پیشگیری وضعی از نقض اسرار تجاری در فضای سایبر

عبدالرضا جوان‌جعفری[1]
دانشیار گروه حقوق دانشگاه فردوسی مشهد
امیرسودمندراد[2]
کارشناس ارشد حقوق جزا و جرم شناسی دانشگاه فردوسی مشهد

تاریخ دریافت: 1393/8/17 تاریخ پذیرش: 1394/9/8

چکیده

چالش‌های بسیاری که فضای تبادل اطلاعات، فراروی اسرار تجاری به‌عنوان اطلاعاتی ارزشمند پدیدآورده است، دخالت گسترده دولت‌ها را در به‌کارگیری ابزارهای قهرآمیزی که دارای آثار بازدارندگی قوی‌تری باشد به همراه دارد. لکن ویژگی‌های منحصربه‌فرد فضای سایبر به همراه تنوع شیوه‌های سوءاستفاده از اسرار تجاری، امکان شناسایی نقض‌کننده حق را به حداقل رسانیده و موجب طرح این ایده گردیده است که سیاست کیفری جاری قابلیت اثربخشی لازم در زمینه حمایت از اسرار تجاری را ندارد. لذا دارندگان اسرار تجاری به‌منظور حفاظت از اطلاعات حیاتی خود ناگزیر به استفاده از پویاترین ابزارهای امنیتی موجود می‌باشند؛ مضافاً آن‌که قانون‌گذار بخشی از هزینه پیشگیری از جرم را بر دوش آنان قرار داده است. این موضوع رسالتی است که پژوهش حاضر در قالب بررسی تدابیر پیشگیرانه وضعی در صدد شناسایی روش‌های متنوع آن است. هرچند در ادامه به این جمع‌بندی می‌رسیم که اسرار تجاری به دلیل دارا بودن ارزش مالی یا رقابتی بسیار، همواره مورد توجه نفوذگرانی است که با استفاده از پیشرفته‌ترین بدافزارهای موجود اقدام به دستیابی چنین اطلاعاتی می‌نمایند و بزه‌دیدگان به‌ندرت توانایی مقابله با آنان را دارند. لذا دارنده به‌منظور رسیدن به یک امنیت قابل قبول، نیازمند حمایت‌های مضاعفی از سوی برخی نهادهای دولتی و غیردولتی است که ارائه پیشنهادهایی در این زمینه، پایان‌بخش مباحث مطرح شده در این نوشتار خواهد بود.

---

1 - نویسنده مسئول javan-j@um.ac.ir

2- soodmandrad@gmail.com

کلیدواژه‌ها: اسرار تجاری، فضای سایبری، امنیت اطلاعات، پیشگیری وضعی، دسترسی غیرمجاز.

طبقه‌بندی JEL: k14، k22، k42

1. مقدمه

ورود به عصر فناوری اطلاعات و ارتباطات دوران نوینی از زندگی بشر را که از آن به‌عنوان جامعه اطلاعاتی یاد می‌شود، به وجود آورده است. فضای سایبر به عنوان نمادین‌ترین محصول این جامعه، فرصت‌های بی‌بدیلی را در اختیار انسان قرار داده است تا بتواند حجم انبوهی از اطلاعات را در آن جستجو کرده یا ذخیره نماید. این روند به نوعی موجب درخشان‌تر شدن چهره اطلاعات به‌ویژه یافته‌های علمی و اقتصادی گردیده است. دستیابی غیرمجاز به چنین اطلاعات ارزشمندی سیر صعودی حملات هدفمند سایبری را در چند سال اخیر به دنبال داشته است. در این میان، اندیشه حمایت از اسرار تجاری به عنوان اطلاعات دارای ارزش مستقل اقتصادی یا رقابتی اهمیتی مضاعف پیدا نموده است.

قانون متحدالشکل اسرار تجاری امریکا، راز تجاری را این‌گونه تعریف می‌کند: «اطلاعات از جمله فرمول، الگو، ترکیب، برنامه، وسیله، روش، فن (تکنیک) یا فرایندی که: اولاً ارزش اقتصادی آن، به‌طور بالفعل یا بالقوه از این امر ناشی می‌شود که عموماً بر هیچ‌کس معلوم نیست و به‌راحتی برای اشخاص دیگری که می‌توانند از افشا یا به‌کارگیری آن به منفعت اقتصادی برسند در دسترس نیست. ثانیاً تلاش‌های متعارفی بر حسب اوضاع‌واحوال حاکم برای سری نگه‌داشتن آن انجام گرفته باشد (Allesan, 2014: 70). ماده 65 قانون تجارت الکترونیکی کشورمان نیز اسرار تجاری را شامل مصادیق متنوعی از داده‌های محرمانه همچون؛ فرمول‌ها و الگوها، نرم‌افزارها، ابزار و روش‌ها، تألیفات منتشر نشده، روش‌های انجام تجارت و دادوستد، فنون، نقشه‌ها، فراگردها، اطلاعات مالی، فهرست مشتریان و طرح‌های تجاری دانسته است که دارنده اطلاعات تلاش‌های معقولانه‌ای برای حفظ و حراست از آن‌ها انجام داده باشد.

هم اکنون به‌منظور حمایت از اسرار تجاری در فضای مجازی دو نوع رویکرد اساسی اتخاذ می‌گردد. رویکرد نخست، اتخاذ تدابیر کیفری است که در جهت بازدارندگی و پیشگیری از تکرار جرم اهمیت دارد. تصویب قانون تجارت الکترونیکی و قانون جرائم رایانه‌ای پاسخی مناسب

به پاره‌ای از دغدغه‌های به وجود آمده در این رابطه است. قانون‌گذار در این قوانین، اصل حق را مشمول حمایت انحصاری دانسته و برای نقض‌کننده آن قائل به مسئولیت کیفری و مدنی شده است. لکن این روش در مرحله اجرا با موانعی نظیر عدم سهولت در شناسایی نقض‌کننده حق و معضل در جمع‌آوری ادّله الکترونیکی مواجه است که ناشی از ویژگی‌های خاص جرائم سایبری و عدم اجماع در خصوص شناسایی و پیگیری این گونه جرائم در عرصه بین‌الملل است. این امر موجب طرح این ایده گردیده که سیاست کیفری جاری قابلیت اثربخشی لازم برای حمایت از اسرار تجاری در فضای مجازی را ندارد.

رویکرد دوم پیشگیری از وقوع یا ارتکاب جرم بر پایه الگوها و معیارهای گوناگون علمی و فنی است که می‌تواند با توجه به محدودیت‌های موجود در اتخاذ تدابیر سرکوبگرانه، نقش مؤثری ایفاء نماید. ضمن آن که قانون‌گذار بخشی از هزینه پیشگیری از وقوع جرم را بر دوش دارندگان اسرار (به‌عنوان بزه‌دیدگانی بالقوه) گذاشته و حمایت‌های خود را منوط به اقدامات پیشگیرانه متعارفی از سوی آن‌ها نموده است.

بی‌گمان مبارزه کیفری علیه جرائم نقض اسرار تجاری به‌رغم داشتن معایب و مشکلات بسیار در جای خود لازم و ضروری است. کما این‌که دارنده سّر تجاری نیز بر طبق قانون مکلف به رعایت تدابیر امنیتی متعارف می‌باشد؛ اما پرسشی که مطرح می‌شود آن است که آیا پاسخ‌های واکنشی در این زمینه کارایی لازم را دارند؟ اگر پاسخ منفی است، مناسب‌ترین راهکارهای امنیتی کدامند؟ و رویکردهای کنشی از جمله پیشگیری وضعی تا چه میزان قادر به پاسخ‌گویی در شرایط موجود می‌باشند؟ نهایتاً اینکه اتخاذ چنین اقداماتی تا چه حد می‌تواند امنیت اطلاعات را تضمین نماید؟

به‌طورکلی مناسب‌ترین تدابیری که می‌تواند زمینه کاهش فرصت ارتکاب جرم نقض اسرار تجاری را فراهم نماید، افزایش ریسک ارتکاب جرم و کاهش عایدی مورد انتظار آن است. لذا می‌توان امنیت اطلاعات تجاری در فضای سایبر را با سه معیار اساسی مورد بررسی قرار داد. نخست؛ قابلیت اعتماد و رازداری می‌باشد که با این طریق سعی در پیشگیری از دسترسی اشخاص ناصالح به اطلاعات می‌شود تا به واسطه آن، داده‌های محرمانه به‌صورت غیر مجاز افشا نشوند. دوم؛ حفظ صحت و تمامیت اطلاعات در برابر مجموعه عوامل مخربی است که موجب تغییر یا حذف غیرمجاز داده‌ها می‌گردد و سوم؛ به‌کارگیری تدابیر نظارتی در برابر شنود غیرمجاز یا دسترسی

غیرمجاز افرادی است که قصد دستیابی به اطلاعات محرمانه را دارند. تحقق این امر وابسته به امنیت سیستم‌های سخت‌افزاری و نرم‌افزاری در محیط الکترونیکی و فیزیکی دارد.

ازاین‌رو در این مقاله، تلاش داریم با توجه به‌ضرورت حمایت همه‌جانبه از حقوق و منافع دارندگان اسرار تجاری، پس از تحلیل نا کار آمدی رویکردهای کیفری (بخش دوم) به بررسی انواع تدابیر پیشگیرانه در بخش سوم بپردازیم و در نهایت انواع تدابیر پیشگیرانه وضعی را به‌عنوان موضوع اصلی مقاله با تفصیل بیشتری مورد مطالعه قرار داده و مناسب‌ترین راهکارها را در زمینه پیشگیری وضعی به‌منظور جلوگیری از نقض اسرار تجاری ارائه دهیم. در جمع‌بندی نهایی پیشنهادهایی در زمینه بالا بردن امنیت بیشتر اطلاعات بیان خواهد شد.

2. ناکارآمدی پاسخ‌های واکنشی (کیفری)

زمینه‌های مساعدی که فضای مجازی برای ارتکاب جرم فراهم نموده است و دشوار بودن رویارویی با این‌گونه جرائم، دولت‌ها را به دخالت گسترده در حقوق کیفری چه از نظر ماهوی و چه از نظر آیین دادرسی کیفری وادار نموده است (Alipour, 2011:28). چنان که با اصرار بر تأیید مقررات کیفری و روش‌های رسمی یا قانونی برخورد با جرم، هم اکنون قوانین متنوعی در راستای اعمال مجازات و اقدامات مؤثرتر برای شناسایی مرتکبین تصویب گردیده است که دارای آثار بازدارندگی و پیشگیرانه قوی‌تری می‌باشد. تدابیری نظیر عدم حمایت کیفری از بزه‌دیده سهل‌انگار، گسترش مسئولیت کیفری، شناسایی شروع به جرم به‌عنوان جرم تام، توسعه حوزه جرائم مطلق، گسترش مفهوم معاونت و کاهش عناصر تشکیل دهنده جرم، تنها بخشی از نوآوری-هایی است که در قانون جرائم رایانه‌ای، پیش‌بینی شده است (Javan Jafari, 2010:16).

اما مشکلاتی که در عرصه اجرای قوانین سایبری پدید آمده است، بیشتر از آنی است که قابل تصور باشد. جرائم سایبری دارای ویژگی‌های متمایزی نسبت به سایر جرائم کلاسیک هستند. در بسیاری از مواقع حتی پس از کشف جرم، مجرم کیلومترها دور از دسترس مقامات اجرایی، قانونی و قضایی قرار دارد و امکان تعقیب و تحقیق از وی وجود ندارد. همکاری‌ها در عرصه بین‌الملل نیز هنوز بدان حد نرسیده است که برای مبارزه با این جرائم راهکاری قوی و هماهنگ اندیشیده شود، به‌طوری‌که بتوان مجرم را در هر نقطه‌ای از جهان که یافت شود بر اساس قوانین بین‌الملل مورد تعقیب و مجازات قرار داد. لذا عدم وجود یک استراتژی واحد در اتخاذ سیاست‌های کیفری

مشترک و بالطبع توسل اغلب کشورها به قوانین داخلی و تفاسیر مختلفی که از جرائم ارتکابی و نتایج حاصل به عمل می‌آورند، این ایده را مطرح می‌سازد که حقوق جزا در برابر طیف وسیعی از جرائم سایبری به استیصال رسیده است.

علاوه بر این، در مرحله رسیدگی به جرائم نقض اسرار تجاری اغلب تشخیص این که اسرارتجاری از دارنده قانونی آن به نحو غیرمجاز تحصیل شده دشوار است؛ زیرا ممکن است شخصی به‌طور کاملاً اتفاقی به اسرار دسترسی پیدا کرده باشد و بدون آن که اهمال یا خطایی مرتکب شود داده‌های ارزشمند فوق را افشا نماید. همچنین این امکان وجود دارد که پیگیری و اقامه دعوا با توجیه‌هایی همچون مهندسی معکوس و کشف مستقل[1] بی‌نتیجه به پایان برسد و مالک اسرار از اقناع وجدانی دادرس ناتوان شده و خسارات شدیدی را متحمل گردد (Rahbari, 2010:228). هرچند تعیین مجازات متناسب با شدت و وخامت جرم ارتکابی نیز با توجه به نتایج مخرّب و جبران‌ناپذیر افشای چنین اطلاعاتی عملاً توسط دستگاه عدالت کیفری غیرممکن است.

بی‌گمان قانون‌گذار با اشراف بر وجود چنین موانعی بخشی از هزینه پیشگیری از وقوع جرم را بر دوش دارندگان اسرار تجاری قرار داده و حمایت‌های خود را منوط به انجام اقدامات پیشگیرانه از سوی آن‌ها نموده است. چنان که در ماده 65 قانون تجارت الکترونیکی، دارنده اسرار تجاری را به تلاش‌های معقولانه برای حفظ و حراست از اطلاعات محرمانه خود توصیه نموده است. در ماده 1 قانون جرائم رایانه‌ای نیز در خصوص دسترسی غیرمجاز به سیستم‌های رایانه‌ای یا مخابراتی، شرط پیگرد متهم را اتخاذ تدابیر ایمنی و حفاظتی از سوی دارندگان اطلاعات قرار داده است. لذا دارنده راز تجاری چنان که بخواهد مشمول حمایت‌های قانونی قرارگیرد، چاره‌ای جز اتخاذ اقدامات امنیتی متعارف با در نظر گرفتن نوع و درجه محرمانگی اطلاعات خود ندارد.

1- مهندسی معکوس شیوه‌ای است که به کمک آن می‌توان با بررسی دقیق یک محصول؛ اجزا، عناصر سازنده و نحوه کارکرد آن، همان محصول یا کالای مشابه آن را تولید کرد. این فرایند از طریق وارونه سازی و با جدا کردن اجزا و عناصر و ساخت دوباره آن صورت می‌گیرد. کشف مستقل نیز بدین معناست که شخص در اثر تلاش فکری و تحقیقاتی خود و با شیوه‌ای خاص و استفاده از منابع انسانی و مالی به اسرار تجاری دست یابد.

3. اتخاذ تدابیر کنشی (پیشگیرانه)

توسعه روزافزون فضای سایبر ازیک‌طرف و وجود محدودیت در اجرای قوانین الزام‌آور کیفری در بعد داخلی و بین‌المللی از طرفی دیگر، دولت‌ها را به این نتیجه رسانیده که نه می‌توانند به نقش ارعابی و بازدارنده قوانین کیفری خوش‌بین باشند و نه منطقی است که در امر کنترل پدیده‌های مجرمانه، در انتظار وقوع یک اتفاق مجرمانه بنشینند و سپس واکنش نشان دهند. لذا در وهله نخست، رویکردی پیشگیرانه را در رئوس برنامه‌های خود گنجانیده‌اند. از میان تدابیر گوناگون پیشگیری از وقوع جرم، الگوی پیشگیری اجتماعی[1] و پیشگیری وضعی[2] در حال حاضر جایگاه برجسته‌ای یافته است که در این قسمت به توضیح هر یک در ارتباط با موضوع این نوشتار می‌پردازیم.

3-1. پیشگیری اجتماعی

پیشگیری اجتماعی عوامل اجتماعی جرم‌زا را در یک جامعه هدف، مورد بررسی قرار می‌دهد. تدابیری که در راستای پیشگیری اجتماعی به اجرا در می‌آید می‌کوشد، زمینه‌های فردی یا اجتماعی را که سبب بروز انگیزه‌های مجرمانه می‌شود، برطرف کند. لذا این نوع پیشگیری شامل آن گروه از تدابیری است که با مداخله در فرایند بهبود شرایط افراد و سالم‌سازی محیط اجتماعی از وقوع بزه ممانعت می‌نماید (Niazpour,2003:171).

افتخار این طرز تفکر با تمام گرایش‌های آن در این است که مدعی مبارزه با علت و خشکاندن ریشه جرم می‌باشد و رویکردی بزه‌کارمدار به مقوله پیشگیری دارد (Saffari,2003:183)؛ اما زمینه و محل دخالت می‌تواند بزه‌دیده نیز باشد. آنچه در این نوشتار ما بر آن تمرکز داریم، حمایت از دارندگان اسرار تجاری به‌عنوان بزه‌دیدگان بالقوه یا ایده‌آلی است که هر لحظه اطلاعات ارزشمند آنان در معرض افشا قرار دارد؛ بنابراین ادامه این مبحث را با توجه به رویکرد پیشگیری وضعی که سنگ بنای آن بزه‌دیده یا بزه‌دیده مدار است، دنبال می‌کنیم.

1- Social perevention
2- Situational prevention

3-2. پیشگیری وضعی

پیشگیری وضعی در برگیرنده مجموعه تدابیر غیر کیفری است که از طریق از بین بردن یا کاهش فرصت‌های مناسب ارتکاب جرم و نامناسب جلوه دادن شرایط، از ارتکاب بزه جلوگیری می‌نماید؛ به‌عبارت‌دیگر پیشگیری وضعی بر این فرض استوار است که یک انسان متعارف در صورتی تن به خطر می‌دهد که عایدات و یا منافع حاصل از آن عمل ارزشمند باشد. حال اگر این فرض در خصوص مجرمان درست باشد، می‌توان گفت: چنان که به هر شکل بتوان خطرپذیری جرم را افزایش داد یا جاذبه‌ها و منفعت حاصل از آن را کاهش داد، معمولاً مجرمان بالقوه از ارتکاب جرم باز داشته می‌شوند (Najafi Abrandabadi,2003:1285).

ازاین‌رو پیشگیری وضعی، شامل اقدامات کاهش‌دهنده موقعیت‌هایی است که به سمت اشکال خاص جرائم جهت‌گیری شده و با مدیریت، طراحی و به‌کارگیری محیط به‌صورت نظام‌مند، موجب دشوارتر و پر ریسک‌تر کردن یا کاهش سود و منفعت و کاهش معاذیر ارتکاب جرم می‌شود (Paknahad, 2009:243). لذا در پیشگیری وضعی، جرم قابل پیش‌بینی بوده و از طریق کاهش فرصت‌های ارتکاب و آماج‌های آن با اعمال روش‌های متنوعی می‌توان وقوع جرم را ممتنع یا خنثی نمود.

4. انواع تدابیر پیشگیرانه وضعی

بی‌شک دارنده اسرار تجاری قبل از هر اقدامی باید ضمن پیش‌بینی تهدیدات احتمالی، اصول خاصی همچون؛ تشخیص و ارزیابی اطلاعات محرمانه و گزینش تدابیر امنیتی را مدّ نظر قرار دهد. شاید این ایراد در خصوص اتخاذ تدابیر پیشگیرانه وضعی در رابطه با اسرار تجاری مطرح شود که اقدامات پیشگیرانه وضعی فقط آماج‌ها یا موضوعاتی را شامل می‌شود که در عالم خارج به شکل ملموس وجود داشته باشد و در خصوص آماج‌های معنوی راهکاری را عرضه نمی‌کند (Babaei and Najibyan,2011:156). در پاسخ به این ابهام می‌توان گفت، اسرار تجاری طیف وسیعی از داده‌هایی را در بر می‌گیرد که در رایانه‌ها ذخیره شده و یا در لوح‌های فشرده‌ای نگهداری و از آن‌ها محافظت می‌شود، مضافاً آن که انعقاد قراردادهای رازداری با افرادی که به نحوی با این اطلاعات سرو کار دارند می‌تواند کمک مؤثری به عدم افشای این‌گونه اطلاعات بنماید؛ بنابراین

آنچه در ارتباط با موضوع این مقاله در ادامه به بررسی آن خواهیم پرداخت، بیان انواع اقدامات پیشگیرانه‌ای است که هر یک به‌نوعی موجب سخت‌تر نمودن آماج جرم، افزایش خطرات ارتکاب جرم و کاهش دستاوردهای مورد انتظار آن خواهد شد.

1- 4. تدابیر محدودکننده دسترسی

یکی از مهم‌ترین تدابیری که می‌تواند احتمال افشای اطلاعات را به حداقل برساند و خطر طرح دعاوی متعدد را در آینده کاهش دهد، انعقاد قراردادهای محدودکننده با مستخدمین یا سایر اشخاصی است که به هر نحوی به این اطلاعات دسترسی می‌یابند. این اقدامات به‌نوعی موجب از بین بردن عواملی می‌گردد که باعث تحریک یا تشویق فرد به ارتکاب جرم نقض اسرار تجاری می‌شود.

1- 1- 4. موافقت‌نامه عدم‌افشاء (NDA)[1]

مستخدمین، پیمانکاران، مشاوران، شرکا و همکاران شرکت می‌توانند عاملان اصلی جرائم سایبری علیه یک شرکت یا سازمان محسوب شوند (kenneth،2008). قرارداد بهترین رابطه قابل تصور در پیشگیری ازاین‌گونه جرائم می‌باشد. انعقاد قراردادها به شیوه‌ای مطلوب نه‌تنها به اشخاص، حقوقی اعطاء می‌کند که در رسیدگی‌های قضایی اهمیت دارد؛ بلکه از بروز اختلاف در خصوص موضوعات مبهم جلوگیری کرده و خطر طرح دعاوی مختلف را در آینده کاهش می‌دهد. به‌علاوه ضمانت اجراهای پیش‌بینی شده در قراردادها نیز می‌تواند مجرمین را از ارتکاب آن دسته از اعمالی که موجب مطالبه خسارت می‌شود باز دارد (Zybar,2011:228).

در حال حاضر توافق با موضوع تعهد به رازداری بهترین نوع حمایت از اسرار تجاری در ارتباط با کارکنان می‌باشد؛ زیرا اسرار تجاری اغلب با نقض تعهدات ناشی از روابط استخدامی که در نتیجه آن مستخدمی به افشای اسرار حوزه کاری خود می‌پردازد، در معرض خطر قرار می‌گیرد. پیش‌بینی چنین اقدامات احتیاطی توسط دارندگان اسرارتجاری باعث به وجود آمدن زمینه‌هایی

1- Non Disclosure Agreement

می‌گردد تا این اسرار برای مدت طولانی همچنان محرمانه باقی بمانند و ارزش تجاری خود را کماکان حفظ کنند.

این نوع قراردادها به دو طریق منعقد می‌شوند. در قراردادهای یک جانبه یکی از طرفین در برابر دیگری تعهد می‌کند تا اطلاعات سّری را حفظ کرده و از افشای آن خودداری نماید. در قراردادهای دو جانبه طرفین به نحو متقابل داده‌های محرمانه‌ای دارند که با یکدیگر مبادله می‌نمایند و متقابلاً در خصوص عدم افشای اطلاعات متعهد می‌شوند. به گزارش انجمن مدیریت منابع انسانی امریکا، در سال 2004 بیش از نیمی از تعداد واحدهای فعال در این کشور با کارکنان خود قرارداد رازداری منعقد نموده‌اند (Hadavand,2005:164).

انعقاد قراردادهای عدم افشاء در فضای مجازی به‌طورکلی مشابه با انعقاد آن در دنیای واقعی است؛ چراکه پس از شکل‌گیری و ایجاد یک ماهیت حقوقی در فضای الکترونیکی، اوصاف و آثار آن با ماهیتی که در فضای غیرالکترونیکی شکل می‌گیرد تفاوتی نمی‌نماید. بر این اساس هیچ‌گونه تغییری در اصل موجودیت، ماهیت، اوصاف و آثار حقوقی از آن جهت که در فضای الکترونیکی و بستر شبکه‌های اطلاعاتی و ارتباطی به وجود می‌آید، ایجاد نمی‌شود (Rezaei, 2008:30)؛ اما آنچه در یک قرارداد الکترونیکی برای دارندگان اطلاعات اهمیت دارد، تشخیص هویت واقعی و اهلیت اشخاصی است که با آنان تبادل اطلاعات صورت می‌گیرد.

برای اطمینان از این موضوع می‌توان با به‌کارگیری فناوری امضای الکترونیکی مطمئن یا امضای دیجیتالی[1] این اعتماد دست پیدا نمود (Zarkalam,2011:49). این فناوری‌ها که به نظر می‌رسد جزو کاربردی‌ترین روش‌های کنونی می‌باشد، نیازمند تأیید ثالثی است تا امکان برقراری ارتباط و انجام مذاکرات نهایی و در نتیجه انعقاد قرارداد به وجود آید. شخص ثالث در قانون

---

1 - با استفاده از امضای دیجیتالی، تمامیت سند، محرمانه بودن اطلاعات و امنیت داده‌ها تضمین می‌شود. امضای دیجیتالی یک فرایند رمزنگاری است و به معنای رمز دار کردن پیام، با کلید خصوصی و رمزگشایی آن با کلید عمومی است. بدیهی است کلیدهای عمومی و خصوصی به کار گرفته شده فیزیکی نبوده، بلکه به صورت اعداد می‌باشند که به وسیله نرم افزارها و سخت افزارهای خاصی ایجاد می‌شوند. در این روش طرفین به جای در اختیار داشتن یک کلید مشترک، هر کدام یک جفت کلید دارند. کلید عمومی سّری نبوده و می‌تواند در اختیار همه از جمله طرف قرارداد قرارگیرد؛ اما کلید خصوصی کاملاً محرمانه بوده و تنها در اختیار مالک آن می‌باشد. برای اطلاع بیشتر رجوع شود به کتاب مقدمه حقوق سایبر، تألیف سیامک قاجار قیونلو، نشر میزان،چاپ‌اول،1391،ص599.

تجارت الکترونیکی با عنوان دفاتر خدمات صدور گواهی الکترونیکی[1] نامیده می‌شود که یکی از وظایف آنان تأیید صلاحیت و هویت طرفین در یک فرایند تشکیل قرارداد الکترونیکی است.

2- 1- 4. موافقت‌نامه عدم‌رقابت

قرارداد عدم رقابت، نوعی قرارداد پیشگیرانه می‌باشد که میان دارندگان اسرارتجاری با اشخاصی منعقد می‌شود که به هر نحوی به این اطلاعات دسترسی پیدا نموده‌اند و حالا قصد جدایی یا بنیان گذاشتن فعالیت‌های تجاری مستقلی را دارند. به‌موجب این قرارداد یک طرف در برابر دیگری تعهد می‌کند تا به‌منظور حفظ منافع مشروعی تحت شرایطی خاص، برای مدت محدودی به رقابت با او نپردازد. به‌طور مثال کارفرمایی را تصور کنید که اطلاعات محرمانه تجاری خود را که از لحاظ رقابتی دارای اهمیت بسیاری است در اختیار مستخدمی قرار داده است که حالا قصد جدایی و پایه‌گذاری تجارتی مستقل را دارد. این موضوع ممکن است اسرار تجاری را در معرض افشا یا استفاده غیرمجاز مستخدم یا رقبا قرار دهد (Rahbari,2009:159).

در قراردادهای عدم رقابت مالک سّر تجاری باید دقیقاً مشخص نماید، طرف مقابل طی چه مدت، از چه نوع اقداماتی منع گردیده و در چه زمینه‌هایی حق فعالیت ندارد. دارندگان اسرار تجاری می‌توانند جهت اطمینان از این که اطلاعات آنان بعد از خروج و جدا شدن مستخدم یا شریک و اتمام مدت مقرر افشا نخواهد شد، قرارداد عدم افشا یا رازداری را به طور هم‌زمان با قرارداد رقابت منعقد نمایند.

دارنده پس از انعقاد قرارداد، باید از دسترسی مجدد مستخدم مستعفی به رایانه‌های حاوی اسرار تجاری ممانعت به عمل می‌آورد. رمز عبور مستخدم حذف گردد و اطلاعات موجود در فایل‌های رایانه وی در محل امنی ذخیره شود تا در صورت نیاز از آن‌ها استفاده شود.

---

1 - گواهی الکترونیکی، نوعی اعتبار الکترونیکی است که درستی و اعتبار یک کاربر را در اینترنت تأیید می‌کند. این گواهی-نامه‌ها با استفاده از تکنولوژی رمزگذاری عمومی؛ انتقال آن لاین رسمی و قانونی اطلاعات محرمانه یا دیگر اطلاعات حساس را تأیید و تضمین می‌کند. دفاتر خدمات صدور گواهی الکترونیکی نیز واحدهایی هستند که برای ارائه خدمات صدور امضای الکترونیکی مطمئن در کشور تأسیس و خدمات آن‌ها شامل تولید، صدور، ذخیره، ارسال، تأیید، ابطال و به روز نگهداری گواهی‌های اصالت (امضای) الکترونیکی می‌باشد.

2- 4. تدابیر سلب‌کننده دسترسی

توسعه فناوری‌های نوین ارتباطی در کنار مزایای قابل‌توجهی که دارند، در حوزه امنیت اطلاعات چالش‌های زیادی را پدید آورده است. لذا استفاده از پیشرفته‌ترین امکانات و دستاوردهای علمی و فناوری موجود امری اجتناب‌ناپذیر است. هرچند برخی حملات سایبری حتی توسط به‌روزترین ضد بدافزارها تشخیص داده نمی‌شوند و دستیابی به امنیت صددرصدی موضوعی غیرعملی و محال است (Hasanbeygi,2005:82). البته این موضوع قطعاً به معنای توقف استفاده از نرم‌افزارهای ضد بدافزار نیست؛ چراکه تولید چنین نرم‌افزارهایی روز به روز هوشمندتر می‌شود و ممکن است نسخه‌های جدید آن‌ها قادر به تشخیص تهدیدات مختلفی باشند. درهرصورت استفاده از این نرم‌افزارها باعث می‌شود حداقل دارنده متوجه گردد که سیستم رایانه‌ای او دچار تهدید شده تا بتواند شروع به ترمیم خرابی و استفاده از پروتکل‌های بهبود نماید. ازاین‌رو برخی از شرکت‌هایی که دارای اطلاعات محرمانه می‌باشند برای حفاظت بیشتر از داده‌های خود، با اتخاذ تدابیر حفاظتی اقدام به استخدام هکرهایی می‌نمایند تا با نفوذ به سیستم‌های رایانه‌ای شرکت، نقاط قوت و ضعف امنیتی سیستم‌های آنان را کشف کند.

هدف از اجرای تدابیر سلب‌کننده دسترسی، مجموعه اقداماتی می‌باشد که از ورود یا ارسال برخی از داده‌های غیرمجاز جلوگیری به عمل می‌آورد. درصورتی‌که این تدابیر به‌طور مناسبی اجرا شوند تا حد قابل قبولی می‌تواند از افشای اطلاعات تجاری ممانعت نماید. این عمل غالباً بر عهده سخت‌افزارها یا نرم‌افزارهایی چون دیواره آتش، فیلترها، سیستم‌های تشخیص تجاوز، پراکسی‌ها، نرم افزارهای ضد پیام ناخواسته و نرم‌افزارهای ضد پایش می‌باشد.

1- 2- 4. دیواره آتش[1]

یک سیستم رایانه‌ای یا بخشی از نرم‌افزار تخصیص یافته است که بر تماس‌های برقرار شده میان یک رایانه یا شبکه با دیگران نظارت می‌کند. این دیواره مانند دروازه‌بانی است که ارتباطات را تأیید می‌نماید، مانع گذر موارد مشکوک یا غیرمجاز می‌شود و محتوای ورودی به شبکه را پالایش

1- Fire Walls

می‌کند. در واقع سخت‌افزارها یا نرم‌افزارهایی که دیواره آتش را تشکیل می‌دهند، ضمن بررسی اطلاعات و داده‌های در حال تبادل شبکه، مبادله اطلاعات اعم از پست الکترونیکی، انتقال فایل‌ها و سایر عملیات مشابه را مجاز یا متوقف می‌نماید. فناوری دیواره آتش با وجود مزایای متعددی که دارد در برابر نفوذ کارکنان و مستخدمین داخلی شرکت یا افرادی که در سیستم نفوذ نموده‌اند، کارآیی مطلوبی ندارد.

2- 2- 4. سیستم تشخیص تجاوز[1]

این سیستم که دارای مرزهای مشترکی با سیستم قبلی (دیواره‌آتش) می‌باشد، نرم‌افزاری است که در صورت ورود غیرمجاز کاربر بیگانه به رایانه حامل اطلاعات محرمانه، به دارنده آن هشدارهای لازم را می‌دهد. برای فهم بیشتر این سیستم می‌توان آن را در عالم واقع مشابه دزدگیرهایی دانست که برای ورود غیرمجاز طراحی شده‌اند، اما درعین حال بسته به نوع و مدل آن کارهای دیگری را نیز برای حفاظت از امنیت اطلاعات انجام می‌دهد. به طور مثال می‌تواند مهاجمین به سیستم را به خود مشغول نموده و آن‌ها را از حمله به سیستم اصلی باز دارد[2].

3- 2- 4. نرم‌افزارهای ضد پیام‌های ناخواسته[3]

ارسال نامه‌های الکترونیکی با محتوای تجاری یا تبلیغاتی بدون اطلاع و رضایت دارندگان اطلاعات در بسیاری از مواقع موجب فریب و یا تحصیل اطلاعات محرمانه آن‌ها می‌گردد. هکرها ازاین‌روش به‌عنوان شیوه‌ای برای پخش ویروس نیز استفاده می‌نمایند، لذا ارائه‌کنندگان خدمات اینترنتی برای رفع این معضل استفاده از نرم‌افزارها و برنامه‌های ضد spam را توصیه می‌کنند.

1- Intrusion Detection System(IDS)

2 - اوتپست"Outpost" نام نرم‌افزاری است که مجهز به یک دیواره آتش است که با ترکیب بخش ضد ویروس و ضد جاسوس به بخش قدرتمندی رسیده است که می‌تواند در مقابل تمامی حمله‌ها حمایت کرده و امنیتی پایدار را برای سیستم به وجود آورد. اطلاعات بیشتر ررا می‌توان از نشانی؛ http://www.goo.gl/cO44cAAدریافت نمود.

3- Unsolicited Commercial Mail(UCM) or Spam

4- 2- 4. نرم‌افزارهای ضدپایش

برخی برنامه‌های جاسوسی مانند برنامه‌های تروجان و کوکی[1] وجود دارند که برای جمع‌آوری اطلاعات محرمانه از سیستم‌های رایانه‌ای افراد نظیر اطلاعات مربوط به رمز دسترسی آنان به داده-های سّری‌شان به کار می‌رود[2]. به‌طور مثال یکی از روش‌های خرابکاری نسبتاً جدیدی که وجود دارد موسوم به clickJackikg است که با توجه به ضعف مرورگرهای اینترنتی یا ضعف امنیتی سرویس‌دهنده‌های اینترنتی اقدام به نفوذ و سرقت اطلاعات می‌نمایند. در این روش کاربر به‌ظاهر روی یک لینک ناآشنا کلیک می‌نماید اما در نهایت مجوزی صادر می‌کند تا او را هدایت به سایت دیگری نماید که خود از آن بی‌اطلاع است. نرم‌افزارهای متنوعی در ارتباط با مقابله با چنین بدافزارهایی طراحی شده است که می‌توانند به‌طور خودکار آسیب‌پذیری‌های امنیتی را جستجو و کاربر را از وجود آن‌ها آگاه نمایند[3].

5- 2- 4. پراکسی‌ها[4]

نرم‌افزاری می‌باشد که بین یک سرور و یک رایانه کار می‌کند. این سیستم نه تنها صفحات وب‌هایی را که قبلاً بازشده‌اند در حافظه ذخیره می‌کند و باعث افزایش سرعت دسترسی به اینترنت می‌شود، بلکه موجب امنیت در شبکه داخلی شرکت نیز می‌شود؛ زیرا به جای اینکه چندین رایانه در شبکه داخلی به اینترنت متصل باشند، فقط یک سرور پراکسی با اینترنت در ارتباط است و در نتیجه امنیت شبکه از لحاظ ویروس و هک شدن تا حدود زیادی تأمین می‌شود

---

1 - کوکی‌ها (coockies)، معمولاً برنامه‌های مفیدی هستند اما می‌توانند ابزاری برای جمع آوری اطلاعات محرمانه نیز باشند. هرچند که استفاده‌کنندگان از کوکی‌ها موظف‌اند که اذن کاربران را در استقرار آن‌ها بر روی سیستم‌هایشان تحصیل کنند لکن در بسیاری موارد چنین نمی‌کنند.

2 - به نقل از سایت ماهر Cryptolocker ، Zeus و Damon به عنوان خطرناک‌ترین بدافزارهای سال 2014 شناخته شده‌اند. این بدافزارها علاوه بر آن که فایل‌ها را به گونه‌ای غیر قابل برگشت رمزگذاری می‌کنند، باعث سرقت اطلاعات نیز می‌شوند.

3 - نرم‌افزارهایی همچون Kaspersk، Bitdefender و AVIRA به عنوان برترین ضد ویروس‌های سال 2014 شناخته شدند که می‌توانند فایل‌های آلوده را شناسایی و قرنطینه نمایند. اطلاعات بیشتر را می‌توان از نشانی؛www.certcc.ir دریافت نمود

4- Proxy

.(Abbasi,2010:51)

4-2-6. فیلترها[1]

تدابیری است که از ورود یا ارسال برخی داده‌های غیرمجاز جلوگیری می‌کنند. بعضی از آن‌ها عمل یک سویه دارند؛ یعنی از ورود یا خروج داده‌های غیرمجاز جلوگیری می‌نمایند و برخی کاربردی دو سویه داشته و علاوه بر ورودی‌ها، خروجی‌ها را هم تحت کنترل قرار می‌دهند. فیلتر کننده کلیه درخواست‌ها را با فهرست بانک اطلاعاتی خود که از سه جزء نشانی‌دامنه، نشانی-پروتکل اینترنت وکلمه‌های کلیدی تشکیل شده مقایسه می‌نماید. اگر هیچ یک از این نشانی‌ها در فهرست درخواست رایانه وجود نداشته باشد، این درخواست پاک در نظر گرفته می‌شود و در غیر این صورت، درخواست آلوده تشخیص داده شده و مسدود می‌شود.

4-2-7. ناشناس‌کننده و رمزنگارها

ناشناس‌کننده‌ها[2] هویت افراد را در محیط سایبر مخفی می‌کنند و از این طریق به آن‌ها امکان می‌دهد با ایجاد حریم بیشتر، به فعالیت شبکه‌ای بپردازند (Jalali Farahani,2005:145). این اقدام به ویژه برای دارندگان اسرارتجاری که سعی در مخفی نمودن اطلاعات خود را دارند مفید است؛ زیرا بدون آن که فرصت شناسایی خود را به مجرمان سایبری بدهند، داده‌های خود را حفظ می-نمایند.

ماهیت اصلی ابزارهای رمزنگاری[3] نیز همانند ناشناس‌کننده‌هاست با این تفاوت که به جای اطلاعات هویتی افراد، محتوای ارتباطات را نامفهوم می‌کنند. در این روش بر اساس کدهای خاصی، متن اصلی به رمز نوشته تبدیل می‌شود و گیرنده در مقصد به‌وسیله کلیدی که در اختیار دارد آن را رمزگشایی می‌کند. در این نوع رمز نوشته اگر فرد دیگری بخواهد به‌طور غیرمجاز به اطلاعات دسترسی پیدا کند، یا باید از طریق فرآیند رمزنگاری و تحلیل محتوای رمز نوشته به

1- Filtering
2- Anonymizers
3- Encryption

اطلاعات محرمانه دست یابد و یا با تحصیل کلید رمزگشای مرتبط به هدفش برسد (Jalali Farahani,2009:115)[1].

ناشناس کننده‌ها و رمزنگارها یکی دیگر از ابزارهایی است که از بزه‌دیدگی دارندگان اطلاعات محرمانه در فضای سایبر پیشگیری می‌کنند، اما نباید از یاد برد که امکان استفاده از این ابزارها برای مجرمان نیز وجود دارد، زیرا آن ها با پنهان کردن هویت خود یا رمزنگاری محتوای مجرمانه ارتباطاتشان، امکان شناسایی خود را کاهش می‌دهند. لذا این گزینه نسبت به تدابیر پیشگیرانه دیگر از این ضعف برخوردار است که در کنار از بین بردن برخی از فرصت‌های ارتکاب جرم، زمینه ارتکاب برخی از جرائم را فراهم می‌آورد.

4-3. تدابیر صدور مجوز[2]

در این روش این امکان فراهم می‌شود که رایانه حاوی اطلاعات بداند که کاربر کیست و تنها کسانی بتوانند به محیط آن وارد شوند که دارای تأییدیه مورد نظر رایانه باشند. این مجوز در صورتی صادر می‌شود که کاربر توسط سیستم شناسایی شود. این اقدام می‌تواند از ورود افرادی که صلاحیت لازم جهت دسترسی به اطلاعات سّری را ندارند، جلوگیری نماید و تنها به افرادی اجازه عبور دهد که نسبت به هویت و اعمال آن‌ها اطمینان وجود دارد .

برای صدور مجوز یا تصدیق هویت کاربر می‌توان از سیستم‌های شناسایی متنوعی کمک گرفت. در حال حاضر به عقیده کارشناسان بهتر است از مکانیزم‌هایی همچون تصدیق هویت دو عاملی[3] استفاده شود. دو روش در این خصوص کاربرد دارد. روش نخست، استفاده نمودن از کارت‌های هوشمند مبتنی بر نشانه است که اطلاعات زیستی افراد همچون چهره کاربر یا اسکن عنبیه چشم را در خود ذخیره می‌نمایند؛ و روش دوم استفاده از سرویس‌دهنده‌ها و برنامه‌هایی می-

---

1 - True Crypt یکی از نرم‌افزارهایی است که برای رمزدار کردن فایل‌ها طراحی شده و می‌تواند با سرعت بالا، درایوی که ویندوز در آن نصب شده است را رمزدار کند این رمز قبل از اجرای سیستم عامل اجرا می‌شود و در صورتی که کاربر رمز عبور را نداشته باشد، حتی نمی‌تواند سیستم عامل را اجرا کند. اطلاعات بیشتر را می‌توان از نشانی؛ http://www.truecypt.org دریافت

2- Verification or Authentication Technologies
3- Two Factor Authentication

باشد که مانند نگهبان یک سالن عبور و مرور را کنترل می‌کند، مانند امضای دیجیتال (Khanalipour,2011:143).

4-4. تدابیر نظارتی[1]

ابزارهای نظارت الکترونیکی، وظیفه کنترل فعالیت شبکه‌ای افراد را با به‌کارگیری تجهیزات و برنامه‌هایی بر عهده دارند. این‌گونه ابزارهای خاص محیط سایبر، تهدیدات احتمالی را به دو شکل هم‌زمان و غیر هم‌زمان به شکل هشدار به آگاهی دارنده اسرار تجاری می‌رسانند. در حالت نخست (نظارت هم‌زمان)، ابزار الکترونیکی مسئول یا متصدی مربوطه را از فعالیت غیرمجاز در همان زمان آگاه می‌کند، و به‌این‌ترتیب او می‌تواند اقدامات پیشگیرانه مقتضی را انجام دهد؛ اما در حالت دوم (نظارت غیرهم‌زمان)، بسته به میزان دقت ابزار نظارتی، صرفاً بخش‌های گزینش شده‌ای از فعالیت‌های شبکه‌ای ثبت می‌شود تا در فرصتی دیگر با بررسی آن‌ها موارد غیرمجاز مشخص گردد. در این حالت ابزارها و برنامه‌هایی بر روی سیستم نصب می‌شود که کلیه فعالیت‌های شبکه‌ای افراد اعم از مستخدمین یا اشخاص ثالث، حتی ضرباتی که بر روی صفحه کلیدشان زده‌اند یا نقاطی که به‌وسیله موشواره (موس) بر روی آن‌ها کلیک کرده‌اند ضبط گردد (Khanalipour,2011:162). از دیگر ابزارهای نظارتی غیرهمزمان بوکش‌ها یا کاوشگرهای الکترونیکی می‌باشند که وظیفه تشخیص هویت‌های مجازی، کنترل دسترسی‌های مجاز به محتوای محرمانه داده‌ها و حتی تشخیص مصادیق محرمانه منتشر شده را به عهده دارند. در حقیقت این ابزارها آن دسته از کاربران مجازی را شناسایی می‌کنند که با عدم رعایت مقررات مربوط به طبقه‌بندی اطلاعات، قصد دسترسی به اطلاعات غیر مجاز را دارند (Khaleghi Poostchi,2009:46). درعین‌حال یک هکر ممکن است به‌طور غیرمجاز وارد یک شبکه شده و کاوشگری را در آن نصب نماید. در این حالت بوکش‌ها ممکن است خود به ابزاری برای دسترسی به رمزهای ورود و سایر اطلاعات حیاتی تبدیل شوند.

1- Monitoring Measures

5. نتیجه‌گیری

فضای سایبر به‌موازات رشد فنی خود از نظر رشد ساختارهای اخلاقی و کنترل‌کننده‌ای که هر محیطی برای استقرار نظم به آن نیاز دارد بسیار عقب مانده است. در این میان آن دسته از اطلاعات ارزشمندی که جنبه خلاقانه دارند به‌طور گسترده‌ای در معرض حملاتی همچون دسترسی غیرمجاز یا شنود غیرمجاز قرارگرفته‌اند؛ به‌ویژه آن که عدم استراتژی واحد در خصوص چگونگی شناسایی و تعقیب مجرمان سایبری و به‌طورکلی عدم اجماع در به‌کارگیری یک سیاست کیفری مشترک در خصوص جرائم سایبری در عرصه بین‌الملل، موجب گردیده است تا امکان شناسایی نقض‌کننده حق به حداقل برسد. حتی در مرحله رسیدگی به دعوی نقض اسرار تجاری این امکان وجود دارد که ادعای مطروحه با توجیه‌هایی مانند کشف مستقل و مهندسی معکوس بی‌نتیجه به پایان برسد و بزه‌دیده از اقناع وجدان دادرس ناتوان گردد. چنانکه در برخی از دعاوی خسارات حاصله ناشی از افشای اطلاعات به‌قدری سنگین می‌باشد که نه‌تنها دستگاه عدالت قضایی توان تعیین مجازات متناسب با نتایج مخرب آن را ندارد؛ بلکه مجرم نیز قادر به جبران خسارت وارده بر بزه‌دیده نیست. لذا نه می‌توان به نقش ارعابی و بازدارنده قوانین کیفری خوش‌بین بود و نه منطقی است در امر کنترل پدیده مجرمانه در انتظار وقوع یک اتفاق مجرمانه نشست و سپس واکنش نشان داد.

ازاین‌رو رویکرد پیشگیرانه یکی از مهم‌ترین راهکارهای جلوگیری از نقض اسرار تجاری شناخته می‌شود. پیشنهادهایی که در عمل سبب ایجاد مانع در فرایند گذار از اندیشه به عمل مجرمانه و دشوارتر ساختن دسترسی مجرمان بالقوه به موضوع جرم می‌گردد. ضمن آن‌که قانون‌گذار تنها اسراری را مورد حمایت قرار می‌دهد که اقدامات پیشگیرانه معقولی در حفظ و حراست آن‌ها انجام شده باشد.

در این نوشتار ما پیشگیری وضعی را به‌عنوان یک الگوی مؤثر و مناسب در جهت پر ریسک‌تر کردن یا کاهش سود و منفعت حاصل از ارتکاب جرم انتخاب نموده‌ایم. در این نوع پیشگیری دارندگان اسرار تجاری به اتخاذ اقدامات امنیتی در رابطه با مستخدمان (مشخصاً انعقاد قراردادهای رازداری و عدم‌رقابت) و استفاده از دو یا چند نرم‌افزار ضد بدافزار با توجه به نوع اطلاعات محرمانه راهنمایی و توصیه می‌گردند. لکن در این حوزه نیز هر اندازه استفاده از نرم‌افزارهای ضد

بدافزار رواج بیشتری می‌یابد، نفوذگران از ابتکارات جدیدتری در طراحی و استفاده از بدافزارهای متنوع استفاده می‌نمایند؛ این نوع جا به جایی منجر به افزایش کمی و کیفی حملات سایبری و بار نمودن هزینه‌های اضافی بر دارندگان اسرار تجاری می‌گردد. لذا در این رابطه نیازمند ترویج و گسترش پوشش بیمه تجارت الکترونیکی در کنار ایجاد گروه‌های واکنش سریع شامل مراکز امداد و نجات رایانه‌ای در سطوح استانی و ملی و همچنین اتخاذ تدابیری نظیر تدوین سند راهبرد امنیت سایبری، استفاده حداکثری از سخت‌افزارها و نرم‌افزارهای ضد بدافزار تولید داخل با حداقل استفاده از ابزارها و نرم‌افزارهای رایانه‌ای پایه غیربومی، آموزش و تربیت نیروی انسانی متخصص با گرایش امنیت سایبری و تقویت پلیس فتا هستیم.

Referencess

[1] Allesan, M. (2014). "Cyberspace Law", the Institute of Legal Studies and Research in science, , Tehran.(in persian)

[2] Alipour, Hassan. (2011). " Criminal Justice IT ' satisfaction publications , printing , Tehran . (in persian)

[3] Abbasi, Morad. (2010). " Cyberspace and challenges facing the preventive police " , Journal of promoting crime prevention studies , Issue XVII , winter 2010. (in persian)

[4] Babaei, Mohammad Ali and Najibyan, Ali. (2011). "Crime Prevention Challenges," Justice Law Journal, Vol. 75, No. 75. (in persian)

[5] Hadavand, Mehdi. (2005). "The Basics of trade secret protection of the rights of America", the journal of Justice, Issue XVII. (in persian)

[6] HasanBygy, Ebrahim. (2005). “Rights and the Internet in cyberspace ", published by the International Cultural Institute of Political Studies of Contemporary Abrar, printing, Tehran. (in persian)

[7] Jalali Farahani, Amirhossein. (2005). "Situational Prevention of Cybercrime in the Light of Human Rights", Journal of Law and Jurisprudence, Issue 6. (in persian)

[8] Jalali Farahani, Amirhossein. (2005)."Institution-Building for the Prevention of Cybercrime Looking Computer Crimes Act", the multi-agency approach to crime prevention, crime prevention a national articels, first edition, Department of Education Prevention of Police, Tehran. (in persian)

[9] Javan Jafari, Abdorreza. (2010)." Cybercrime and differential approach to criminal law ", Journal of knowledge and development eighteenth year, No. 34. (in persian)

[10] Khaleghi Poostchi, Ali. (2009). "The Prevention of Cyber Crime By Using Information and Communication Technology (ICT)», National scientific-practical conference abstracts, prevention of crime (judiciary - Mashhad),

Mizan publication, first edition , Tehran. (in persian)
[11] KhanaliPour and Ajargah, Sakineh. (2011). “Technical Prevention of Crime ", the publishing, Tehran. (in persian)
[12] Kenneth C.Brancikl:"Insider computer fraud, An in-Depth Framework for Detecting and Definding Insider Attack", Auerbach publication (2008).
[13] Najafi Abrandabadi, alihossein. (2002). “Pleadings course criminology (prevention) "regulatory” Mehdi Seyedzadh, graduate higher education centers in Qom. (in persian)
[14] Niazpour, Amirhossien. (2003), "Delinquency Prevention's rights in Iran", Journal Legal Justice Year Issue (49-48). (in persian)
[15] paknahad, Amir. (2009). "Risk-based Criminal Policy," the Mizan publication, first printing, Tehran. (in persian)
[16] Rahbari, EbrahIm. (2009). "A Trade Secret Law", the printing, Tehran. (in persian)
[17] Rezaei, Ali. (2008) "E-commerce law", the publishing, printing, summer 2009 (in persian).
[18] Safari, Ali . (2001). " Principles of Prevention of Crime " , Journal of Law , No. 33 and 34 , spring to winter 2001. (in persian)
[19] Zybar, Ulrich. (2011)." Computer Crimes " , inversion : Mohammad Nouri and others , Ganje Dansh Press , second edition , Tehran. (in persian)