PERAN AUDITOR TEKNOLOGI INFORMASI DALAM MENGURANGI KEJAHATAN KOMPUTER

Achmad Syaiful Hidayat Anwar
Fakultas Ekonomi Universitas Muhammadiyah Malang
E-mail: iepoel@yahoo.com

Abstract

The development of information and communication technology raise business risks, especially risks associated with security issues, privacy, accuracy and reliability of information. In this case, the factor of safety and control at the Internet-based information systems is a major and important aspect that needs to be managed effectively. This aims to protect information systems from the various possibilities of errors, fraud, crime and unethical use of information technology. The existence and implementation of Information and Electronic Transaction Act (ITE) No. 11 2008, computer forensics and the role of IT auditors is directed at efforts to reduce various forms of computer crime (computer crime), primarily in the business world.

Keywords: *UU ITE No 11/2008, Forensic Computer, Information Technology, Computer crime*

Abstrak

Perkembangan teknologi informasi dan komunikasi meningkatkan risiko usaha, khususnya risiko yang terkait dengan masalah keamanan, privasi, akurasi dan keandalan informasi. Dalam hal ini, faktor keamanan dan kontrol pada sistem informasi berbasis internet merupakan aspek utama dan penting yang perlu dikelola secara efektif. Hal ini bertujuan untuk melindungi sistem informasi dari berbagai kemungkinan kesalahan, penipuan, kejahatan dan penggunaan etis teknologi informasi. Keberadaan dan pelaksanaan Undang-Undang Informasi dan Transaksi Elektronik (ITE) No 11 tahun 2008, forensik komputer dan peran auditor TI diarahkan pada upaya untuk mengurangi berbagai bentuk kejahatan komputer (kejahatan komputer), terutama dalam dunia bisnis.

Kata kunci: *UU ITE No 11/2008 Forensik Komputer, Teknologi Informasi, Komputer kejahatan*

Implementasi teknologi infor-masi dan komunikasi dalam dunia bisnis, telah menjadi bagian penting dalam mencapai kesuksesan. Selain itu, perkembangan teknologi informasi (TI) juga memberikan kontribusi yang besar bagi perkembangan bidang atau profesi audit. Hall dan Singleton (2007) menyatakan bahwa, teknologi informasi telah menginspirasi perekayasaan ulang berbagai proses bisnis suatu entitas. Operasi yang efisien, informasi dan komunikasi yang lebih efektif, terjalinnya kerjasama dan harmonisasi hubungan bisnis dengan pihak ketiga merupakan beberapa benefit yang dapat dicapai perusahaan melalui pemanfaatan teknologi informasi pada berbagai aktivitas bisnis.

Ketersediaan dukungan tekno-logi informasi dan komunikasi (TIK) memungkinkan bagi individu atau suatu entitas bisnis; 1. untuk melakukan berbagai aktivitas bisnis dapat dilakukan secara online dan, 2. memberikan kemudahan dalam melakukan transaksi atau aktivitas bisnis yang lebih bernilai. *Internet, intranet, e-commerce, electronic funds transfer, e-mail, e-newspapaer, e-banking, mobile banking, internet banking, e-payment, electronic data interchange* (EDI), *e-business, e-ticketing, Enterprise Resource Planning* (ERP), merupakan beberapa contoh aplikasi teknologi informasi berbasis dalam dunia bisnis dewasa ini.

Implementasi sistem informasi berbasis teknologi dan web (internet) juga juga memberikan kontribusi yang positif bagi pihak lain. Misalnya, bagi pihak pemasok, akan semakin mudah untuk mengakses atau mendistribusi informasi terkini dari berbagai database dan repositori lainnya.

Bagi perusahaan pengaplikasi, aplikasi internet pada berbagai aktivitas bisnis, akan semakin meningkatkan kemampuan untuk menjaga loyalitas dan resistensi konsumen, memahami kebutuhan dan ekspektasi kebutuhan konsumen untuk saat ini dan di masa yang akan datang, serta dapat meningkatkan kualitas layanan pada konsumen. Dengan demikian, perusahaan dapat memberikan pelayanan yang terbaik bagi para konsumen, terutama ketersediaan informasi yang dibutuhkan oleh konsumen. Sedangkan kontribusi bagi pihak konsumen, aplikasi internet dalam bisnis semakin memudahkan konsumen untuk memperoleh informasi yang akurat dan relevan mengenai produk atau jasa yang dibutuhkan, sebagai pendukung dalam pengambilan keputusan.

Di samping memberikan kon-tribusi yang positif terhadap kemajuan bisnis, perkembangan TI juga memiliki dampak negatif, terutama yang berkaitan dengan risiko dan potensi gangguan. Hal ini dikarenakan faktor keamanan dan pengendalian internal merupakan salah satu faktor penting yang menentukan kesuksesan serta keberlangsungan suatu bisnis. Oleh karena itu, faktor keamanan dan pengendalian internal untuk mengantisipasi, mendeteksi, dan mengevaluasi berbagai kemungkinan terjadinya kesalahan, kecurangan atau kejahatan komputer sangat diperlukan dalam sistem informasi berbasis komputer.

Ada tiga alasan yang mendasari argumen mengenai faktor keamanan dan pengendalian internal, yaitu; *pertama,* perkembangan TI juga memunculkan berbagai risiko bisnis, terutama risiko yang berhubungan

dengan risiko keamanan, privasi, akurasi dan reliabilitas data atau informasi suatu perusahaan. Risiko dari gangguan virus, worm dn trojan juga termasuk bagian dari risiko aplikasi teknologi, yang disebabkan oleh penggunaan teknologi komputer yang tidak etis.

Kedua, informasi merupakan aset penting bagi suatu entitas atau organisasi bisnis. Apabila informasi tersebut dapat diakses secara ilegal dan disalahgunakan oleh para pesing bisnis (kompetitor) atau pihak lain yang tidak memiliki autoritas, maka hal ini dapat menimbulkan kerugian bagi pemilik informasi. Oleh karena itu, proteksi terhadap kerahasiaan dan keamanan informasi dari segala bentuk penyalahgunaan sangat dibutuhkan. Hal ini mengarah pada upaya untuk memproteksi sistem informasi dari berbagai kemungkinan terjadinya kesalahan, kecurangan, penyimpangan, kejahatan dan penggunaan teknologi informasi yang tidak etis (Laudon & Laudon, 2008).

Ketiga, ancaman yang timbul dari para pelaku kejahatan komputer dan internet serta ancaman yang muncul dari perilaku para pengguna komputer atau internet yang tidak etis. Icove dalam Fejer (2009) mengklasifikasi kejahatan komputer ke dalam 4 kriteria yaitu; keamanan yang bersifat fisik *(physical security),* keamanan yang berhubungan dengan orang (personil); termasuk identifikasi, dan profil resiko dari orang yang mempunyai akses (pekerja), keamanan dari data dan media serta teknik komunikasi *(communications)* dan keamanan dalam operasi; termasuk kebijakan *(policy)* dan prosedur yang digunakan untuk mengatur dan mengelola sistem keamanan, dan juga termasuk prosedur setelah serangan *(post attack recovery).*

Berkaitan dengan kejahatan komputer, Budiman (2003) mengklasifikasi kejahatan komputer menjadi dua jenis, yaitu; *cyber fraud* (kejahatan dari aspek sistem organisasi komputer) dan *cybercrime,* dalam hal ini, *cybercrime* merupakan bentuk pelanggaran hukum dengan menggunakan komputer sebagai media. Rid (2008) mengidentifkasi beberapa bentuk penyerangan atau kejahatan komputer pada sistem komputer.

Beberapa bentuk penyerangan atau kejahatan komputer pada sistem komputer tersebut antara lain; 1. Interupsi (perangkat sistem menjadi rusak atau tidak tersedia, yang ditujukan pada aspek ketersediaan *(availability)* dari sistem; 2. Intersepsi (pihak yang tidak berwenang berhasil mengakses asset atau informasi); 3. Modifikasi, dalam hal ini, pihak yang tidak berwenang tidak saja berhasil mengakses, akan tetapi dapat juga mampu mengubah data aset; dan 4. Pabrikasi (pihak yang tidak berwenang menyisipkan objek palsu ke dalam sistem).

Harris (2007) mengidentifikasi beberapa bentuk lain kejahatan atau kecurangan komputer. Beberapa bentuk kecurangan komputer tersebut antara lain; pemalsuan nilai evidentiary data, alterasi (pengubahan) data, sabotase komputer, pembukaan rahasia perdagangan dan industrial serta akuisisi data secara ilegal. Lebih lanjut, Harris memaparkan beberapa kasus kejahatan komputer yang pernah terjadi, khusunya di Indonesia, antara lain; 1. Kasus penggelapan uang melalui Komputer (*Clearing*) BRI Yogyakarta; 2. Kasus pembobolan BNI

46 cabang New York; 3. Kasus mutasi kredit fiktif melalui komputer oleh Bank Office Computer BDN Cab. Jakarta Bintaro Jaya; 4. Kasus pemalsuan nama domain Mustika Ratu.com di Amerika; 5. Kasus hacking pada situs KPU; 6. Kasus pembobolan kartu kredit melalui internet; dan 7. Kasus domain *klikbca.com*, serta beberapa kasus lain terkait dengan masalah keamanan sistem informasi berbasis internet atau berbasis web.

Beberapa kasus yang muncul dalam sistem informasi berbasis komputer maupun internet, berkaitan sangat erat dengan masalah keamanan dan pengendalian. Berdasarkan pemikiran tersebut diatas, penulis kemudian tertarik untuk mengkaji eksistensi UU ITE No. 11/2008, fungsi forensik komputer dan peran auditor teknologi informasi, dalam upaya untuk memprevensi dan atau mereduksi kemungkinan timbulnya kejahatan komputer dan penggunaan teknologi informasi yang tidak etis dalam dunia bisnis.

Artikel ini diharapkan dapat; 1. memberikan kontribusi yang positif bagi pengembangan ilmu pengetahuan dan teknologi, terutama yang berhubungan dengan aplikasi teknologi informasi dan komunikasi dalam dunia bisnis dan 2. dapat dijadikan sebagai referensi pendukung atau sumbangan pemikiran terkait dengan upaya untuk memprevensi atau mereduksi berbagai bentuk Kejahatan Komputer.

Sistematika pembahasan artikel ini diklasifikasi kedalam enam bagian. *Pertama*, pembahasan mengenai risiko teknologi komputer dn internet. *Kedua*, membahas masalah keamanan dan pengendalian sistem informasi berbasis komputer. *Ketiga*, pembahasan tentang eksistensi Undang undang Informasi dan Transaksi Elektronik (UU ITE) No. 11/2008. *Keempat*, fokus pada pembahasan mengenai forensik komputer. Keempat, membahas tentang *Kelima*, mengkaji tentang peran auditor forensik dalam pelaksanaan audit TI. *Terakhir*, membahas mengenai pereduksian masalah-masalah kejahatan dan penggunaan komputer yang tidak etis pada berbagai aktivitas bisnis.

Risiko Teknologi Komputer dan Internet

Implementasi TI, termasuk aplikasi internet dalam bisnis memunculkan berbagai risiko bisnis, terutama risiko yang berhubungan dengan masalah keamanan, akurasi dan reliabilitas data atau informasi suatu perusahaan. Hall dan Singleton, (2007) menyatakan bahwa, risiko keamanan meliputi berbagai risiko yang diasosiasikan dengan akses data (akses secara fisik atau logis) dan integritas data.

Untuk menjamin bahwa akurasi prosedur TI, kelengkapan data, ketepatan waktu dan realiabilitas suatu data, perusahaan harus mampu mengendalikan risiko yang diasosiasikan dengan aktivitas pengumpulan dan pemrosesan data. Berbagai risiko yang diasosiasikan dengan integritas data sering terlihat pada saat pengumpulan data dan berbagai bentuk proses pengumpulan data.

Budhisantosa (2007) juga memiliki pemikiran yang sama bahwa, perkembangan teknologi informasi juga menyertakan beragam isu, salah satunya adalah isu keamanan. Komputer dan perangkat telekomunikasi telah meningkat

perannya dalam beragam aktivitas kejahatan, mulai dari aktifitas memanipulasi database internal perusahaan, penggunaan kartu kredit orang lain dalam transaksi di internet (*carding*), penyusupan komputer, sampai aktifitas terorisme. Perlu untuk dipahami bahwa kejahatan atau kecurangan yang dilakukan melalui teknologi komputer dan koneksi internet, merupakan salah bentuk perilaku yang tidak etis dan sulit untuk dideteksi secara langsung.

Perkembangan teknologi informasi dan komunikasi, termasuk internet yang demikian pesatnya, seharusnya juga didukung oleh eksistensi hukum dan komitmen aparat penegak hukum. Produk hukum tersebut mengarah pada upaya untuk mengatur dan mengendalikan berbagai bentuk aktivitas yang dilakukan melalui komputer atau memanfaatkan koneksi internet. Hal ini bertujuan untuk memprevensi atau mendeteksi timbulnya suatu kejahatan yang dikenal dengan istilah *Cybercrime.*

Berdasarkan beberapa literatur mengidentikkan *cybercrime* sebagai Kejahatan Komputer. Hunton (2004) mendefinisi c*ybercrime* sebagai salah satu bentuk kejahatan yang dilakukan melalui penggunaan suatu jaringan komputer atau jaringan internet. Tujuannya adalah untuk mendapatkan akses ilegal jaringan komputer pihak ketiga misalnya dari agensi pemerintah, perusahaan nonprofit, perusahaan publik atau perusahaan swasta.

Budiman (2003) mengemukakan bahwa, kejahatan komputer (*Kejahatan Komputer*) dapat diklasifikasi menjadi dua yaitu; *computer fraud* dan *Kejahatan Komputer*. *Computer fraud* berkaitan dengan kejahatan atau pelanggaran dari segi sistem organisasi komputer. Sedang *Kejahatan Komputer* mengarah pada kegiatan berbahaya melalui penggunaan media komputer dalam melakukan pelanggaran hukum (*computer as a tool*).

Hall & Singleton (2007) menjelaskan bahwa kejahatan komputer dapat disebabkan oleh delapan faktor. *Pertama*, Faktor peluang atau kesempatan, Umumnya disebabkan oleh lemahnya sistem keamanan dan pengendalian internal perusahaan pada sistem operasi komputer dan internet, sehingga terdapat celah yang digunakan untuk melakukan suatu kecurangan, penyimpangan atau penyalahgunaan TI. Selain itu, hal ini juga dapat disebabkan oleh integritas pribadi yang rendah serta adanya peluang yang tinggi, akan mendorong seseorang untuk melakukan kecurangan.

Kedua, Tekanan situasional. Dalam hal ini, kecurangan atau kejahatan dapat terjadi pada kondisi seseorang sedang berada dalam tekanan situasional yang tinggi. *Ketiga*, Faktor karakter, sikap dan perilaku para pengguna TI, Faktor ini berkaitan dengan moralitas, aspek religi dan perilaku etis para pengguna TI. Artinya, walaupun ada peluang atau kesempatan dan sedang berada dalam tekanan situasional yang tinggi, namun selalu mengutamakan integritas, moral dan dampak yang ditimbulkan, maka kecil kemungkinan bagi seseorang tersebut untuk berbuat curang.

Keempat, Kurangnya independensi auditor, Kurangnya independensi auditor dapat terjadi karena auditor dikontrak oleh klien untuk melakukan aktivitas non-akuntansi misalnya jasa

konsultasi, *outsourcing* audit internal dan jasa non keuangan lain.

Kelima, Kurangnya independensi komisaris, Kurangnya independensi komisaris dapat disebabkan oleh beberapa faktor, antara lain; a) komisaris memiliki hubungan pribadi dengan dewan komisaris di perusahan lain, b) hubungan dagang sebagai pemsok atau pelanggan utama perusahaan, c) hubungan keuangan sebagai pemegang saham utama atau menerima pinjaman pribadi dari perusahaan dan d) memiliki hubungan operasional sebagai karyawan perusahaan.

Keenam, Skema kompensasi eksekutif yang meragukan, yang mengacu pada penyalahgunaan kompensasi berbasis saham oleh pihak eksekutif. *Ketujuh,* Praktik akuntansi yang tidak wajar, Terkait dengan pemilihan dan penggunaan berbagai teknik akuntansi yang tidak wajar, umumnya banyak ditemui pada kasus kecurangan laporan keuangan.

Kedelapan, Lemahnya sistem pengendalian internal perusahaan, Berbagai bentuk kecurangan, penipuan dan kejahatan TI dapat direduksi apabila perusahaan memiliki sistem pengendalian internal yang efektif, yang mampu untuk memprevensi dan mendeteksi adanya indikasi kecurangan, serta dapat membatasi ruang gerak para pelaku kejahatan.

Penyebab lain munculnya kejahatan teknologi antara lain; kompleksitas aplikasi bisnis berbasis TI dan internet, koneksi sistem informasi suatu perusahan ke suatu jaringan yang semakin bertambah, kemampuan para pengguna komputer yang semakin meningkat, kemudahan untuk memperoleh software yang dapat digunakan untuk tujuan yang tidak baik, misalnya software digunakan untuk membongkar *password*, software untuk menciptakan virus dan software untuk masuk ke sebuah jaringan internet atau situs perusahaan.

Untuk menginvestigasi dan menganalisis kedua kejahatan di atas, maka digunakan forensik teknologi informasi. Selain itu, untuk membuktikan tindak kejahatan yang menggunakan teknologi informasi, tidak hanya pihak administrator sistem informasi yang harus memahami forensik komputer, namun, para aparat penegak hukum seperti kepolisian dan lembaga peradilan serta kalangan bisnis juga perlu memahami forensik komputer.

Hall dan Singleton (2007) menyatakan bahwa, dalam mengantisipasi atau mereduksi risiko TI, manager dan auditor harus menilai risiko untuk menentukan bagaimana mempergunakan sumber daya untuk melakukan managemen risiko. Managemen risiko bertujuan untuk menyeimbangkan risiko yang berlawanan dengan kebutuhan suatu organisasi. Untuk menyeimbangkan risiko, perusahaan hendaknya melakukan penilaian risiko dengan menjalankan aktivitas yang meliputi: 1. Proses mengidentifikasi, 2. Mengukur, dan 3. Menentukan level risiko yang dapat diterima sejak tidak ada organisasi yang mampu menggunakan sumber daya untuk mengendalikan risiko hingga pada level nol.

Tiga pendekatan yang dapat digunakan dalam proses penilaian risiko TI, yaitu; 1. Mengidentifikasi ancaman/eksposur, misalnya; gangguan virus, *worm* dan *trojan*, ancaman kerahasiaan data, ketersediaan data, integritas data, ketepatan waktu, akurasi data dan infrastruktur TI; 2.

Menilai atau mengevaluasi vulnerabilitas terhadap ancaman atau eskposure, misalnya; untuk menjaga kerahasiaan data dapat dilakukan dengan membatasi akses data pada user yang tidak diotorisasi atau akses pada tempat tertentu untuk personal yang tidak diotorisasi; dan 3. Penentuan batasan level risiko yang dapat ditoleransi (menilai kemungkinan vulnerabilitas), misalnya; kesempatan akses oleh pengguna yang tidak diotorisasi sebesar 5 %.

Hunton (2004) menambahkan bahwa, metoda lain yang dapat digunakan dalam menilai risiko adalah dengan cara mengidentifikasi proses TI kemudian mengembangkan set indikator risiko yang berhubungan dengan penilaian risiko. Indikator risiko akan menentukan kebutuhan pengendalian. Indikator risiko merupakan cerminan dari pengendalian internal atau tujuan pengendalian. Perusahaan dapat mencatat keberadaan risiko indikator pada masing-masing proses TI. Hal ini bertujuan untuk menentukan apakah pengendalian diperlukan atau tidak, bergantung pada hasil analisis tentang keberterimaan suatu risiko.

Pengukuran dan penilaian risiko merupakan hal yang penting karena berkaitan dengan tindakan seorang auditor TI untuk membatasi lingkup audit dan memaksimalkan efisiensi dan keefektifan audit TI. Terkait dengan hal tersebut, terdapat beberapa cara untuk mengukur risiko. Salah satunya adalah dengan cara mengkalkulasi nilai kerugian yang diharapkan. Dengan melakukan perencanaan dan pengendalian yang efektif terhadap berbagai risiko dan potensi gangguan yang muncul, perusahaan dapat memprevensi atau mereduksi potensi terjadinya *Kejahatan Komputer*.

Keamanan dan Pengendalian Sistem Informasi Berbasis Komputer

Pada introduksi diatas telah dijelaskan bahwa aplikasi TIK dalam bisnis mengandung risiko, terutama yang berkaitan dengan masalah keamanan dan potensi gangguan. Hal ini dapat terjadi karena; 1. informasi merupakan salah satu aset berharga bagi suatu entitas bisnis; 2. TI itu sendiri juga memiliki beberapa kelemahan; 3. Heterogenitas karakter dan intensi para pengguna komputer; 4. Teknologi komputer dapat melakukan kegiatan apapun; 5. Faktor persaingan bisnis yang tidak selalu sehat; serta 6. Aktivitas yang dilakukan melalui komputer dan koneksi internet yang tidak kasat mata dan sulit untuk dideteksi.

Konsep keamanan dan pengendalian dalam sistem informasi berbasis komputer hendaknya diarahkan pada upaya perusahaan untuk; 1. mencegah atau mengantisipasi kemungkinan terjadinya kesalahan, penyimpangan atau penggunaan komputer yang tidak etis; 2. mendeteksi adanya indikasi penyalahgunaan teknologi; serta 3. mengkoreksi atau mengevaluasi sistem informasi.

Perencanaan sistem keamanan dan pengendalian sistem informasi yang baik, merupakan langkah awal dalam merancang sistem keamanan dan pengendalian sistem informasi. Perancangan sistem keamanan dan pengendalian diarahkan pada upaya untuk mengurangi ancaman dan potensi gangguan keamanan,

mereduksi risiko atau dampak negatif yang muncul dalam pengaplikasian teknologi serta untuk mengantisipasi penyalahgunaan teknologi. Untuk tujuan keamanan sistem informasi dan kelancaran aktivitas bisnis, perusahaan dapat menerapkan sistem keamanan dan pengendalian berlapis. Sistem keamanan dan pengendalian berlapis diterapkan pada masing-masing tahapan dalam sistem informasi (input, proses, *output* dan dokumentasi sistem).

Garfinkel (1995) mengemukakan bahwa keamanan komputer *(computer security*) mencakup enam aspek; 1. *privacy atau Confidentiality;* berhubungan dengan usaha untuk menjaga informasi dari orang yang tidak berhak mengakses data yang sifatnya privat dan data yang diberikan ke pihak lain untuk keperluan tertentu; 2. *integrity;* menekankan bahwa informasi tidak boleh dimodifikasi atau diubah tanpa seijin pemilik informasi; 3. *authentication;* berkaitan dengan keaslian data atau informasi, pihak-pihak yang berhak untuk mengakses data atau informasi, serta originalitas server; 4. *availability;* menyangkut aspek ketersediaan data atau informasi saat dibutuhkan*;* 5. *access control;* mengacu pada pengaturan akses informasi; serta 6. *non-repudiasi*; untuk menjaga agar seseorang tidak menyangkal telah melakukan transaksi.

Berkaitan dengan kejahatan komputer, aspek penting lain yang juga harus diketahui dan dipahami oleh perusahaan atau suatu organisasi bisnis adalah, pengenalan dan pemahaman terhadap bentuk-bentuk gangguan keamanan dalam sistem informasi berbasis komputer dan koneksi internet. Secara umum, bentuk-bentuk gangguan dalam sistem operasi komputer dan gangguan pada koneksi internet antara lain; akses ke data atau informasi secara ilegal (penyadapan, penyalinan dan pengrusakan data atau informasi), akses dan modifikasi informasi oleh pihak yang tidak memiliki autoritas, gangguan virus, worm dan *hacking*, pemalsuan nama domain dan kerusakan pada perangkat sistem informasi.

Berdasarkan penjelasan tersebut diatas dapat ditegaskan bahwa, keamanan sistem operasi komputer dan keamanan koneksi internet, merupakan hal terpenting dalam sistem informasi berbasis komputer dan jaringan internet. Prosedur *logon, login*, penggunaan PIN (*Personal Identification Number), password* (kata sandi), *access token*, penggunaan *biometric* security, daftar pengendalian akses, *firewall*, enkripsi, *steganography* (membuat informasi yang rahasia seakan-akan tidak terlihat) dan *cryptography* (persamaan matematik yang digunakan untuk enkripsi dan dekripsi), merupakan contoh bentuk-bentuk sistem keamanan dan pengendalian pada sistem operasi komputer. Keamanan sistem operasi secara keseluruhan dipengaruhi oleh bagaimana hak akses diberikan dan digunakan.

Eksistensi UU Informasi dan Transaksi Elektronik (UU ITE) No. 11 Tahun 2008

Penyusunan Undang-undang Informasi dan Transaksi Elektronik (UU ITE) yang telah ditetapkan dan disahkan pada tanggal 25 Maret 2008 lalu, merupakan wujud dukungan pemerintah dalam menyikapi perkembangan dan implementasi teknologi informasi (TI), khususnya

dalam dunia bisnis. Tentunya, penetapan UU ITE 2008 ini bertujuan agar pemanfaatan teknologi informasi dilakukan secara aman dan etis, serta mampu memprevensi, mendeteksi atau mereduksi kejahatan dan kecurangan yang dilakukan melalui penggunan teknologi informasi.

Sebagai UU pertama yang mengatur masalah TI, UU ITE dapat berfungsi sebagai; 1. *cyber law;* hukum yang mengatur terkait dengan pertukaran informasi dan transaksi elektronik melalui Internet; 2. pedoman atau arahan terhadap kegiatan komunikasi informasi dan transaksi bisnis yang dilakukan secar elektronik atau melalui internet; dan 3. pengendali terhadap kemungkinan penggunaan komputer yang tidak etis dan munculnya berbagai bentuk kejahatan atau kecurangan yang dilakukan melalui internet.

Kasus domain mustika ratu.com, *klikbca.com*, pembobolan kartu kredit, situs-situs yang mengandung unsur pornografi dan pornokasi, gangguan virus, worm dan hacking, merupakan beberapa bentuk kejahatan komputer dan perilaku pengguna yang tidak etis. Penyusunan UU ITE 2008 didasarkan pada beberapa pertimbangan, yang dikaitkan dengan perkembangan teknologi informasi.

Ada lima pertimbangan penyusunan UU ITE. *Pertama,* bahwa globalisasi informasi telah menempatkan Indonesia sebagai bagian dari masyarakat informasi dunia sehingga mengharuskan dibentuknya pengaturan mengenai pengelolaan Informasi dan Transaksi Elektronik di tingkat nasional sehingga pembangunan Teknologi Informasi dapat dilakukan secara optimal, merata, dan menyebar ke seluruh lapisan masyarakat guna mencerdaskan kehidupan bangsa.

Kedua, bahwa perkembangan dan kemajuan Teknologi Informasi yang demikian pesat telah menyebabkan perubahan kegiatan kehidupan manusia dalam berbagai bidang yang secara langsung telah memengaruhi lahirnya bentuk-bentuk perbuatan hukum baru. *Ketiga*, bahwa penggunaan dan pemanfaatan Teknologi Informasi harus terus dikembangkan untuk menjaga, memelihara, dan memperkukuh persatuan dan kesatuan nasional berdasarkan Peraturan Perundang-undangan demi kepentingan nasional.

Keempat, bahwa pemanfaatan Teknologi Informasi berperan penting dalam perdagangan dan pertumbuhan perekonomian nasional untuk mewujudkan kesejahteraan masyarakat. *Kelima*, bahwa pemerintah perlu mendukung pengembangan Teknologi Informasi melalui infra-struktur hukum dan pengaturannya sehingga pemanfaatan Teknologi Informasi dilakukan secara aman untuk mencegah penyalahgunaannya dengan memperhatikan nilai-nilai agama dan sosial budaya masyarakat Indonesia;

Eksistensi UU ITE 2008 ini diharapkan dapat memberikan kontribusi yang positif untuk aktivitas distribusi informasi dan mampu memberikan jaminan keamanan bagi individu atau suatu organisasi bisnis dalam melakukan transaksi bisnis secara *online*. Dukungan dari para penegak hukum juga sangat dibutuhkan, utamanya dalam menyikapi segala bentuk kejahatan komputer yang dilakukan oleh pihak-pihak tertentu.

Pemberian sanksi hukum yang jelas dan tegas, mental dan sikap objektif serta independensi para penegak hukum, merupakan beberapa faktor penting dalam menyelesaikan berbagai masalah terkait dengan keamanan dalam bidang informasi dan transaksi elektronik yang dilakukan oleh suatu entitas. Pemberlakuan efek jera pada para pelaku kejahatan teknologi, dapat dijadikan sebagai dasar pertimbangan bagi para penegak hukum, dalam memutuskan sanksi hukum yang tepat dan relevan dengan pelanggaran hukum yang dilakukan oleh pelaku kejahatan komputer. Tentunya hal ini bertujuan untuk membatasi ruang gerak para pelaku kejahatan dan untuk mereduksi kejahatan komputer.

Forensik Komputer

Parra (2002) mendefinisi forensik komputer sebagai suatu proses untuk mengidentifikasi, memelihara, menganalisis, dan mempergunakan bukti digital menurut hukum yang berlaku. Forensik komputer yang kemudian meluas menjadi forensik teknologi informasi masih jarang digunakan oleh pihak berwajib, terutama pihak berwajib di Indonesia. Budhisantosa (2007) memaknai forensik komputer sebagai disiplin yang mengkombinasikan elemen dari hukum dan pengetahuan komputer dalam mengumpulkan dan menganalisa data dari sistem komputer, jaringan, komunikasi nirkabel, dan perangkat penyimpanan sedemikian sehingga dapat dibawa sebagai barang bukti di dalam penegakan hukum.

McKemmish (1999) mengemukakan bahwa, pada forensik komputer atau forensik teknologi informasi, terdapat empat elemen kunci. *Pertama,* Identifikasi dari Bukti Digital. Identifikasi bukti digital merupakan tahapan paling awal forensik dalam teknologi informasi. Pada tahapan ini dilakukan identifikasi dalam hal ini bukti itu berada, dalam hal ini bukti itu disimpan, dan bagaimana penyimpanannya untuk mempermudah tahapan selanjutnya. Banyak pihak yang mempercayai bahwa forensik di bidang teknologi informasi itu merupakan forensik pada komputer. Sebenarnya forensik bidang teknologi informasi sangat luas, bisa pada telepon seluler, kamera digital, *smart cards*, dan sebagainya. Banyak kasus kejahatan di bidang teknologi informasi itu berbasiskan komputer. Tetapi perlu diingat, bahwa teknologi informasi tidak hanya komputer/ internet.

Kedua, Penyimpanan Bukti Digital. Penyimpanan bukti digital termasuk tahapan yang paling kritis dalam forensik. Pada tahapan ini, bukti digital dapat saja hilang karena penyimpanannya yang kurang baik. Penyimpanan ini lebih menekankan bahwa bukti digital pada saat ditemukan akan tetap tidak berubah baik bentuk, isi, makna, dan sebagainya dalam jangka waktu yang lama. Ini adalah konsep ideal dari penyimpanan bukti digital.

Ketiga, Analisis Bukti Digital. Analisis bukti digital meliputi analisis terhadap proses pengambilan, pemrosesan, dan interpretasi dari bukti digital merupakan bagian penting dalam analisa bukti digital. Setelah diambil dari tempat asalnya, bukti tersebut harus diproses sebelum diberikan kepada pihak lain yang membutuhkan. Pemrosesan ini memerlukan beberapa skema tergantung dari masing-masing kasus yang dihadapi.

Keempat, Presentasi Bukti Digital. Presentasi bukti digital merupakan proses persidangan, dalam hal ini, bukti digital akan diuji otentifikasi dan korelasi dengan kasus yang ada. Presentasi di sini berupa penunjukan bukti digital yang berhubungan dengan kasus yang disidangkan. Proses penyidikan ini sampai dengan proses persidangan memakan waktu yang cukup lama, maka sedapat mungkin bukti digital masih asli dan sama pada saat diidentifikasi oleh investigator untuk pertama kalinya.

Budiman (2003) menyatakan bahwa, terdapat dua metoda yang umum digunakan untuk forensik pada komputer, yaitu *search and seizure* dan pencarian informasi (*discovery information*). Dalam hal ini, investigator melakukan observasi atau pengamatan langsung ke dalam kasus teknologi informasi yang dihadapi. Diharapkan investigator mampu mengidentifikasi, menganalisa, dan memproses bukti yang berupa fisik. Investigator juga berwenang untuk melakukan penyitaan terhadap bukti yang dapat membantu proses penyidikan, tentunya di bawah koridor hukum yang berlaku.

Search dan *seizure* sendiri meliputi pemulihan dan pemrosesan dari bukti komputer secara fisik. Walaupun banyak hal yang positif, metode ini juga memberikan penekanan dan batas-batas untuk investigator agar hipotesis yang dihasilkan sangat akurat. Adapun penekanan dan batas-batas untuk investigator tersebut adalah 1. Tidak merubah bukti asli; 2. Tidak mengeksekusi program pada bukti (komputer) terutama *Operating System*-nya; 3. Tidak mengizinkan tersangka untuk berinteraksi dengan bukti (komputer); 4. Segera mungkin mem-*backup* bukti yang ada di dalam komputer tersangka. Jika pada saat diidentifikasi komputer masih nyala, jangan dimatikan sampai seluruh data termasuk *temporary* selesai dianalisa dan disimpan; 5. Merekam seluruh aktifitas investigasi; serta 6. Memindahkan bukti ke tempat penyimpanan yang lebih aman (opsional)

Penekanan batas-batas bagi investigator sangat berguna dalam pengumpulan, penanganan, dan penyimpana bukti agar dalam jangka waktu yang lama (sejak proses penyidikan sampai proses persidangan) bukti tersebut tidak berubah. Proses *search* dan *seizure* sendiri dimulai dari perumusan suatu rencana. Cara yang paling sering digunakan adalah membuat software khusus untuk mencari bukti.

Selain merupakan cara yang tepat untuk melakukan forensik teknologi informasi, pembuatan software khusus ini juga membuktikan adanya metodologi penelitian yang ilmiah. Parra (2002) menjelaskan lima tahapan dalam *search* dan *seizure* ini. *Pertama,* mengidentifikasi permasa-lahan yang sedang dihadapi untuk menentukan apakah memerlukan respon yang cepat atau tidak. Apabila tidak memerlukan respon yang cepat, maka dilanjutkan pada penelitian permasalahan.

Kedua, merumuskan hipotesis yang dilakukan setelah melakukan identifikasi permasalahan dan penelitian permasalahan. Hal ini bertujuan agar data yang didapat selama kedua proses di atas dapat digunakan untuk merumuskan hipotesis. *Ketiga,* melakukan pengujian

hipotesis secara konsep dan empiris untuk memperoleh sebuah kesimpulan. *Keempat*, melakukan evaluasi hipotesis apabila hasil pengujian tidak sesuai dengan yang diharapkan. *Kelima*, melakukan evaluasi hipotesis terhadap dampak yang lain, apabila hipotesis tersebut terbukti.

Dalam kaitanya dengan upaya untuk mereduksi *Kejahatan Komputer*, forensik komputer dapat memberikan kontribusi yang positif, terutama untuk melakukan pembuktian adanya indikasi kesalahan, penyimpangan, penggunaan TI yang tidak etis, termasuk penyalahgunaan teknologi komputer dan koneksi internet, untuk kepentingan pribadi.

Peran Auditor Forensik

Peran auditor forensik atau auditor investigasi sangat penting dalam hubungannya dengan upaya untuk mendeteksi, menganalisis dan melakukan pembuktian terhadap indikasi adanya penyimpangan, kecurangan maupun kejahatan komputer. Berkaitan dengan audit teknologi informasi, auditor teknologi informasi (TI) perlu mengetahui dan memahami peran dan fungsi operasi komputer dalam gambaran umum pengendalian. Hal ini bertujuan agar auditor TI dapat menilai berbagai resiko yang mengancam sistem akuntansi terutama yang berbasis komputer. Selain itu, pemahaman auditor TI terkait dengan operasi komputer, juga akan memudahkan auditor TI dalam melakukan pelacakan atau penelusuran terhadap faktor-faktor yang menyebabkan terjadinya penyimpangan, kecurangan atau kejahatan komputer.

Hall dan Singleton (2007) memaparkan bahwa, kegagalan sistem operasi disebabkan oleh faktor ketidaksengajaan dan faktor yang disengaja. Faktor yang tidak disengaja misalnya; kegagalan *hardware* yang menyebabkan sistem operasi gagal, kesalahan dalam program aplikasi pengguna yang tidak dapat diterjemahkan oleh sistem operasi. Kegagalan sistem yang tidak disengaja dapat menyebabkan seluruh segmen memori masuk kedalam disket atau printer, sehingga menyebabkan pengungkapan secara tidak sengaja mengenai informasi yang bersifat rahasia.

Faktor kegagalan system yang disengaja dapat berupa; 1. akses data atau informasi secara ilegal atau melanggar privasi pengguna, untuk memperoleh keuntungan pribadi; 2. gangguan virus dan worm; dan 3. pencurian atau pengrusakan data dan atau informasi. Perencanaan dan implementasi pengendalian yang dilakukan secara konservatif dapat mereduksi berbagai resiko atau ancaman terkait dengan operasi komputer (Hall dan Singleton, 2007). Kegagalan perencanaan dan implementasi pengendalian sistem operasi secara umum disebabkan karena faktor ketidaksengajaan dan faktor yang disengaja .

Aktivitas audit yang dilakukan oleh audit TI terkait dengan kegiatan transaksi yang dilakukan secara elektronik (mis. *e-business* dan *e-commerce*), bertujuan untuk: 1. Memverifikasi aspek keamanan dan integritas berbagai transaksi *e-commerce;* 2. Memverifikasi bahwa berbagai prosedur pembuatan cadangan telah cukup untuk menjaga keamanan fisik berbasis data dan integritas; 3. Memberikan keyakinan yang memadai bahwa seluruh transaksi EDI telah

diotorisasi, divalidasi dan sesuai dengan perjanjian bisnis, tidak terdapat akses data atau informasi secara ilegal, mitra dagang yang sah hanya memiliki akses ke data yang diotorisasi, dan terdapat pengendalian yang memadai untuk memastikan adanya jejak audit yang lengkap untuk semua transaksi EDI.

Bentuk-bentuk pengendalian yang dapat dilakukan antara lain; 1. Pengendalian validasi untuk memastikan bahwa kode identifikasi mitra dagang yang terkait diverifikasi sebelum transaksi diproses; 2. Pengendalian akses ke file pemasok, tingkat akses yang harus dimiliki seorang mitra dagang ke *record* basis data perusahaan dan simulasi akses dengan mengambil sampel salah satu mitra dagang dan mencoba untuk melanggar berbagai hak aksesnya; 3. Pengendalian jejak audit untuk memastikan bahwa sistem EDI menghasilkan daftar transaksi yang menelusuri berbagai transaksi melalui semua tahap pemrosesan.

Hall dan Singleton (2007) mengemukakan bahwa, auditor TI dapat melakukan berbagai uji pengendalian yaitu dengan melakukan: 1. Verifikasi semua pesan dari daftar transaksi untuk memastikan bahwa semua pesan yang mengalami gangguan telah berhasil ditransmisi ulang; 2. Verifikasi daftar transaksi untuk memastikan bahwa semua pesan telah diterima dengan urutan yang benar; 3. Kajian terhadap berbagai prosedur keamanan yang mengatur administrasi kunci enkripsi data; 4. Verifikasi proses enkripsi dengan dengan mentransmisikan sebuah pesan pengujian dan memeriksa isinya pada setiap berbagai tahap saluran, mulai dari lokal pengiriman hingga penerimaan; serta 5. Kajian kecukupan *firewall* untuk menilai keefektifan *firewall*, yang meliputi: fleksibilitas, layanan proksi, penyaringan, pemisahan sistem, alat audit, menguji kelemahan (aspek keamanan) dan menguji prosedur pengendalian *password.*

Dalam pelaksanaan audit TI, auditor TI juga dapat menggunakan bantuan software utilitas yang memfasilitasi; 1. Penilaian keamanan dan integritas; 2. Perolehan pemahaman suatu sistem aplikasi; 3. Penilaian kualitas data; 4. Penilaian kualitas program; 5. Pengembangan program; serta 6. Penilaian efisiensi operasional. *Generalized Audit Software* (GAS) merupakan *tools* major yang dapat membantu auditor TI untuk mengumpulkan dan menganalisis bukti-bukti pada sistem aplikasi.

Salah satu contoh GAS yang popular dalam kegiatan audit teknologi informasi adalah *Audit Command Language (ACL)*, sistem pakar audit, software utilitas dan software statistis. Software audit generalisasian ini dikembangkan untuk memudahkan pekerjaan auditor dalam; 1. mengumpulkan berbagai bukti-bukti dari berbagai lingkungan hardware dan software; 2. mengembangkan kapa-bilitas audit secara cepat; dan 3. meminimisasi knowledge teknis auditor yang dibutuhkan untuk memperoleh kembali dan memanipulasi data dalam sistem informasi berbasis komputer.

Secara fungsi, GAS memiliki beberapa fungsi yaitu; fungsi akses file atau data, fungsi reorganisasi file, fungsi seleksi, fungsi statistis (peyampelan dan evaluasi sampel), fungsi aritmetik (komputasi), fungsi

stratifikasi, fungsi kreasi dan pemutakhiran file dan fungsi pelaporan. Berkaitan dengan kegiatan audit, kapabilitas GAS dapat digunakan untuk menyelesaikan tugas-tugas audit untuk; 1. Menguji eksistensi, akurasi, kelengkapan, konsistensi dan ketepatan waktu pemeliharaan data dalam media penyimpanan komputer; 2. Menguji kualitas proses yang dilekatkan pada suatu sistem aplikasi; 3. menguji eksistensi isi data entitas untuk penyajian melalui pemfasilitasan observasi fisik dan penghitungan entitas melalui penyampelan statistis; serta 4. Melakukan review analitis untuk mengawasi indikator utama audit.

Di sisi lain, GAS juga memiliki beberapa keterbatasan. *Pertama*, pengumpulan bukti tidak selalu tepat waktu, karena GAS digunakan untuk memperoleh bukti pada *state* sistem aplikasi hanya beberapa waktu setelah data diproses. *Kedua*, GAS hanya dapat dijalankan dalam melakukan pengujian terbatas pada pengujian untuk memverifikasi autentisitas, akurasi dan kelengkapan proses logis. *Ketiga*, GAS memiliki keterbatasan cara untuk menentukan kecenderungan sistem aplikasi membuat kesalahan. Oleh karena itu, aplikasi GAS perlu dikelola secara wajar dan tepat, misalnya melakukan kegiatan pengembangan dan implementasi berbagai software.

Software audit spelisasian dapat dikembangkan dengan; 1. melakukan responsibilitas total untuk pengembangan dan pengimplemen-tasian software; 2. menggunakan jasa programer; dan 3. bekerja sama dengan pemasok software untuk menyediakan software yang dibutuhkan perusahaan. Satu hal yang juga perlu dipahami oleh auditor adalah, perlunya untuk mengevaluasi level pengendalian internal pada saat software audit digunakan, terutama yang berhubungan dengan masalah keamanan dan integritas.

Upaya Pengurangan Kejahatan Komputer

Eksistensi UU ITE 2008 ini diharapkan dapat memberikan kontribusi yang positif untuk aktivitas distribusi informasi dan mampu memberikan jaminan keamanan bagi individu atau suatu organisasi bisnis dalam melakukan transaksi bisnis secara online. Dalam kaitanya dengan upaya untuk mereduksi Kejahatan Komputer, forensik komputer dapat memberikan kontribusi yang positif, terutama untuk melakukan pembuktian adanya indikasi kesalahan, penyimpangan, penggunaan TI yang tidak etis, termasuk penyalahgunaan teknologi komputer dan koneksi internet, untuk kepentingan pribadi.

Peran auditor forensik atau auditor investigasi sangat penting dalam hubungannya dengan upaya untuk mendeteksi, menganalisis dan melakukan pembuktian terhadap indikasi adanya penyimpangan, kecurangan maupun kejahatan komputer. Konvergensi UU ITE 2008, penyelenggaraan forensik komputer dan keterlibatan auditor TI, merupakan langkah konkret terkait dengan upaya-upaya yang dapat dilakukan untuk mereduksi berbagai bentuk kecurangan maupun kejahatan komputer.

Kesimpulan

Pada sistem informasi berbasis teknologi komputer dan jaringan

internet, faktor keamanan dan pengendalian pada sistem informasi berbasis internet merupakan aspek penting dan utama yang perlu dikelola secara efektif. Hal ini bertujuan untuk memproteksi sistem informasi dari berbagai kemungkinan terjadinya kesalahan, kecurangan, penyimpangan, kejahatan dan penggunaan teknologi informasi yang tidak etis. Konsep keamanan dan pengendalian dalam sistem informasi berbasis komputer hendaknya diarahkan pada upaya perusahaan untuk: 1. mencegah atau mengantisipasi kemungkinan terjadinya kesalahan, penyimpangan atau penggunaan komputer yang tidak etis; 2. mendeteksi adanya indikasi penyalahgunaan teknologi; dan 3. mengkoreksi atau mengevaluasi sistem informasi.

Konvergensi UU ITE 2008, penyelenggaraan forensik komputer dan keterlibatan auditor TI, merupakan langkah konkret terkait dengan upaya-upaya yang dapat dilakukan untuk mereduksi berbagai bentuk kecurangan maupun kejahatan komputer. Tentunya dalam hal ini, juga diperlukan dukungan dari pemerintah, masyarakat dan para penegak hukum juga sangat dibutuhkan, utamanya dalam menyikapi segala bentuk kejahatan komputer yang dilakukan oleh pihak-pihak tertentu. Pemberian sanksi hukum yang jelas dan tegas, mental dan sikap objektif serta independensi para penegak hukum, merupakan beberapa faktor penting dalam menyelesaikan berbagai masalah terkait dengan keamanan dalam bidang informasi dan transaksi elektronik yang dilakukan oleh suatu entitas.

DAFTAR PUSTAKA

Anonim. 2008. *Undang-undang Informasi dan Teknologi Elektronik No. 11 Tahun 2008*. Jakarta

Budhisantosa, Nugroho. 2007. *Selintas Forensik Komputer*. www.bentengdigital.com. Tanggal akses 28 Maret 2009

Budiman, Rahmadi. 2003. *Computer Forensic; Apa dan Bagaimana*. Artikel Penelitian. Institut Teknologi Bandung.

Fejer. 2009. *Klasifikasi Kejahatan Komputer*. Artikel. www.indoskripsi.com. Tanggal Akses, 26 Maret 2009.

Garfinkel, Simson. 1995. *PGP: Pretty Good Privacy*. O'Reilly & Associates, Inc.

Hall, James A., dan Tommie Singleton. 2007. *Audit dan Assurance Teknologi Informasi***.** Edisi 2. penerbit Salemba Empat. Jakarta.

Harris, Freddy. 2007. *Kesiapan Aspek Pengaturan Perundang undangan dalam Mengatasi Permasalahan Keamanan Transaksi Melalui Internet***.** www.apricot.net, Tanggal Akses; 28 Maret 2009.

Hunton. 2004. *Core Concepts of Information Technology Auditing.* Leyh Publishing. United Stated of Amerika.

Kemmish Mc., Rodney. 1999. *What is Forensic Computing*. Australian Institut of Criminology.

www.aic.gov.au. Tanggal Akses 26 Maret 2009.

Laudon, Kenneth C., dan Jane P. Laudon. 2008. *Sistem Informasi Managemen*. Edisi 10. Penerbit Salemba Empat. Jakarta.

McKemmish, Rodney. 1999. *What is Forensic Computing*. Australian Institut of Criminology, Canberra. www.aic.gov.au. Tanggal Akses 28 Maret 2009.

Parra, Moroni. 2002. *Computer Forensic*. www.giac.org. Tanggal Akses 3 April 2009.

Rahardjo, Budi. 2005. *Keamanan Sistem Informasi Berbasis Internet*. Artikel. PT Insan Infonesia - Bandung & PT INDOCISC – Jakarta.

Rid, Reo 2008. *Model Penyerangan Sistem Komputer*. http://blog.re.or.id. tanggal Akses: 28 Maret 2009.

Weber, Ron. 1999. *Information System Control and Audit*. Penerbit Prentice Hall. New Jersey.