

BAB V

PENUTUP

A. Kesimpulan

Berdasarkan hasil analisis terhadap rumusan masalah, maka dapat disimpulkan :

1. Penerapan prinsip kehati-hatian pada jual-beli data nasabah sangat diperlukan dalam kegiatan usaha di perbankan untuk menghindari tersebarnya data-data nasabah seperti Nomor Induk Kependudukan (NIK), limit penarikan uang pada rekening serta data kartu kredit atau data penting lainnya yang dari data tersebut bisa digunakan para penjahat untuk melakukan pembobolan rekening. Tujuan dari diterapkan prinsip kehati-hatian terhadap data nasabah yaitu sebagai pencegahan agar tidak terjadinya jual-beli data nasabah. Penerapan prinsip kehati-hatian dilaksanakan oleh penyelenggara yang mana pada perbankan disebut sebagai pihak afiliasi. Namun, karena alasan tertentu, tidak selamanya pihak afiliasi tersebut terus bekerja. Maka untuk menerapkan prinsip kehati-hatian, bank melakukan upaya preventif dan represif yang bertujuan untuk tidak adanya akses terjadi kebocoran data nasabah yang dilakukan oleh pihak internal maupun pihak yang sudah tidak menjabat dari internal bank. Tindakan preventif berupa seperti pencegahan terhadap pengendalian agar tidak ada kebocoran data seperti menumbuhkan kesadaran terhadap pencegahan Tindakan fraud khususnya data pribadi dan yang dilakukan dengan perjanjian kode etik dan pakta integritas terhadap para karyawan, pemantauan terkait profil karyawan dan sistem yang terjaga. Tindakan represif bank jika terjadi kebocoran data nasabah jika jual-beli data nasabah dilakukan oleh internal, maka bank akan menemukan penyebab dan motif yang dilakukan oleh pegawai bank tersebut serta dari dampak kerugian yang ditimbulkan akan dinaikan ke kepolisian, namun jika dilakukan oleh

pihak eksternal maka bank akan melakukan perbaikan terhadap sistem dan dilaporkan pada kejahatan *cyber* atas pencurian data

2. Bentuk perlindungan hukum bagi nasabah yang datanya dijual-belikan oleh mantan pegawai bank di Indonesia yaitu dengan nasabah yang dirugikan mengajukan pengaduan kepada pihak yang berwenang, seperti kepada bank yang telah merugikan nasabah tersebut, otoritas jasa keuangan (OJK) atau kepada bank Indonesia. Perlindungan hukum dapat berupa upaya hukum perdata ataupun pidana dapat ditempuh oleh nasabah, dengan dikenakan tanggung jawab secara perdata yang tertuang pada Pasal 26 UU ITE yakni para pihak yang dirugikan dapat mengajukan gugatan terhadap perolehan data pribadi tersebut tanpa adanya persetujuan dari pihak yang dirugikan, sehingga digugat dalam hal Perbuatan Melawan Hukum (PMH) atas dasar kesalahan berdasarkan ketentuan (1365 Kitab Undang-undang Hukum Perdata), Dalam hal tanggung jawab pidana, dapat dikenakan Pasal 32 UU ITE dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp 2.000.000.00,00 (dua miliar rupiah).

B. Saran

1. Terkait sistem keamanan yang ada pada perbankan sudah dilaksanakan dengan sangat ketat, akan tetapi tidak menutup kemungkinan seseorang mantan karyawan melakukan *hacking* melalui sistem tersebut dan tidak adanya perjanjian antara bank dan mantan pegawai bank terkait keharusan mantan pegawai bank untuk tetap menjaga rahasia data nasabah yang menjadi celah untuk melakukan tindakan kejahatan. Maka dari itu melalui penerapan prinsip kehati-hatian bank, maka penulis menyarankan dibuatnya perjanjian antara bank dengan mantan pegawai bank sebagai penerapan dari prinsip kehati-hatian. Terkait belum adanya peraturan khusus yang mengatur mengenai perlindungan data pribadi, sehingga penulis mengharapkan rancangan undang-undang terkait perlindungan data pribadi segera disahkan untuk terjaminnya perlindungan atas data pribadi setiap individu.

2. Upaya terhadap perlindungan data nasabah yang dilakukan oleh bank sudah mencakup secara preventif yakni kehati-hatian oleh pegawai bank dan secara represif jika terjadi kebocoran data nasabah, akan tetapi penting juga dilakukan pengawasan dan pembinaan kepada mantan pegawai bank terkait rahasia data nasabah.