

BAB V

PENUTUP

A Kesimpulan

Setelah dilakukan kajian dan analisis yuridis perlindungan hukum bagi korban tindak pidana pencurian data pribadi melalui sistem elektronik dalam hukum positif di Indonesia, maka dapat disimpulkan sebagai berikut:

1. Modus terjadinya pencurian data pribadi melalui sistem elektronik biasa dilakukan oleh pelaku dengan meretas atau mengakses sistem elektronik secara ilegal. Teknik peretasan yang paling banyak dilakukan pelaku untuk mencuri data pribadi dari sistem elektronik yaitu teknik *Web Application Vulnerability* dan *Phishing*. Teknik *Web Application Vulnerability* dilakukan dengan mengeksploitasi kerawanan atau celah keamanan pada sistem elektronik, sedangkan teknik *Phishing* dilakukan dengan menyisipkan kode-kode berbahaya pada dokumen atau email, sehingga ketika korban membuka dokumen tersebut, kode akan dieksekusi oleh pelaku. Modus tersebut melanggar Pasal 30 ayat (2) UU ITE yang berbunyi “setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/ atau sistem elektronik milik orang lain dengan cara apapun dengan tujuan untuk memperoleh informasi elektronik dan/ atau dokumen elektronik”.
2. Bentuk perlindungan hukum bagi korban meliputi perlindungan preventif (pencegahan) maupun perlindungan represif (penegakan hukum). Perlindungan hukum secara preventif dilakukan dengan

menjalankan kewajiban-kewajiban pengamanan data pribadi serta sadar dengan pentingnya keamanan informasi bagi pemilik sistem elektronik maupun pemilik data pribadi seperti yang telah diatur di dalam peraturan perundang-undangan. Hal tersebut sebagai upaya untuk mencegah atau meminimalisir modus terjadinya pencurian data pribadi melalui kegiatan peretasan dan akses secara ilegal. Perlindungan hukum secara represif merupakan upaya penegakkan hukum setelah terjadi pencurian data pribadi. Korban dapat melaporkan tindak pencurian data pribadi kepada penegak hukum atas dalil pelanggaran Pasal 30 Ayat (2) *juncto* pasal 46 Ayat (2) UU ITE. Bagi pemilik data pribadi dapat mengajukan gugatan secara perdata terhadap pemilik sistem elektronik karena dianggap lalai menjaga keamanan data pribadi sesuai dengan ketentuan Pasal 26 UU ITE.

3. Penerapan perlindungan hukum terhadap korban tindak pidana pencurian data pribadi hingga saat ini masih belum optimal, pasalnya masih belum ada dari banyaknya kasus pencurian data pribadi yang terselesaikan secara tuntas apalagi hingga pemberian restitusi bagi korban yang dirugikan. Penyebab utamanya karena norma hukum yang mengatur perlindungan data pribadi masih samar-samar dan belum lengkap. Selain itu, juga disebabkan karena modus pencurian data pribadi menggunakan teknologi yang sangat canggih, sehingga pelaku pencurian data pribadi sangat sulit untuk dilacak dan dijerat dengan Pasal 30 Ayat (2) UU ITE. Saat ini, terdapat lembaga pemerintah yaitu

BSSN yang memiliki kewenangan untuk menangani kasus pencurian data pribadi, namun tidak sampai dalam upaya penegakan hukum. Upaya BSSN dalam penanganan insiden kebocoran data pribadi dilakukan melalui monitoring dan deteksi insiden kebocoran data pribadi. Selain itu juga melalui kegiatan layanan aduan insiden siber. Korban pencurian data pribadi dapat menyampaikan aduan kepada BSSN untuk dilakukan penelusuran lebih lanjut sehingga mendapatkan titik terang dari kasus pencurian data pribadi. Kemudian dilanjutkan dengan penyelesaian secara mediasi atau alternatif lainnya antara pemilik data pribadi dan pemilik sistem elektronik dengan Kementerian Kominfo sebagai mediatornya. Jika pemilik sistem elektronik terbukti melanggar pengelolaan data pribadi maka dapat diberikan sanksi administratif, berupa peringatan lisan, tertulis, hingga pencabutan izin.

B Saran

Setelah menulis skripsi ini, saran yang dapat penulis sampaikan yaitu sebagai berikut:

1. Pemilik data pribadi maupun pemilik sistem elektronik supaya menerapkan mekanisme keamanan informasi secara serius untuk melindungi data pribadi sehingga dapat terhindar dari modus pencurian data pribadi.
2. Bagi lembaga negara baik lembaga legislatif, pemerintah, dan lembaga yang terkait lainnya supaya mendorong RUU Perlindungan Data Pribadi untuk segera disahkan, supaya

pelaksanaan perlindungan data pribadi memiliki payung hukum yang lengkap dan kuat sehingga dapat dijalankan secara optimal.

3. Sambil menunggu RUU Perlindungan Data Pribadi disahkan, fungsi perlindungan data pribadi yang dilaksanakan BSSN dan Kementerian Kominfo melalui jalur aduan dengan penyelesaian secara mediasi dan alternatif lainnya harapannya dapat diselesaikan secara tuntas dan optimal.

