PENGARUH MOTIVASI TERHADAP PERLINDUNGAN DATA PERIBADI PELAJAR KOLEJ VOKASIONAL DI MALAYSIA DALAM PENGGUNAAN PERKHIDMATAN RANGKAIAN SOSIAL

MUHAMAD HASNAN BIN ABDULLAH

UNIVERSITI PENDIDIKAN SULTAN IDRIS

2021

PENGARUH MOTIVASI TERHADAP PERLINDUNGAN DATA PERIBADI PELAJAR KOLEJ VOKASIONAL DI MALAYSIA DALAM PENGGUNAAN PERKHIDMATAN RANGKAIAN SOSIAL

MUHAMAD HASNAN BIN ABDULLAH

05-4506832 pustaka.upsi.edu.my Perpustakaan Tuanku Bainun Kampus Sultan Abdul Jalil Shah PustakaTBainun ptbupsi

DISERTASI DIKEMUKAKAN BAGI MEMENUHI SYARAT UNTUK MEMPEROLEH IJAZAH SARJANA PENDIDIKAN
(TEKNOLOGI MAKLUMAT)
(MOD PENYELIDIKAN DAN KERJA KURSUS)

FAKULTI SENI, KOMPUTERAN DAN INDUSTRI KREATIF
UNIVERSITI PENDIDIKAN SULTAN IDRIS

2021

05-4506832 pustaka.upsi.edu.my Perpustakaan Tuanku Bainun Kampus Sultan Abdul Jalil Shah PustakaTBainun ptbupsi

UPSI/IPS-3/BO 32
Pind : 00 m/s: 1/1

UNIVERSITI PENDIDIKAN SULTAN IDRIS
SULTAN IDRIS EDUCATION UNIVERSITY

Sila Taipkan (√):

Kertas Projek	
Sarjana Penyelidikan	
Sarjana Penyelidikan Dan Kerja Kursus	✓
Doktor Falsafah	

INSTITUT PENGAJIAN SISWAZAH
PERAKUAN KEASLIAN PENULISAN

Perakuan ini telah dibuat pada **16** (hari bulan) **FEBRUARI** (bulan) 20**21**.

i. Perakuan pelajar :

Saya, **MUHAMAD HASNAN BIN ABDULLAH, M20181000813, FAKULTI SENI, KOMPUTERAN DAN INDUSTRI KREATIF** (SILA NYATAKAN NAMA PELAJAR, NO. MATRIK DAN FAKULTI) dengan ini mengaku bahawa disertasi/~~tesis~~ yang bertajuk **PENGARUH MOTIVASI TERHADAP PERLINDUNGAN DATA PERIBADI PELAJAR KOLEJ VOKASIONAL DI MALAYSIA DALAM PENGGUNAAN PERKHIDMATAN RANGKAIAN SOSIAL** adalah hasil kerja saya sendiri. Saya tidak memplagiat dan apa-apa penggunaan mana-mana hasil kerja yang mengandungi hak cipta telah dilakukan secara urusan yang wajar dan bagi maksud yang dibenarkan dan apa-apa petikan, ekstrak, rujukan atau pengeluaran semula daripada atau kepada mana-mana hasil kerja yang mengandungi hak cipta telah dinyatakan dengan sejelasnya dan secukupnya

_____
Tandatangan pelajar

ii. Perakuan Penyelia:

Saya, **DR NOOR ANIDA ZARIA BINTI MOHD NOOR** dengan ini mengesahkan bahawa hasil kerja pelajar yang bertajuk **PENGARUH MOTIVASI TERHADAP PERLINDUNGN DATA PERIBADI PELAJAR KOLEJ VOKASIONAL DI MALAYSIA DALAM PENGGUNAAN PERKHIDMATAN RANGKAIAN SOSIAL** dihasilkan oleh pelajar seperti nama di atas, dan telah diserahkan kepada Institut Pengajian Siswazah bagi memenuhi sebahagian/sepenuhnya syarat untuk memperoleh Ijazah **SARJANA PENDIDIKAN (TEKNOLOGI MAKLUMAT)**.

16 FEBRUARI 2021 _____

Tarikh Tandatangan Penyelia

UPSI/IPS-3/BO 31
Pind : 01 m/s: 1/1

UNIVERSITI PENDIDIKAN SULTAN IDRIS
SULTAN IDRIS EDUCATION UNIVERSITY

INSTITUT PENGAJIAN SISWAZAH /
INSTITUTE OF GRADUATE STUDIES

BORANG PENGESAHAN PENYERAHAN ~~TESIS~~/DISERTASI/~~LAPORAN KERTAS PROJEK~~
DECLARATION OF THESIS/DISSERTATION/PROJECT PAPER FORM

Tajuk / Title: PENGARUH MOTIVASI TERHADAP PERLINDUNGAN DATA PERIBADI PELAJAR KOLEJ VOKASIONAL DI MALAYSIA DALAM PENGGUNAAN PERKHIDMATAN RANGKAIAN SOSIAL

No. Matrik /*Matric's No.*: M20181000813

Saya / *I* : MUHAMAD HASNAN BIN ABDULLAH

(Nama pelajar / *Student's Name*)

mengaku membenarkan Tesis/Disertasi/Laporan Kertas Projek (~~Kedoktoran~~/Sarjana)* ini disimpan di Universiti Pendidikan Sultan Idris (Perpustakaan Tuanku Bainun) dengan syarat-syarat kegunaan seperti berikut:-
acknowledged that Universiti Pendidikan Sultan Idris (Tuanku Bainun Library) reserves the right as follows:-

1. ~~Tesis~~/Disertasi/~~Laporan~~ Kertas Projek ini adalah hak milik UPSI.
   The thesis is the property of Universiti Pendidikan Sultan Idris
2. Perpustakaan Tuanku Bainun dibenarkan membuat salinan untuk tujuan rujukan dan penyelidikan.
   Tuanku Bainun Library has the right to make copies for the purpose of research only.
3. Perpustakaan dibenarkan membuat salinan ~~Tesis~~/Disertasi ini sebagai bahan pertukaran antara Institusi Pengajian Tinggi.
   The Library has the right to make copies of the thesis for academic exchange.
4. Sila tandakan (√) bagi pilihan kategori di bawah / *Please tick (√) for category below*:-

☐	**SULIT/*CONFIDENTIAL***	Mengandungi maklumat yang berdarjah keselamatan atau kepentingan Malaysia seperti yang termaktub dalam Akta Rahsia Rasmi 1972. / Contains confidential information under the Official Secret Act 1972
☑	**TERHAD/*RESTRICTE***	Mengandungi maklumat terhad yang telah ditentukan oleh organisasi/badan di mana penyelidikan ini dijalankan. / Contains restircted information as specified by the organization where research was done.
☐	**TIDAK TERHAD / *OPEN ACCESS***	

(Tandatangan Pelajar/ *Signature*)

(Tandatangan Penyelia / *Signature of Supervisor*)
& (Nama & Cop Rasmi / *Name & Official Stamp*)

Tarikh: 16 FEBRUARI 2021

Catatan: Jika Tesis/Disertasi ini **SULIT** @ **TERHAD**, sila lampirkan surat daripada pihak berkuasa/organisasi berkenaan dengan menyatakan sekali sebab dan tempoh laporan ini perlu dikelaskan sebagai **SULIT** dan **TERHAD**.

Notes: If the thesis is CONFIDENTAL or RESTRICTED, please attach with the letter from the related authority/organization mentioning the period of confidentiality and reasons for the said confidentiality or restriction

PENGHARGAAN

Alhamdulillah bersyukur ke Hadrat Ilahi dengan limpah dan kurniaNya, dengan berkat kekasihNya, junjungan besar Nabi Muhammad S.A.W, dengan berkat guru-guru, karomah dan hikmah kedua ibu dan bapa dapatlah saya menyiapkan laporan disertasi bagi memenuhi syarat untuk menperolehi ijazah sarjana pendidikan.

Pertama sekali saya ingin merakamkan jutaan terima kasih kepada penyelia Dr Noor Anida Zaria binti Mohd Noor yang banyak membantu dan memberikan pandangan dalam menyiapkan laporan disertasi ini. Terima kasih saya ucapkan kepada kedua ibu dan bapa yang sentiasa mendoakan kesejahteraan dan keselamatan roh dan jasad saya semasa menyambung pengajian ini.

Tidak dilupakan kepada isteri Nur Atiqah binti Abd Hamid yang banyak berkorban masa dan tenaga serta tidak putus memberikan sokongan dan dorongan kepada saya dalam menyiapkan laporan ini serta anak – anak yang dikasihi yang sentiasa memahami semasa menjalankan kajian ini.

Akhir sekali, jutaan terima kasih kepada semua pihak yang terlibat dalam menjayakan kajian ini secara langsung mahupun tidak langsung. Hanya Allah sahaja yang dapat membalas jasa kalian dengan memberikan kebaikan berlipat ganda.

ABSTRAK

Perkongsian data peribadi yang tidak terkawal di kalangan pelajar dalam penggunaan perkhidmatan rangkaian sosial dapat mengakibatkan pencerobohan data sekiranya langkah perlindungan data peribadi tidak diamalkan. Kajian ini dibangunkan untuk meramal pengaruh motivasi terhadap perubahan tingkah laku perlindungan data peribadi di kalangan pelajar Kolej Vokasional seluruh Malaysia berdasarkan Teori Motivasi Perlindungan. Reka bentuk kuantitatif berdasarkan pendekatan kajian korelasi digunakan dalam membangunkan kajian ini dengan melibatkan seramai 214 orang pelajar Kolej Vokasional yang mengambil jurusan Teknologi Sistem Komputer dan Rangkaian di seluruh Malaysia. Soal selidik digunakan dalam mengumpul data dan dianalisis menggunakan analisis deskriptif dan regrasi berganda. Dapatan menunjukkan ancaman ganjaran maladaptif menyumbang sebanyak 14.9%, ancaman kelemahan menyumbang sebanyak 4.3% dan tanggapan keyakinan diri menyumbang sebanyak 2% terhadap perubahan tingkah laku perlindungan data peribadi dalam penggunaan perkhidmatan rangkaian sosial. Kesimpulan daripada kajian ini membuktikan ancaman ganjaran maladaptif dan ancaman kelemahan merupakan faktor bagi penilaian ancaman manakala tanggapan keyakinan diri merupakan faktor bagi penilaian tanggapan yang dapat mempengaruhi perubahan tingkah laku perlindungan data peribadi dalam penggunaan perkhidmatan rangkaian sosial. Implikasi kajian ini dapat membantu dalam merangka atau menambah baik program kesedaran dan kurikulum berkaitan keselamatan siber khususnya perlindungan data peribadi di kalangan pelajar Kolej Vokasional.

MOTIVATIONAL INFLUENCES ON PERSONAL DATA PROTECTION AMONG VOCATIONAL COLLEGE STUDENTS IN REGARDS TO THE USE OF SOCIAL NETWORKING SERVICES IN MALAYSIA

ABSTRACT

Uncontrolled sharing of personal data among students when using the social networking services, can result in data intrusion if personal data protection measures are not practiced. This study was developed to predict the influence of motivational changes in personal data protection behavior, among Vocational College students throughout Malaysia, based on Protection Motivation Theory. The quantitative design-based on the correlation study approach was used in developing this study, by involving a total of 214 Vocational College students majoring in Computer and Networking Systems Technology throughout Malaysia. Questionnaires were used in data collection and analyzed by using descriptive analysis and multiple regression analysis. The findings show that the threat of maladaptive rewards contributes 14.9%, the threat of vulnerability contributes 4.3% and the notion of self-confidence contributes 2% to the changes in personal data protection behavior, in the use of social networking services. The conclusions from this study prove that maladaptive reward threats and vulnerability threats are factors for threat appraisal while self-confidence perceptions is the factor for response appraisal that can influence changes in personal data protection behavior in regards to the use of social networking services. The implications of this study can help in designing or improving awareness programmes and curriculum related to cyber security, especially in relations to the protection of personal data among Vocational College students.

KANDUNGAN

Muka Surat

SENARAI JADUAL

SENARAI RAJAH

SENARAI SINGKATAN

ASEAN	Association of Southeast Asian Nation
UiTM	Universiti Teknologi Mara
TMP	Teori Motivasi Perlindungan
ARPA	Advanced Research Project Agency
ARPANET	Advanced Research Project Agency Network
IMP	Interface Massage Processors
PRNET	Packet Radio Network
SATNET	Atlantic Packet Satellite Network
TELNET	Teletype Network Protocol
FTP	File Transfer Protocol
TCP	Transmission Control Protocol
IP	Internet Protocol
NSF	National Science Foundation
PRS	Perkhidmatan Rangkaian Sosial

SENARAI LAMPIRAN

BAB 1

PENGENALAN

1.1 Pendahuluan

Kedudukan dunia global pada era transformasi digital begitu kritikal disebabkan oleh peningkatan serangan siber secara global yang memberi kesan negatif kepada sesebuah negara (Forum Ekonomi Dunia, 2019). Kajian terhadap keselamatan siber di negara ASEAN menunjukkan terdapat pihak tertentu menggunakan negara ASEAN bagi melancarkan serangan siber kepada dunia global di mana Malaysia, Indonesia dan Vietnam merupakan kawasan tumpuan global bagi melakukan serangan siber (Dobberstein et al., 2018).

Sebanyak 75% kes pada tahun 2020 berkaitan insiden serangan siber yang dilaporkan menunjukkan pencerobohan data berada pada tahap tertinggi dalam insiden serangan siber di Malaysia (CyberSecurity Malaysia, 2020). Pencerobohan data bukan hanya memberi kesan kepada syarikat korporat malah turut memberi kesan kepada individu sekiranya data tersebut jatuh ke tangan pihak yang tidak bertanggungjawab yang menyebabkan aktiviti jenayah siber seperti penipuan dan pemalsuan identiti

semakin berleluasa (Nur et al., 2017). Justeru itu, perlindungan terhadap data khususnya data peribadi perlu diberikan perhatian dalam kalangan pelajar sebagai pengguna internet.

Tidak dinafikan penggunaan teknologi seperti internet banyak memberi manfaat terhadap golongan pelajar khususnya dalam pembelajaran mereka (Abd Rahim et al., 2019; Mangold, 2016; Zahri et al., 2017). Penggunaan aplikasi internet dan media sosial seperti *Youtube*, *Facebook* dan *Whatsapps* (Suruhanjaya Komunikasi dan Multimedia Malaysia, 2015) memberi kesan positif terhadap pembelajaran mereka. Keghairahan dalam menerokai internet dan penggunaan media sosial ini membuatkan para pelajar terdedah dengan ancaman dan risiko seperti penipuan dan pemalsuan identiti (Abd Rahim et al., 2019).

Tambahan pula, sikap terlalu berkongsi apa jua maklumat dalam media sosial menggalakkan pihak yang tidak bertanggungjawab atau penceroboh mengintip dan mencuri maklumat peribadi mereka tanpa diketahui. Menurut Syazwan, Lukman, & Azhar, (2017) penggunaaan profil di media sosial menyebabkan maklumat-maklumat peribadi seperti nama, nombor telefon dan email begitu mudah diperolehi serta dapat digunakan untuk tujuan pemalsuan identiti dan penipuan. Oleh itu, kepentingan dalam mengenal pasti hubungan antara pengetahuan berkaitan teknologi keselamatan dan sikap terhadap kesedaran keselamatan siber dalam menghasilkan tingkah laku siber yang efektif supaya dapat melindungi data peribadi daripada disalahgunakan oleh penceroboh.

Pendidikan keselamatan siber bertujuan untuk memberi kesedaran terhadap ancaman siber serta menyediakan pengetahuan dan kemahiran kepada pelajar dalam menangani ancaman tersebut (Alshaikh et al., 2019). Peningkatan insiden pencerobohan data di peringkat global mahupun kebangsaan (CyberSecurity Malaysia, 2019; Forum Ekonomi Dunia, 2019; Gemalto, 2019; Dobberstein et al., 2018) menunjukkan keberkesanan program pendidikan siber dalam menghasilkan tingkah laku yang efektif untuk melindungi data peribadi boleh dipertikaikan (Dark & Mirkovic, 2015; Shillair, 2018).

Insiden kebocoran data yang berlaku di UiTM pada 25 Januari 2019 melibatkan sebanyak 1 juta data pelajar alumni melibatkan 13 kampus cawangan UiTM dicuri (Md Zain, 2019) dan sekiranya data tersebut dijual atau digunakan untuk aktiviti jenayah, maka tidak mustahil peningkatan jenayah akan meningkat dari tahun ke tahun. Ini dapat dielakkan sekiranya sikap terhadap kesedaran keselamatan dan perubahan tingkah laku terhadap ancaman siber di kalangan pelajar dapat mencegah pelajar tersebut menjadi mangsa dalam pencerobohan data peribadi. Seterusnya dapat membantu pihak kerajaan dalam mengurangkan aktiviti jenayah siber yang berlaku.

1.2 Latar Belakang Kajian

Statistik yang dikeluarkan oleh laman web *Breach Level Index* (Gemalto, 2019) menyatakan sebanyak 14 billion data yang direkodkan hilang atau dicuri sejak tahun 2013. Menurut laporan *Global Risk* 2019 *Insight*, pencerobohan data peribadi berada pada tempat ketiga di dalam 10 risiko atau ancaman yang dihadapi oleh dunia global (Forum Ekonomi Dunia, 2019).

Kajian yang dijalankan oleh CyberSecurity Malaysia, (2020) melaporkan sebanyak 4906 insiden penipuan atas talian melibatkan *phishing*, penipuan terhadap pekerjaan, penipuan terhadap perjudian dan pelaburan haram direkodkan pada tahun 2020. Hal ini menunjukkan secara jelas menunjukkan insiden pencerobohan data peribadi yang begitu serius di negara ini.

Kes pencerobohan data bukan sahaja melibatkan sektor kerajaan mahupun swasta malah individu turut menjadi mangsa dalam pencerobohan data ini dimana data peribadi tersebut digunakan oleh pihak yang tidak bertanggungjawab demi mengaut keuntungan dan seterusnya dapat memberi implikasi yang negatif terhadap negara.

Pertumbuhan ekonomi sesebuah negara turut terjejas akibat daripada ancaman pencerobohan data peribadi. Kajian tinjauan *Cost of Data Breach* yang dikeluarkan oleh Ponemon Institute (2020) menyatakan sebanyak 3.86 juta kos kerugian yang ditanggung negara dunia akibat daripada pencerobohan data peribadi. Sektor peruncitan dan kewangan merupakan sektor industri yang terjejas teruk akibat daripada pencerobohan data peribadi (Trustwave, 2019).

Implikasi daripada ancaman ini menyebabkan rakyat sesebuah negara berada dalam kemiskinan serta kesusahan daripada segi ekonomi yang boleh menimbulkan masalah sosial di kalangan rakyat seperti aktiviti jenayah. Tambahan pula, kajian Symantec (2019) menunjukkan penjenayah siber dapat meraih keuntungan pendapatan sebanyak 2.2 juta dolar setiap bulan dengan hanya menggunakan 10 maklumat kad kredit yang dicuri daripada laman web e-dagang. Ini secara jelas menunjukkan peningkatan terhadap jenayah siber di masa akan datang sekiranya isu pencerobohan data peribadi tidak ditangani secara efisen (Dobberstein et al., 2018; Nur et al., 2017).

Tingkah laku seseorang individu memainkan peranan penting dalam melindungi data peribadi. Penyelidik bersetuju bahawa pengguna internet merupakan kelemahan terbesar dalam rantaian keselamatan (Crossler et al., 2013; van Schaik et al., 2017; Wiederhold, 2014). Penyelidik dari Institut *Ponemon* mendapati kelemahan pengguna berpunca daripada peranti pengguna yang dijangkiti oleh *malware*, hilang atau dicuri (Ponemon Institute, 2019).

Pengguna internet juga seringkali digunakan oleh penceroboh sebagai medium perantara dalam melakukan serangan siber seperti memancing data (*phishing*) (Trustwave, 2019). Menyedari hal ini, kebanyakan penyelidik telah melakukan kajian secara empirikal terhadap pembangunan pendidikan dan program latihan keselamatan siber supaya pengguna internet khususnya para pelajar dapat melindungi data peribadi mereka daripada diceroboh oleh pihak yang tidak bertanggungjawab (D'Arcy et al., 2014; Warkentin et al., 2016).

Kementerian Pendidikan Malaysia dengan kerjasama DIGI dan Suruhanjaya Komunikasi dan Multimedia Malaysia juga telah melancarkan program kesedaran *CyberSafe* di kalangan pelajar sekolah diseluruh negara (Suruhanjaya Komunikasi dan Multimedia Malaysia, 2014) dengan tujuan untuk meningkatkan kefahaman dan kesedaran pelajar terhadap ancaman siber yang berlaku pada hari ini.

Kajian yang dilakukan oleh penyelidik hanya tertumpu kepada pengetahuan dan kesedaran berkaitan keselamatan siber pelajar secara umum (Jin et al., 2018; Park et al., 2017). Sesetengah kajian mengkaji berkaitan tingkah laku dalam keselamatan siber tanpa melihat pengetahuan teknologi keselamatan dan kesedaran keselamatan terhadap perubahan tingkah laku (Ng et al., 2009; Stanton et al., 2005) serta terdapat kajian yang

hanya menfokuskan kepada hubungan motivasi individu terhadap tingkah laku (Liang & Xue, 2010).

Selain itu, pengetahuan terhadap teknologi keselamatan tidak dapat menjamin penurunan bilangan insiden yang melibatkan pencerobohan data sekiranya perubahan terhadap tingkah laku tidak berlaku (Chmura, 2017; Soomro et al., 2016). Di samping itu, perubahan tingkah laku bukan sekadar menyediakan maklumat berkaitan risiko dan bertindak balas terhadap ancaman keselamatan bahkan pelajar harus mempunyai motivasi, niat dan sikap yang membawa kepada perubahan tingkah laku (Bada & Sasse, 2014). Justeru itu, hubungan antara pengetahuan teknologi dan kesedaran berkaitan keselamatan mengubah tingkah laku pelajar dalam melindungi data peribadi agar dapat membantu mengurangkan pencerobohan terhadap data peribadi khususnya terhadap pelajar.

1.3 Pernyataan Masalah

Perkembangan teknologi pada hari ini memberi kesan positif terhadap penggunaan peranti mudah alih seperti telefon pintar dan *tablet* berbanding penggunan komputer peribadi dan komputer riba. Para pelajar lebih gemar menggunakan telefon pintar atau *tablet* dalam mendapatkan maklumat melalui kemudahan internet. Ini dibuktikan dengan peningkatan sebanyak 22% pelajar yang berumur antara 13 hingga 17 tahun yang menggunakan telefon pintar atau *tablet* pada tahun 2018 berbanding tahun sebelumnya (Anderson & Jiang, 2018).

Peningkatan dalam penggunaan peranti mudah alih memberi impak yang positif terhadap pembangunan aplikasi terutamanya dalam perhidmatan rangkaian sosial. Banyak aplikasi perhidmatan rangkaian sosial yang telah dibangunkan oleh pembangun aplikasi untuk berkongsi maklumat dan mencari kenalan baru. Pada tahun 2018, aplikasi *Youtube* mendapat tempat di hati pengguna terutamnya para pelajar berbanding aplikasi *Facebook* yang sebelum ini berada pada tangga teratas aplikasi media sosial (OfCom, 2019). Selain itu, aplikasi *Instagram* dan *Snapchat* juga telah menunjukkan peningkatan penggunaan di kalangan pelajar (Anderson & Jiang, 2018).

Peranan perkhidmatan rangkaian sosial sebagai wadah kepada pembelajaran pelajar tidak dapat dinafikan. Pelbagai manfaat yang boleh diperolehi oleh para pelajar dalam menggunakan medium internet dan media sosial seperti peningkatan pencapaian akademik, motivasi, penglibatan dan kepuasan pelajar (Demirbilek & Talan, 2018; Roopchund et al., 2019; Silva-López et al., 2017). Akan tetapi risiko dalam penggunaan teknologi ini juga dapat memberikan kesan negatif kepada pelajar sekiranya tidak dikawal oleh guru dan ibu bapa.

Menurut kajian yang dijalankan oleh Gogus dan Saygın (2019), kebanyakan pelajar yang menggunakan perkhidmatan rangkaian sosial terutamanya *Facebook* tidak menyedari bahawa maklumat yang dikongsi pada platform tersebut dapat dilihat oleh orang asing. Hasil dapatan kajian oleh Syazwan et al. (2017) mengesahkan pelajar yang menggunakan media sosial mudah terdedah dengan serangan siber seperti buli siber, pemalsuan identiti, penipuan atas talian dan berita palsu.

Konsep perkongsian maklumat yang diperkenalkan dalam penggunaan perkhidmatan rangkaian sosial menyebabkan pelajar terlalu ghairah berkongsi segala maklumat termasuklah data peribadi mereka secara tidak sedar seperti maklumat diri dan gambar mereka (Abd Rahim et al., 2019; Livingstone et al., 2019). Kesan daripada tingkah laku tersebut, penjenayah siber mudah mengesan kedudukan para pelajar seterusnya membuka ruang untuk melakukan jenayah yang lebih besar seperti penculikan, peras ugut dan pornografi kanak-kanak.

Pendidikan atau program berkaitan kesedaran keselamatan siber telah banyak dilakukan berbentuk latihan (Choi, 2013; Mangold, 2016; Suruhanjaya Komunikasi dan Multimedia Malaysia, 2014; Zahri et al., 2017), kempen (Bada & Sasse, 2014) panduan dalam melayari internet (Cyber Security, 2014; International Telecommunication Union, 2009) dan kurikulum yang diterapkan dalam pelajaran pelajar di sekolah (Pruitt-Mentle, 2011; Sadaghiani-Tabrizi, 2018). Akan tetapi, keberkesanan segala bentuk program atau pendidikan keselamatan siber yang telah dijalankan masih boleh dipertikaikan daripada segi perubahan tingkah laku pelajar semasa berada atas talian.

Menurut Bada & Sasse (2014), kurangnya kefahaman dan persepsi pelajar semasa berada atas talian merupakan dua faktor yang mempengaruhi kegagalan perubahan tingkah laku pelajar terhadap keselamatan siber. Selain itu, kebanyakan penyelidik melakukan kajian lebih menfokuskan ke arah pengetahuan dan penggunaan teknologi keselamatan dalam membantu meningkatkan kesedaran dan tingkah laku pelajar (Alemany et al., 2019; Gogus & Saygın, 2019; Sundaram & Radha, 2019) berbanding kajian terhadap perubahan tingkah laku tersebut.

Ini dibuktikan dengan kajian yang dilakukan oleh Youn dan Shin (2019) yang mendapati bahawa berlaku ketidakseimbangan antara kebimbangan berkaitan perlindungan data peribadi dengan tingkah laku para pelajar yang juga dikenali sebagai paradoks privasi. Selain itu, masih kurang lagi kajian yang menfokuskan pengaruh motivasi terhadap perubahan tingkah laku terutamanya dalam penggunaan perkhidmatan rangkaian sosial (Boss et al., 2015; Posey et al., 2015; Yoon et al., 2012; Zhang et al., 2018).

Oleh yang demikian, suatu kajian perlu dilakukan untuk mengenal pasti hubungan antara pengaruh motivasi terhadap tingkah laku perlindungan data peribadi dalam penggunaan perkhidmatan rangkaian sosial agar dapat membantu dalam menurunkan bilangan insiden pencerobohan data peribadi seterusnya membangunkan pendidikan keselamatan siber yang lebih berkesan.

1.4 Matlamat Kajian

Kajian ini bertujuan untuk meramalkan pengaruh motivasi terhadap perubahan tingkah laku perlindungan data peribadi di kalangan pelajar Teknologi Sistem Komputer dan Rangkaian Kolej Vokasional di Malaysia dalam penggunaan perkhidmatan rangkaian sosial berdasarkan Teori Motivasi Perlindungan.

1.5 Objektif kajian

Kajian ini mempunyai dua objektif yang ingin dicapai iaitu:

i. Mengenal pasti faktor penilaian ancaman (keparahan, kelemahan dan ganjaran maladaptif) dalam mempengaruhi perubahan tingkah laku perlindungan data peribadi di kalangan pelajar dalam penggunaan perkhidmatan rangkaian sosial.
ii. Mengenal pasti faktor penilaian tanggapan (keyakinan diri dan keberkesanan tindak balas) dalam mempengaruhi perubahan tingkah laku perlindungan data peribadi di kalangan pelajar dalam penggunaan perkhidmatan rangkaian sosial.

1.6 Soalan Kajian

Persoalan kajian ini dikenalpasti berpandukan objektif kajian seperti berikut:

i. Adakah ancaman keparahan merupakan peramal bagi perubahan tingkah laku perlindungan data peribadi di kalangan pelajar dalam penggunaan perkhidmatan rangkaian sosial?
ii. Adakah ancaman kelemahan merupakan peramal bagi perubahan tingkah laku perlindungan data peribadi di kalangan pelajar dalam penggunaan perkhidmatan rangkaian sosial?
iii. Adakah ancaman ganjaran maladaptif merupakan peramal bagi perubahan tingkah laku perlindungan data peribadi di kalangan pelajar dalam penggunaan perkhidmatan rangkaian sosial?
iv. Adakah tanggapan keyakinan diri merupakan peramal bagi perubahan tingkah laku perlindungan data peribadi di kalangan pelajar dalam penggunaan perkhidmatan rangkaian sosial?

v. Adakah tanggapan keberkesanan tindak balas merupakan peramal bagi perubahan tingkah laku perlindungan data peribadi di kalangan pelajar dalam penggunaan perkhidmatan rangkaian sosial?

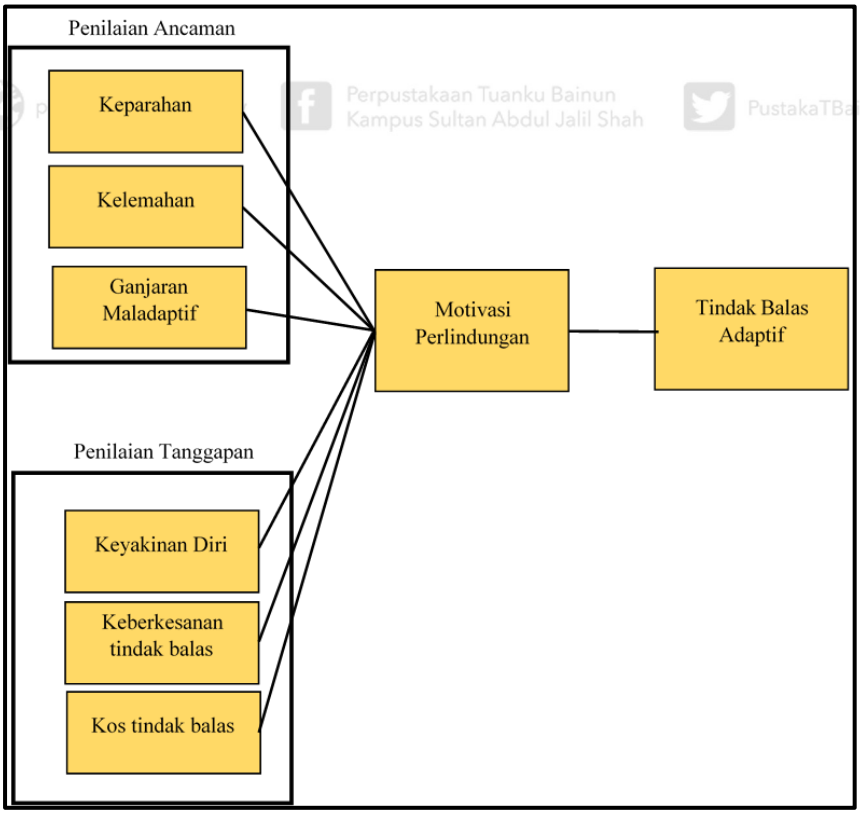
1.7 Hipotesis Kajian

Berdasarkan soalan kajian yang dibangunkan, berikut adalah hipotesis yang akan dinilai dalam kajian ini.

i. Ancaman keparahan merupakan peramal yang signifikan bagi perubahan tingkah laku perlindungan data peribadi di kalangan pelajar dalam penggunaan perkhidmatan rangkaian sosial.
ii. Ancaman kelemahan merupakan peramal yang signifikan bagi perubahan tingkah laku perlindungan data peribadi di kalangan pelajar dalam penggunaan perkhidmatan rangkaian sosial.
iii. Ancaman ganjaran maladaptif merupakan peramal yang signifikan bagi perubahan tingkah laku perlindungan data peribadi di kalangan pelajar dalam penggunaan perkhidmatan rangkaian sosial.
iv. Tanggapan keyakinan diri merupakan peramal yang signifikan bagi perubahan tingkah laku perlindungan data peribadi di kalangan pelajar dalam penggunaan perkhidmatan rangkaian sosial.
v. Tanggapan keberkesanan tindak balas merupakan peramal yang signifikan bagi perubahan tingkah laku perlindungan data peribadi di kalangan pelajar dalam penggunaan perkhidmatan rangkaian sosial.

1.8 Kerangka Teori

Kajian ini menggunakan Teori Motivasi Perlindungan (TMP) yang dibangunkan oleh R. W. Rogers pada tahun 1975 (Herath & Rao, 2009) bagi mendapatkan kefahaman mendalam berkaitan perubahan tingkah laku dan sikap seseorang apabila berhadapan dengan situasi yang terancam. Kebiasaannya, teori ini digunakan untuk memujuk para pengguna agar mengikut nasihat atau cadangan yang positif dengan menggunakan ketakutan dan ancaman. Penggunaan TMP juga berpotensi dalam meramalkan niat seseorang individu selepas menerima sesuatu perkara yang menakutkan yang akan membawa kepada tindak balas yang positif atau tingkah laku yang di ingini. Rajah 1.1 menunjukkan Teori Motivasi Perlindungan.

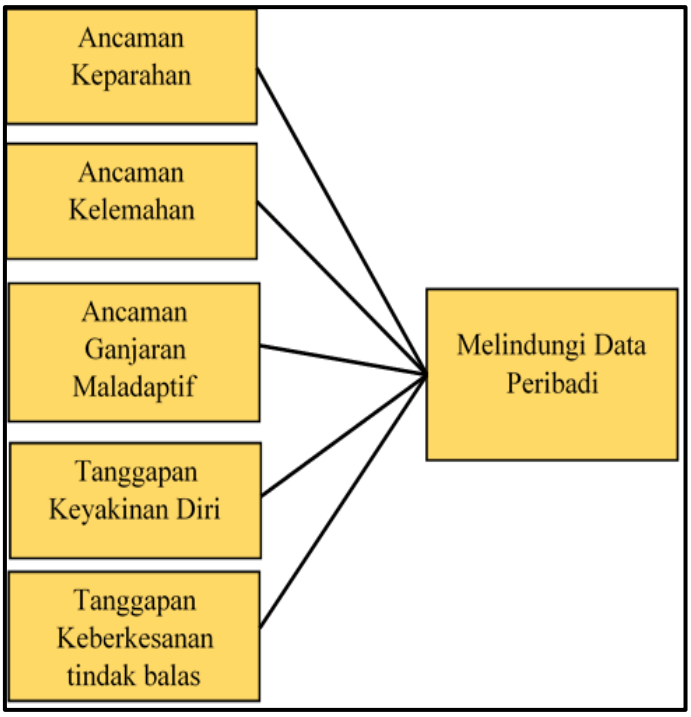


Rajah 1.1. Kerangka Teori. Sumber daripada Boss et al., 2015

1.9 Kerangka Konseptual

Kerangka konseptual bagi kajian ini dibina berdasarkan Teori Motivasi Perlindungan yang diubahsuai berdasarkan objektif kajian yang telah ditetapkan. Fokus kajian ini adalah untuk mendapatkan kefahaman yang mendalam berkaitan faktor yang dapat mengubah tingkah laku pelajar terhadap perlindungan data peribadi dalam penggunaan perkhidmatan rangkaian sosial.

Pemboleh ubah perantara iaitu motivasi perlindungan tidak diambil kira dalam kajian ini. Ini disebabkan oleh hubungan yang tidak jelas di antara niat dan proses kognitif yang terdapat dalam teori tersebut (Gurung et al., 2009). Selain itu, terdapat kajian lepas mendapati bahawa niat mempunyai hubungan terus dengan tingkah laku selari dengan teori harapan yang lebih fokuskan hasil iaitu tingkah laku (Gurung et al., 2009; Maddux & Rogers, 1983; Woon et al., 2005)



Rajah 1.2. Kerangka Konseptual

Kajian ini hanya tertumpu kepada lima daripada enam pemboleh ubah yang telah dinyatakan dalam teori tersebut iaitu keparahan yang dirasakan, kelemahan yang dirasakan, ganjaran maladaptif, keyakinan diri dan keberkesanan tindak balas. Pemboleh ubah kos tindak balas tidak diambil kira dalam kajian ini kerana tiada sebarang kos yang diperlukan dalam menggunakan sebarang aplikasi perkhidmatan rangkaian sosial yang dimuat turun daripada Android market seperti *Google Play* atau *Apple Apps Store* (Businge et al., 2019). Kerangka konseptual ditunjukkan dalam Rajah 1.2.

1.10 Kepentingan Kajian

Kekurangan kajian-kajian lepas terhadap tingkah laku keselamatan siber dalam melindungi data peribadi pelajar menyebabkan kajian ini amat penting dijalankan. Selain itu, kajian ini juga memberi impak positif secara praktikal mahupun teori. Ini dijelaskan seperti berikut:

A. Praktikal

Pembangunan pendidikan dan latihan keselamatan siber di negara ini dapat dipertingkatkan melalui kajian hasil dapatan ini. Cadangan yang diperolehi daripada kajian ini dapat digunakan dalam membangunkan pendidikan keselamatan siber yang berkesan dan memberi impak positif terhadap pelajar agar dapat melindungi data peribadi mereka di alam siber.

Fokus pendidikan keselamatan siber bukan hanya daripada segi pengetahuan malah kesedaran yang berterusan perlu diberikan supaya pelajar sentiasa berjaga-jaga dalam mendedahkan data peribadi mereka di media sosial. Selain itu, ketakutan yang diberikan akan memberi impak yang positif kepada tingkah laku mereka sekaligus dapat membantu pihak kerajaan dalam mengurangkan kadar mangsa jenayah siber yang semakin meningkat dewasa ini.

Dengan dapatan kajian ini juga dapat membantu pihak kerajaan khususnya Kementerian Pendidikan Malaysia dalam merangka atau menambah baik pendidikan keselamatan siber di kalangan pelajar khususnya dalam melindungi data peribadi seterusnya insiden jenayah siber melibatkan penyalahgunaan data peribadi dapat dikurangkan.

B. Teori

Penggunaan teori Teori Motivasi Perlindungan (TMP) dalam kajian ini dapat diperkasakan dalam pelbagai bidang. Pada asalnya, TMP digunakan hanya bidang psikologi kesihatan sahaja dimana dengan menggunakan ketakutan seseorang individu dapat memotivasikan tingkah laku yang betul. Justeru itu, penggunaan TMP dalam kajian ini dapat menyumbang ke arah pengukuhan teori ini bukan sahaja bidang kesihatan malah teori ini dapat digunakan dalam pelbagai bidang khususnya pendidikan keselamatan siber untuk melindungi data peribadi pelajar.

Kerangka konseptual yang dibangunkan dalam kajian ini berdasarkan TMP memperlihatkan hubungan terus antara penilaian proses kognitif terhadap tingkah laku seseorang individu. Hubungan ini memberikan impak positif terhadap pengembangan teori ini dan menguatkan lagi kebolehgunaan teori ini dalam bidang keselamatan siber.

Penggunaan Teori Tingkah Laku Terancang dan Teori Tindakan Beralasan yang seringkali digunakan oleh kebanyakan penyelidik dalam mengkaji tingkah laku manusia berdasarkan kepercayaan (Gurung et al., 2009). Walau bagaimanapun, kajian ini memberi perspektif baru dalam mengkaji tingkah laku berdasarkan ketakutan yang diberikan kepada seseorang.

1.11 Skop dan Batasan Kajian

Skop kajian ini memberi tumpuan terhadap konsep utama dan metodologi kajian yang digunakan. Secara umumnya, kajian ini melihat daripada segi hubungan secara terus antara penilaian ancaman dan penilaian tanggapan terhadap tingkah laku perlindungan data peribadi dalam penggunaan perkhidmatan rangkaian sosial di kalangan pelajar Teknologi Sistem Komputer dan Rangkaian Kolej Vokasional.

Dalam konteks ini, tumpuan diberikan kepada perlindungan data peribadi disebabkan oleh peningkatan insiden pencerobohan data peribadi di peringkat antarabangsa mahupun kebangsaan (CyberSecurity Malaysia, 2019; Forum Ekonomi Dunia, 2019; Gemalto, 2019; Dobberstein et al., 2018).

Selain iu, pendedahan diri pelajar di alam maya terutamanya dalam penggunaan perkhidmatan rangkaian sosial mengakibatkan kehilangan privasi (Gogus & Saygın, 2019) dan membuka ruang untuk menjadi mangsa jenayah siber seperti penipuan dan buli siber (Chen et al., 2019; Fansher & Randa, 2019) .

Daripada segi batasan kajian pula, kajian ini memfokuskan kepada pelajar semester 5 program Teknologi Sistem Komputer dan Rangkaian yang telah mengambil kursus Keselamatan Rangkaian di Kolej Vokasional seluruh Malaysia. Hal ini kerana, pelajar –pelajar tersebut telah mempunyai pengetahuan yang mendalam dan sentiasa terdedah dengan isu-isu berkaitan keselamatan siber berbanding dengan pelajar-pelajar program dan sekolah yang lain (Demirbilek & Talan, 2018; van Schaik et al., 2017).

Di samping itu, golongan pelajar ini juga merupakan pengguna internet terbesar di Malaysia berbanding golongan lain (Suruhanjaya Komunikasi dan Multimedia Malaysia, 2018) dimana mereka seringkali menjadi mangsa jenayah siber seperti penipuan, pemalsuan identiti, dan buli siber (MyCERT, 2018).

1.12 Definisi Operasional

Definisi operasional bertujuan menjelaskan definasi bagi setiap pemboleh ubah yang digunakan dalam kajian ini. Pemboleh ubah yang digunakan dalam kajian ini diterangkan secara mendalam seperti berikut:

1.12.1 Ancaman Keparahan

Ancaman keparahan merujuk kepada penilaian seseorang terhadap kesan keparahan yang berpunca daripada peristiwa keselamatan yang mengancam (Mohamed & Ahmad, 2012; Zhang et al., 2018). Menurut Yoon, Hwang, dan Kim (2012), ancaman keparahan didefinasikan sebagai ketakutan individu terhadap kepentingan sesuatu ancaman. Dalam konteks kajian ini, ancaman keparahan merujuk kepada penilaian seseorang individu terhadap kesan daripada pencerobohan data peribadi melalui perkhidmatan rangkaian sosial.

1.12.2 Ancaman Kelemahan

Ancaman kelemahan berkait dengan persepsi seseorang individu yang mengalami kesan negatif berpunca daripada tingkah laku yang berisiko (Sedek et al., 2018). Terdapat beberapa penyelidik (Adhikari & Panda, 2018; Mohamed & Ahmad, 2012) yang mendefinasikan ancaman kelemahan sebagai darjah kepercayaan seseorang individu terhadap ancaman yang akan berlaku kepada mereka. Berdasarkan definasi diatas, kajian ini mentakrifkan ancaman kelemahan sebagai kepercayaan seseorang individu terhadap ancaman keselamatan seperti penyalahgunaan maklumat peribadi dan penipuan yang berlaku dalam perkhidmatan rangkaian sosial.

1.12.3 Ancaman Ganjaran Maladaptif

Faedah atau ganjaran yang akan diperoleh daripada pilihan tingkah laku dikenali sebagai ganjaran maladaptif (Adhikari & Panda, 2018; Mohamed & Ahmad, 2012). Dengan kata lain, seseorang individu berpotensi untuk melindungi data peribadi mereka atau tidak bergantung kepada ganjaran atau faedah yang akan diperolehi. Konteks kajian ini mendefinasikan ancaman ganjaran maladaptif ini sebagai ganjaran atau faedah yang akan diperolehi dengan mendedahkan maklumat peribadi dalam perkhidmatan rangkaian sosial seperti mendapat kenalan baru, diskaun yang diperoleh terhadap barangan dalam talian dan penyertaan dalam permainan atas talian.

1.12.4 Tanggapan Keyakinan Diri

Menurut Yoon et al. (2012), tanggapan keyakinan diri merujuk kepada keupayaan seseorang individu dalam melaksanakan tingkah laku yang dicadangkan manakala Posey, Roberts, dan Lowry (2015) berpendapat bahawa tanggapan keyakinan diri merupakan kepercayaan seseorang individu terhadap diri dalam melaksanakan tingkah laku yang dicadangkan. Kesimpulan yang boleh dibuat berdasarkan kedua-dua pendapat bahawa tanggapan keyakinan diri didefinasikan sebagai kepercayaan terhadap diri dan keupayaan seseorang individu melindungi data peribadi mereka dalam perkhidmatan rangkaian sosial.

1.12.5 Tanggapan Keberkesanan Tindak Balas

Tanggapan keberkesanan tindak balas didefinasikan sebagai kepercayaan dan keyakinan seseorang individu bertindak balas terhadap cadangan dan saranan yang diberikan (Adhikari & Panda, 2018; Yoon et al., 2012). Bagi konteks kajian ini, tanggapan keberkesanan diri ditakrifkan sebagai kemampuan dan keyakinan seseorang individu menggunakan tetapan privasi dalam perkhidmatan rangkaian sosial bagi melindungi data peribadi mereka.

1.12.6 Perlindungan Data Peribadi

Perlindungan data peribadi merujuk kepada prosedur untuk melindungi data atau maklumat seseorang individu terhadap pencerobohan data (Ciriani et al., 2007). Menurut Akta Perlindungan Data Peribadi 2010 (Parlimen Malaysia, 2010), perlindungan data peribadi bermaksud pematuhan terhadap prinsip perlindungan data peribadi yang merangkumi prinsip am, notis dan pilihan, penzahiran, keselamatan, penyimpanan, integriti data dan akses. Kajian ini menfokuskan kemampuan seseorang individu atau pengguna dalam melindungi data peribadi daripada ancaman keselamatan dalam perkhidmatan rangkaian sosial.

1.13 Rumusan dan Pengorganisasian Kajian

Terdapat lima bab dalam kajian ini dimana bab pertama telah membincangkan berkaitan latar belakang masalah, penyataan masalah objektif kajian, persoalan kajian, kerangka teori, kepentingan kajian, skop dan batasan kajian serta definasi operasional yang digunakan dalam kajian ini.

Bab kedua akan meninjau literatur berkaitan perkembangan internet, media sosial, perkhidmatan rangkaian sosial, konsep perlindungan data peribadi dan hubungan, teori serta pemboleh ubah yang digunakan dalam kajian ini dalam menentukan pengaruh motivasi terhadap perlindungan data peribadi.

Bab tiga menerangkan metodologi kajian yang merangkumi reka bentuk kajian, populasi dan sampel, instrumen yang digunakan, kesahan instrumen, kebolehpercayaan instrumen, kajian rintis, prosedur pengumpulan data dan kaedah menganalisis data yang telah diperolehi.

Seterusnya, bab empat menerangkan analisis yang telah dilakukan setelah proses pengumpulan data selesai dijalankan. Selain itu, perbincangan terhadap data yang telah diperolehi diterangkan dengan lanjut dalam bab ini.

Akhir sekali, bab lima menerangkan kesimpulan yang akan dilakukan berdasarkan hasil dapatan dan perbincangan. Setelah itu, penyelidik akan mengemukakan cadangan kajian yang dapat dilakukan pada masa akan datang.