasis rekayasa sosial

2. Apakah terdapat pengaruh dari kepercayaan (trust) terhadap kerentanan serangan siber berbasis rekayasa social ?

a) Apakah terdapat pengaruh dari kepercayaan yang bersumber dariprovider pada kerentanan serangan siber berbasis rekayasa social ?

b) Apakah terdapat pengaruh dari kepercayaan yang bersumber daripengguna lain pada kerentanan serangan siber berbasis rekayasa sosial?

3. Apakah terdapat pengaruh dari pengalaman masa lalu (*past experience*) terhadap kerentanan sosial?

1.6 Pembatasan Masalah

Pembatasan masalah survei yang dilakukan adalah kerentanan sosial yang dilakukan dalam perilaku kejahatan melalui interaksi pada media sosialberbasis pesan yaitu aplikasi pesan Whatsapp (*Whatsapp Messaging*)

1.7 Tujuan Penelitian

Berdasarkan permasalahan yang ada, untuk itu tujuan yang diharapkan antara lain :

1. Mengetahui pengaruh dari motivasi (*motivation*) terhadap kerentanan pada serangan siber berbasis rekayasa sosial baik motivasi yang sifatnya hedonis maupun sosial/utilitarian.

2. Mengetahui pengaruh dari kepercayaan (*trust*) terhadap kerentanan pada serangan siber berbasis rekayasa sosial baik kepercayaan pada provider (Whatsapp) atau pengguna media sosial tersebut
3. Mengetahui pengaruh dari pengalaman masa lalu (*past experience)* terhadap kerentanan pada serangan siber berbasis rekayasa sosial

1.8 Manfaat Penelitian

Manfaat penelitian yang dapat diambil dari penelitian ini, antara lain:

1. Peneliti memberikan kontribusi untuk menambah dan memperluas informasi tentang pengaruh motivasi (*motivation*) dan kepercayaan (*trust*) terhadap kerentanan serangan siber berbasis rekayasa sosial.
2. Bagi Perusahaan Sebagai sumber bahan referensi bagi penelitian di bidang pemasaran di media sosial di masa mendatang dan sebagai bahan untuk menambah khasanah pengetahuan mengenai kerentanan serangan siber berbasis rekayasa sosial di media sosial pesan padakhususnya.

1.9 Sistematika Penulisan

Secara umum skripsi ini meliputi paparan sistematika penulisan yang diklasifikasikan menjadi lima bab dan juga beberapa sub bab sebagai berikut:

BAB I PENDAHULUAN

Di bab ini menjabarkan latar belakang, ruang lingkup masalah,identifikasi masalah, perumusan masalah,tujuan penelitian,manfaat penelitian serta sistematika penulisan.

BAB II LANDASAN TEORI

Menjabarkan teori-teori yang berkaitan dengan topik bahasan, antara lain landasan teori, kerangka pemikiran dan hipotesis.

BAB III METODOLOGI PENELITIAN

Menjelaskan tentang metode pengumpulan dan penganalisisan data, meliputi obyek penelitian, desain penelitian, teknik pengumpulan data, populasi sampel dan metode pengambilansampel, variabel operasional, teknik pengolahan dan analisis data.

BAB IV ANALISIS DATA DAN PEMBAHASAN

Terdiri dari deskripsi lokasi penelitian, analisis data danpembahasan hasil penelitian dan implikasi.

BAB V KESIMPULAN DAN SARAN

Mencakup kesimpulan, keterbatasan penelitian dan saran