

ضرورت حمایت قانونی از اسرار و حق حریم در عصر فناوری اطلاعات

مصطفی السان¹، محمدرضا منوچهری²

چکیده

حمایت از اسرار امنیتی، دولتی، تجاری و حق حریم با ورود جامعه به عصر فناوری اطلاعات و امکان دسترسی سریع به آنها در تمامی نقاط جهان اهمیت فوق‌العاده‌ای یافته است. در این مقاله، به تفصیل ضرورت حمایت از اسرار (اعم از اسرار تجاری، امنیتی، ملی و شخصی) و ضمانت‌اجراهای قانونی و عملی برای حمایت همه‌جانبه از آنها بررسی می‌شود. در بررسی موضوع، مبانی رایج برای تشخیص اسرار و نیز مفهوم «تعهد به عدم افشای اطلاعات» بررسی شده و راهکارهای لازم ارایه می‌گردد.

کلید واژه

اسرار تجاری - اسرار دولتی - اسرار امنیتی - حقوق - تعهدات.

۱- مقدمه

پیدایش وسایل الکترونیکی ارتباط در عصر حاضر، جابجایی سریع اطلاعات و آگاهیها را از تمامی جهات امکانپذیر ساخته است. آنچه که در تصور بشر نمی‌گنجید، اکنون به واقعیت بدل گردیده و به راحتی می‌توان طرف کمترین زمان قابل تصور اصوات، تصاویر، کتابها، اسناد، مدارک و... را به هر کجای دنیا ارسال نمود. این رابطه دو سویه میان فرستنده و گیرنده، اگرچه کارآیی اعجاب‌آوری داشته و بسیاری از مشکلات موجود فراراه صنعت و علم را از میان برداشته، اما در پاره‌ای از موارد نیز به حکم طبیعت امور، دارای زیانها و مضراتی بوده است. در میان وسایل گوناگون ارتباط، به‌ویژه اینترنت، گمنامی بدون خطری را موجب شده که به نسل جدیدی از جاعلان و سارقان هویت، جسارت می‌بخشد.

اگرچه «حقوق اسرار»^۳ و «حقوق اسرار تجاری»^۴ پیشینه‌ای طولانی دارد، با اینحال اعمال آن به دلیل مسائلی چون گمنامی^۵، سرقت شخصیت^۶، وجود شخصیت دیجیتالی و نفوذ هکرها در شبکه در عصر فناوری اطلاعات با پاره‌ای از دشواریها و

۱- دانشجوی دوره دکتری حقوق خصوصی، دانشکده حقوق دانشگاه شهید بهشتی.

۲- دانشجوی کارشناسی ارشد حقوق خصوصی، دانشکده حقوق دانشگاه شهید بهشتی.

3 - The Law of Secrets

4 - Trade Secret Law

5 - Anonymity

6 - Identity Theft

ابهامات روبرو شده است. امروزه، امکان دارد که اسرار ملی و نظامی یک کشور به هر دلیل از سوی دولتهای دیگر در معرض دید عموم قرار داده شود؛ چرا که اینترنت امکان آن را فراهم ساخته است. و یا اینکه حق حریم¹ شخص نقض شده و حیثیت او با افشای اسرار خصوصیش به گونه‌ای بر باد رود که راهی برای اعاده آن نباشد.

این مباحث و مسایل دیگری که در این مقاله طرح خواهد شد، لزوم بررسی و تأکید بر مفهوم بنیادین «حقوق اسرار» را در سطح داخلی و بین‌المللی آشکار می‌سازد، چرا که نقض محرمانگی اسرار به بهانهٔ فقدان قانون یا نظام بین‌المللی خاص امکان دارد که دولتها را روبروی هم قرار می‌دهد یا اشخاص را روانه دادگاهی سازد که ترفندی جز قواعد عام مسؤولیت برای مجازات مرتکبین در اختیار ندارد. حتی در مواردی که گمنامی به مفهوم کامل آن به دلیل ناایمن بودن سیستم‌های رایانه‌ای محقق است، عامل زبان یا افشاکننده‌ای در کار نخواهد بود که بتوان مسؤولیت را بر وی بار نمود.

بررسی موضوع در گفتارهای جداگانه به شرح زیر انجام می‌شود.

- کلیات
- مبانی حقوق اسرار در عصر فناوری اطلاعات
- حقوق اسرار و فناوری اطلاعات
- ایمنی اسرار و عوامل توجیه کننده افشای اسرار در عصر فناوری اطلاعات

۲- کلیات

قبل از ورود به بحث باید مفهوم «سر» «حقوق اسرار» و «حق حریم» مشخص گردیده و محدوده هر کدام در عصر فناوری اطلاعات تبیین شود.

۱-۲- مفهوم «سر»

سرّ یا راز، عبارت از هر چیزی پنهانی است که مخفی بودن آن برای دارنده یا دارندگان موجب امتیاز می‌باشد. راز در مفهوم عام آن شامل تمام واقعیتها، پدیده‌ها، تصورات و دانسته‌ها و حتی تلخکامیها، اشتباهات و خطاهایی است که دارنده متمایل به افشای آنها نیست و از آگاهی یافتن دیگران به آن رموز به هر دلیل متضرر می‌شود.

افشای سر، بر خلاف مفهوم لغوی، به معنی اطلاع یافتن تمام مردم به محتوای آن نیست؛ بلکه امکان دارد با آگاهی و لو یک نفر افشای سر تحقق یابد. بنابراین در این مفهوم، راز و افشا دارای مفهومی متفاوت با معنای لغوی بوده و اصطلاح فنی به شمار می‌آید. چرا که برای مثال فرمول ساخت یک ریز پردازنده که هزار نفر از کارکنان شرکت سازنده به آن آگاهی دارند، در مفهومی عرفی به هیچ وجه راز به شمار نمی‌آید، ولی حقوق اسرار در محرمانه بودن مورد مزبور و تعهد کارکنان به عدم افشای آن تردیدی ندارد.

در تعریف اسرار تجاری، عده‌ای آن را به «رازی که موجب امتیازی بالقوه یا بالفعل برای دارنده آن در امر تجارت است؛ یا هر چیزی که دارنده آن را با اقدام متعارف به عنوان یک راز نگاه می‌دارد»، تعریف کرده‌اند. (گسمر، ۲۰۰۴)

ماده ۲ قانون حمایت از اسرار دولتی جمهوری خلق چین^۲ مصوب ۱۹۹۸ در تعریف «اسرار دولتی» مقرر می‌دارد: «اسرار دولتی عبارت از تمام چیزهایی است که به امنیت و منافع ملی ارتباط می‌یابد، تعیین محدوده این اسرار با قانون بوده و تنها اشخاص معینی برای مدت محدود حق آگاهی از آن را دارند». این بدین معنی است که اگر یک موضوع مخفی به اطلاع اشخاصی برسد که از آن آگاهی نداشته‌اند، امنیت و منافع ملی صدمه خواهد دید. (کنترل و سانسور اطلاعات در چین، ۲۰۰۳: ۱۸)

۲-۲- مفهوم «حقوق اسرار»

اسرار از گذشته و عملاً مورد حمایت بوده‌اند. برای نمونه، در چین باستان، مجازات افشای اسرار یک گروه به دیگران، زجرکشی بود. (گسمر، ۲۰۰۴) اگر از داستانها و افسانه‌هایی که در مورد اسرار و رموز هست بگذریم، با اینکه حمایت از اسرار به

1 - Privacy

2 - Law on the Protection of State Secrets, P.R.C 1988

معنی تعیین ضوابط دقیق علمی برای حفظ و جلوگیری از افشای آنها پیشینه‌ای طولانی دارد، ولی تعریف حق و تعهد در مورد اسرار و اطلاعات محرمانه چندان سابقه نداشته و قواعد موجود در این زمینه، حتی در حال حاضر نیز ناقص می‌باشد. این وضعیت از دو بعد قابل بررسی است: از یک طرف، به لحاظ تاریخی، کشورها همواره به حفاظت از اسرار دولتی و امنیتی توجه داشته و به اسرار اقتصادی توجهی نداشته‌اند. این جنبه به مرور زمان اصلاح گردید و چنانچه خواهیم گفت، در حال حاضر حمایت قانونی از اسرار تجاری و جلوگیری و وضع ضمانت اجرا برای افشای آنها اهمیت زیادی یافته است. در جهان امروز که قدرت اقتصادی و نه توان نظامی تعیین کننده استراتژیها و قابلیت‌هاست، اسرار تجاری نیز مورد حمایت هستند. برای مثال، در ایالات متحده قانون جاسوسی اقتصادی¹ در ۱۱ اکتبر ۱۹۶۶ تصویب گردیده و به ضابطه‌مند کردن قواعد حاکم بر حفاظت اسرار اقتصادی و تعیین ضمانت اجرا برای نقض حقوق اسرار پرداخته است. (چارنی، ۲۰۰۲: ۶۰)

از سوی دیگر، بحث دقیق و حقوقی از اسرار دولتی نیز فی الواقع بعد از انتشار کتاب «Spycatcher»^۲ توسط شخصی به نام پیتر رایت^۳ که سابقاً در سرویس امنیتی انگلیس^۴ کار می‌کرد، طرح گردید. او در این کتاب اطلاعات محرمانه‌ای را افشا نمود که به هیچ وجه با مصالح دولت انطباق نداشت. (دیویس، ۲۰۰۴: ۱۳) این امر و گسترش وسایل گوناگون صوتی و تصویری برای استراق سمعی و بصری منجر به تصویب قوانین و مقرراتی در کشورهای مختلفی در جهت منع و تعیین ضمانت اجرا برای افشای اسرار شده است. بنابراین، مبنای «حقوق اسرار» را تعهد به عدم افشای اسرار^۵ و در صورت نقض این تعهد، مجازات و مسؤولیت مدنی مرتکب تشکیل می‌دهد. بدیهی است که میزان تعهد و مسؤولیت بسته به نوع اسرار و نحوه افشا متفاوت خواهد بود.

۳-۲- مفهوم حق حریم

واژه «Privacy» را عده‌ای از نویسندگان به «حق خلوت» نیز ترجمه کرده‌اند. عبارت جایگزین مذکور در بیان مفهوم Privacy نارساست و اگرچه واژه حق حریم نیز معادل دقیق Privacy نمی‌باشد، ولی بهتر از حق خلوت به نظر می‌رسد. چرا که برای داشتن حریم خصوصی و حق بر آن نیازی به (خلوت) در مفهوم عرفی آن وجود ندارد. در این مفهوم، حق حریم دارای معنی عام و دربرگیرنده حق هر شخص بر جان، تن، آزادی... و از جمله - بنابر آنچه به بحث ما ارتباط می‌یابد - به مفهوم حق هر شخص به داشتن اطلاعات مخفی و تکلیف‌مطلوعین به عدم افشای آنهاست. حق حریم بر همین اساس شامل کلیه اشخاص - اعم از حقیقی و حقوقی - بوده و تجاوز به آن از سوی هر کس که باشد، محکوم و مشمول ضمانت‌های اجرایی است.

فصل اول باب دوم «لایحه حقوق شهروندی و تاسیس نهاد ملی دفاع از حقوق شهروندی» به «حق بر حریم خصوصی» اختصاص یافته است. به موجب ماده ۲۰ لایحه مذکور، «کلیه شهروندان حق دارند که اطلاعات خصوصی آنها محرمانه بماند و از تعرض مصون بماند». نیز به موجب ماده ۵۸ قانون تجارت الکترونیکی، مصوب ۱۳۸۲/۱۰/۱۷ «ذخیره و پردازش یا توزیع «داده‌پیام»‌های مبین ریشه‌های قومی یا نژادی، دیدگاه‌های عقیدتی، مذهبی، خصوصیات اخلاقی و «داده‌پیام»‌های راجع به وضعیت جسمانی، روانی و یا شخصی اشخاص بدون رضایت صریح آنها به هر عنوان غیر قانونی است». چنانچه ملاحظه می‌شود، در دو مقرر فوق مفهوم عامی از حق حریم ارایه شده و افشای اسرار و اطلاعات خصوصی افراد ممنوع گردیده است. اگرچه در کشورهای دیگر نیز مقررات مشابهی به تصویب رسیده - و ما به مناسبت، برخی از آنها را مورد بررسی قرار خواهیم داد - با اینحال بعضی از نویسندگان ادعا نموده‌اند که با ورود به عصر فناوری اطلاعات باید حق حریم را به فراموشی سپرد. (فرومکین، ۲۰۰۰) در جای خود به این ادعا پاسخ خواهیم گفت.

1 - Economic Espionage Act 1996.

۲- نام کامل کتاب و مشخصات ناشر آن به شرح زیر است:

Peter Wright, Spycatcher: the Candid Autobiography of a Senior Intelligence Officer (Toronto: Stoddard, 1987).

3 - Peter Wright

4 - Military Intelligence 5 [MI5].

5 - Obligation of Confidence

۳- مبانی حقوق اسرار در عصر فناوری اطلاعات

حقوق اسرار همانند سایر رشته‌های حقوقی از قواعد معینی تبعیت می‌کند. این قواعد در اغلب موارد مشابه با سایر رشته‌ها هستند، با این وجود گسترش استفاده از وسایل الکترونیکی برای ارتباط، نقش برخی از مبانی و اصول را پررنگ کرده است. این مبانی را به شرح زیر می‌توان خلاصه نمود.

۳-۱- محرمانه بودن اطلاعات

ارایه اطلاعات از هر نوع که باشد، علی‌الاصول افشای آن به حساب نمی‌آید، مگر اینکه به تصریح قانون یا سازمان معین یا به تشخیص عرف آن اطلاعات در زمره اسرار شمرده شوند. لذا، چنانچه قاضی مگاری^۱ نیز در پرونده‌ای^۲ ابراز داشته، اطلاعات باید دارای معیارهای لازم برای محرمانه بودن باشند تا افشای آنها مستوجب مسؤولیت باشد. (وای‌سان، ۱۹۷۷: ۵۸۸)

بنابراین، چنانچه از ماده ۱ و ۲ «قانون مجازات انتشار و افشای اسناد محرمانه و سری دولتی» مصوب ۱۳۵۳ نیز برمی‌آید، اسناد دولتی در صورتی سری یا محرمانه محسوب می‌گردند که سازمان مربوطه اقدامات متعارف^۳ را برای حفاظت از آنها انجام داده و در حد امکان تعهد به عدم افشا را به کارکنان خود یادآور شده باشد. همانند حالت سنتی، وظیفه «احتیاط متعارف» از مقامات بالای سازمان شروع شده و به پایین استمرار می‌یابد. در جهت جلوگیری از افشای الکترونیکی اطلاعات، مدیریت اجرایی سازمان یا مؤسسه ذیربط باید به طور دقیق مصادیق مشکوک ارایه الکترونیکی داده‌ها را با لحاظ جوانب علمی و فنی مشخص کرده و معیارهای لازم را برای حفاظت از اطلاعات معرفی نمایند. (لیندبرگ و بنجستون، ۲۰۰۲: ۱۲۲)

ماده ۱ قانون فوق، اسناد دولتی را عبارت از «هر نوع نوشته یا اطلاعات ثبت یا ضبط شده مربوط به وظایف و فعالیتهای وزارتخانه‌ها و مؤسسات دولتی و وابسته به دولت و شرکتهای دولتی از قبیل: مراسلات، دفاتر، پرونده‌ها، عکس‌ها، نقشه‌ها، کلیشه‌ها، نمودارها، فیلم‌ها، میکروفیلم‌ها و نوارهای ضبط صوت که در مراجع مذکور تهیه و یا به آن مراجع رسیده است»، می‌داند. ذکر عبارت «از قبیل» نشان از محدود نبودن دامنه اسناد دولتی به موارد مذکور دارد و لذا با توسعه فناوری می‌توان، لوحهای فشرده (سی‌دی‌های) حاوی اطلاعات، حافظه رایانه، دیسکت‌ها، عکس‌ها و تصاویر ضبط شده توسط دوربین‌های تلفن همراه و موارد دیگر را در فرض تحقق شرط «محرمانه بودن» در زمره اسناد دولتی سری یا محرمانه قلمداد کرد.

به موجب «آیین‌نامه طرز نگهداری اسناد سری و محرمانه دولتی و طبقه بندی و نحوه مشخص نمودن نوع اسناد و اطلاعات»، طبقه هر سند را مسؤول واحد تهیه‌کننده آن سند تعیین می‌کند (ماده ۳) که تردیدی در اجرای این اصل در مورد اسرار الکترونیکی وجود ندارد. به طور کلی به نظر می‌رسد که کلیه قوانین و مقررات موجود در مورد اسرار دولتی، امنیتی و تجاری و اقتصادی را باید در مورد شکل الکترونیکی این اسناد نیز اجرا نمود.

۳-۲- تعهد به عدم افشاء

یکی از مبانی مهم حقوق اسرار، «تعهد به عدم افشاء» می‌باشد در این معنی، علی‌الاصول از فردی می‌توان انتظار عدم افشای اسرار را داشت که به موجب قانون یا عرف بر این امر تعهد داشته باشد. در حقوق کامن‌لا، این تعهد ممکن است مبتنی بر تراضی و توافق طرفین یا بر مبنای انصاف باشد. برای مثال، تعهدات پزشکان، وکلا، کارکنان، مستخدمین و قضات در عدم افشاء را تنها می‌توان بر مبنای انصاف توجیه نمود. (بین‌بریج، ۱۹۹۹: ۲۸۵)

در حقوق ایران، این تعهد اغلب مبنای قانونی دارد و برای مثال تعهد «کلیه کسانی که به مناسبت شغل یا حرفه خود محرم اسرار می‌شوند» در غیر از موارد امنیتی به موجب ماده ۶۴۸ و در موارد مربوط به امنیت داخلی و خارجی کشور بنابر ماده ۵۰۱

1 - Megarry J.
2 - Coco v. Clarck [1969].
3 - Due Diligence

قانون مذکور به صراحت بیان شده و برای نقض این تعهد، مجازات تعیین گردیده است. به علاوه ماده ۲ قانون مجازات انتشار و افشای اسناد محرمانه و سری دولتی را نیز در صورت تحقق مصادیق آن می توان در مورد مرتکبین اعمال نمود. در مورد ذخیره، پردازش و یا توزیع «داده پیام» های شخصی مبین ریشه های قومی یا نژادی، دیدگاه های عقیدتی، مذهبی و... نیز چنانچه گفته شد، ماده ۵۸ قانون تجارت الکترونیکی (ق.ت.ا) تعیین تکلیف کرده و اسرار تجاری در مواد ۶۴ و ۶۵ قانون مذکور مورد حمایت قرار گرفته اند. با لحاظ آنچه گفته شد، در وضعیت کنونی حقوق ایران تمامی اسرار (دولتی، امنیتی، حریم شخصی، تجاری و اقتصادی) به موجب قانون و با ضمانت اجرای کیفری تحت حمایت قرار گرفته اند و افشای آنها به شیوه الکترونیکی موجب مسؤولیت کیفری خواهد بود.

با فرض اثبات «تعهد به عدم افشاء» در مورد شخص معین:

الف. وی نمی تواند به حسن نیت یا عدم سوءنیت خود در افشای اسرار استناد نماید و برای نمونه در ارایه اطلاعات از طریق نامه الکترونیکی، مدعی تصور مجاز بودن گیرنده پیام شود، مگر اینکه دلایل قانع کننده ای برای صحت ادعای خود ارایه نموده یا اثبات نماید که تمامی اقدامات متعارف را برای حفاظت اطلاعات به انجام رسانیده است. چنانچه در پرونده معروف اسپای کچر، قاضی پرونده^۱، ادعای آقای رایت (مؤلف کتاب) را نپذیرفت و اعلام داشت:

«در مورد مسأله، او باید با لحاظ اوضاع و احوال (قراین و عرف) می دانست که اطلاعات محرمانه هستند و عمداً چشم خود را بر روی حقایق نمی بست». (وای سان، ۱۹۹۷: ۵۷۰)

ب. مسؤولیت او محدود به مسؤولیت کیفری نخواهد بود و تمامی خسارات مادی و معنوی وارده را نیز متحمل خواهد گردید. این نوع از ضمان به ویژه در افشای اسرار تجاری الکترونیکی اهمیت ویژه ای می یابد. چرا که این اسرار به تصریح ماده ۶۵ ق.ت.ا «به طور مستقل دارای ارزش اقتصادی بوده و در دسترس عموم قرار ندارد و تلاشهای معقولانه ای برای حفظ و حراست از آنها انجام شده است».

۳-۳- معیار شخصی و عینی اسرار

مسأله ای که در حقوق اسرار امکان طرح آن وجود دارد این است که چه معیاری برای تشخیص اسرار و افشای آنها وجود دارد؛ در این مورد امکان ارایه دو معیار را می توان بررسی نمود.

۳-۳-۱- معیار شخصی

به موجب این معیار، اطلاعات محرمانه در فضای مجازی تنها برای افرادی ایجاد مسؤولیت می کند که به موجب قانون یا قرارداد، مکلف به حفاظت از آن اسرار می باشند. به عبارت دیگر تعهد به عدم افشاء فقط برای افرادی قابل تصور است که اسرار از هر قسم به طور مستقیم در اختیار ایشان قرار گرفته و تعهد به عدم افشاء نیز به آنها یادآوری شده است. ماده ۲ قانون مجازات انتشار و افشای اسناد محرمانه و سری دولتی و ماده ۵۰۱ ق.م.ا در مورد اسرار امنیتی، علی الظاهر بر همین مبنا تنظیم شده اند. چراکه در ماده ۲ افشا یا انتشار اسرار توسط کارکنان سازمان و تعیین مجازات برای این عمل، مطرح گردیده و در ماده ۵۰۱ ق.م.ا افشای اسرار «به نحوی که متضمن نوعی جاسوسی باشد» قابل مجازات شناخته است.

۳-۳-۲- معیار عینی

اسرار (اعم از تجاری و امنیتی) مطلقاً تحت حمایت قانون قرار دارند و هر کس آنها را افشا نماید، حسب مورد مسؤولیت کیفری یا مدنی یا هر دو نوع را متحمل خواهد بود. در مقابل دیدگاه کسانی که معتقدند، «باید با لحاظ اوضاع و قراین، تعهد به عدم افشا به شخص مورد نظر یادآوری شده باشد». (بین بریج، ۱۹۹۹: ۲۲۴) شاید بتوان با تمسک به نظر قاضی مگاری در پرونده کوکو علیه کلارک چنین اظهار نظر نمود که، «اگر از اوضاع و احوال، عرفاً برآید که خواننده از محرمانه بودن اطلاعات آگاهی داشته یا این واقعیت را استنباط نموده و با این وجود آنها را افشا کرده باشد، باید وی را مسؤول دانست. معیار عینی به

عنوان یک معیار جهانی پذیرفته نشده و همین امر باعث می شود که در مورد افشای اطلاعات ناخواسته¹، یعنی اطلاعات محرمانه‌ای که شخص یا اشخاص به طور ناخواسته و بدون سوءنیت به دست می آورند، تعیین مسؤول با اشکال روبرو گردد. پر واضح است که در روابط اینترنتی، اعمال معیار عینی نقش مهمی در ممانعت از افشای اسرار (بازدارندگی) و یا مجازات افشا کنندگان خواهد داشت. چرا که، اگرچه شخص اطلاعات را ناخواسته به دست آورده، اما در آگاه نمودن دیگران از آن حداقل حسن نیت نداشته است.

در خصوص اطلاعات ناخواسته، رویه قضایی اندکی وجود دارد، با این وجود دارندگان این اطلاعات را باید بر مبنای ملاک عینی مسؤول دانست. در کامن لا این مسؤولیت مبتنی بر انصاف² می باشد. بدین معنی که وجداناً و انصافاً نمی توان اسرار امنیتی یا تجاری متعلق به دیگران را افشا نمود حتی اگر آن اسرار ناخواسته و اتفاقی دریافت شده باشد.

۳-۳-۳- تمایز میان دو معیار

معیار عینی و شخصی هر کدام دارای تفاوتها و وجوه برجسته‌ای می باشند که به اختصار می توان چنین برشمرد:

۱-۳-۳- تفاوت در اثبات

با امکان اعمال معیار شخصی، اثبات مسؤولیت تسهیل می گردد. زیرا با اثبات اینکه شخص تعهد به عدم افشا داشته و آنرا نقض نموده، باید علی‌الاصول وی را مسؤول دانست، مگر اینکه قوه قاهره یا عامل توجیه کننده دیگری در میان باشد. حال آنکه در صورت تمسک به معیار عینی، باید دریافت اسرار از سوی شخص مورد نظر، افشای عالمانه آن اسرار و مسؤولیت کیفری (سوءنیت) وی را احراز نمود. بنابراین اگر شخصی ناخواسته اطلاعاتی را از طریق نامه الکترونیکی یا تبادل الکترونیکی داده³ دریافت دارد، در صورتی می توان او را مسؤول دانست که بر سری بودن آن اطلاعات آگاهی داشته و عالماً آنها را افشا کرده باشد.

۲-۳-۳- تفاوت در مسؤولیت

اشخاصی که به حکم قانون (وظیفه) یا قرارداد ملزم به عدم افشای اسرار مرتبط با کار خود هستند، به طور مستقیم و به موجب قانون مسؤولند. به لحاظ علم و اطلاع ایشان و آموزشهای لازم، باید مسؤولیت کیفری و مدنی ایشان را محقق و در صورت علم و عمد در افشای اسرار، مجازات مشددی را برای افراد مذکور در نظر گرفت. به موجب ماده ۷۵ قانون تجارت الکترونیکی، «... هر کس در بستر مبادلات الکترونیکی به منظور رقابت، منفعت و یا ورود خسارت به بنگاههای تجاری، صنعتی، اقتصادی و خدماتی، با نقض حقوق قراردادهای استخدام مبنی بر عدم افشا اسرار شغلی و یا دستیابی غیر مجاز، اسرار تجاری آنان را برای خود تحصیل نموده، یا برای اشخاص ثالث افشا نماید به حبس از شش ماه تا دو سال و نیم و جزای نقدی معادل پنجاه میلیون (۵۰/۰۰۰/۰۰۰) ریال محکوم خواهد شد».

اشخاصی که به طور ناخواسته اطلاعاتی را به دست می آورند، علی‌الاصول در قبال آنها مسؤولیتی ندارند، مگر اینکه با علم به محرمانه و سری بودن آن، نسبت به افشا اقدام نمایند. مسؤولیت این دسته از افراد چون بر مبنای انصاف محقق می شود، بیشتر صبغه مدنی و مالی دارد. البته در صورت وضع قانون خاص مسؤولیت کیفری نیز منتفی نخواهد بود.

۴- حقوق اسرار و فناوری اطلاعات

اطلاعات مایه قدرت است و تحصیل اسرار دیگران به قصد بهره برداری نیز از این حقیقت خارج نیست. امروزه، فناوری اطلاعات و توانمندی کشورها در این زمینه از عوامل اقتدار آنها به شمار می آید و بدیهی است که تلاش دولتها برای کسب اطلاعات از راههای قانونی و غیر قانونی گسترش خواهند یافت. در این راستا، ورود به عصر دیجیتال، اختراع و عرضه انواع فرستنده‌ها و گیرنده‌های الکترونیکی، گمنامی اینترنتی و ابهامات موجود در روابط مجازی منجر به ایجاد زمینه‌ای برای سوءاستفاده شده است.

1 - Unsolicited Information

2 - Equitable Obligation

3 - Electronic Data Interchange [EDI].

بر همین اساس باید مدعی شد که جز در صورت وجود یک نظام قدرتمند و علمی برای حمایت از اسرار، نمی توان از دست یازیهای دیگران به دور بود. بین المللی شدن مساله و افشای اسرار نظامی و امنیتی در اینترنت - که بارها انجام شده - نیز بر این واقعیت دلالت دارد. بر خلاف نظر نویسندهای که اختراع دوربین، تلفنهای تصویری، دستگاههای دیدهبانی، پیگردی الکترونیکی، انواع میکروفونها، گوشیها، وسایل هوشمند شنیداری و دیداری، نامه الکترونیکی، مبادله الکترونیکی داده و... را موجب تضعیف حق حریم دانسته، (فرومکین ۲۰۰۰: ۱۴۶۳) با وضع ضوابط فنی و حقوقی به راحتی می توان از مشکلات ناشی از ظهور فناوری جدید کاست و آن را به حداقل ممکن رسانید.

۱-۴- گمنامی

عدهای فکر می کردند فضای مجازی^۱ بهشت بی قانونیست که در آن مقنن داخلی یا بین المللی توان وضع قاعده ندارد و حتی اگر چنین نماید، ضمانت اجرایی وجود نخواهد داشت. این - بهشت و از سوی زیاندیدگان جهنم از همان ابتدای ظهور روابط اینترنتی به هیچ وجه ملاحظه نشد، چرا که آنچه در اینترنت رخ می دهد به عالم خیال تعلق نداشته و به وقایع عالم حقیقی شباهت دارد. (رامبرگ، ۲۰۰۲: ۱۰۹)

گمنامی اینترنتی به معنی نامعلوم بودن هویت افرادی است که از طریق این شبکه با یکدیگر ارتباط برقرار می کنند. پر واضح است که اگر این گمنامی به مفهوم عرفی آن محقق باشد، در آن صورت هر قانونی برای کنترل فعالیت های اینترنتی محکوم به بی اعتباری خواهد بود. حال آنکه در اکثر موارد با رهگیریهایی دقیق علمی، رد پای افراد و در نتیجه هویت ایشان شناسایی می شود و بر همین اساس اعمال مجازات برای یاغیان شبکه (هکرها) و افشاکنندگان اسرار امکان پذیر است.

۲-۴- بی قانونی

ممکن است این ادعا مطرح شود که قانون خاصی برای جلوگیری از افشای اسرار در فضای اینترنت وجود ندارد و در عمل با مرتکبین چنین اعمالی برخورد نمی شود: عدهای به راحتی مسایل خصوصی مردم را به تصویر می کشند و به طور برخت^۲ در اینترنت ارایه می دهند، مشخصات تاسیسات نظامی و امنیتی دولتهای دیگر را فاش می کنند، با ارایه تصاویر ساختگی و مستهجن منجر به هتک حیثیت افراد می شوند و... بدون آنکه مورد پیگرد قرار گرفته و مجازات شوند.

این ادعا تنها در روابط بین المللی صحیح می نماید، چرا که دولتها حقیقتاً خود را ملزم به رعایت حقوق اسرار امنیتی نمی دانند و متأسفانه افشای اسرار کشورهای دیگر از سوی دولتها (دولتی شدن نقض اسرار) با هیچ مانعی روبرو نیست؛ ولی در حقوق داخلی، اعمال قوانین راجع به حفاظت اطلاعات و حمایت از اسرار در روابط الکترونیکی، با هیچ تردیدی روبرو نیست و حتی برخی از کشورها، مقررات صریحی در منع افشای الکترونیکی اسرار وضع نموده اند.

بنابر گزارش روزنامه خلق^۳، وزارت امنیت داخلی چین^۴ در ژوئن ۲۰۰۰ بخشنامه ای صادر کرد که تمام سازمانها و اشخاص را از افشا، طرح یا انتقال اسرار دولتی در پایگاههای اینترنتی^۵، تابلوهای اعلان عمومی، واحدهای گپ زنی^۶ و از طریق نامه الکترونیکی منع کرده است. (فوستر و گودمن، ۲۰۰۰: ۳۱) به علاوه، به موجب قانون خاص^۷ در این کشور تصریح شده که از اینترنت نمی توان برای صدمه به امنیت داخلی، افشای اسرار دولتی، متضرر ساختن جامعه، آسیب رساندن به منافع ملی، جامعه یا گروه، حقوق شهروندان یا شرکت در افعال مجرمانه، استفاده نمود. (مقررات ایمنی و مدیریت شبکه های اطلاعات رایانه ای و اینترنت چین مصوب ۳۰ دسامبر ۱۹۷۷، ماده ۴-۱)

1 - Cyberspace

2 - Online

3 - People's Daily

4 - Ministry of State Security of PRC.

5 - Websites

6 - Chat room

7 - Regulation on the Security and Management of Computer Information Networks and the Internet 1997.

در انگلیس، قانون اسرار رسمی¹ افشای اسرار به اشخاص غیر مجاز را ممنوع و مستوجب کیفر دانسته است. در مورد سایر اسرار در اغلب موارد مسؤولیت مبتنی بر انصاف یا قواعد عام حقوق مدنی خواهد بود.

۳-۴- اعمال قواعد حقوق اسرار در عرصه بین‌المللی

یکی از مهمترین ابهامات حقوق اسرار، تردید در امکان اجرای قواعد آن در عرصه بین‌المللی است: آیا می‌توان با تمسک به موازین بین‌المللی افشای اسرار را به طور الکترونیکی منع نمود؟ اگر دولتی به طور خودسرانه اطلاعات سری متعلق به تجهیزات نظامی و استراتژیک کشوری را در اینترنت منتشر نماید، چه ضمانت‌اجرایی علیه آن دولت وجود خواهد داشت؟ آیا می‌توان علیه آن دولت در محاکم دیصلاح بین‌المللی طرح دعوی نمود؟ سرانجام اینکه در فرض صلاحیت، کدام قانون بر اختلاف طرفین اعمال خواهد شد؟

رویه بین‌المللی در زمینه شناسایی حقوق اسرار و محکوم کردن نقض آن بسیار اندک و حتی در مورد نقض حقوق اسرار امنیتی و نظامی ناموجود است. شاید زمانی تحولات حقوق مالکیت معنوی که اکنون حمایت از اسرار و علایم تجاری را نیز پوشش داده، به این عرصه کشیده شود و بتوان راه‌حلهای آن را اعمال نمود. با این وجود برخی از قواعد عام حقوق بین‌الملل را می‌توان برای منع افشای اسرار به کار گرفت، که از جمله آنها اصل حسن‌نیت و احترام متقابل است.

کشورها سالهاست که امکان سرقت الکترونیکی اطلاعات امنیتی را دریافته‌اند. در آمریکا این اعتقاد وجود دارد که هرکس (چه حرفه‌ای و چه تازه‌کار) همواره برای دسترسی به اطلاعات دولتی و محرمانه تلاش کرده‌اند؛ عده‌ای از دولت‌ها با مقاصد مشکوک یا روابط سیاسی متزلزل نسبت به ایالات متحده، به طور ناملموس در استفاده از شیوه‌های فنی جاسوسی و وسایل ارتباط الکترونیکی برای مقاصد دفاعی، نظامی و استراتژیک دخالت داشته‌اند. (چن، ۲۰۰۲: ۶۴) تشریح این وضعیت در ایالات متحده نشان از دوراندیشی محققان این کشور دارد، وگرنه امکان چنین سوءاستفاده‌ای از وسایل ارتباطی مدرن علیه منافع ملی تمام کشورها قابل تصور است و همین امر نیاز به سنجش و تقویت سیستم‌های اطلاعات سری در سطح ملی و فراملی را آشکار می‌سازد.

در سطح بین‌المللی، علاوه بر اسرار اقتصادی و تجاری، باید تصمیمات مهم مملکتی، تصمیمات دیپلماتیک و سیاست خارجی، اسرار مربوط به وضعیت اجتماعی و شهروندان و اسرار راجع به فناوریهای علمی و تحقیقاتی را در زمره اطلاعاتی محسوب داشت که افشای آنها، نقض حقوق اسرار تجاری به شمار می‌آید. با اینحال می‌توان مواردی را تصور نمود که دولتی به خاطر منافع ملی و در شرایط اضطراری حقوق دولت دیگر، یا در سطح داخلی شهروندان، را نسبت به اسرار و اطلاعات محرمانه نقض نماید. چنانکه بعد از انفجار یک بمب در ساختمان فدرال اوکلاهما سیتی، سازمان بازرسی فدرال² آمریکا احضاریه‌ای به تمام دارندگان دوربینهای تصویربرداری، عکاسی، وسایل دیداری و شنیداری و ویدئوها و به طور کلی همه مالکین وسایل تجسس الکترونیکی ارسال داشت. (هوبر، ۱۹۷۷: ۱۹۵) این وضعیت نمود تحول در مفهوم حق حریم و حق بر داشتن راز می‌باشد که نیازهای امنیتی و اجتماعی آن را تحمیل می‌نماید.

۵- ایمنی اسرار و عوامل توجیه کننده افشای اسرار در عصر فناوری اطلاعات

با ظهور فناوریهای جدید شنیداری و دیداری، گوشیه‌ها و حسگرهایی که حتی امکان جاسازی آنها در حشرات یا کفش شخص مأمور حفاظت از اطلاعات نیز وجود دارد، ماهواره‌هایی که هزاران کیلومتر دورتر از زمین لحظه به لحظه جزئیات وقایع را به گیرنده‌ها منتقل می‌نمایند و نمونه‌های فراوانی که گاه بحث آن در رسانه‌های همگانی مطرح می‌گردد، ایمنی و حفاظت از اسرار نیز بسیار سخت شده است: دیگر قابل اعتماد بودن مأمورین یا کارکنان کافی نیست، باید از وسایل الکترونیکی پیشرفته، جدیدترین امکانات و دستاوردهای علمی و فناوری نیز بهره گرفت. از سوی دیگر، در مواردی به هیچ وجه نمی‌توان از افشای اطلاعات جلوگیری نمود و یا حتی افشای اسرار توجیه پذیر است. این موضوع را به طور جداگانه تشریح می‌نماییم.

1 - Official Secrets Act 1989.

2 - Federal Bureau of Investigation [FBI]

۱-۵- ایمنی اسرار در عصر فناوری اطلاعات

امنیت اطلاعات در عصر روابط الکترونیکی در اکثر موارد بعد حقوقی نداشته و بیشتر به مسایل علمی و فنی ارتباط می یابد. تحقیقات زیادی در زمینه ایمنی داده های رایانه ای از حیث عدم امکان نفوذ اشخاص غیر مجاز انجام و نتایج آن آرایه شده (از جمله مقاله های: لیندبرگ و بنجستون، ۲۰۰۲؛ وانگ و دیگران، ۲۰۰۲) که می توان به آنها مراجعه نمود. حتی برخی از نویسندگان تقویت سیستم های الگوریتمی را پیشنهاد می نمایند؛ به گونه ای که حتی معروفترین سرویس های جاسوسی نیز توان شکستن (یافتن رمز ورود) آن را نداشته باشند. (هوبر ۱۹۷۷: ۱۹۰)

میزان ایمنی اطلاعات محرمانه و سری در برابر نفوذ هکرها و جاسوسان حرفه ای و متخصص در سیستم های الکترونیکی، از نظر حقوقی دارای آثار زیر می باشد.

نخست. از نظر حقوقی، تنها می توان از اسراری حمایت نمود که جنبه های علمی و فنی در حفاظت از آنها مراعات شده باشد. چنانچه قسمت اخیر ماده ۶۵ قانون تجارت الکترونیکی (در مورد اسرار تجاری) «تلاش های معقولانه برای حفظ و حراست را شرط سری بودن داده پیام های الکترونیکی محسوب داشته است.

دوم. نفوذ به اطلاعاتی که درجه معقول و متعارفی از ایمنی را دارا می باشند در هر صورت موجب مسؤولیت است؛ زیرا با این اقدام «سوءنیت» مرتکب آشکار می گردد. چنانچه در پرونده ای 1 قاضی پرونده 2 اظهار داشت که تعهد به عدم افشا، محدود به مواردی که در آن اشخاص دارای رابطه قراردادی هستند نمی باشد، بلکه سوءاستفاده یک نفر از موقعیتی که برای تحصیل اطلاعات سری داشته نیز، می تواند منجر به مسؤولیت شود. (بین بریج، ۱۹۹۹: ۲۸۷) دلیل این وضعیت آشکار است: از یک سو، همواره عده ای معین و محدود بر اسرار آگاهی دارند و ایمن سازی اسرار توسط ایشان انجام می شود. لذا نمی توان آنها را به طور کامل کنترل کرد. از طرف دیگر در عصر فناوری اطلاعات، وسایل الکترونیکی روز به روز در حال پیشرفت و تحول هستند و چه بسا قبل از آگاهی و بهره گیری از جدیدترین فناوری، شخصی با دست یافتن به آن، نسبت به افشای اسرار اقدام نماید که در این صورت نیز نمی توان راه را بر او بست.

۲-۵- عوامل توجیه کننده افشای اسرار در عصر فناوری اطلاعات

اگر محرمانه بودن اسرار در فضای مجازی اثبات گردید، اصل بر این است که نمی توان آنها را افشا کرد. مگر اینکه همان مصلحتی که ایجاب کرده آن اطلاعات مخفی بمانند، افشای آنها را اقتضا نماید. به عبارت دیگر تنها با حکم قانون یا دادگاه می توان اسرار را فاش نمود. مقررات موجود نیز بر این واقعیت تصریح دارند. به موجب ماده ۶۴ قانون تجارت الکترونیکی، «به منظور حمایت از رقابتهای مشروع و عادلانه در بستر مبادلات الکترونیکی تحصیل غیر قانونی اسرار تجاری و اقتصادی بنگاهها و مؤسسات برای خود یا افشای آن برای اشخاص ثالث در محیط الکترونیکی جرم محسوب و مرتکب به مجازات مقرر در این قانون خواهد رسید».

به عنوان استثنای بر اصل عدم امکان افشای اسرار، دادگاه می تواند دستور رمزگشایی الکترونیکی را صادر نماید. به موجب ماده ۱۰۴ قانون آیین دادرسی دادگاه های عمومی و انقلاب در امور کیفری مصوب ۱۳۷۸، «در مواردی که ملاحظه، تفتیش و بازرسی مراسلات پستی، مخابراتی، صوتی و تصویری مربوط به متهم برای کشف جرم لازم باشد، قاضی به مراجع ذیربط اطلاع می دهد که اشیاء فوق را توقیف نموده و نزد او بفرستد...». و بنابر تبصره همین ماده، «کنترل تلفن افراد جز در مواردی که به امنیت کشور مربوط است یا برای احقاق حقوق اشخاص به نظر قاضی ضروری تشخیص داده شود، ممنوع است». در بند اخیر ماده ۱۰۵ قانون اخیرالذکر تصریح نموده که اسناد سری دولتی نیز در صورت ضرورت با اجازه رئیس قوه قضاییه برای کشف جرایم و تحقیقات کیفری قابل آرایه می باشد.

1 - Saltman Engineering Co v. Campbell Engineering Co Ltd [1963].

2 - Lord Greene

از بعد تطبیقی، افشای اسرار و اطلاعات محرمانه بدست آمده از طریق وسایل الکترونیکی در حقوق خارجی نیز در موارد خاصی مجاز شناخته شده است. چنانچه ای در پرونده ای، خواهان ادعا نمود که پلیس یک کپی از عکسهای او را به متصدیان فروشگاه محلی ارایه نموده، که آن عکس او را در حال سرقت از اشیای فروشگاه نشان می دهد. در آن پرونده خواهان متهم به سرقت بود، ولی بدان محکوم نشد. (البته بعدها بدان محکوم گردید). قاضی اظهار داشت که پلیس در استفاده از عکسها که امکان داشت به عنوان جزیی از اسرار محرمانه به شمار آیند، به هر شیوه ای که تمایل داشت، آزاد نبوده است. البته به استناد محکومیتهای مکرر خواهان و اینکه عکسها فقط به متصدیان فروش داده شده بود، چنین حکم داد که عمل پلیس - بدون هیچگونه شک و شبهه ای - در جهت حفظ منافع عمومی بوده و پلیس با حسن نیت برای مقابله با جرایم و کاهش سرقت اقدام کرده است. (بین بریج، ۱۹۹۹: ۲۹۶)

ادعای اشتباه در ارایه اطلاعات الکترونیکی محرمانه به اشخاص غیر مجاز نیز اصولاً پذیرفته نیست. مگر اینکه مدعی با دلایل قابل قبول اثبات نماید که خطای رایانه ای منجر به رسوخ اسرار در شبکه شده و اقدامات معمول را برای جلوگیری از این کار انجام داده است. به نظر می رسد در مورد کلیه اسرار بتوان «اجبار» و «قوه قاهره» را از عوامل توجیه کننده ارایه اسرار به اشخاص غیر مجاز یا نشر آنها در شبکه به شمار آورد؛ زیرا اگرچه قوانین و مقررات در این مورد بحث زیادی به عمل نیاورده اند، ولی از قواعد عام می توان آن را استنباط نمود.

۶- نتیجه گیری

حقوق اسرار هنوز به طور کامل شکل نگرفته است: اگر برخی از قواعد عام را می توان برای طرح بعضی از مباحث از رشته های دیگر به عاریت گرفت، در این حیطه باید از اصول خاصی بحث کرد که تنها در حقوق اسرار جاریند. تعهد به عدم افشای اطلاعات مربوط به دیگران یا مرتبط با نظم عمومی و ملی در فضای مجازی تقریباً در رویه قضایی پذیرفته شده است، با اینحال این تمام بحث نیست: باید به موجب قوانین دقیق و تخصصی این علم را تثبیت کرد. در این راه قضات و دکترین کمک کار خواهند بود، اما مهمترین نقش را «پیگرد» و «اجرا» خواهد داشت. در روابط الکترونیکی - به ویژه، اینترنت - این تحقیق و اجرای اصول است که حداقل در سطح داخلی از رخنه بر حریم دیگران خواهد کاست و راه را بر متجاوزین به حقوق خصوصی و عمومی خواهد بست. در سطح جهانی، طرح حقوق اسرار به مفهوم تکلیف دولتها و اتباع به عدم افشای اسرار امنیتی و نظامی متعلق به اتباع یا نهادهای دولتی دیگر دول و حق آنها به تعقیب در دادگاههای بین المللی هنوز هم در ابهام قرار دارد و برخی از دولتها با افشای اسرار دول دیگر و توجیه سیاسی عمل زشت خود سعی در ممانعت از شکل گیری این روند را دارند. به دلیل فقدان یا نقص ضوابط یا کنترل موجود، اینترنت به محلی برای رد و بدل کردن اطلاعات خصوصی، اقتصادی و تجاری - و در برخی از موارد حتی دستکاری شده - دیگران بدل شده است. این بی قانونی ناشی از گمنامی را چنانچه گفته شد، می توان با ایمن کردن سیستم های اطلاعاتی یا تعیین کیفر برای متخلفین جبران نمود.

در زمینه جاسوسی الکترونیکی - اعم از اینترنتی، ماهواره ای و یا با استفاده از سایر وسایل ارتباط - کشورمان می تواند به عنوان پیشگام در این زمینه در سطح جهانی عمل نموده و با طرح آن در مراجع ذیصلاح بین المللی زمینه تصویب کنوانسیونها و مقررات دقیق جهانی را برای ضابطه مند کردن ارایه اطلاعات، جلوگیری از جاسوسی و دروغ پردازی از طریق وسایل ارتباطی جدید و اعمال ضمانت اجراهای متناسب برای متخلفین، فراهم آورد.

۷- منابع

۱- آیین نامه طرز نگاهداری اسناد سری و محرمانه دولتی و طبقه بندی و نحوه مشخص نمودن نوع اسناد و اطلاعات، مصوب جلسه یکم دیماه ۱۳۵۴ هیأت وزیران، به نقل از روزنامه رسمی شماره ۹۰۵۶ - ۱۳۵۴/۱۱/۱۳.

- ۲- قانون (لایحه) تأسیس نهاد ملی دفاع از حقوق شهروندی، مطروحه در کمیسیون لوایح دولت، برای دیدن متن لایحه، به سایت سخنگوی دولت رجوع شود: gov.ir/Commission.asp?CatID=197-www.spk
- ۳- قانون تجارت الکترونیکی (ایران) ، مصوب ۱۳۸۲/۱۰/۱۷، روزنامه رسمی ۱۳۸۲/۱۱/۱۱ - سال ۵۹، شماره ۱۷۱۶۷.
- ۴- قانون مجازات انتشار و افشای اسناد محرمانه و سری دولتی، مصوب ۲۹ بهمن ماه ۱۳۵۳. به نقل از روزنامه رسمی شماره ۸۷۹۴ - ۱۳۵۳/۱۲/۲۴.
- ۵- قانون مجازات جرایم نیروهای مسلح جمهوری اسلامی ایران، مصوب ۱۸ مرداد ۱۳۷۱ کمیسیون امور قضایی و حقوقی مجلس شورای اسلامی، به نقل از روزنامه رسمی شماره ۱۳۸۴۸ - ۱۳۷۱/۷/۲.
- ۶- مجموعه قوانین و مقررات جزایی، تدوین غلامرضا حجتی اشرفی، زیر نظر غلامعلی امیری، چاپ اول انتشارات گنج دانش، تهران ۱۳۸۱.
- 7- Bainbridge, David. Intellectual Property, Fourth Edition, Financial Times, Pitman Publishing, Harlow, England 1999.
- 8- Charney Scott, Transition Between Law Enforcement and National Defense, Security in the Information Age: New Challenges, New Strategies, Joint Economic Committee G01 Dirksen Senate Office Building, Washington, D.C. Internet Address: <http://www.house.gov/jec>
http://www.fas.org/irp/congress/2002_rpt/jec_sec.pdf
- 9- Chen, Angeline, The Definition and Integration of Law Enforcement and National Defense Efforts with Regard to Critical Infrastructure Protection, In: Security in the Information Age: New Challenges, New Strategies, Joint Economic Committee G01 Dirksen Senate Office Building, Washington, D.C. Internet Address: http://www.fas.org/irp/congress/2002_rpt/jec_sec.pdf
- 10- Davies, Philip.H.J, the Use and Abuse of Intelligence: 'Spin' , Open Government and the Politicisation of Intelligence in Britain, Political Studies Association, 2004. In: <http://www.psa.ac.uk/cps/2004/Daviesph.pdf>
- 11- Foster, William & Goodman, Seymour E. The Diffusion of the Internet in China, A report of the Center for International Security and Cooperation (CISAC), Stanford University, November 2000 <http://www.public.asu.edu/~wfoste1/chinainternet.pdf>
- 12- Froomkin A. Michael, The Death of Privacy? Stanford Law Review, Vol. 52 May 2000.
- 13- Gesmer, Lee. T. Protection of Trade Secrets in the Computer Industry <http://www.gesmer.com/publications/tradesecrets/4.php>
- 14- Huber, Peter. Law and Disorder in Cyberspace, Oxford University Press, New York 1997.
- 15- Lindberg, Agne & Henrik Bengtsson. Database—Aided IPR Due Diligence, In: Law and Information Technology Swedish Views, An anthology produced by the IT Law Observatory of the Swedish ICT Commission, Edited By: Peter Seipel, Information and Communication, Technology Commission Report, Stockholm 2002. Swedish Government Official Reports. http://www.itkommissionen.se/dynamaster/file_archive/030116/7e0e41f75b311025949bac25873c241e/Swedish%20Views%20antalogi%20rapport.pdf
- 16- Ramberg, Christina. Contracting on the Internet — Trends and Challenges for Law, In: Law and Information Technology Swedish Views, An anthology produced by the IT Law Observatory of the Swedish ICT Commission, Edited By: Peter Seipel, Information and Communication, Technology Commission Report, Stockholm 2002. Swedish Government Official Reports. http://www.itkommissionen.se/dynamaster/file_archive/030116/7e0e41f75b311025949bac25873c241e/Swedish%20Views%20antalogi%20rapport.pdf
- 17- Wai San, Mary Wong, The Nature of the Test of Confidential Obligations and its Implications for the Law of Confidence, Singapore Journal of Law studies [SJLS], 1997.
- 18- Information Control and Self—Censorship in the PRC and the Spread of SARS, Congressional—Executive Commission on China, Publication Date: May 7, 2003, www.cecc.gov .
www.cecc.gov/pages/news/prcControl_SARS.pdf