BAB I

PENDAHULUAN

1.1. Latar Belakang

Perkembangan teknologi informasi yang makin pesat seiring berjalannya waktu membuat teknologi dan informasi menjadi hal yang sentral dalam masyarakat. Dalam hal ini juga menjadi kebutuhan pokok bagi masyarakat untuk meningkatkan produktivitas keseharian mereka dengan akses yang cepat dalam memperoleh informasi, yang membuat kemajuan teknologi informasi dan komunikasi menjadi pengubah pola hidup masyarakat dan memicu terjadinya perubahan sosial, budaya, ekonomi, pertahanan, keamanan, dan penegakan hukum.

Kepolisian Negara Republik Indonesia atau yang sering disingkat Polri mengemban tugas yang luas diantaranya keamanan dan ketertiban masyarakat, penegakan hukum, perlindungan, pengayoman, dan pelayanan kepada masyarakat, yang bertujuan untuk mewujudkan keamanan dalam negeri yang meliputi terpeliharanya keamanan dan ketertiban masyarakat, tertib dan tegaknya hukum, terselenggaranya perlindungan, pengayoman, dan pelayanan kepada masyarakat, serta terbinanya ketentraman masyarakat dengan menjunjung tinggi hak azasi manusia. Mereka pun mempunyai posisi penting sebagai penegak hukum, dan melaksanakan amanat Undang-undang menegakan ketertiban, dan keamanan masyarakat. Sebagai pelaksana Undang-undang Polri bertugas melakukan penyidikan

tindak pidana yang dilaksanakan oleh penyidik/penyidik pembantu pada fungsi reserse kriminal maupun fungsi operasional Polri lainya yang diberi wewenang oleh Undang-undang untuk melakukan penyidikan.

Penyidik adalah pejabat polisi negara Republik Indonesia atau pejabat pegawai negeri sipil tertentu yang diberi wewenang khusus oleh Undang-undang untuk melakukan penyidikan. Penyidikan adalah serangkaian tindakan penyidik dalam hal dan menurut cara yang diatur dalam undang-undang ini untuk mencari serta mengumpulkan bukti yang dengan bukti itu membuat terang tentang tindak pidana yang terjadi dan guna menemukan tersangkanya[1].

Polri tidak hanya menangani kejahatan konvensional yang diatur dalam Kitab Undang-undang Hukum Pidana saja tetapi juga kejahatan nonkonvensional. Dikarenakan kejahatan terus berkembang, seiring kemajuan teknologi dan informasi di tengah masyarakat yang tidak hanya membawa dampak positif namun juga memberikan dampak negatif contohnya kejahatan dunia maya seperti kasus penipuan bisnis *online*.

Dalam hal kejahatan nonkonvensional yang berhubungan dengan kejahatan di media sosial atau menggunakan alat-alat elektronik atau lewat media informasi lainya dan yang berdampak merugikan di atas, maka diterbitkan Undang-undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) tidak secara khusus mengatur mengenai tindak pidana penipuan. Selama ini tindak pidana penipuan sendiri diatur

[1] Undang-undang No. 8 Tahun 1981 tentang Hukum Acara Pidana Pasal 1 nomor 1 dan 2.

dalam Pasal 378 Kitab Undang-Undang Hukum Pidana (KUHP), dengan rumusan Pasal sebagai berikut : "*Barangsiapa dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum dengan menggunakan nama palsu atau martabat (hoedaningheid) palsu; dengan tipu muslihat, ataupun rangkaian kebohongan, menggerakkan orang lain untuk menyerahkan barang sesuatu kepadanya, atau supaya memberi utang maupun menghapuskan piutang, diancam, karena penipuan, dengan pidana penjara paling lama 4 (empat) tahun".* [2]

Walaupun Undang-Undang ITE tidak secara khusus mengatur mengenai tindak pidana penipuan, namun terkait dengan timbulnya kerugian konsumen dalam transaksi elektronik terdapat ketentuan Pasal 28 Ayat (1) UU ITE yang menyatakan : "*Setiap orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam transaksi elektronik"*.

Terhadap pelanggaran Pasal 28 Ayat (1) Undang-Undang ITE diancam pidana penjara paling lama 6 tahun dan atau denda paling banyak 1 miliar, sesuai pengaturan Pasal 45 ayat (2) Undang-Undang ITE. Jadi rumusan-rumusan Pasal 28 Ayat (1) Undang-Undang ITE dan Pasal 378 KUHP tersebut dapat diketahui bahwa keduanya mengatur hal yang berbeda. Walaupun begitu kedua tindak pidana tersebut memiliki suatu kesamaan yaitu dapat mengakibatkan kerugian bagi orang lain.

---

[2] Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik Pasal 2.

Teknologi informasi dan komunikasi telah dimanfaatkan dalam kehidupan sosial masyarakat, dan telah memasuki berbagai faktor kehidupan baik sektor pemerintahan, bisnis, perbankan, pendidikan, kesehatan, dan kehidupan pribadi. Manfaat teknologi informasi dan komunikasi selain memberikan dampak positif juga disadari memberi peluang untuk dijadikan sarana melakukan kejahatan baru (*cyber crime*). Sehingga dapat dikatakan bahwa teknologi informasi dan komunikasi bagaikan pedang bermata dua, dimana selain memberikan kontribusi positif bagi peningkatan kesejahteraan, kemajuan, dan peradaban manusia, juga menjadi sarana potensial dan sarana efektif untuk melakukan perbuatan melawan hukum.[3]

Pada jaringan komputer seperti internet, masalah kriminalitas menjadi semakin kompleks karena ruang lingkupnya yang luas. Kriminalitas dalam internet atau *cyber crime* pada dasarnya adalah suatu tindak pidana yang berkaitan dengan *cyber space* (ruang yang diwujudkan melalui jaringan komputer), baik yang menyerang fasilitas umum di dalam *cyber space* atau pun kepemilikan pribadi.

Macam-macam kejahatan yang dapat timbul dari internet, seperti penipuan, penghinaan, pornografi, *Money laundering* dan terorisme juga dapat dilakukan melalui internet. Kejahatan dalam internet ini dapat dibedakan menjadi tiga bagian yaitu pelanggaran akses, pencurian data, dan

---

[3] Sunarso, Siswanto, *Hukum Informasi dan Transaksi Elektronik: Studi Kasus Prita Mulyasari*, Jakarta, 2009, Rineka Cipta, hal. 40.

penyebaran informasi untuk tujuan kejahatan seperti melakukan penipuan melalui internet.

Penipuan melalui internet atau penipuan berbasis *online* merupakan kejahatan yang marak terjadi saat ini. Pengguna internet yang semakin meningkat ternyata membuka kesempatan yang lebih besar bagi para penipu *online* untuk mendapatkan uang atau keuntungan dari internet. Ada banyak sekali pengguna internet yang mencari peluang melalui bisnis *online*, dan ini memberikan ide bagi para *scammer* (pelaku penipuan berbasis *online*) untuk meraup keuntungan.

Ada banyak modus penipuan di dunia maya, mulai dari toko *online* hingga penawaran bisnis *online*. Penipuan yang berkedok bisnis *online* dapat tersamar dengan sangat baik, bahkan orang yang sudah sering bermain internet tidak sadar bahwa dia sedang tertipu. Penipuan bisnis *online* bisa dilakukan dengan berbagai modus, berikut ini modus yang biasa digunakan oleh pelaku untuk menjerat korbannya seperti melakukan modus penipuan bisnis *online* berupa pembajakan akun. Biasanya pelaku akan membajak akun-akun yang dianggap menguntungkan, seperti akun media sosial tokoh ternama. Jika sudah mampu dibajak maka aksi penipuan bisa dilancarkan dengan menggunakan akun dari seseorang yang terkenal sehingga mudah dipercaya saat ditawari produk, atau yang lebih parah disuruh mentransfer sejumlah uang. Modus penipuan bisnis *online* yang paling sering dijumpai pada saat bertransaksi seperti barang yang tidak terkirim atau tidak sampai

ke penerima, atau barang yang sampai kepada konsumen tidak sama dengan barang yang diperjual-belikan.

Begitupun kasus yang terjadi pada korban atas nama Then Meriana Mahasiswa yang beralamat di Apartemen Gate Way Tower Emeral C lantai 2 No 2 Cicadas Kota Bandung, berdasarkan Laporan Polisi dengan nomor LPB/20/01/2018/Jabar pada hari Senin tanggal 08 Januari 2018. Dia melaporkan ke Ditreskrimsus Polda Jabar setelah membeli Hp Iphone di situs olx seharga Rp. 4.550.000 (empat juta lima ratus lima puluh ribu rupiah) tetapi sampai saat ini barang belum sampai juga. Dengan adanya kejadian tersebut pelapor mengalami kerugian kurang lebih Rp. 4.550.000 (empat juta lima ratus lima puluh ribu rupiah).

Meskipun kasus penipuan bisnis *online* adalah termasuk kejahatan baru dan diatur di dalam Undang-Undang yang baru akan tetapi tidak bisa kita pungkiri bahwa dampaknya akan sangat besar pada kehidupan bermasyarakat dan bernegara karena kadangkala suatu perbuatan dapat merugikan orang lain.

Dalam kurun waktu dari bulan Januari-Juli 2018 data kejahatan *Cyber Crime* terutama dalam hal kasus penipuan bisnis *online* yang diterima atau tangani oleh Direktorat Reserse Kriminal Khsus Polda Jawa Barat dapat dilihat berdasarkan tabel di bawah ini :

Tabel 1.1
Data Kasus Penipuan Bisnis *Online* di Unit IV Subdit II *Cyber Crime*
Direktorat Reserse Kriminal Khusus Polda Jawa Barat
dari Bulan Januari – Juli 2018

Bulan							Jumlah
Januari	**Februari**	**Maret**	**April**	**Mei**	**Juni**	**Juli**	
11	10	12	2	2	2	9	48

(Sumber : Laporan Polisi yang Masuk ke Unit IV Subdit II *Cyber Crime* Direktorat Reserse Kriminal Khusus Polda Jawa Barat)

Dari tabel di atas menunjukan bahwa jumlah kasus tindak pidana penipuan bisnis *online* di wilayah hukum Polda Jawa Barat pada bulan Januari – Juli 2018 relatif tinggi dengan 48 kasus maka dengan itu Penyidik Direktorat Reserse Kriminal Khusus Subdit II Unit IV *Cyber Crime* dapat memberikan penanganan terhadap kasus tersebut untuk diselesaikan sehingga dapat dilihat pentingnya peran Penyidik Direktorat Reserse Kriminal Khusus Polda Jawa Barat Subdit II Unit IV *Cyber Crime.*

Berdasarkan latar belakang tersebut penulis tertarik untuk melakukan penelitian terhadap peran Direktorat Reserse Kriminal Khusus dalam penyidikan kasus kejahatan *cyber crime* khususnya dalam kasus penipuan bisnis *online* yang dituangkan dalam bentuk tugas akhir dengan judul : **PERAN PENYIDIK DIREKTORAT RESERSE KRIMINAL KHUSUS DALAM PENYIDIKAN KASUS PENIPUAN BISNIS *ONLINE* DI WILAYAH HUKUM POLDA JAWA BARAT.**

1.2. Identifikasi Masalah

Dari uraian latar belakang masalah di atas, maka dapat dirumuskan identifikasi masalah sebagai berikut :

1. Bagaimana peran Penyidik Direktorat Reserse Kriminal Khusus dalam melakukan penyidikan terhadap pelaku tindak pidana penipuan bisnis *online* di wilayah hukum Polda Jawa Barat.
2. Apa yang menjadi faktor pendukung dan penghambat Penyidik Direktorat Resesrse Kriminal Khusus dalam proses penyidikan tindak pidana penipuan bisnis *online* di wilayah hukum Polda Jawa Barat.
3. Apa upaya-upaya yang dilakukan oleh Direktorat Reserse Kriminal Khusus dalam penyidikan untuk penanganan terjadinya tindak pidana penipuan bisnis *online* di wilayah hukum Polda Jawa Barat.

1.3. Maksud Dan Tujuan

Adapun maksud penulis melakukan penelitian ini adalah untuk memenuhi salah satu Tugas Akhir Program Studi Diploma III Kepolisian Universitas Langlangbuana dan sebagai sumbangsih konsep pemikiran tentang peran Penyidik Direktorat Reserse kriminal Khsus Polda Jawa Barat dalam penyidikan kasus penipuan bisnis *online*.

Sedangkan tujuan dari penelitian ini, adalah :

1. Untuk mengetahui proses penyidikan kasus penipuan bisnis *online* di wilayah hukum Polda Jawa Barat.

2. Untuk mengetahui dukungan dan hambatan apa saja yang mempengaruhi upaya Penyidik dalam melakukan penyidikan kasus penipuan bisnis *online* di wilayah hukum Polda Jawa Barat.
3. Untuk mengetahui upaya yang dilakukan Penyidik Direktorat Reserse Kriminal Khusus dalam penyidikan untuk penanganan terjadinya kasus penipuan bisnis *online* di wilayah hukum Polda Jawa Barat.

1.4. Kegunaan Penelitian

1.4.1. Aspek Teoritis

Adapun aspek teoritis dari penulisan ini adalah sebagai berikut :

1. Menjadi bahan penelitan untuk kajian yang sejenis.
2. Memberikan kontribusi untuk menambah wawasan akan bahayanya penipuan bisnis *online*.
3. Gambaran mengenai peran Direktorat Reserse Kriminal Khusus Polda Jawa Barat khususnya Unit *Cyber Crime* dalam melakukan penyidikan kasus penipuan bisnis *online*.

1.4.2. Aspek Praktis

Adapun aspek praktis dari penulisan ini adalah sebagai berikut :

1. Memberikan informasi kepada masyarakat bahwa penggunaan media sosial harus digunakan dengan arif dan tidak digunakan untuk penipuan bisnis *online*.
2. Memberikan masukan serta sebagai pedoman bagi aparat penegak hukum dalam menentukan langkah-langkah dan kebijakan dalam mengungkap suatu peristiwa kejahatan.