PENGEMBANGAN KONSEKUENSI POSITIF DARI KONTROL DETERENSI PADA METODE ANTI PEMBAJAKAN PERANGKAT LUNAK

Maimun
Fakultas Ilmu Komputer, Universitas Esa Unggul
Jalan Arjuna Utara No.9, Kebon Jeruk, Jakarta, 11510
maimun@esaunggul.ac.id

Abstract

The software is the main attraction for computer users who are useful in completing work in various fields. Software is the intellectual property and creator property that needs to be protected. But the great interest in using software has ignored factors that weaken morals and ethics to commit crime. Unwittingly, unlicensed software users have fertilized piracy crimes. Not only does this have a negative impact on the growth of the creative industry, it is also a threat of cyber crime to its users. Current anti-piracy methods emphasize preventive control as intellectual property protection, even though deterrence control is very effective in changing crime behavior. Negative consequences are not enough to have a avoidance effect, so it is necessary to develop positive consequences as a counterbalance in order to attract potential offenders to change their evil behavior. The new approach developed in deterrence control aims to increase the positive and negative consequences seen from legal, social, economic, and security factors.

Keywords*: software anti-piracy method, deterrence control, preventive control,*

Abstrak

Perangkat lunak menjadi daya tarik sendiri bagi para pengguna komputer yang bermanfaat dalam menyelesaikan suatu pekerjaan di berbagai bidang. Perangkat lunak merupakan hak kekayaan intelektual dan properti pencipta yang perlu dilindungi. Namun besarnya minat penggunaan perangkat lunak telah mengabaikan faktor yang melemahkan moral dan etika untuk melakukan tindakan kejahatan. Tanpa disadari, pengguna perangkat lunak tidak berlisensi telah menyuburkan kejahatan pembajakan. Hal ini tidak hanya membawa dampak buruk bagi pertumbuhan industri kreatif bahkan merupakan ancaman kejahatan siber bagi penggunanya. Metode anti pembajakan saat ini menekankan kontrol preventif sebagai proteksi intelektual properti, padahal kontrol deterensi sangat efektif merubah perilaku kejahatan. Konsekuensi negatif tidak cukup memberikan efek penghindaran, untuk itu perlu dikembangkan konsekuensi positif sebagai penyeimbang agar menjadi daya tarik calon pelaku untuk merubah perilaku jahatnya. Pendekatan baru yang dikembangkan pada kontrol deterensi bertujuan untuk meningkatkan konsekuensi positif maupun negatif dilihat dari faktor hukum, sosial, ekonomi, dan keamanan.

Kata kunci : metode anti pembajakan perangkat lunak, kontrol deterensi, kontrol preventif

Pendahuluan

Penggunaan perangkat lunak telah menjadi kebutuhan dasar di era teknologi infomasi. Beberapa bidang pekerjaan menuntut penggunaan perangkat lunak yang handal diantaranya pendidikan, pemasaran, periklanan, seni, dan teknik. Di dunia pendidikan misalnya, para mahasiswa dituntut untuk bereksplorasi dengan beberapa aplikasi perangkat lunak sekaligus sebagai peralatan pendukung untuk menyelesaikan tugas-tugas yang kompleks. Di dunia pendidikan misalnya, dukungan kampus dalam menyediakan perangkat lunak yang berlisensi terbatas telah direalisasi namun mahasiswa lebih tertarik memilih paket perangkat lunak bajakan yang lebih lengkap, populer dan ekonomis.

Penjualan dan penyebaran perangkat lunak tidak berlisensi dan tidak sah masih menjadi perhatian serius karena dapat memberikan ancaman serius bagi pengguna komputer dan juga berdampak pada industri kreatif pengembang perangkat lunak. Berdasarkan survey BSA tahun 2016 (BSA, 2016), sebesar 39 persen komputer di dunia terpasang perangkat lunak tanpa lisensi dan 15 persen karyawan perusahaan menyembunyikannya di kantor untuk mendukung pekerjaan mereka**.** Fakta menarik lainnya di tahun 2015, jumlah pengguna perangkat lunak tidak berlisensi di dominasi oleh negara berkembang yang berada di kawasan benua Afrika, Timur Tengah dan Asia Pasifik seperti Libia, Zimbabwe, Yaman, Bangladesh, Irak dan Indonesia sedangkan negara maju memiliki dampak kerugian ekonomi tertinggi dari perangkat lunak illegal seperti Amerika Serikat sebesar USD 9.095 kemudian diikuti oleh negara Cina USD 8.657 dan India USD 2.684.

Menurut laporan dari Symantec tahun 2015, jumlah kejahatan siber dengan menanamkan malware meningkat cukup siginifikan antara lain Ransomware naik 35 persen, Mobile App Malware naik 77 persen, dan Web Malware naik 300 persen (Symantec, 2016). Perangkat lunak asli telah dibongkar dan dimodifikasi oleh para hacktivism kemudian ditanamkan virus dan malware untuk menginfeksi komputer korban dimulai saat terpasang di komputer mereka. Penjahat siber dengan mudah dapat menganalisa trafik, memory, database dan log files untuk mencuri informasi pribadi dan data kredensial seperti biodata, kata sandi, rekening bank.

Beberapa metode anti pembajakan telah diterapkan secara bersamaan dan berlapis untuk melindungi perangkat lunak dari ancaman penggunaan yang tidak sah, keaslian produk, kelengkapan layanan, hak intelektual properti pengembang, dan serangan siber. Metode anti pembajakan dengan menerapkan kontrol preventif dan deterensi diperkenalkan sebelumnya (Gopal dan Sanders, 1997) melalui jurnalnya pada tahun 1997. Menurut mereka, kontrol preventif membutuhkan dukungan keuangan untuk membangun teknologi anti pembajakan sedangkan kontrol deterensi menggunakan pendekatan moral dan emosi dengan menciptakan rasa bersalah dan rasa malu dari perilaku kriminal seseorang. Selain itu, Korhonen juga menjelaskan tentang metode preventif yang tidak hanya melibatkan tindakan teknis saja tetapi menambahkan tindakan etika, dan legal di dalamnya. (Korhonen, 2015).

Penulis memiliki ketertarikan untuk membahas tentang kontrol preventif dengan mengklasifikasikan beberapa tipe pembajakan terbaru kemudian memfokuskan pada pengembangan konsekuensi pada kontrol deterensi. Pendekatan dengan kontrol deterensi diharapkan akan lebih efektif untuk meredam perilaku manusia sebelum kejahatan terjadi dengan menimbang konsekuensi yang akan diterima baik positif dan negatif dengan melihat faktor hukum, sosial, ekonomi, dan keamanan.

Metode Penelitian

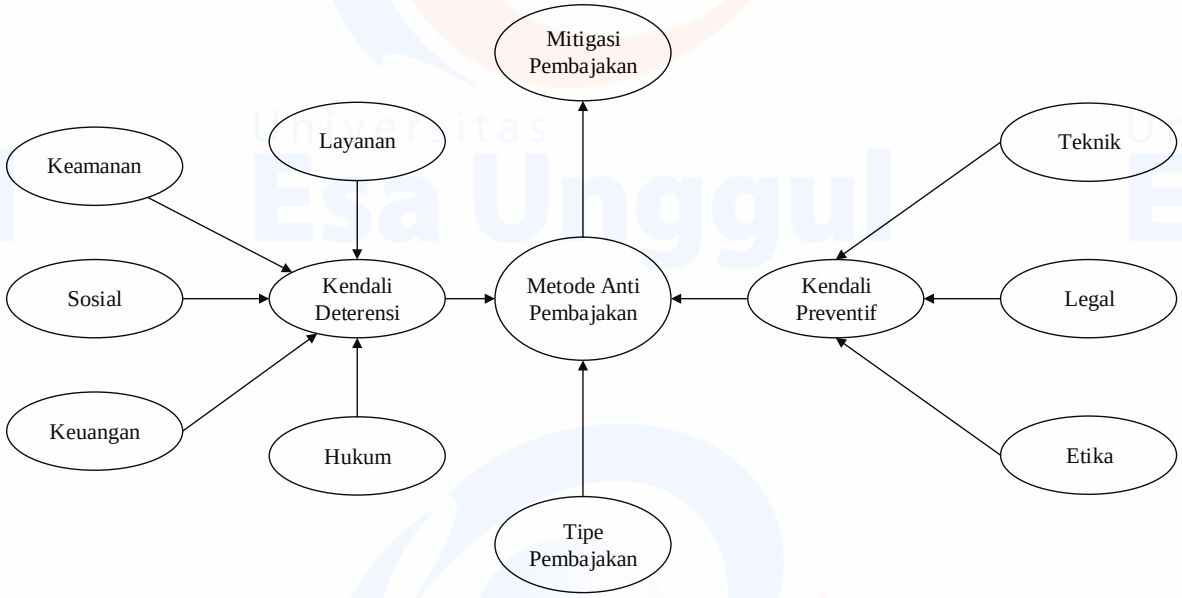
Metode anti pembajakan saat ini terdiri dari kontol preventif dan kontrol deterensi. Penulis mengadopsi metode preventif (Korhonen, 2015) dan kontrol deterensi (Gopal dan Sanders, 1997) kemudian dikembangkan dengan cara mengklasifikasikan kembali tipe pembajakan perangkat lunak sebagai dasar penentuan kontrol. Pada kontrol deterensi ditambahkan konsekuensi positif dan negatif yang didasarkan pada faktor hukum, sosial, ekonomi dan keamanan (Gambar 1). Kontrol preventif adalah kontrol terdepan dalam proteksi intelektual properti pemilik, penggunaan yang tidak sah, dan pengerusakan perangkat lunak. Kontrol ini tidak hanya menerapkan pendekatan teknis saja melainkan memerlukan pendekatan etika dan hukum. Industri perangkat lunak terlebih dahulu harus memahami tipe pembajakan yang berkembang saat ini kemudian menerapkan kontrol yang efektif, bukan semua kontrol, untuk mengatasi pembajakan secara efektif.

Tipe Pembajakan Perangkat Lunak

Beberapa pembajakan tidak hanya dilakukan oleh pelaku kejahatan murni seperti hacker yang bertujuan menguasai dan menyebarkan untuk kepentingan pribadi tetapi pengguna atau end-user tanpa disadari juga melakukan tindakan pembajakan. Seorang pekerja dari sebuah perusahaan dapat menjadi tersangka pembajakan bila penggunaan perangkat lunak tidak sesuai "*License*

Agreement "yang biasa ditemukan saat audit berkala.

Pengukuran yang dilakukan tahun 1997 (Gopal dan Sanders, 1997), ada empat faktor yang memperngaruhi seseorang melakukan pembajakan yaitu kurangnya informasi tentang konsekuensi hukum, indeks etika yang rendah, pelaku pria lebih banyak dibandingkan dengan wanita dan usia muda lebih berpeluang melakukan pembajakan.



Gambar 1
Klasifikasi Tipe Pembajakan dalam Penentuan Kontrol Deterensi dan Preventif

Survey BSA menginformasikan beberapa tipe pembajakan yang menjadi perhatian para pengembang. (BSA, 2014). Korhonene dalam papernya telah merangkum teknik pembajakan baik menggunakan software maupun hardware. (Korhonen, 2015).

1) *Mischanneling*
   Pembajak menggunakan lisensi yang tidak sesuai dengan License agreement, misalnya lisensi akademis yang digunakan untuk tujuan komersial. Tipe pembajakan ini hanya memanfaatkan kelemahan proteksi.
2) *Softlifting*
   Tipe ini menyalahgunakan lisensi dimana lisensi digunakan secara bersamaan untuk beberapa komputer. Kondisi ini sering digunakan oleh end user yang memiliki 2 komputer lebih ataupun perusahaan yang memiliki komputer client yang banyak.
3) *Hard-disk Loading*
   Penyalinan harddisk atau image untuk digunakan pada harddisk lainnya dengan menggunakan lisensi yang sama. Beberapa provider komputer sering melakukan hal ini dalam penjualan komputer baru atau tujuan komersial lainnya agar menarik pelanggan.
4) *Client Server Overuse*
   Perusahaan menggunakan server yang tersentralisasi untuk menyediakan perangkat lunak bagi client sehingga dapat diinstalasi secara bersamaan melalui jaringan. Namun hal ini dapat dikategori pelanggaran bila lisensi tersedia untuk sejumlah komputer yang ter-*install*.
5) *Cracking dan Serial*
   Pengguna perangkat lunak bajakan sangat popular dengan teknik pembajakan ini.Software free trial atau evaluasi dapat digunakan tanpa batasan waktu dengan mengelabuhi sistem proteksi menggunakan file crack. File crack adalah file yang telah dimodifikasi dengan tool debugger . Sedangkan Serial palus dapat dihasilkan dari pembangkit kunci dengan membongkar sistem enkripsi dari perangkat lunak.

6) *Internet dan Cloud Piracy*
   Bentuk pembajakan ini memanfaatkan internet sebagai media distribusi perangkat lunak bajakan. Pengguna disediakan link untuk mengunduh secara bebas atau melakukan pertukaran perangkat lunak pada website tertentu atau menggunakan jaringan peer to peer untuk transfer. Pembajak dapat melakukan web attack untuk mendapat versi evaluasi yang dapat dimodifikasi tanpa perlu lisensi. Media penyimpanan virtual atau cloud storage juga dapat dimanfaatkan untuk mendistribusikan perangkat lunak bajakan.
7) *Counterfeiting*
   Tujuan dari pembajakan ini adalah menyisiplan kode malicious kemudian menghilangkan proteksi anti tamper sehingga terlihat absah. Setelah proteksi dihilangkan, perangkat lunak dengan mudah di duplikasi, didistribusi dan dijual dengan memasukkan materi copyrightnya seperti manual, license agreement, label, kartu registrasi dan fitur keamanan.
8) *Hardware Piracy*
   Teknik pembajakan menggunakan perangkat keras meliputi execution trace analysis, mod-chip spoofing device dan machine emulator. Analisis trace bertujuan mengumpulkan informasi dari log perangkat lunak kemudian memprediksi enkripsi, perangkat spoofing mod-chip melakukan pemantauan sinyal pada jalur transaksi di memori, dan mesin emulator adalah alat untuk melewati otorisasi dari sistem proteksi perangkat lunak.
9) *Reverse Engineering*
   Tool yang digunakan dalam reverse engineering adalah debugger, disassambler dan decompiler. Debugger melakukan analisis pada hexadesimal, disassambler melakukan eksekusi kode assambler dan decompiler memodifikasi original code menjadi source code baru.
10) *Tampering*
    Tipe pembajakan ini memerlukan perhatian lebih karena tampering melakukan modifikasi pada perangkat lunak untuk tujuan merusak, mengendalikan dan mencuri aset dari pengguna. Pembajak menanamkan unwanted program seperti virus ataupun malware didalamnya sebagai otomatisasi modifikasi.

Penerepan Kontrol Preventif

Setelah mengetahui tipe pembajakan, kontrol apa saja yang perlu diterapkan menjadi tantangan bagi pengembang. Untuk menentukan penerapan kontrol preventif ada tiga pendekatan (Cronin, 2003) yaitu etika, legal dan teknik.

1) Pendekatan Etika
   Kontrol ini bertujuan untuk membangun, memperbaiki sikap moral, perilaku, pola pikir masyarakat terhadap aksi pembajakan. Bila indeks etika meningkat, seseorang akan memiliki rasa bersalah dan rasa malu untuk melakukan aksi melawan hukum. Pendekatan etika meliputi edukasi etika, kampanye anti pembajakan, pemberian amnesti, penggunaan *free trial* atau *online access*. Edukasi etika membangun pola pikir masyarakat bahwa yang mereka lakukan merugikan orang banyak atau ekonomi nasional. Masyrakat harus mengerti tentang kompensasi bagi pemilik intelektual properti dan keuntungan penggunaan perangkat lunak berlisensi. Kampanye anti pembajakan lebih menginformasikan tentang perbuatan yang boleh dan tidak terhadap penggunaan perangkat lunak. Menurut jurnal (Higgins, dkk., 2005) menyatakan bahwa 89 persen pengguna perangkat lunak dari kalangan mahasiswa tidak mengetahui informasi tentang larangan, hukuman dan etikanya. Pemberian amnesti adalah sikap memberi kesempatan kepada pelaku pembajakan untuk menghentikan aksinya tanpa mendapat penahanan. Selain itu, pengembang juga dapat memahami kerentanan dari sistem proteksinya untuk diperbaiki. *Software Trial* atau *Online Access* kini telah banyak diterapkan oleh perusahaan dengan memberikan kesempatan kepada calon pengguna perangkat lunak untuk mengunduh *software trial* dengan batasan waktu agar pengguna dapat mengeksplor fitur dan kehandalannya tanpa harus menggunakan bajakan. Bahkan beberapa perusahaan telah menyediakan akses online secara gratis tanpa harus menginstal dan menggunakan lisensi pada komputer mereka.

2) Pendekatan Legal

Legal adalah pernyataan hak cipta seseorang dan hak kepemilikan yang sah atas produk yang berkekuatan hukum. Pelanggaran atas hak ciptaa akan menghadapi sanksi hukum berupa denda atau penjara. Aksi ini membutuhkan dukungan dari pemerintah sebagai pembentuk undang-undang. Perundang-undangan Indonesia telah mengatur tentang hak kekayaan intelektual dan properti yaitu UU Hak Cipta No.28 tahun 2014 dan tentang penggunaan teknologi dan transaksi elektronik yaitu UU ITE No.11 tahun 2008. Produk intelektual tidak hanya berlaku nasional, organisasi dunia juga telah mengatur hak intelektual dan properti melalui World Intelectual Property Organization.

Copyright merupakan hak legalitas pencipta atas intelektual properti untuk memberikan salinan atau publikasi kepada pengguna perangkat lunak secara sah. *Copyright* memiliki sanksi hukum bagi yang menyalin secara tidak sah atau membajak tanpa sepengetahuan pemilik intelektual properti. Pada era online, international copyright juga diatur untuk memperluas publikasi ke seluruh dunia terutama distribusi melalui Internet.

Paten adalah hak eksklusif yang diberikan kepada seseorang atas penemuannya berupa teori, metode, perangkat lunak, mesin, dll untuk membuat, mendistribusi dan memakai atas namanya sendiri. Produk yang telah dipatenkan tidak dapat dikembangkan oleh orang lain dan berlaku pada waktu dan tempat tertentu.

End User License Agreement (EULA) diberikan oleh pengembang kepada user berupa perjanjian tertulis bahwa pengguna perangkat lunak akan mematuhi dan menyetuji aturan yang tertuang dalam lisensi. Persetujuan lisensi berkekuatan hukum dan bila terjadi pelanggaran dapat dikenakan sanksi hukum.

Policy adalah aturan yang diterapkan pada perusahaan untuk mengatur penggunaan perangkat lunak berlisensi untuk menjaga komitmen dalam mematuhi hukum. Software asset management (BSA, 2014) efektif mengurangi penggunaan perangkat lunak bajakan oleh karyawan. Sentralisasi layanan perangkat lunak akan mengurangi dampak pembelian, upgrade perangkat lunak yang tidak sah. Audit rutin merupakan bentuk pemantauan terhadap perangkat lunak tidak sah dan menjaga layanan terbaru.

3) Pendekatan Teknik

Pembongkaran proteksi perangkat lunak terhadap teknik proteksi seperti enkripsi, *copyright* dan manipulasi lisensi telah membuat gerah pengembang perangkat lunak. Aktivitas illegal tersebut mampu mencari celah untuk membongkar proteksi. Perusahaan harus mengeluarkan dana cukup besar untuk meningkatkan pertahanan akibatnya pengembang memasang harga tinggi untuk produkny. Harga perangkat lunak yang tinggi juga memicu suburnya pembajakan khususnya beberapa negara berkembang yang memiliki tingkat perekonomina rendah. Menurut Holleyman (Holleyman, 2012), penjualan komputer yang berisi perangkat lunak berlisensi di Amerika mengalami penurunan signifikan antara tahun 2006 hingga 2010.

Obfuscation merupakan teknik anti pembajakan yang bertujuan mengelabuhi tipe pembajak seperti reverse engineering ataupun tampering dengan mengubah bentuk source code, byte code atau binary executable code sebenarnya menjadi kabur tanpa mengubah operasinya sehingga menjadi sulit dianalisa. Teknik ini bukan untuk melindungi tapi menyembunyikan mekanisme proteksi yang ada.

Tamper Proofing adalah teknik melawan tampering. Saat terjadi tampering, kode anti tampering memeriksa apakah source code masih sama, bila tidak program akan menjadi malfunction atau tidak berfungsi. Mekanisme anti tampering adalah dengan melakukan pengecekan kode, pengawasan, peremajaan, dan penggunaan kriptografi.

Encryption digunakan untuk melindungi kode eksekusi dengan menggunakan program enchiper. Untuk membuka kode terenkripsi membutuhkan pertukaran kunci publik. Kendalanya pembajak dapat mencari celah untuk mendapatkan kunci publik tersebut. Untuk itu perlu update versi sistem secara berkala untuk menghasilkan pasangan kunci yang berbeda.

Watermarking / Fingerprinting bertujuan memunculkan identitas kepemilikan intelektual properti yang sah dengan menanamkan copyright kedalam kode perangkat lunak. Dinamis watermark disimpan dalam dynamic state lebih responsif dan aman dibandingkan statis watermark yang disimpan di aplikasi eksekutabel. Fingerprinting mengidentifikasi sistem yang dijalankan oleh program.

Guards melakukan pengawasan saat program berjalan dan memastikan bebas dari tampering. Software Agent dapat ditempatkan di jaringan untuk mengawasi program eksekusi. Guards juga menerapkan checksum terhadap kode agar untuk mengetahui bila ada modifikasi.

Tethering digunakan untuk melakukan pembacaan identitas komputer seperti kode aktivasi produk. Identitas yang terbaca adalah Mac Address dan ID CPU yang akan dikirimkan ke vendor system operasi.

Token digunakan sebagai otentikasi sah untuk mengakses program. Token menggunakan media perangkat keras seperti CD, Dongle ataupun smart card. Token dengan perangkat lunak berupa license key atau kode aktivasi.

Setelah mengetahui tipe pembajakan diatas, perusahaan pengembang dapat menempatkan kontrol preventif yang tepat. Rekomendasi penempatan kontrol untuk mengatasi tipe pembajakaan, dapat melihat tabel 1.

Tabel 1.
Penerapan Kontrol Preventif berdasarkan TIpe-tipe Pembajakan

Tipe Pembajakan	Tujuan	Penerapan Kontrol Preventif		
		Etika	Legal	Teknik
Mischanneling	Penggunaan lisensi yang tidak sesuai	Shareware /Free Trial Kampanye	Regular Audit License agreement	Encryption Simple Checking
Client Server Overuse	Server mendistribusi software ke client melebihi jumlah lisensi	Kampanye	License agreement Regular Audit	Simple Checking Watermarking Observation
Softlifting	Copyright digunakan pada banyak komputer	Shareware /Free Trial Kampanye	License agreement Copyright Regular Audit	Tethering Simple Checking
Hardisk Loading	Menyalin image untuk digunakan pada komputer lain	Amnesti Kampanye	License Agreement Copyright Regular Audit	Simple Checking Watermarking
Cracking & Serial	Membongkar proteksi dengan kode lisensi palsu / patch	Kampanye Amnesti	License Agreement Regular Audit	Obfuscation Simple Checking
Internet Piracy	Mendistribusikan software bajakan melalui internet	Shareware /Free Trial Amnesti Kampanye	International Copyright Paten Regular Audit	Watermarking Simple Checking Encryption
Counterfeiting	Memasukkan kode *malicious*, menghapus proteksi, distribusi dan menjual copyright	Kampanye Amnesti	Regular Audit Patents	Obfuscation Simple Checking Observation

Tipe Pembajakan	Tujuan	Penerapan Kontrol Preventif		
		Etika	Legal	Teknik
Hardware Piracy	Membongkar proteksi dengan teknik analisis trace, spoofing device dan machine emulator	Kampanye Amnesti	Regular Audit Copyright	Simple Checking Encryption Watermarking
Reverse Engineering	Menggunakan tool debugger, disassembler, decompiler	Kampanye Amnesti	Regular Audit Copyright Paten	Obfuscation Observation Watermarking Encryption
Tampering	Memodifikasi kode secara manual atau otomatis dengan virus	Kampanye Amnesti	Regular Audit Copyright	Obfuscation Observation Simple Checking

Kontrol deterensi telah dikenal dalam dunia kriminologi untuk mengatasi tingkah laku manusia yang cenderung melawan hukum seperti pembajakan intelektual dengan memberikan efek jera agar tidak melakukannya kembali. (Sherizen, 1993). Kontrol preventif bertujuan lebih kepada bagaimana melindungi aset intelektual properti dan membutuhkan dukungan keuangan untuk meningkatkan teknik proteksi sedangkan metode deterensi menggunakan pendekatan emosi dan moral untuk menciptakan konsekuensi lebih besar baik positif maupun negatif meliputi hukum, sosial, ekonomi, keamanan dan layanan.

Sanksi atau Penghargaan

Pelaku pembajakan akan menerima konsekuensi hukum apabila melakukan tindak kejahatan yang tertera dalam undang-undang. Konsekuensi hukum yang diterima oleh pelaku pencurian intelektual properti bervariasi di setiap negara. Penerapan hukuman disesuaikan besarnya tindakan kejahatan yang dilakukan seperti ancaman penjara dan pembayaran pinalti atau denda. Sanksi hukum berdasarkan UU HAKI di Indonesia, pelanggaran ringan hak cipta akan dikenakan pidana penjara 1 tahun dan/atau denda Rp.100.000.000,- (seratus juta rupiah) sedangkan pelanggaran berat hak cipta dalam bentuk pembajakan akan dihukum paling lama 10 tahun dan denda paling banyak Rp. 4.000.000.000,- (empat milyar rupiah). (BSA, 2016). Berdasarkan Hukum Copyright Amerika Serikat, tindak pidana berupa pengerusakan proteksi copyrigh dihukum penjara maksimal 5 tahun dan/atau denda maksiml USD 500.000,- (lima ratus ribu us dollar). (United States Constitution, 2016).

Konsekuensi tersebut di atas berdampak negatif bagi pelaku tindak pidana, hal ini terlihat tidak cukup adil bagi masyarakat yang tidak melakukan tindak pidana. Perlu adanya penerapan konsekuensi positif sebagai pilihan agar masyarakat lebih menerima konsekuensi positif. Penerapan konsekuensi positif dapat berupa reward atau bonus.

Reward dapat diberikan kepada masyarakat yang melaporkan adanya tindakan pembajakan. BSA melalui websitenya telah menerapkan program "Report Software Piracy Now !" di tahun 2017. (BSA, 2017). BSA menjamin laporan yang diterima bersifat rahasia kecuali diperlukan oleh kepolisian. Pelapor diharapkan adalah masyarakat dan pekerja dari sebuah perusahaan yang tidak mematuhi hukum. Reward yang diberikan adalah hingga USD 250.000,- (dua ratus lima puluh ribu dollar) tergantung besaran kontrak penyelesaian sengketa.

Pengasingan atau Penghormatan

Masyarakat yang memiliki cara berfikir rasional memiliki kemampuan untuk menimbang sebuah perilaku kejahatan. Indeks moral dan etika di masyarakat dipengaruhi oleh sikap religius, tingkatan pendidikan, budaya dan hubungan sosial walaupun ada faktor lain yang mempengaruhi seperti psikologi dan ekonomi dan sebagainya. Teori deterensi (Siponen, dkk., 2012) menyatakan

bahwa sanksi, rasa malu dan bersalah serta sikap moral dapat mengatasi pembajakan perangkat lunak.

Pengasingan masyarakat merupakan dampak sosial bagi pelaku kejahatan. Pelaku akan merasa takut untuk dikutuk, diabaikan, diasingkan oleh masyarakat atas tindak kejahatan. Para penjahat atau mantan narapidana lebih sulit diterima oleh masyarakat setelah mereka keluar dari penjara. Untuk kejahatan dunia maya, pembajakan perangkat lunak dapat diperlakukan seperti halnya kejahatan dunia nyata. Sosial media salah satu cara yang pernah diterapkan aplikasi iOS dengan mengirimkan pesan Tweet secara otomatis saat aplikasi bajakan digunakan.

Penghormatan adalah sikap positif perusahaan yang diberikan kepada pekerjanya yang mampu melindungi aset perangkat lunak dan berkomitmen menggunakan lisensi yang sah terhadap penggunaan perangkat lunak. Perusahaan dapat memberikan penghargaan terhadap pekerja yang bersikap taat hukum sebaliknya apabila menemukan pekerjanya melakukan pengunduhan perangkat lunak secara tidak sah di Internet dapat diberikan sanksi teguran hingga pemecatan yang memberikan efek malu dan moral dihadapan rekan kerjanya.

Rugi atau Untung

Penggunaan perangkat lunak bajak tidak hanya memberikan dampak ekonomi bagi pengembang tetapi dampak ekonomi juga dirasakan oleh pengguna. Sering kali perangkat lunak bajakan tidak sesuai ekspetasi pembeli bajakan.

Kerugian penggunaan perangkat lunak bajakan adalah program sering kali mengalami kendala error, bug atau kegagalan program. Tidak adanya dukungan layanan lengkap seperti patch, upgrade, customer support, dokumentasi teknik, dan pelatihan online mengurangi kenyamanan dan kehandalan dari produk. Pengguna bajakan terpaksa harus mengeluarkan dana lebih untuk membeli dan mengunduh versi bajakan terbaru. Hal ini menambah daftar kerugian dari penggunaan perangkat lunak bajak

Keuntungan penggunanan perangkat lunak berlisensi adalah jaminan keaslian produk, dukungan layanan lengkap, kenyamanan dan kepuasan pelanggan, minimnya kerugian finansial. Selain itu penggunaan perangkat lunak berlisensi mendukung penegakan hukum, memberikan hak intelektual properti bagi pencipta dan meningkatkan perekonomian nasional termasuk di dalamnya sumber daya manusia, pembangunan industri kreatif, mengurangi biaya produksi.

Bahaya atau Aman

Pembobolan perangkat lunak menggunakan teknik tampering menanamkan program otomatisasi modifikasi. Unwanted program ini dapat berupa virus, worms, trojan dan spyware yang bertujuan mencari celah kerentanan. (BSA, 2009). Teknik *tampering* ini dapat diantisipasi dengan penggunaan patch dan update namun karena perangkat lunak bajakan tidak dilengkapi layanan teknis maka kemungkinan besar perangkat lunak bajakan menjadi tidak aman.

Bahaya penggunaan bajakan adalah ancaman keamanan dari infeksi program malicious atau malware yang dapat merusak perangkat komputer atau pun pencurian informasi. Saat komputer melakukan pengunduhan secara tidak sah, website pembajak memanfaatkan malware untuk menginfeksi jaringan dan memori dari korban.

Hasil survey oleh BSA, hubungan pembajakan perangkat lunak dengan infeksi malware adalah berbanding lurus. Infeksi malware pada perangkat lunak bajakan banyak ditemukan kasusnya di beberap negara maju seperti Turki, Spanyol, Rusia, Brasil. Website yang menyediakan perangkat lunak bajakan terinfeksi malware sekitar 25 persen. (BSA, 2009).

Untuk keamanan, pemilihan penggunaan perangkat lunak harus memperhatikan sumber penyedia layanan penjualan atau vendor yang sah. Pembelian online juga harus memastikan website yang diakses adalah asli bukan fake website dan menggunakan secure http (https). Transaksi finansial di internet bisa menjadi target serangan untuk mencuri informasi pribadi dan rekening bank atau kartu kredit. Data dari survey BSA, 53 persen produk yang dibeli tidak sesuai pesanan, 36 persen produk tidak bekerja, 14 persen bajakan, dan 12 persen tidak diterima.

Kesimpulan

Perangakat lunak merupakan hak intelektual properti seseorang yang perlu dilindungi. Industri komputer terus meningkat dan membutuhkan daya intelektual untuk menciptakan perangkat yang dapat mendukung pekerjaan pengguna komputer. Oleh karena itu, sikap moral yang harus ditanamkan adalah bagaimana menggunakan perangkat lunak tersebut sebijak mungkin tanpa harus mengorbankan karya seseorang. Indeks moral yang tinggi dapat menjaga emosi diri untuk menahan melakukan tindak kejahatan.

Konsekuensi negatif selalu menjadi andalan bagai pengembang untuk memberikan efek jera. Manfaat yang diterima dari penggunaan, penyebaran, dan pembajakan perangkat lunak tidaklah sebanding dengan efek negatif nya seperti sanksi hukum, pengasingan sosial, kerugian layanan dan bahaya infeksi virus atau *malware*.

Namun konsekuensi positif memberikan efek yang lebih menarik kepada pelaku kejahatan. Perilaku jahat dapat diredam dengan memberikan pilihan yang rasional dan memperbaiki moral dengan tindakan positif seperti mendapatkan reward, penghormatan sosial, dukungan layanan penuh dan aman dari kejahatan siber. Pengembangan konsekuensi positif ini masih dapat dikembangkan kembali melalui penelitan yang intensif untuk mendapatkan solusi terbaik dan efektif dalam mengurangi tindakan pembajakan.

Daftar Pustaka

Anckaert, B., Sutter, B. D., Bosschere, K. D. (2004). Software Piracy Prevention through Diversity. *In Proceedings of the 4th ACM workshop on Digital Rights Management – DRM'04*. p. 63. New York. USA. Diakses dari http://doi.org/10. 1145/1029146.1029157

Business Software Alliance. (2009). Software Piracy on the Internet: A Threat to Your Security. The Business Alliance Diakses dari http://portal.bsa.org/internet report2009/2009internetpiracy report.pdf

Business Software Alliance. (2014). Software Asset Management Guide. The Business Alliance Diakses dari http://www.bsa.org/~/media/Files/Tools_And_Resources/Guides/Software ManagementGuide/ SoftwareManagementGuide_English.pdf

Business Software Alliance. (2016). Seizing Opportunity Through License Compliance: BSA Global Software Survey. The Software Alliance. Diakses dari http://globalstudy.bsa. org/2016/downloads/studies/ BSA_GSS_US.pdf.

Business Software Alliance. (2017). Report Software Piracy Now. The Business Alliance. Diakses dari https://reporting.bsa.org.

Cronin, G. (2003). A Taxonomy of Methods for Software Piracy Prevention. Dept. of Comp. Science, University of Auckland. New Zealand. Diakses dari http://profs.sci.univr.it/~giaco/download/Watermarking-Obfuscation/piracytaxono my.pdf

Higgins, G. E., Wilson, A. L., Fell, B. D. (2005). An Application of Deterrence Theory to Software Piracy. *Journal of Criminal Justice and Popular Culture*. vol. 12(3), pp. 166-184.

Korhonen, J. (2015). Piracy Prevention Methods in Software Business. B.S. thesis, Dept. of Information, University of Oulu, Oulu, Finland. Diakses dari http://jultika.oulu.fi/files/nbnfioulu-201605131733.pdf

Siponen, M., Vance, A., Willison, R. (2012). New Insights into The Problem of Software Piracy: The Effect of Neutralization, Shame, and Moral Beliefs. *Journal Information and*

Management. vol. 49. pp. 334-341. Diakses dari http://dx.doi.org /10.1016/ j.im.2012.06.004.

Presiden Republik Indonesia. (2014). Undang-undang Nomor 28 tentang Hak Cipta. Indonesia.

Gopal, R. D., Sanders, G. L. (1997). Preventive and Deterrent Controls for Software Piracy. *Journal of Management Information Systems*. vol. 13. no. 4. pp. 29-47.

Holleyman, R. (2012). Software Prices and Piracy in the Developing World: Correlation vs. Causation. BSA TechPost. Diakses dari http://techpost.bsa.org /2012/02/07/software-prices-and-piracy-in-the-developing-world-correlation-vs-causation/

Sherizen, S. (1993). Can Computer Crime be Dettered?. *In Proceeding of Conference, Defense Personnel Security Research Center*. pp. 15-26.

Symantec. (2016). Internet Security Threat Report. Symantec Corp., USA. vol. 21. Diakses dari https://www.symantec.com/content/dam/symantec/docs/reports /istr-21-2016-en.pdf

United States Constitution. (2016). Copyright Law of the United States and Related Laws Contained in Title 17 of United States Code. USA. Diakses dari https:// www.copyright.gov/title17/title17.pdf