Nomor Kelompok: 3
Anggota:
- Angelique Gabriella Halim 6182201030
- Olivia 6182201006
- Fauzan Rhamzy 6182201081
- Nadhira Saffanah Zahra 6182201048

Rangkuman “The Legal System and Ethics in Information Security”

1. Introduction

Teknologi berkembang jauh lebih cepat dari sistem legal, sehingga belum ada perlindungan terhadap penyalahgunaan teknologi. Dalam situasi ketidakjelasan peraturan ini, etika penting agar teknologi digunakan secara bertanggungjawab dan etis.

Meskipun ini bukan perlindungan yang “nyata”, tapi dalam masyarakat, *social acceptance* dan *peer pressure* memainkan peran penting dalam etika untuk membatasi penyalahgunaan teknologi.

2. Security and the Law

Bagian berikut menganalisis permasalahan yang dihadapi sistem legal yang berurusan dengan kejahatan berbasis komputer dan kesulitannya :

2.1. Tantangan yang Dihadapi oleh Sistem Legal

2.1.1. Perkembangan Teknologi yang Pesat

Perkembangan teknologi yang pesat membuat peluang untuk melakukan kejahatan dalam bidang teknologi semakin luas. Diperlukannya hukum yang bisa memberikan perlindungan terhadap kejahatan-kejahatan tersebut. Namun, hukum bersifat reaktif dan membutuhkan waktu untuk proses pengesahannya, sehingga hukum cukup sulit untuk menyesuaikan diri dengan perkembangan teknologi yang pesat.

2.1.2. Pelaksana Hukum yang Tidak Terampil dalam Teknologi

Pemahaman akan teknologi dibutuhkan dalam menangani kasus pengadilan yang terkait. Sayangnya, tidak semua pelaksana hukum memiliki pemahaman tersebut. Walaupun pemilihan keputusan dalam pengadilan ditentukan dengan bantuan ahli, keputusan tersebut tidak bisa dipilih tanpa pemahaman dasar.

2.1.3. Beberapa Peran Komputer dalam Kriminalitas

Komputer tidak memiliki kemampuan untuk bertindak sesuai keinginannya, melainkan komputer hanya menjalankan instruksi manusia, sehingga komputer tidak bisa ditahan oleh pengadilan. Beberapa situasi yang perlu diperhatikan yaitu, pencurian komputer beserta data di dalamnya, pencurian data untuk akses tidak sah, penggunaan sistem komputer untuk pengembangan virus, hak cipta serta penggunaan ilegal

perangkat lunak. Pengidentifikasian situasi-situasi tersebut merupakan tanggung jawab pencipta hukum untuk menetapkan hukum yang memadai serta hukuman yang pantas untuk mencegah hal tersebut.

2.1.4. Yurisdiksi

Pemrosesan suatu kasus pengadilan membutuhkan yurisdiksi atas individu/subjek dari suatu perkara. Sistem ini berfungsi dengan baik dalam penanganan perkara yang berbasis wilayah. Namun, sistem ini kurang tepat jika berurusan dengan penanganan perkara terkait jaringan komputer dan internet. Hal ini disebabkan karena penggunaan internet tidak terikat oleh batas geografi.

2.1.5. Kejahatan Komputer yang Disembunyikan

Perusahaan memiliki tanggung jawab untuk menyimpan informasi klien. Jika terjadi kebocoran atau pencurian data, maka perusahaan akan berusaha yang terbaik untuk menyembunyikan kasus tersebut dari publik, dengan tidak terlibat dengan pengadilan, bahkan jika pelakunya sudah diketahui. Hal ini merugikan sistem legal karena akan menyebabkan ketidaktahuan akan ancaman yang harus diwaspadai.

2.1.6. Kurangnya Riwayat Kasus Kejahatan Komputer

Kriminalitas dalam bidang komputer adalah hal yang baru, sehingga tidak banyak riwayat kasus yang terkait bidang ini di pengadilan. Dengan tidak adanya riwayat kasus, pemikiran dan perhatian yang besar harus dikerahkan untuk memastikan pemilihan keputusan yang benar dan hukuman yang pantas.

2.1.7. Motif dan Usia dari Pelaku Kejahatan

Kasus yang kuat membutuhkan motif, alat (kemampuan), serta peluang. Dengan internet, alat (kemampuan) dan peluang cukup mudah dicari, namun motif umumnya tidak dilakukan dengan motif kebencian, melainkan tantangan dari *cyber-crime* tersebut, terutama bagi remaja. Pencegahan yang tidak dilakukan dengan baik akan menyebabkan lebih banyak remaja merasa aman dari hukum dan melakukan kejahatan yang lebih serius.

2.1.8. Anonimitas yang Ditawarkan oleh Internet

Menjadi anonimus dalam beraktivitas di internet menimbulkan rasa aman sehingga memunculkan keberanian dalam melakukan aktivitas ilegal. Butuh waktu yang cukup lama untuk aksi kejahatan komputer terdeteksi, dan pada saat itu, penjahat tersebut sudah bisa menutupi jejak mereka dan menjaga anonimitas mereka. Dan di banyak kasus, mereka tidak pernah tertangkap.

2.2. Bagaimana Peran dari Hukum

Meskipun banyak hukum yang mengatur kejahatan yang bersifat tradisional seperti pencurian, penipuan, dan penyalahgunaan sudah ada, munculnya teknologi komputer dan internet menambah tantangan yang tidak bisa diatasi oleh hukum-hukum tersebut.

Untuk menghadapinya, banyak hukum yang telah dimodifikasi agar sesuai dengan teknologi digital. Sebagai contoh, undang-undang hak cipta yang awalnya hanya melindungi karya seni dan literatur, pada tahun 1980-an telah diperluas untuk mencakup perangkat lunak komputer. Namun, hukum hak cipta tidak melindungi ide dasar atau algoritma yang mendasari perangkat lunak tersebut, yang dianggap sebagai kekayaan intelektual yang lebih berharga.

Selain itu, ada pula upaya untuk memberikan perlindungan lebih kepada perangkat lunak melalui paten perangkat lunak. Namun, paten ini tidak melindungi algoritma dasar dari program, hanya proses untuk menjalankan ide, yang sering kali sulit untuk diterapkan pada perangkat lunak. Oleh karena itu, meskipun perlindungan paten tersedia, proses untuk mendapatkannya memakan waktu dan biaya yang besar, yang mungkin tidak sesuai dengan kebutuhan para pengembang perangkat lunak.

Dengan pesatnya perkembangan e-commerce, kebutuhan akan hukum yang mengatur kontrak, transaksi bisnis, dan pengolahan data melalui internet menjadi sangat mendesak. Undang-undang seperti E-SIGN (Undang-Undang Tanda Tangan Elektronik) di Amerika Serikat telah disahkan untuk melindungi transaksi elektronik, dan ini semakin memperjelas pentingnya penyesuaian hukum untuk mengakomodasi perkembangan teknologi digital.

Merek dagang, yang dapat mencakup nama domain di dunia maya, juga menjadi bagian penting dalam regulasi digital. Masalah distribusi ilegal dan penyalahgunaan merek dagang yang sudah ada untuk keuntungan pribadi diatur oleh organisasi internasional seperti WIPO, yang mengembangkan pedoman terkait masalah nama domain di internet.

Selain itu, hukum utilitas yang mengatur penyedia layanan internet (ISP) juga menjadi perdebatan, terutama terkait apakah ISP harus diperlakukan sebagai perusahaan utilitas biasa seperti penyedia listrik atau air. Meskipun beberapa negara sudah mulai memberlakukan regulasi untuk mengontrol akses ke situs web, di AS, upaya untuk mengatur ketidaksopanan dan pornografi di internet sering kali dibatalkan oleh pengadilan karena dianggap tidak konstitusional.

Dalam konteks hukum tort, yang mengatur perbuatan salah yang mengakibatkan kerugian, aspek-aspek seperti kewajiban untuk menjaga kerahasiaan data, masalah privasi dalam basis data, dan tanggung jawab atas kesalahan dalam informasi yang ada dalam basis data juga menjadi bagian dari regulasi yang relevan dengan keamanan komputer.

Terakhir, ada juga undang-undang yang secara langsung menangani kejahatan komputer, dan beberapa undang-undang tersebut telah diterapkan di

Amerika Serikat untuk mengatur tindakan yang melibatkan komputer, seperti penipuan dan akses ilegal ke sistem komputer.

2.3. Hukum dan Peraturan yang Berlaku untuk Keamanan

Kemajuan teknologi mendorong penyesuaian hukum untuk mengatasi tantangan keamanan di era komputer. Undang-undang yang mengatur keamanan komputer secara spesifik dirancang untuk menangani pelanggaran seperti akses tidak sah ke suatu sistem dan menetapkan standar bukti yang diperlukan dalam proses penegakkan hukum. Undang-undang tersebut akan menjadi dasar kebijakan yang memastikan penerapan prinsip keamanan dan perlindungan.

Di Amerika Serikat, terdapat undang-undang utama yang mengatur kejahatan yang dilakukan pada komputer, antara lain:

- **18 U.S.C. § 1029**: Mengatur larangan penggunaan perangkat akses seperti token atau kata sandi secara tidak sah.
- **18 U.S.C. § 1030**: Mengatur larangan akses elektronik tanpa izin, termasuk yang mengarah pada tindakan penipuan.
- **18 U.S.C. § 1362**: Memberikan perlindungan terhadap tindakan perusakan sistem komunikasi secara sengaja.
- **18 U.S.C. § 2511**: Melarang penyadapan komunikasi suara maupun elektronik tanpa otorisasi.
- **18 U.S.C. § 2701**: Menegaskan larangan akses ilegal terhadap data yang disimpan secara elektronik.
- **18 U.S.C. § 2702**: Membatasi kewenangan penyedia layanan untuk mengungkapkan informasi pribadi pengguna tanpa persetujuan.
- **18 U.S.C. § 2703**: Mengatur prosedur bagi pemerintah dalam memperoleh akses ke data elektronik melalui penyedia layanan.

3. Etika dalam Keamanan

Pengguna harus memiliki tanggung jawab dan etika dalam menggunakan internet, sumber daya komputer, hardware, dan software. Mustahil untuk merumuskan hukum yang mengatur segala perilaku yang dapat diterima masyarakat. Sebagai gantinya, masyarakat bergantung pada etika untuk membangun kesadaran terhadap perilaku yang bisa diterima masyarakat. Setiap individu dapat mempercayai etika yang berbeda dan tidak dapat dipaksakan. Etika bisa diubah menyesuaikan situasi lebih mudah dibandingkan hukum.

Kebanyakan organisasi telah membuat kode etik untuk dipatuhi anggotanya, misalnya *Computer Ethics Institute* membuat 10 *Commandments of Computer Ethics,* yaitu **JANGAN:**

1. menggunakan komputer untuk mencelakai orang lain
2. mengganggu pekerjaan komputer orang lain
3. mengintip *file* komputer orang lain.
4. Memakai komputer untuk mencuri
5. Memakai komputer untuk memberi informasi tidak benar

6. Menyalin/memakai *software* tanpa membayar
7. Memakai komputer orang lain tanpa izin
8. Mengambil ciptaan orang lain
9. Tidak berpikir mengenai konsekuensi sosial program yang anda buat
10. Menggunakan komputer tanpa mempertimbangkan dan menghargai sesama manusia.

Mendorong pengguna untuk mematuhi standar etis membutuhkan usaha bersama. Penting untuk semua negara berpikir bagaimana mereka dapat mendorong perilaku *cyber* yang etis kepada para penduduknya.

4. Kesimpulan

Teknologi telah merevolusi dunia dengan menghilangkan batasan geografis dalam komunikasi dan aktivitas bisnis. Tetapi kemajuan teknologi ini menimbulkan tantangan baru, seperti kebutuhan akan keamanan sistem komputer untuk melindungi data yang ditransmisikan melalui jaringan. Sehingga dirancang kebijakan hukum yang dapat menghukum pelaku kejahatan dunia maya, sekaligus menekankan pentingnya penerapan etika dalam penggunaannya.

Meskipun sistem hukum tidak sepenuhnya sempurna, tetapi sistem hukum memegang peranan penting dalam menjaga infrastruktur teknologi agar tetap aman. Para pengelola keamanan sistem perlu memahami bagaimana hukum dapat membantu mereka melindungi data dan jaringan secara lebih efektif. Di sisi lain, perusahaan juga harus memprioritaskan budaya etika yang kuat dalam penggunaan teknologi. Hal ini penting karena banyak kejahatan maya yang berasal dari dalam organisasi itu sendiri. Dengan membangun lingkungan kerja yang mengutamakan perilaku etis, risiko terjadinya aktivitas ilegal di bidang teknologi dapat diminimalkan.