BAB I

PENDAHULUAN

1.1 Latar Belakang

Di era digital dewasa ini, masyarakat banyak diberikan berbagai informasi yang beraneka macam melalui teknologi yang semakin canggih. Contohnya dalam kemajuan teknologi informasi terutama pada bidang komputer dan internet. Teknologi informasi ini melibatkan beraneka macam jenis komputer dengan tipologi jaringan yang belum pernah diduga sebelumnya dalam perkembangan sejarah internet.

Di Indonesia sendiri teknologi dan informasi baru berkembang dengan pesat pada tahun 1994 berbeda dengan negara maju yang sudah lebih dahulu memiliki perkembangan internet dan teknologi (Nurhadrayani dkk., 2017). Generasi digital immigrants secara natural memiliki kesulitan dalam mempelajari teknologi dan menganggap teknologi merupakan penemuan terbaru yang sulit diterima (Apidana dkk., 2020). masyarakat Indonesia yang terlahir sampai dengan sebelum tahun 1994 karena generasi ini tidak terbiasa menggunakan teknologi dan merupakan generasi yang memiliki risiko tinggi terkena penipuan.

Saat ini, yang terhubung dengan internet bukan hanya komputer, melainkan juga *netbook* dan *smartphone* (Sugeng 2020:1) Istilah telematika diartikan sebagai telekomunikasi dan informatika *(telecommunication and informatics)* yang merupakan perpaduan antara computer *(computing)* dan komunikasi *(communication)* (Maskun 2022:1). Internet dan teknologi juga berperan penting dalam menjawab kebutuhan- kebutuhan manusia dan

memberikan dampak positif dalam kehidupan manusia, namun teknologi dan internet tersebut tidak hanya memberikan keuntungan saja melainkan juga dampak negatif, contohnya kejahatan siber (Budiastanti, 2017).

Kejahatan siber atau dikenal juga sebagai *Cyber crime* merupakan sebuah bentuk kejahatan berbasis komputer dengan tujuan kriminal seperti menghancurkan reputasi korban dan dapat menimbulkan kerugian dalam bentuk fisik maupun mental secara langsung atau tidak langsung (Andriani, 2023). Teknologi dan informasi semakin berkembang pesat dan mempermudah aspek - aspek kehidupan manusia saat ini. Keberadaan teknologi komunikasi yang ada, menjadikan manusia sebagai pribadi yang berpikir instan dan menemukan berbagai kemudahan tanpa memerlukan banyak waktu seperti dahulu (Marpaung, 2018).

Kemajuan teknologi informasi dan komunikasi (TIK) dalam beberapa tahun terakhir telah mengubah lanskap komunikasi dan interaksi manusia secara drastis. Salah satu platform yang paling populer digunakan oleh masyarakat untuk berkomunikasi adalah *Whatsapp. Whatsapp* memungkinkan pengguna untuk saling bertukar pesan teks, suara, dokumen, dan gambar secara mudah dan cepat. Namun, bersamaan dengan manfaatnya, teknologi ini juga membawa potensi risiko yang signifikan yaitu risiko keamanan siber. Sebagian pengguna *Whatsapp* yang memiliki kurangnya pemahaman akan teknologi lebih mendalam hanya mengetahui cara dasar penggunaan *Whatsapp* saja, seperti mengirim pesan, melakukan panggilan telepon, dan membagi konten media lain seperti gambar maupun video. Kurangnya pemahaman akan teknologi ini dapat memicu munculnya sejumlah resiko (Alaby:2020).

Di Indonesia, kejahatan siber diatur dalam Undang - Undang Nomor 19 Tahun 2016 yang merupakan revisi dari Undang - Undang no 19 tahun 2016 tentang Perubahan Atas Undang - Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik. Berbagai cara dapat dilakukan untuk pembuktian di pengadilan dan penyidikan oleh pihak kepolisian dalam kejahatan siber, antara lain dengan mengoptimalkan Undang - Undang tersebut, mengembangkan pengetahuan dan kemampuan penyidik di dunia siber, serta menambah dan meningkatkan fasilitas forensik komputer di Kepolisian Republik Indonesia.

Kejahatan tindak pidana dunia maya *(Cyber crime)* setiap tahunnya mengalami peningkatan yang sangat pesat, hal ini dikarenakan semakin berkembangnya teknologi komputer yang berdampak pada kehidupan manusia. Segala kemudahan yang didapat dari teknologi komputer pada kenyataannya tidak hanya berdampak baik bagi kehidupan manusia karena beberapa diantaranya ternyata juga ikut memberikan dampak yang buruk (Widodo:2011)

Phishing yang merupakan salah satu bentuk kejahatan siber yang melibatkan penipuan terhadap individu untuk memberikan informasi pribadi, seperti kredensial login atau nomor kartu kredit, dengan menyamar sebagai entitas yang dapat dipercaya. Meningkatnya teknologi digital telah membuat serangan phishing menjadi lebih canggih dan lebih sulit dideteksi, yang mengarah pada meningkatnya kebutuhan akan strategi penegakan hukum yang efektif untuk memerangi jenis kejahatan siber ini.

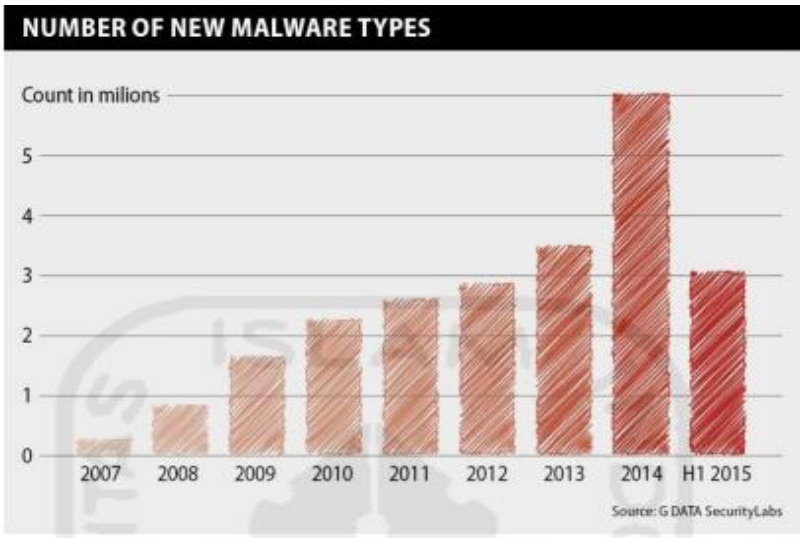
Banyak orang yang memanfaatkan teknologi komputer sebagai media untuk melakukan tindak kejahatan yang bertentangan dengan hukum. Beragam tujuan yang dimiliki para pelaku ini beberapa diantaranya adalah untuk mencari keuntungan. Banyak cara yang dilakukan untuk mempermudah kegiatan kejahatan yang melibatkan teknologi komputer ini salah satunya adalah memanfaatkan kelemahan sistem jaringan komputer dengan menyusupkan program yang digunakan sebagai media untuk mencuri informasi dari sebuah sistem perangkat elektronik seperti smartphone, dan juga tablet. program ini disebut sebagai *Mobile Malware.* (Mathur.2013:1)

Malware merupakan (singkatan dari istilah Bahasa Inggris malicious software, yang berarti perangkat lunak yang mencurigakan) yang menginveksi telpon pintar atau smartphone adalah program komputer yang diciptakan dengan maksud dan tujuan tertentu dari penciptanya dan merupakan program yang mencari kelemahan dari software. Umumnya *Mobile Malware* diciptakan untuk membobol atau merusak suatu software atau sistem operasi melalui *script* yang disisipkan secara tersembunyi oleh pembuatnya (EduCSIRT, 2019:1)

Mobile Malware didefinisikan sebagai perangkat lunak jahat, program komputer jahat, atau perangkat lunak jahat, seperti virus. Virus komputer bekerja dengan cara menempel pada suatu file perangkat elektronik yang menargetkan perangkat seluler seperti ponsel cerdas, dan tablet. *Malware* biasanya berupa *file executable*, (file yang berisi sebuah program yang dapat dieksekusi atau dijalankan sebagai program pada sistem Komputer) bekerja dengan cara melakukan *social engineering files* berbahaya dengan

menampilkannya seperti *file* yang terlihat tidak berbahaya, *Mobile Malware* seluler dapat memiliki banyak tujuan (Bhudisantosa:2014), seperti mencuri data, mendaftarkan pengguna ke layanan transaksi dan menagih mereka untuk layanan yang tidak mereka setujui, atau mengunci perangkat atau data dan meminta uang untuk peluncurannya (Meserve:2023:1).

Menurut data yang dirilis oleh *G Data Security Labs* pada tahun 2015, terdapat 3,045,722 varian *Malware* baru. Program-program berbahaya ini memiliki ancaman keamanan yang dapat berdampak pada kerugian seperti pencurian informasi.



Gambar 1.2 New Varian *Malware* (G Data, 2015)

Mobile Malware terdiri dari perangkat lunak yang disisipi kode untuk mendapatkan informasi penting dari pengguna seperti akun bank, password, dan informasi lainnya yang diinginkan oleh pembuatnya. Penyebaran *Mobile Malware* telah menjadi ancaman serius dalam lingkungan digital, dan penjahat siber semakin canggih dalam menciptakan metode untuk mengeksploitasi celah keamanan dalam platform sosial, salahsatunya adalah *Whatsapp*. Salah

satu modus penyebaran *Mobile Malware* yang semakin umum adalah melalui modus file undangan palsu.

Cyber crime adalah kumpulan alat, kebijakan, keamanan konsep, upaya perlindungan keamanan, pedoman, pendekatan manajemen risiko, tindakan, pelatihan, praktik terbaik, jaminan dan teknologi yang dapat digunakan untuk melindungi dunia maya lingkungan dan organisasi serta aset pengguna (Kshetri, 2013). Cara kerja dari modus *Cyber crime* ini adalah pelaku mengirimkan dokumen *Malware* dengan format undangan pernikahan melalui aplikasi *Whatsapp* yang Jika file tersebut diklik akan meminta akses untuk melakukan aktivitas Baca SMS atau MMS. Jika sudah di klik maka akan otomatis mengizinkan akses dalam ponsel korban, ponsel yang sudah diizinkan maka pesan yang tersimpan di HP atau kartu SIM akan dapat dibaca oleh Pelaku jahat.

Ketika seluruh permintaan tersebut diberikan maka program tersebut sudah terpasang di ponsel korban aktor jahat memiliki kemungkinan untuk mengakses riwayat informasi SMS-*Banking* seperti kode pin dari riwayat SMS yang biasanya tidak dihapus oleh korban. Berbekal informasi tersebut aktor jahat dapat melakukan pengiriman uang dari rekening korban. Kasus seperti ini banyak terjadi di kota kota bersar salah satu korbannya adalah Silvia (52), pengusaha aksesori kendaraan asal Lawang, Kabupaten Malang, Jawa Timur, kehilangan uang tabungan Rp 1,4 miliar di rekeningnya usai membuka dokumen undangan nikah palsu yang dikirim via *Whatsapp* (Kompas:2023:1).

Hilmy F. Ali, kuasa hukum korban, menjelaskan dokumen undangan nikah palsu itu berisi file aplikasi APK (*Aplication Package*) berukuran 5 MB

dan dikirim ke korban via *Whatsapp* oleh nomor tak dikenal pada Rabu, 24 Mei 2023, pukul 10.00 WIB. Setelah link undangan nikah palsu berisi file aplikasi APK penipuan dibuka, uang tabungan korban di bank terkuras Rp 1,4 miliar. Uang tabungan tersebut raib dalam beberapa kali transaksi yang tidak diketahui korban. Hilmi menerangkan, saat korban membuka *File* undangan nikah itu, yang muncul ternyata bukan undangan nikah sebagaimana mestinya, melainkan gambar seperti brosur iklan. Setelah dibuka, korban pun memblokir nomor pengirimnya. Pada Rabu, 24 Mei 2023, pukul 21.00 WIB, korban dijelaskan menerima pemberitahuan bahwa terdapat upaya ilegal untuk mengakses e-mailnya.

Dari pemberitahuan itu, korban kemudian memindahkan data ke ponsel lain dan mengganti *password* e-mailnya. Aksi pengurasan rekening terjadi setelah itu. Pada Rabu, 25 Mei 2023, pukul 21.00 WIB, Hilmi mengatakan terdapat aktivitas transfer dana dari dua rekening milik korban ke tiga nomor rekening tak dikenal. Selain itu, ada juga transaksi aneh tak dikenal via m-Banking layanan perbankan, lalu beberapa transfer dana ke QRIS, dan beberapa aktivitas pembelian pulsa ke sebuah nomor ponsel yang tak dikenal.

Kehadiran Undang - Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik dalam pemanfaatan Teknologi Informasi, media, dan teknologi komunikasi telah mengubah perilaku masyarakat dan peradaban manusia, khususnya di Indonesia. Perkembangan teknologi informasi dan komunikasi juga menyebabkan dunia menjadi tanpa batas (*borderless*) dan menyebabkan perubahan sosial, ekonomi, dan budaya yang signifikan berlangsung begitu cepat. Teknologi Informasi saat ini menjadi pedang

bermata dua karena selain memberikan kontribusi bagi peningkatan kesejahteraan, kemajuan dan peningkatan kesejahteraan, juga menjadi sarana yang efektif untuk melakukan perbuatan melawan hukum.

Penelitian *Malware* masih berfokus pada analisis perilaku hal ini dibuktikan dengan seringnya analisis *Malware* dilakukan menggunakan teknik *signature based*, teknik ini digunakan untuk melakukan analisis berbasis pada *data base* perilaku *Malware*, akan tetapi dalam beberapa penelitian seperti yang dilakukan oleh (Chiang 2016) dan (Jasiul, Szpyrka, and Sliwa 2014) yang menjelaskan bahwa tingkat keberhasilan metode yang diterapkan untuk mendeteksi *Malware* tergantung pada keadaan model *Malware* tersebut. Penggunaan teknik *signature based* sangat tergantung pada perilaku *Malware* yang dianalisis. Analisis menjadi sulit ketika *Malware* yang dianalisis merupakan *Malware* baru yang menggunakan teknik kebingungan (*obfuscation*) dan kompresi (*packing*).

Saat ini indonesia mempunyai aturan hukum khsusu yang dikenal dengan hukum siber atau hukum telematika. Secara detail isi pasal tersebut yang menerangkan tentang perbuatan yang dianggap melawan hukum. menurut Undang - Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang - Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik berupa penipuan situs. Undang - Undang ini dapat dipandang sebagai langkah awal pemerintah dalam menangani *Cyber crime*. Kejahatan phising tidak bisa disamakan dengan penipuan biasa, karenaaksi *Phising* (Penipuan) memanfaatkan kemajuan sistem teknologi.

Kebutuhan akan perlindungan hukum bagi pengguna internet dalam era digital semakin meningkat, namun masih terdapat kelemahan dalam sistem hukum yang ada saat ini. Undang- Undang Informasi dan Transaksi Elektronik (*Electronic Information and Transactions Law*) belum mampu menjangkau seluruh aspek kejahatan siber dan belum memberikan perlindungan yang memadai bagi korban.

Pada saat ini Indonesia dalam menangani hukum siber mengacu pada ketentuan Undang - Undang no 19 tahun 2016 tentang Perubahan Atas Undang - Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik (UU ITE) mengatur beberapa ketentuan yang berkaitan dengan kegiatan phising atau penipuan online, Pasal 26 UU ITE yang menyebutkan bahwasannya;

> Melarang setiap orang untuk mengakses sistem elektronik milik orang lain tanpa hak atau melawan hukum. Dalam konteks kejahatan phishing, pelaku yang melakukan akses tanpa izin atau dengan cara memalsukan identitas untuk memperoleh data pribadi korban, telah melakukan pelanggaran terhadap ketentuan ini.

Kemudian dalam pasal 30 UU ITE yang berbunyi;

> Melarang setiap orang untuk membuat atau menyebarkan informasi palsu dan menyesatkan yang dapat menimbulkan kerugian atau kehilangan bagi orang lain. Dalam konteks kejahatan phishing, pelaku yang membuat atau menyebarkan informasi palsu dan menyesatkan dengan tujuan untuk memperoleh data pribadi korban, telah melanggar ketentuan ini.

Serta Pasal 28 ayat (1) Undang - Undang Nomor 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik (UU ITE) melarang:

> “ Setiap Orang dengan sengaja, dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik ”

Para penipu dapat menggunakan *Mobile Malware* untuk menginfeksi perangkat ponsel dengan aplikasi palsu atau *Malware* yang dapat mencuri

informasi pribadi pengguna, termasuk data login atau informasi keuangan. Dalam skenario ini, penipu dapat mengirim pesan melalui *Whatsapp* dengan lampiran file undangan palsu yang sebenarnya adalah *Malware*. Ketika pengguna membuka file tersebut, perangkatnya bisa terinfeksi *Malware* yang memungkinkan penipu untuk mengakses data pribadi atau bahkan mengendalikan perangkat pengguna.

Sebagaimana diberitakan Tribun Jatim, total transaksi yang tak dikenal mencapai Rp1,4 miliar. Terkurasnya rekening itu melalui belasan kali transaksi sejak pukul 22.00 WIB hingga 03.00 WIB. Setelah korban memeriksa rekening, ternyata tabungannya hanya tersisa Rp 2 juta. Transaksi tak dikenal yang menguras tabungan Rp 1,4 miliar itu dijalankan aplikasi mobile banking. Namun, anehnya, korban mengaku tidak pernah mengunduh aplikasi mobile banking di ponsel miliknya. Saat dicek di aplikasi, nomor telepon yang digunakan untuk mendaftar mobile banking juga bukan milik dan tak dikenali korban. Hilmi menduga penipu mendaftar dengan nomornya sendiri yang bukan milik korban, setelah memiliki akses ke rekening korban. Saat ini, korban dan kuasa hukumnya tengah melakukan upaya pengaduan ke kepolisian. (Tribunjatim:2022)

Pada Pasal 40 ayat (2) Undang undang Nomor 19 Tahun 2016 secara tegas menyatakan :

ayat 2	Pemerintah melindungi kepentingan umum dari segala jenis gangguan sebagai akibat penyalahgunaan Informasi Elektronik dan Transaksi Elektronik yang mengganggu ketertiban umum, sesuai dengan ketentuan peraturan perundangundangan.
ayat (2a)	Pemerintah wajib melakukan pencegahan penyebarluasan dan penggunaan Informasi Elektronik dan/atau Dokumen

Elektronik yang memiliki muatan yang dilarang sesuai dengan ketentuan peraturan perUndang - Undangan.

ayat (2b) Dalam melakukan pencegahan sebagaimana dimaksud pada ayat (2a), Pemerintah berwenang melakukan pemutusan akses dan/atau memerintahkan kepada Penyelenggara Sistem Elektronik untuk melakukan pemutusan akses terhadap Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar hukum.

Dari isi pasal tersebut sudah jelas menyatakan bahwa pemerintah wajib mengupayakan perlindunggan serta pencegahan terhadap kasus yang merugikan korban akbibat penyalahgunaan Informasi Elektronik dan Transaksi Elektronik yang mengganggu ketertiban umum yang dilakukan oleh pelaku dengan modus mengirimkan file *Mobile Malware* dengan modus undangan palsu pada aplikasi *Whatsapp*, tapi pada kenyataannya masih terjadi kesenjangan antara *das sollen* dan *das sein* dalam kasus ini sehingga undang - undang atau peraturan yang diharapkan bisa mengatur hal tersbut pada kenyataanya berbeda dengan yang terjadi dalam realita masyarakat.

Tidak bisa dipungkiri bahwa Kasus seperti ini tidak hanya terjadi di kota kota besar, namun juga terjadi di daerah daerah kecil seperti kabupaten buleleng, Buleleng merupakan salah satu kabupaten di provinsi Bali, Indonesia. Ibu kotanya adalah Singaraja. Buleleng berbatasan dengan Laut Jawa di sebelah utara, Selat Bali di sebelah barat, Kabupaten Karangasem di sebelah timur. Kabupaten Jembrana, Bangli, Tabanan serta Badung di sebelah selatan.

Tabel 1.1
Usia 5 Tahun keatas Penduduk bali yang mengakses TIK 2022

Kabupaten/Kota *Regency/ Municipality*	Jenis Aktivitas / *Type of Activity*		
	Menggunakan Telepon Seluler *Using Celluler Phone*	Menggunakan Komputer* *Using Computer*	Mengakses Internet** *Internet Access*
Jembrana	89,53	10,57	70,10
Tabanan	75,73	12,72	66,16
Badung	85,83	27,03	79,68
Gianyar	80,69	17,62	67,28
Klungkung	78,70	13,09	65,85
Bangli	75,09	13,01	62,66
Karangasem	75,32	5,66	54,08
Buleleng	83,57	7,83	59,91
Denpasar	91,32	20,84	84,51
Jumlah / *Total* :	**83,51**	**15,94**	**70,59**

Sumber: Badan Pusat Statistik Provinsi Bali 2022

Dilansir dari Badan Pustat Statistik Provinsi Bali, Persentase Penduduk Usia 5 Tahun ke Atas yang Mengakses Teknologi Informasi dan Komunikasi (TIK) dalam 3 Bulan Terakhir Menurut Kabupaten/Kota, tahun 2022, 83,57% masyarakat Buleleng telah menggunakan telepon seluler dan 59,91% telah mengakses internet. Salah satu cara penggunaan internet adalah bermedia sosial menggunakan *Whatsapp*. *Whatsapp* menjadi aplikasi pesan instan yang paling banyak digunakan di Indonesia. Pengguna internet di Indonesia ada 171 juta atau 64,4% menggunakan internet, di mana 83% dari 171 juta itu adalah pengguna *Whatsapp*. Direktur Kebijakan *Whatsapp* Asia Pasifik, Clair Deevy juga mengatakan bahwa pengguna di Indonesia jumlahnya terbesar di dunia (Kominfo, 2019:1).

Angka ini terbilang cukup besar untuk daerah kecil seperti kabupaten buleleng, dan sangat berpotensi menimbulkan kejahatan *cyber*, salahsatunya adalah penipuan dengan modus file undangan pada aplikasi *Whatsapp*. Kepala

Urusan Administrasi dan Ketatausahaan kepolisian resor buleleng Dewa Gede Agung Sugiharta menyebutkan bahwa belum ada laporan terkait kasus tersebut, yang ada hanya laporan terkait pembobolan rekening yang hanya diselesaikan dengan pembuatan surat kepada pihak bank untuk memblokir nomor ATM, Namun pada kenyataannya kasus telah terjadi di kabupaten buleleng yang membuat kasus ini menarik untuk diteliti.

Pada beberapa waktu lalu kasus ini telah terjadi kepada seorang mahasiswa undiksha, yang mengakibatkan akses ponsel dari mahasiswa tersebut sepenuhnya dikontrol oleh si pelaku. Pelaku tersebut mengirimkan file dokumen *Mobile Malware* dengan format undangan pernikahan dari *Whatsapp* korban yang sudah di kontrol penuh oleh pelaku untuk menjangkau lebih banyak korban. Namun tidak ada kerugian material dalam kasus karena korban telah menarik tunai dari rekening yang tersimpan dalam ponsel tersebut. Sayangnya korban masih enggan untuk melaporkan kejadian ini ke pihak berwajib dengan alasan yang belum diketahui pasti

Menyebarkan *Mobile Malware* dapat dianggap sebagai bentuk akses atau transmisi data yang tidak sah, yang dapat dihukum berdasarkan Undang - Undang Nomor 19 tahun 2016 tentang Informasi dan Transaksi Elektronik Tergantung pada sifat dan dampak *Mobile Malware*. *Mobile Malware* berpotensi masuk dalam ketentuan seperti penipuan, akses tidak sah, atau sabotase (Monappa:2018)., yang dapat dihukum berdasarkan KUHP Indonesia. Konsekuensi hukum dapat bervariasi tergantung pada beratnya pelanggaran, niat individu, dan faktor lainnya. Jika seseorang terbukti menyebarkan *Mobile Malware* menggunakan Modus penipuan file undangan di *Whatsapp* di

Indonesia, maka ia dapat dikenakan sanksi seperti denda, penjara, atau keduanya, tergantung pada ketentuan spesifik yang dilanggar.

Menurut KUHP, Adapun beberapa pasal yang berpotensi menjerat pelaku penipuan dengan *Mobile Malware*, antara lain.

1. Penipuan

   Penipuan diatur dalam Pasal 378 KUHP, dengan bunyi sebagai berikut.

   > " Barang siapa dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum dengan memakai nama palsu atau martabat palsu, dengan tipu muslihat, ataupun rangkaian kebohongan, menggerakkan orang lain untuk menyerahkan barang sesuatu kepadanya, atau supaya memberi hutang maupun menghapuskan piutang, diancam karena penipuan, dengan pidana penjara paling lama 4 tahun."

2. Penerobosan

   Jika pelaku menerobos atau menjebol suatu sistem elektronik tertentu, menggunakan identitas dan password korban dengan tanpa hak, ia dapat dijerat Pasal 30 ayat (3) jo. Pasal 46 ayat (3) UU ITE, sebagai berikut.

   > " Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apapun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan dipidana penjara paling lama 8 tahun dan/atau denda paling banyak Rp800 juta."

   Selain itu, jika *Mobile Malware* dirancang untuk mengumpulkan atau mengeksploitasi data pribadi tanpa izin, *Mobile Malware* tersebut dapat melanggar Peraturan Menteri (Permen) No 20 Tahun 2016 tentang Perlindungan Data Pribadi (PDP) di Indonesia yang mengatur pengumpulan, penggunaan, dan pengungkapan data pribadi. Menyebarkan *Mobile Malware* yang membahayakan data pribadi dapat dianggap sebagai pelanggaran terhadap Undang - Undang ini.

Kasus seperti ini mencerminkan ancaman nyata terhadap keamanan data pribadi dan privasi individu. Sumadi mengatakan bahwa “Dalam hal menangani kasus *Cyber crime* khususnya tindak pidana penipuan transaksi elektronik diperlukan spesialisasi aparat penyidik yang dapat dipertimbangkan sebagai salah satu cara untuk melaksanakan upaya penegakan hukum terhadap *Cyber crime* (Sumady:2015:199). Dalam era digital, data pribadi memiliki nilai yang sangat tinggi, dan tindakan seperti penyebaran *Mobile Malware* dapat mengakibatkan kerugian finansial dan pelanggaran privasi yang serius (M.yang:2017). Oleh karena itu, perlindungan data dan pemahaman tentang hukum siber menjadi semakin penting.

Oleh karena itu, sangat penting untuk dikaji atau ditelaah lebih lanjut terkait dengan penipuan dengan modus file undangan palsu pada aplikasi *Whatsapp* di kabupaten buleleng , seperti penanganan secara hukum, sosialisasi, dan peningkatan sumber daya, Sehingga diperlukan adanya suatu penelitian dengan judul “**Implementasi Undang - Undang ITE No 19 Tahun 2016 Terkait Penipuan Menggunakan *Mobile Malware* Pada Aplikasi *Whatsapp* Di Kabupaten Buleleng**”.

1.2 Identifikasi Masalah

Berdasarkan latar belakang yang telah diuraikan diatas, maka terdapat identifikasi masalah yang akan dijadikan bahan penelitian sebagai berikut.

1. Penipuan menggunakan *Mobile Malware* terjadi di kabupaten buleleng karena kurangnya edukasi dan sosialisasi terhadap aktivitas dunia maya yang membuat para korban tidak waspada terhadap kejahatan modus baru yang ada di ponsel pintar atau gadget.

2. Penegakan hukum terhadap penipuan menggunakan *Mobile Malware* belum dapat ditangani secara tuntas oleh aparat penegak hukum di wilayah hukum kabupaten buleleng.
3. Rendahnya keamanan aplikasi *Whatsapp* untuk mendeteksi aktivitas – aktivitas berbahaya termasuk mengirimkan *Mobile Malware* dalam bentuk undangan palsu sebagai modus penipuan baru di sosial media

1.3 Pembatasan Masalah

Dalam suatu permasalahan adanya suatu pembatasan berfungsi untuk mengarahkan suatu permasalahan tersebut menjadi lebih terstruktur dan tidak menyimpang dari pokok permasalahan itu sendiri. Maka dari itu dalam penelitian ini, permasalahan yang dilihat memiliki urgensi yaitu mengenai implementasi Undang - Undang ITE no 19 tahun 2016 terkait penipuan menggunakan *Mobile Malware* pada aplikasi *Whatsapp* di kabupaten buleleng. Penyajiannya dikaji berdasarkan data dan fakta yang diperoleh di lapangan serta dihimpun dari berbagai media berita, artikel, maupun jurnal terkait. Adapun uraian pembatasan masalah bahasan ini yaitu Penegakan hukum penipuan menggunakan *Mobile Malware* pada aplikasi *Whatsapp* di kabupaten buleleng dan hambatan dalam pelaksanaan implementasi Undang - Undang ITE no 19 tahun 2016 terkait penipuan menggunakan *Mobile Malware* pada aplikasi *Whatsapp* di kabupaten buleleng.

1.4 Rumusan Masalah

Setelah menguraikan pembatasan masalah, maka dalam penelitian ini dapat dirumuskan dua rumusan masalah yang hendak dijawab dalam penelitian ini, yaitu:

1. Bagaimana Peran Kepolisian Resor Buleleng dalam Penegakan Hukum Terhadap Kasus Penipuan dengan Modus File Undangan Palsu Pada Aplikasi *Whatsapp*?
2. Apa saja kendala dan hambatan yang dihadapi kepolisianpada pelaksanaan penegakan hukum terhadap pelaku ?

1.5 Tujuan Penelitian

Berdasarkan rumusan masalah tersebut, tujuan penelitian ini dapat dibedakan menjadi tujuan umum dan tujuan khusus, yakni sebagai berikut.

1. **Tujuan Umum**

   Dalam penelitian ini yang menjadi tujuan umum penelitian adalah untuk mengetahui dan menganalisa tentang Implementasi Undang - Undang ITE no 19 tahun 2016 terkait penipuan menggunakan *Mobile Malware* pada aplikasi *Whatsapp* di kabupaten buleleng.

2. **Tujuan Khusus**

   a) Untuk mengetahui implementasi Undang - Undang ITE no 19 tahun 2016 terkait penipuan menggunakan *Mobile Malware* pada aplikasi *Whatsapp* di kabupaten buleleng.

   b) Untuk mengkaji dan menganalisis hambatan dalam implementasi Undang - Undang ITE no 19 tahun 2016 terkait penipuan menggunakan *Mobile Malware* pada aplikasi *Whatsapp* di kabupaten buleleng.

1.6 Manfaat Penelitian

Dari hasil penelitian ini diharapkan dapat berguna baik secara teoritis maupun praktis. Adapun manfaat yang diharapkan dari penelitian ini yakni sebagai berikut.

1. Manfaat Teoritis

Hasil penelitian ini diharapkan dapat memberikan manfaat, baik dalam aspek ilmiahnya maupun dalam implementasi Undang - Undang ITE no 19 tahun 2016 terkait penipuan menggunakan *Mobile Malware* pada aplikasi *Whatsapp* di kabupaten buleleng.

2. Manfaat Praktis

a) Bagi Penulis

Menambah wawasan di bidang ilmu hukum khususnya mengenai implementasi Undang - Undang ITE no 19 tahun 2016 terkait penipuan menggunakan *Mobile Malware* pada aplikasi *Whatsapp* di kabupaten buleleng.

b) Bagi Masyarakat

Menambah pemahaman dan memperluas wawasan bagi masyarakat mengenai implementasi Undang - Undang ITE no 19 tahun 2016 terkait penipuan menggunakan *Mobile Malware* pada aplikasi *Whatsapp* di kabupaten buleleng.

c) Bagi Pemerintah dan Aparat Penegak Hukum

Diharapkan dapat memberikan sumbangsih pemikiran serta evaluasi untuk aparat penegak hukum dalam penegakan hukum terhadap kejahatan modus baru khususnya *Cyber crime* di Kabupaten Buleleng.

d) Bagi Peneliti Sejenis

Sebagai sumbangsih pikiran dalam pelaksanaan penelitian sejenis serta sebagai bacaan baru bagi peneliti ilmu hukum