BAB IV

PENUTUP

4.1. Kesimpulan

1. Penentuan *tempus delicti* dalam tindak pidana siber berupa *phising* oleh penegak hukum ialah banyak melibatkan berdasarkan teori-teori hukum yang ada. Hal tersebut terjadi karena adanya ketidaklengkapan peraturan perundang-undangan di Indonesia yang mengatur hukuman pidana bagi pelakunya. Berdasarkan peraturan perundang-undangan di Indonesia, penegak hukum sejauh ini dalam hal menentukan *tempus delicti* ialah berpacuan dengan Kitab Undang-Undang Hukum Pidana (KUHP) dan Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). Jadi apabilaUndang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) sebagai aturan khusus tidaklah lengkap, maka Kitab Undang-Undang Hukum Pidana (KUHP) di gunakan sebagai acuan. Hal tersebut berlaku sebaliknya, dengan memperhatikan unsur-unsur yang ada dalam tindakan *phising*. Poin utama yang digunakan acuan dalam menentukan *tempus delicti* ialah adanya waktu pengiriman dan penerimaan dalam melancarkan tindakan *phising*, yang dimana melibatkan sistem informasi atau perangkat lunak dan perangkat keras sebagai alat yang menghasilkan

sistem atau dokumen hasil *phising* yang sekaligus sebagai alat bukti dalam tindak pidana siber berupa *phising*.

2. Terjadinya pencurian data ialah suatu hal yang melekat dalam tindak pidana siber berupa *phising*. Hal tersebut terbukti dalam perkara nomor 155/Pid.Sus/2018/PN.Cbn. dan perkara nomor 85/Pid.Sus/2022/PN.Bjb. Cara pelaku melancarkan aksi *phising*nya ialah dengan di buatnya sistem untuk mengambil data pribadi korban secara tidak wajar yang sekaligus merugikan korban. Hal tersebut sulit dalam hal penanganan dan pencegahan, karena belum adanya peraturan perundang-undangan di Indonesia yang mengatur terkait penjatuhan hukuman bagi pelaku. Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) dan Kitab Undang-Undang Hukum Pidana (KUHP) hanya mengatur mengenai larangan pencurian data pribadi tersebut, tanpa adanya tindak lanjut mengenai penjatuhan hukuman bagi pelaku.

4.2. Saran

1. Bagi Pemerintah

   Pencurian data dalam pengaturan hukum di Indonesia belum diatur, sehingga terjadi kekosongan hukum yang memungkinkan kekacauan di masyarakat. Tidak satupun pasal dalam Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan

Transaksi Elektronik (UU ITE) yang dapat menjerat pelaku perbuatan *phising* sekaligus pencurian data yang terjadi di dalamnya, sehingga diperlukan pembaharuan hukum di masa yang akan datang atas hal tersebut. Rancangan Kitab Undang-Undang Hukum Pidana (RKUHP) juga belum mengatur perbuatan mendapatkan data identitas diri menggunakan teknik *phising*. Bab viii tentang tindak pidana terhadap telematika dan informatika hanya diatur tentang penggunaan dan perusakan informasi elektronik dan domain, tanpa hak mengakses komputer dan sistem elektronik dan pornografi anak melalui komputer.

Kriminalisasi perbuatan pencurian data dalam *phising* harus dilakukan secara cepat, mengingat *phising* berkembang sangat pesat. Badan legislatif agar segera melakukan pengkajian ulang khususnya di bidang teknologi dan informatika dalam Rancangan Kitab Undang-Undang Hukum Pidana (RKUHP), sehingga ketika disahkan di masa yang akan datang tidak ada lagi kekosongan norma terhadap perbuatan pencurian data dengan menggunakan teknik *phising* serta dapat mewujudkan kodifikasi hukum pidana nasional. Rancangan Undang-Undang (RUU) tentang perlindungan data pribadi baiknya juga harus segera di sahkan, agar dapat memberikan landasan hukum untuk menjamin perlindungan data pribadi masyarakat Indonesia di manapun tersebut berada.

2. Bagi Masyarakat

Masyarakat harus lebih berhati-hati, terlebih ketika adanya sesuatu yang tidak dikenal secara tiba-tiba mengirimkan sebuah link. Kiriman-

kiriman yang menggiurkan atau yang secara tidak wajar tidaklah perlu tergesa-gesa untuk memencet link dalam kiriman tersebut. Langkah yang perlu dilakukan ketika mendapat sebuah link untuk kemudian di arahkan memencet link tersebut ialah baiknya mencari informasi terlebih dahulu di internet terkait kebenaran kiriman tersebut. Kemudian juga dapat menghubugi secara langsung *hotline* atau *customer service* pusat dari kiriman tersebut.