حمایت قانونی از اسرار و حریم خصوصی در عصر فناوری اطلاعات

ماشاءالله بناء نیاسری*

محمدرضا منوچهری**

تاریخ دریافت:۹۴/۱/۳۱ تاریخ پذیرش:۹۴/۶/۲۵

چکیده

حمایت از اسرار اقتصادی، تجاری و امنیتی و حریم خصوصی، از مسائل مهم در عصر فناوری اطلاعات در سطح جهانی به شمار می‌آید. حمایت قانونی شامل ترتیبات عدم افشا، مقررات استخدامی و سایر شروط قراردادی می‌شود. مفهوم حریم خصوصی به معنای توانایی یک شخص یا گروه برای محرمانه نگه‌داشتن خودشان یا اطلاعاتی در رابطه با خودشان و در نتیجه، اظهار هر چیزی است که خود بخواهند. محدوده و محتوای چیزی که محرمانه محسوب می‌شود در فرهنگ‌ها و اشخاص مختلف متفاوت است امّا اصل موضوع در همه جا پذیرفته شده است. وقتی که چیزی برای شخصی محرمانه باشد، این به طور معمول به این معنا است که برای آن شخص ذاتاً ویژه یا دارای حساسیت می‌باشد. محدودهٔ حریم خصوصی به طور جزئی با محرمانگی و امنیت، ارتباط می‌یابد که به معنای امکان استفادهٔ اختصاصی و در نتیجه، حمایت از اطلاعات است. حریم خصوصی همچنین می‌تواند شامل تمامیت جسمانی شخص نیز باشد. در این مقاله، به بحث در خصوص اهمیت و ضرورت حمایت از این اطلاعات و اسرار می‌پردازیم. تعهد به عدم افشا، یکی از مهم‌ترین معیارها در این زمینه است که باید مورد بررسی قرار گیرد.

واژگان کلیدی: *اسرار تجاری، اسرار دولتی، اسرار امنیتی، حقوق و تعهدات.*

*استادیار دانشکده حقوق دانشگاه شهید بهشتی.

Niasari@gmail.com

**دانشجوی دکتری حقوق خصوصی دانشگاه شهید بهشتی(نویسنده مسؤول).

mr.manouchehri19@yahoo.com

مقدمه

پیدایش وسایل الکترونیکی ارتباط در عصر حاضر، جابه‌جایی سریع اطلاعات و آگاهی‌ها را از تمامی جهات امکان‌پذیر ساخته است. آنچه که در تصوّر بشر نمی‌گنجید، اکنون به واقعیت بدل گردیده و به راحتی می‌توان ظرف کمترین زمان قابل تصوّر، اصوات، تصاویر، کتاب‌ها، اسناد، مدارک و ... را به هر کجای دنیا ارسال نمود. این رابطهٔ دو سویه میان فرستنده و گیرنده، اگرچه کارایی اعجاب‌آوری داشته است امّا در پاره‌ای از موارد نیز به حکم طبیعت امور، دارای زیان‌ها و مضرّاتی بوده است. در میان وسایل گوناگون ارتباط، به ویژه اینترنت، گمنام بودن، خطری را موجب شده است که به نسل جدیدی از جاعلان و سارقانِ هویت، جسارت می‌بخشد.

اگرچه «حقوق اسرار»[1] و «حقوق اسرار تجاری»[2] پیشینه‌ای طولانی دارد با این‌حال اِعمال آن، به دلیل مسائلی چون گمنامی،[3] سرقت شخصیت،[4] وجود شخصیت دیجیتالی و نفوذ هکرها در شبکه در عصر فناوری اطلاعات، با پاره‌ای از دشواری‌ها و ابهامات روبه‌رو شده است. امروزه امکان دارد که اسرار ملّی و نظامی یک کشور به هر دلیل از سوی دولت‌های دیگر در معرض دید عمومی قرار داده شود؛ چراکه اینترنت، امکان آن را فراهم ساخته است؛ یا اینکه حقّ حریمِ[5] شخص نقض شده و حیثیت او با افشای اسرار خصوصی‌اش به گونه‌ای بر باد رود که راهی برای اعادهٔ آن نباشد.

این مباحث و مسائل 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؛ چراکه نقض محرمانگی اسرار به بهانهٔ فقدان قانون یا نظام بین‌المللی خاص امکان دارد که دولت‌ها را روبه‌روی هم قرار دهد یا اشخاص را روانهٔ دادگاه سازد که ترفندی جز قواعد عام مسؤولیت برای مجازات مرتکبین در اختیار ندارد. حتّی در مواردی که گمنامی به مفهوم کامل آن، به دلیل ناامن بودن سیستم‌های رایانه‌ای محقّق است، عامل زیان یا

1- Thelaw of Secrets.
2- Trade secret law.
3- Anonymity.
4- Identity Theft.
5- privacy.

افشاکننده‌ای درکار نخواهد بود که بتوان مسؤولیت را بر وی بار نمود. در ادامه به بررسی موضوع در گفتارهای جداگانه می‌پردازیم:

۱- کلیات

قبل از ورود به بحث باید مفهوم «سر»، «حقوق اسرار» و «حقّ حریم» مشخص گردد و محدودهٔ هر کدام در عصر فناوری اطلاعات تبیین شود.

۱-۱- مفهوم «سِر»

سر یا راز، عبارت از هر چیز پنهانی است که مخفی بودن آن برای دارنده یا دارندگان موجب امتیاز باشد. راز، در مفهوم عام آن شامل تمام واقعیت‌ها، پدیده‌ها، تصوّرات، دانسته‌ها و حتّی تلخ‌کامی‌ها، اشتباهات و خطاهایی است که دارنده تمایلی به افشای آنها ندارد و از آگاهی یافتن دیگران به آن رموز به هر دلیل متضرّر می‌شود. افشای سر، برخلاف مفهوم لغوی، به معنی اطلاع‌یافتن تمام مردم از محتوای آن نیست بلکه امکان دارد با آگاهی حتّی یک نفر، افشای سر تحقّق یابد. بنابراین در این مفهوم، راز و افشا، دارای مفهومی متفاوت با معنای لغوی بوده است و اصطلاحی فنّی به شمار می‌آید؛ چراکه برای مثال، فرمول ساخت یک ریزپردازنده 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 تعهّد کارکنان به عدم افشای آن تردیدی ندارد.

در تعریف اسرار تجاری، عدّه‌ای آن را به «رازی که موجب امتیازی بالقوه یا بالفعل برای دارندهٔ آن در امر تجارت است یا هر چیزی که دارندهٔ آن را با اقدام متعارف به عنوان یک راز نگاه می‌دارد» تعریف کرده‌اند(Gesmer,2004).

ماده ۲ قانون حمایت از اسرار دولتی جمهوری خلق چین مصوّب ۱۹۹۸،[1] در تعریف «اسرار دولتی» مقرّر می‌دارد: «اسرار دولتی، عبارت از تمام چیزهایی است که به امنیت و منابع ملّی ارتباط می‌یابد. تعیین محدودهٔ این اسرار با قانون بوده و تنها اشخاص معیّنی برای مدّت محدود حقّ 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 منابع ملّی صدمه

1- Law on the protection of state secrets, P.R.C, 1988.

خواهد دیـد(*Information Control and Self_Censorship in the PRC and the spread of SARS,*2003,p.18).

۲-۱- مفهوم «حقوق اسرار»

اسرار، از گذشته و در عمل مورد حمایت بوده‌اند. برای نمونـه، در چـین باسـتان، مجـازات افشای اسرار یک گروه به دیگران زجرکشی بـود(Gesmer,2004). اگـر از داسـتان‌هـا و افسانه‌هایی که در مورد اسرار و رموز هست بگذریم با اینکه حمایـت از اسـرار بـه معنـی تعیین ضوابط دقیق علمی برای حفظ و جلوگیری از افشای آنهـا پیـشینه‌ای طـولانی دارد ولی تعریف حق و تعهد در مورد اسرار و اطلاعات محرمانه چندان سابقه نداشـته و قواعـد موجود در این زمینه، حتی در حال حاضر نیز ناقص می‌باشد. این وضعیت از دو بُعـد قابـل بررسی است: از یک طرف، به لحاظ تاریخی، کشورها همواره به حفاظت از اسرار دولتی و امنیتی توجه داشته و به اسرار اقتصادی توجّهی نداشته‌اند. این جنبه به مرور زمان اصـلاح 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 کـه قـدرت اقتصادی و نه توان نظامی، تعیین‌کنندهٔ استراتژی‌ها و قابلیت‌هاست، اسرار تجاری نیز مورد حمایت هستند. برای مثال: در ایالات متحـده، قـانون جاسوسـی اقتـصادی[1] در ۱۱ اکتبـر ۱۹۶۶ تصویب گردید و به ضابطه‌مندکردن قواعد حاکم بر حفاظت اسرار اقتصادی و تعیین ضمانت اجرا برای نقض حقوق اسـرار پرداختـه اسـت(Charney,2002,p.60). از سـوی دیگـر، بحـث دقیـق و حقـوقی از اسـرار دولتـی نیـز فـی‌الواقـع بعـد از انتـشار کتـاب «catcher Spy»[2] توسط شخصی به نام *پیتر رایت*[3] که سابقاً در سرویس امنیتی انگلیس[4] کار می‌کرد طرح گردید. او در این کتاب اطلاعات محرمانه‌ای را افشا نمود کـه بـه هـیچ وجه با مصالح دولت انطباق نداشت(Davies,2004,p.13). ایـن امـر و گـسترش وسـایل

1- Economic Espionage Act, 1996.

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

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

3- Peter Wright.

4- Military Intelligence 5 [MI5].

گوناگون صوتی و تصویری برای استراق سمعی و بصری، منجر به تصویب قوانین و مقرّراتی در کشورهای مختلف در جهت منع و تعیین ضمانت اجرا برای افشای اسرار شده است؛ بنابراین، مبنای «حقوق اسرار» را تعهد به عدم افشای اسرار[1] و در صورت نقض این تعهد، مجازات و مسؤولیت، بسته به نوع اسرار و نحوهٔ افشا متفاوت خواهد بود.

۳-۱- مفهوم حق حریم

واژهٔ «privacy» را عدّه‌ای از نویسندگان به «حق خلوت» نیز ترجمه کرده‌اند. عبارت جایگزین مذکور در بیان مفهوم privacy نارساست و اگرچه اصطلاح «حق حریم» نیز معادل دقیق privacy نمی‌باشد ولی بهتر از «حق خلوت» به نظر می‌رسد؛ چراکه برای داشتن حریم خصوصی و حق بر آن، نیازی به «خلوت» در مفهوم عرفی آن وجود ندارد. در این مفهوم، حقّ حریم، دارای معنی عام و در برگیرندهٔ حق هر شخص بر جان، تن، آزادی و ... و از جمله ـ بنابر آنچه به بحث ما ارتباط می‌یابد ـ به مفهوم حق هر شخص به داشتن اطلاعات مخفی و تکلیف مطّلعین به عدم افشای آنهاست. حق حریم، بر همین اساس شامل کلیهٔ اشخاص اعم از حقیقی و حقوقی بوده و تجاوز به آن از سوی هرکس که باشد محکوم و مشمول ضمانت‌های اجرایی است.

فصل اوّل از باب دوّم لایحه «حقوق شهروندی و تأسیس نهاد ملّی 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 و از تعرّض مصون بماند». همچنین به موجب ماده ۵۸ قانون تجارت الکترونیکی، مصوّب ۱۳۸۲/۱۰/۱۷، ذخیره و پردازش یا توزیع «داده پیام‌های» مبیّن ریشه‌های قومی یا نژادی، دیدگاه‌های عقیدتی، مذهبی، خصوصیات اخلاقی و داده‌پیام‌های راجع به وضعیت جسمانی، روانی و یا شخصی اشخاص، بدون رضایت صریح آنها به هر عنوان، غیر قانونی است».

چنانچه ملاحظه می‌شود در دو مقرّرهٔ فوق، مفهوم عامی از حق حریم ارائه شده و افشای اسرار و اطلاعات خصوصی افراد، ممنوع گردیده است. اگرچه در کشورهای دیگر نیز مقرّرات مشابهی به تصویب رسیده است 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

1- Obligation of Confidence.

حریم را به فراموشی سپرد (Froomkin,2000, Vol.52, p.1463) که در جای خود بـه ایـن ادعا پاسخ خواهیم گفت.

۲- مبانی حقوق اسرار در عصر فناوری اطلاعات

حقوق اسرار همانند سایر رشته‌های حقوقی، از قواعد معیّنی تبعیت می‌کند. این قواعـد در اغلب موارد، مشابه با سایر رشته‌ها هـستند. بـا ایـن وجـود، گـسترش اسـتفاده از وسـایل الکترونیکی برای ارتباط، نقض برخی از مبانی و اصول را پر رنگ کرده است. این مبانی را به شرح زیر می‌توان خلاصه نمود:

۲-۱- محرمانه بودن اطلاعات

ارائه اطلاعات از هر نوع که باشد علی‌الاصول، افشای آن به حساب نمی‌آید مگر اینکه به تصریح قانون یا سازمان معیّن یا به تشخیص عرف، آن اطلاعات در زمرهٔ اسـرار شـمرده شوند؛ لذا، چنانچه قاضی *مگاری*[1] نیز در پرونده‌ای[2] ابراز داشته است، اطلاعات باید دارای معیارهـای لازم بـرای محرمانـه بـودن باشـند تـا افـشای آنهـا مـستوجب مـسؤولیت باشد(San&Wong,1997, p.588).

بنابراین، چنانچه از مـواد ۱و۲ «قـانون مجـازات انتـشار و افـشای اسـناد محرمانـه و سرّی دولتی مصوّب ۱۳۵۳» نیز برمی‌آیـد اسـناد دولتـی در صـورتی سـرّی یـا محرمانـه می‌گردند که سازمان مربوطه اقدامات متعارف[3] را برای حفاظت از آنها انجام داده و در حدّ امکان، تعهد به عدم افشا را به کارکنان خود یادآور شده باشد؛ همانند حالت سنّتی، وظیفهٔ «احتیاط متعارف» از مقامات بالای سازمان شروع شده و به پـایین اسـتمرار مـی‌یابـد. در جهت جلوگیری از افشای الکترونیکی اطلاعـات، مـدیریت اجرایـی سـازمان یـا مؤسـسهٔ ذی‌ربط باید به طور دقیق مصادیق مشکوک ارائه الکترونیکی داده‌ها را بـا لحـاظ جوانـب علمی و فنی مـشخص کـرده و معیارهـای لازم را بـرای حفاظـت از اطلاعـات، معرفـی نمایند(Lindberg & Bengtsson,2002,p.122).

ماده‌ی ۱ قانون فوق، اسناد دولتی را عبارت از «هر نوع نوشته یا اطلاعات ثبـت یـا ضـبط شده مربوط به وظایف و فعالیت‌های وزارتخانه‌هـا و مؤسـسات دولتـی و وابـسته بـه دولـت و

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

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 دامنهٔ اسناد دولتی به مواد مذکور دارد و لذا با توسعهٔ فناوری می‌توان لوح‌های فشرده حاوی اطلاعات «CD»، حافظه رایانه، دیسکت‌ها، عکس‌ها و تصاویر ضبط شده توسط دوربین‌های تلفن همراه و موارد دیگر را در فرض تحقّق شرط «محرمانه بودن» در زمره اسناد دولتی سرّی یا محرمانه قلمداد کرد.

به موجب «آیین‌نامه طرز نگهداری اسناد سرّی و محرمانهٔ دولتی و طبقه‌بندی و نحوهٔ مشخص نمودن نوع اسناد و اطلاعات»، طبقهٔ هر سند را مسؤول واحد تهیه‌کنندهٔ آن سند تعیین می‌کند (ماده‌ی ۳) که تردیدی در اجرای این اصل در مورد اسرار الکترونیکی وجود ندارد. به طور کلّی به نظر می‌رسد که کلیه قوانین و مقرّرات موجود در مورد اسرار دولتی، امنیتی و تجاری و اقتصادی را باید در مورد شکل الکترونیکی این اسناد نیز اجرا نمود.

۲-۲- تعهد به عدم افشا

یکی از مبانی مهم حقوق اسرار، «تعهّد به عدم افشا» می‌باشد. در این معنی، علی‌الاصول، از فردی می‌توان انتظار عدم افشای اسرار را داشت که به موجب قانون یا عرف بر این امر، تعهّد داشته باشد. در حقوق «کامن لا»، این تعهّد ممکن است مبتنی بر تراضی و توافق طرفین یا بر مبنای انصاف باشد. برای مثال: تعهدات پزشکان، وکلا، کارکنان، مستخدمین و قضات، در عدم افشا را تنها می‌توان بر مبنای انصاف توجیه کرد(Bainbridge, 1999,p.285).

در حقوق ایران، این تعهّد اغلب مبنای قانونی دارد و برای مثال: تعهّد کلیهٔ کسانی که به مناسبت شغل یا حرفهٔ خود محرم اسرار می‌شوند در غیر از موارد امنیتی، به موجب ماده ۶۴۸ و در موارد مربوط به امنیت داخلی و خارجی کشور، بنا بر ماده ۵۰۱ 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 سرّی دولتی را نیز در صورت تحقّق مصادیق آن می‌توان در مورد مرتکبین اِعمال نمود. در مورد ذخیره، پردازش و یا توزیع داده‌پیام‌های شخصی مبیّن ریشه‌های قومی یا نژادی، دیدگاه‌های 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 گرفته‌اند. 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 اجرایی کیفری تحت حمایت قرار گرفته‌اند و افشای آنها به شیوه الکترونیکی، موجب مسؤولیت کیفری خواهد بود.

با فرض اثبات «تعهّد به عدم افشا» در مورد شخص معین؛ اولاً: او نمی‌تواند به حسن‌نیت یا عدم سوءنیت خود در افشای اسرار استناد نماید و برای نمونه در ارائهٔ اطلاعات از طریق نامهٔ الکترونیکی، مدّعی تصوّر مُجاز بودن گیرندهٔ پیام شود مگر اینکه دلایل قانع‌کننده‌ای برای صحّت ادعای خود ارائه نموده یا اثبات نماید که تمامی اقدامات متعارف را برای حفاظت اطلاعات به انجام رسانیده است؛ چنانکه در پروندهٔ معروف *اسپای کچر*، قاضی پرونده (Lord Goff)، ادعای آقای *رایت* (مؤلّف کتاب) را نپذیرفت و اعلام داشت: «در مورد مسأله، او باید با لحاظ اوضاع و احوال (قراین و عرف) می‌دانست که اطلاعات، محرمانه هستند و عامداً چشم خود را بر روی حقایق نمی‌بست»(San&Wong,1997,p.570). ثانیاً: مسؤولیت او محدود به مسؤولیت کیفری نخواهد بود و تمامی خسارات مادّی و معنوی وارده را نیز متحمّل خواهد گردید. این نوع از ضمان، خصوصاً در افشای اسرار تجاری الکترونیکی اهمیت ویژه‌ای می‌یابد؛ چراکه این اسرار، به تصریح ماده ۶۵ ق.ت.ا «به طور مستقل دارای ارزش اقتصادی بوده و در دسترس عموم قرار ندارند و تلاش‌های معقولانه‌ای برای حفظ و حراست از آنها انجام شده است».

۳-۲- معیار شخصی و عینی اسرار

مسأله‌ای 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 ارائه دو معیار را می‌توان بررسی نمود.

۱-۳-۲- معیار شخصی

به موجب این معیار، اطلاعات محرمانه در فضای مجازی تنها برای افرادی ایجاد مسؤولیت می‌کند که به موجب قانون یا قرارداد، مکلّف به حفاظت از آن اسرار می‌باشند؛ به عبارت دیگر، تعهّد به عدم افشا فقط برای افرادی قابل تصوّر است که اسرار از هر قسم به طور مستقیم در اختیارشان قرار گرفته و تعهّد به عدم افشا نیز به آنها یادآوری شده

است. ماده ۲ قانون مجازات انتشار و افشای اسناد محرمانـه و سـری دولتـی و مـاده ۵۰۱ ق.م.ا در مورد اسرار امنیتی، علی‌الظاهر بر همین مبنا تنظیم شده‌انـد؛ چراکـه در مـاده ۲، افشا یا انتشار اسرار توسط کارکنان سازمان و تعیـین مجـازات بـرای ایـن عمـل، مطـرح گردیده و در ماده ۵۰۱ ق.م.ا، افشای اسرار «به نحوی که متضمّن نوعی جاسوسی باشد» قابل مجازات شناخته شده است.

۲-۳-۲- معیار عینی

اسرار (اعم از تجاری و امنیتی) مطلقاً تحت حمایت قانون قرار دارند و هرکس آنها را افشا نماید حسب مورد مسؤولیت کیفری یا مدنی یا هر دو نوع را متحمّل خواهد بود. در مقابلِ دیدگاه کسانی که معتقدند «باید با لحاظ اوضاع و قراین، تعهّد به عدم افـشا، بـه شـخص موردنظر یادآوری شده باشد»(San&Wong,1997,p.570) شاید بتوان با تمسّک به نظر قاضی *مگاری* در پروندهٔ «کوکو علیه کلارک» چنین اظهارنظر نمود که: «اگر از اوضـاع و احوال، عرفاً چنین برآید که خوانده، از محرمانه‌بودن 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 است و همین امر باعث می‌شـود که در مورد افشای اطلاعات ناخواسته[1] و بدون سوءنیت، تعیین مسؤول با اشکال رو به رو گردد. پر واضح است که در روابط اینترنتی، اِعمال معیار عینی، نقض مهمی در ممانعت از افشای اسرار (بازدارندگی) و یا مجازات افشاکنندگان خواهد داشت؛ چراکه اگرچه شـخص، اطلاعات را ناخواسته به دست آورده امّا حـداقل در آگـاه نمـودن دیگـران نـسبت بـه آن اطلاعات حسن‌نیت نداشته است.

در خصوص اطلاعات ناخواسته، رویهٔ قضایی اندکی وجود دارد. با این وجود، دارندگان این اطلاعات را باید بر مبنای ملاک عینی، مسؤول دانست. در «کامن لا»، این مسؤولیت مبنی بر انصاف[2] می‌باشد؛ بدین معنی که وجداناً و انصافاً نمی‌توان اسرار امنیتی یا تجـاری متعلّق به دیگران را افشا نمود حتّی اگر آن اسرار، ناخواسته و اتفاقی دریافت شده باشد.

1- Unsolicited Information.
2- Equitable Obligation.

۳-۳-۲- تمایز میان دو معیار

معیار عینی و شخصی، هر کدام دارای تفاوت‌ها و وجوه برجسته‌ای می‌باشند که به اختصار می‌توان چنین برشمرد:

۱-۳-۳-۲- تفاوت در اثبات

با امکان اِعمال معیار شخصی، اثبات مسؤولیت، تسهیل می‌گردد؛ زیرا با اثبات اینکه شخص، تعهد به عدم افشا داشته و آن را نقض نموده است باید علی‌الاصول وی را مسؤول دانست مگر اینکه قوّهٔ قاهره یا عامل توجیه‌کنندهٔ دیگری در میان باشد. حال آنکه در صورت تمسّک به معیار عینی، باید دریافت اسرار از سوی شخص موردنظر، افشای عالمانهٔ آن اسرار و مسؤولیت کیفری (سوءنیت) وی را احراز نمود؛ بنابراین، اگر شخصی ناخواسته اطلاعاتی را از طریق نامهٔ الکترونیکی یا تبادل الکترونیکی داده[1] دریافت دارد در صورتی می‌توان او را مسؤول دانست که بر سرّی بودن آن اطلاعات آگاهی داشته و عالماً آنها را افشا کرده باشد.

۲-۳-۳-۲- 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 محقّق و در صورت علم و عمد در افشای اسرار، مجازات مشدّدی را برای افراد مذکور در نظر گرفت. به موجب ماده ۷۵ قانون تجارت الکترونیکی: «... هرکس 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 افشای اسرار شغلی و یا دستیابی غیرمجاز، 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 می‌آورند، علی‌الاصول در قبال آنها

1- Electronic Data Interchange [EDI].

مسؤولیتی ندارند مگر اینکه با علم به محرمانه و سری بودن آن، نسبت به افـشا اقـدام نماینـد. مسؤولیت این دسته از افراد چون بر مبنای انصاف محقّق می‌شود بیشتر صـبغهٔ مـدنی و مـالی دارد. البته در صورت وضع قانون خاص، مسؤولیت کیفری نیز منتفی نخواهد بود.

۳- حقوق اسرار و فناوری اطلاعات

اطلاعات، مایهٔ قدرت است و تحصیل اسرار دیگران به قصد بهره‌برداری نیز از این حقیقت خارج نیست. امروزه، فناوری اطلاعات و توانمندی کشورها در این زمینه، از عوامل اقتـدار آنها به شمار می‌آید و بدیهی است که تلاش دولت‌ها بـرای کـسب اطلاعـات از راه‌هـای قانونی و غیرقانونی، گسترش خواهند یافت. در این راستا، ورود به عصر دیجیتال، اختراع و عرضهٔ انواع فرستنده‌ها و گیرنده‌های الکترونیکی، گمنامی اینترنتی و ابهامـات موجـود در روابط مجازی، منجر به ایجاد زمینه‌ای برای سوءاستفاده شده است. بر همین اساس، بایـد مدعی شد که جز در صورت وجود یک نظام قدرتمنـد و علمـی بـرای حمایـت از اسـرار، نمی‌توان از دست‌یازی‌های دیگران به دور بود. بین‌المللی شـدن مـسأله و افـشای اسـرار نظامی و امنیتی در اینترنت (که بارها انجام شده است) نیز بـر ایـن واقعیـت دلالـت دارد. برخلاف نظر نویسنده‌ای که اختراع دوربین، تلفن‌های تـصویری، دسـتگاه‌هـای دیـدبانی، پیگردی الکترونیکی، انواع میکروفون‌ها، گوشی‌ها، وسایل هوشمند شـنیداری و دیـداری، نامهٔ الکترونیکـی، مبادلـهٔ الکترونیکـی داده و ... را موجـب تـضعیف حـقّ حـریم دانـسته است(Froomkin,2000,vol.52,p.1463) با وضع ضوابط فنـی و حقـوقی، بـه راحتـی می‌توان از مشکلات ناشی از ظهور فناوری جدید کاست و آن را به حداقل ممکن رسانید.

۳-۱- گمنامی

عدّه‌ای فکر می‌کردند فضای مجازی،[1] بهشت بی‌قانونی است که در آن مقـنّن داخلـی یـا بین‌المللی، توان وضع قاعده ندارد و حتّی اگر چنین نماید ضمانت اجرایـی وجـود نخواهـد داشت. این بهشت (و از سوی زیان‌دیدگان، جهنم)، از همان ابتدای ظهور روابط اینترنتی، به هیچ‌وجه ملاحظه نشد؛ چراکه آنچه در اینترنت رخ می‌دهد به عالم خیال تعلّق نداشته و به وقایع عالم حقیقی شباهت دارد(Ramberg,2002,p.109).

1- Cyberspace.

گمنانی اینترنتی، به معنی نامعلوم بودن هویت افرادی است که از طریق این شبکه با یکدیگر ارتباط برقرار می‌کنند. در آن صورت، هر قانونی برای کنترل فعالیت‌های اینترنتی، محکوم به بی‌اعتباری خواهد بود؛ حال آنکه در اکثر موارد با رهگیری‌های دقیق علمی، ردّ پای افراد و در نتیجه هویت ایشان شناسایی می‌شود و بر همین اساس اعمال مجازات برای یاغیان شبکه (هکرها) و افشاکنندگان اسرار، امکان‌پذیر است.

۲-۳- بی‌قانونی

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 نمی‌شود. عدّه‌ای به‌راحتی مسایل خصوصی مردم را به تصویر می‌کشند و به طور برخط[1] در اینترنت ارائه می‌کنند؛ مشخصات تأسیسات نظامی و امنیتی دولت‌های دیگر را فاش می‌کنند؛ با ارائهٔ تصاویر ساختگی و مستهجن، منجر به هتک حیثیت افراد می‌شوند و ...، بدون اینکه مورد پیگرد قرار گیرند و مجازات شوند.

این ادعا تنها در روابط بین‌المللی صحیح می‌نماید؛ چراکه دولت‌ها حقیقتاً خود را ملزم به رعایت حقوق اسرار امنیتی نمی‌دانند و متأسفانه افشای اسرار کشورهای دیگر از سوی دولت‌ها (دولتی شدن نقض اسرار) را هیچ مانعی رو به رو نیست. ولی در حقوق داخلی، اِعمال قوانین راجع به حفاظت اطلاعات و حمایت از اسرار در روابط الکترونیکی، بدون تردید امکان‌پذیر است و حتّی برخی از کشورها مقرّرات صریحی در منع افشای الکترونیکی اسرار وضع نموده‌اند. بنابر گزارش روزنامهٔ خلق،[2] وزارت امنیت داخلی چین[3] در ژوئن ۲۰۰۰، بخشنامه‌ای صادر کرد که تمام سازمان‌ها و اشخاص را از افشا، طرح یا انتقال اسرار دولتی در پایگاه‌های اینترنتی،[4] تابلوهای اعلان عمومی، واحدهای گپ‌زنی[5] و نیز نامهٔ الکترونیکی منع کرده است(Foster & Goodman,2000,p.31). به علاوه، به موجب قانون خاص،[6] در این کشور تصریح شده است که از اینترنت نمی‌توان برای صدمه

1- Online.
2- People's Daily.
3- Ministry of State Security of PRC.
4- Websites.
5- Chatroom.
6- Regulation on the Security and Management of Computer Information Networks and the Internet.1997.

به امنیت داخلی، افشای اسرار دولتی، متضرّر ساختن جامعه، آسیب رساندن به منافع ملّی جامعه یا گروه، حقوق شهروندان و یا شرکت در افعال مجرمانه استفاده نمود.[1]

در انگلیس، قانون اسرار رسمی،[2] افشای اسرار به اشخاص غیرمجاز 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.

۳-۳- اِعمال قواعد حقوق اسرار در عرصه بین‌المللی

یکی از مهم‌ترین ابهامات حقوق اسرار، تردید در امکان اجرای قواعد آن در عرصهٔ بین‌المللی است. آیا می‌توان با تمسّک به موازین بین‌المللی، افشای اسرار را به طور الکترونیکی منع نمود؟ اگر دولتی به طور خودسرانه اطلاعات سرّی متعلّق به تجهیزات نظامی و استراتژیک کشوری را در اینترنت منتشر نماید چه ضمانت اجرایی علیه آن دولت وجود خواهد داشت؟ آیا می‌توان علیه آن دولت در محاکم ذی‌صلاح بین‌المللی طرح دعوی نمود؟ سرانجام اینکه در فرض صلاحیت، کدام قانون بر اختلاف طرفین اعمال خواهد شد؟

رویهٔ بین‌المللی در زمینهٔ شناسایی حقوق اسرار و محکوم کردن نقض آنها، بسیار اندک است و حتّی در مورد نقض حقوق اسرار امنیتی و نظامی، اصولاً وجود ندارد. شاید زمانی تحوّلات حقوق مالکیت معنوی که اکنون حمایت از اسرار و علایم تجاری را نیز پوشش داده است، به این عرصه کشیده شود و بتوان راه‌حل‌های آن را اِعمال نمود. با این وجود، برخی از قواعد عام حقوق بین‌الملل را می‌توان برای منع افشای اسرار به کار گرفت که از جملهٔ آنها، اصل حسن‌نیت و احترام متقابل است.

سال‌ها است که کشورها امکان سرقت الکترونیکی اطلاعات امنیتی را دریافته‌اند. در آمریکا این اعتقاد وجود دارد که هکرها (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 فنّی جاسوسی و وسایل ارتباط الکترونیکی برای مقاصد دفاعی، نظامی و استراتژیک دخالت داشته‌اند(Chen,2002,p.64). تشریح این وضعیت در ایالات متحده نشان از

۱- مقرّرات ایمنی و مدیریت شبکه‌های اطلاعات رایانه‌ای و اینترنت چین مصوّب ۳۰ دسامبر ۱۹۷۷، ماده۴-۱.

2- Official Secrets Act, 1989.

دوراندیشی محقّقان این کشور دارد وگرنه امکان چنین سوءاستفاده‌ای از وسایل ارتباطی مدرن علیه منافع ملّی تمام کشورها قابل تصوّر است و همین امر نیاز به سنجش و تقویت سیستم‌های اطلاعات سرّی در سطح ملّی و فرا ملّی 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 زمرهٔ اطلاعاتی محسوب داشت که افشای آنها، نقض حقق اسرار به شمار می‌آید. با این حال می‌توان مواردی را تصوّر نمود که دولتی به خاطر منافع ملّی 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 «اوکلاهاما سیتی»، «سازمان بازرسی فدرال امریکا»[1] احضاریه‌ای به تمام دارندگان دوربین‌های تصویربرداری، عکاسی، وسایل دیداری و شنیداری ارسال داشت(Huber,1997,p.195). این وضعیت، نمود تحوّل در مفهوم حقّ حریم و حقّ داشتن راز می‌باشد که نیازهای امنیتی و اجتماعی، آن را تحمیل می‌نماید.

٤- ایمنی اسرار و عوامل توجیه‌کنندهٔ افشای اسرار در عصر فناوری اطلاعات

با ظهور فناوری‌های جدید شنیداری و دیداری، گوشی‌ها و حسگرهایی که حتّی 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 و 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 حتّی افشای اسرار، توجیه‌پذیر است. این موضع را به طور جداگانه تشریح می‌نماییم.

1- Federal Bureau of Investigation [FBI].

۱-٤- ایمنی اسرار در عصر فناوری اطلاعات

امنیت اطلاعات در عصر رُبات‌های الکترونیکی در اکثر موارد بُعد حقوقی نداشته و بیشتر به مسائل علمی و فنی ارتباط می‌یابد. تحقیقات زیادی در زمینه‌ی ایمنی داده‌های رسانه‌ای، از حیث عدم امکان نفوذ اشخاص غیرمجاز، انجام و نتایج آن ارائه شده است که می‌توان به آنها مراجعه نمود.[۱] حتّی برخی از نویسندگان، تقویت سیستم‌های الگوریتیم را پیشنهاد می‌نمایند؛ به‌گونه‌ای که حتّی معروف‌ترین سرویس‌های جاسوسی نیز توان شکستن (یافتن رمز ورود) آن را نداشته باشند(Huber,1997,p.190).

میزان ایمنی اطلاعات محرمانه و سرّی در برابر نفوذ هکرها و جاسوسان حرفه‌ای و متخصص در سیستم‌های الکترونیکی، از نظر حقوقی دارای آثار زیر می‌باشد:

نخست) از نظر حقوقی، تنها می‌توان از اسراری حمایت نمود که جنبه‌های علمی و فنی در حفاظت از آنها مراعات شده باشد. چنانچه قسمت اخیر ماده ۶۵ قانون تجارت الکترونیکی (در مورد اسرار تجاری) «تلاش‌های معقولانه برای حفظ و حراست» را شرط سرّی بودن داده‌پیام‌های الکترونیکی محسوب داشته است.

دوّم) نفوذ به اطلاعاتی که درجهٔ معقول و متعارفی از ایمنی را دارا می‌باشند در هر صورت موجب مسؤولیت است؛ زیرا با این اقدام «سوءنیت» مرتکب آشکار می‌گردد. چنانکه در پرونده‌ای[۲] قاضی پرونده (Lord Greene) اظهار داشت که تعهد به عدم افشا، محدود به مواردی که در آن اشخاص دارای رابطهٔ قراردادی هستند نمی‌باشد بلکه سوءاستفادهٔ یک نفر از موقعیتی که برای تحصیل اطلاعات سرّی داشته است نیز می‌تواند منجر به مسؤولیت شود(Bainbridge,1999,p.287). دلیل این وضعیت آشکار است؛ از یک سو، همواره عده‌ای معیّن و محدود بر اسرار آگاهی دارند و ایمن‌سازی اسرار توسط ایشان انجام می‌شود؛ لذا نمی‌توان آنها را به طور کامل کنترل کرد. از طرف دیگر در عصر فناوری اطلاعات، وسایل الکترونیکی روز به روز در حال پیشرفت و تحوّل هستند و چه بسا قبل از آگاهی و بهره‌گیری از جدیدترین فناوری، شخصی با دست یافتن به آن، نسبت به افشای اسرار اقدام نماید که در این صورت نیز نمی‌توان راه را بر او بست.

۱- ازجمله: مقاله‌های لیندبرگ و بنجستون، ۲۰۰۲و وانگ و دیران، ۲۰۰۲.

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

۲-٤- عوامل توجیه‌کنندهٔ افشای اسرار در عصر فناوری اطلاعات

اگر محرمانه بودن اسرار در فضای مجازی اثبات گردید اصل بر این است کـه نمـی‌تـوان آنها را افشا کرد مگر اینکه همان مصلحتی که ایجاب کرده آن اطلاعـات مخفـی بماننـد افشای آنها را تقاضا نماید؛ به عبارت دیگر، تنها با حکم قانون یا دادگاه می‌تـوان اسـرار را فاش نمود. مقرّرات موجود نیز بر این واقعیت تصریح دارنـد. بـه موجـب مـاده ۶۴ قـانون تجارت الکترونیکی، «به منظور حمایت از رقابت‌های مشروع و عادلانه در بستر مبـادلات الکترونیکی، تحصیل غیرقانونی اسرار تجاری و اقتصادی بنگاه‌ها و مؤسسات برای خود یا افشای آن برای اشخاص ثالث در محیط الکترونیکی، جرم محسوب و مرتکب به مجازات مقرّر در این قانون خواهد رسید».

به عنوان استثنای بر اصل عدم امکان افشای اسرار، دادگاه می‌تواند دستور رمزگـشایی الکترونیکی را صادر نماید. به موجب ماده ۱۰۴ قانون آیین دادرسی دادگاه‌های عمـومی و انقلاب در امور کیفـری مـصوّب ۱۳۷۸، «در مـواردی کـه ملاحظـه، تفتـیش و بازرسـی مراسلات پستی، مخابراتی، صوتی و تصویری مربوط به متهم برای کشف جرم لازم باشد قاضی به مراجع ذی‌ربط اطلاع می‌دهد که اشیای فوق را توقیف نموده و نزد او بفرستد...» و بنابر تبصرهٔ همین ماده، «کنترل تلفن افراد جز در مواردی که به امنیـت کـشور مربـوط است یا برای احقاق حقوق اشخاص، به نظر قاضی ضروری تـشخیص داده شـود ممنـوع است». در بند اخیر ماده ۱۰۵ قانون اخیرالذکر تصریح نموده است که اسناد سـرّی دولتـی نیز در صورت ضرورت با اجازهٔ رئیس قوّه قضائیه برای کشف جرایم و تحقیقـات کیفـری قابل ارائه می‌باشد.

از بُعد تطبیقی، افـشای اسـرار و اطلاعـات محرمانـهٔ بدسـت آمـده از طریـق وسـایل الکترونیکی، در حقوق خارجی نیز در موارد خاصی مجاز شـناخته شـده اسـت؛ چنانکـه در پرونده‌ای[1] خواهان ادعا نمود که پلیس، یک کپی از عکس‌های او را به متصدیان فروشگاه محلی ارائه نمود که او را در حال سرقت اشیای فروشگاه نشان مـی‌دهـد. در آن پرونـده، خواهان متهم به سرقت بود ولی بدان محکوم نشد (البته بعـدها بـه آن محکـوم گردیـد). قاضی اظهار داشت که پلیس در استفاده از عکس‌ها که امکان داشت به عنـوان جزئـی از

1- Hellwell v. Chief Constable Derbyshire [1984].

اسرار محرمانه به شمار آیند به هر شیوه‌ای که تمایل داشت آزاد نبوده است. البته به استناد محکومیت‌های مکرّر خواهان و اینکه عکس‌ها فقط به متصدیان فروش داده شده بود چنین حکم داد که عمل پلیس (بدون هیچ‌گونه شک و شبهه‌ای) در جهت حفظ منافع عمومی بوده و پلیس، با حسن‌نیت برای مقابله با جرایم و کاهش سرقت اقدام کرده است(Bainbridge,1999,p.296).

ادعای اشتباه در ارائه اطلاعات الکترونیکی محرمانه به اشخاص غیرمجاز نیز اصولاً پذیرفته نیست مگر اینکه مدعی، با دلایل قابل قبول اثبات نماید که خطای رایانه‌ای منجر به رسوخ اسرار در شبکه شده و اقدامات معمول را برای جلوگیری از این کار انجام داده است. به نظر می‌رسد در مورد کلیهٔ اسرار بتوان «اجبار» و «قوّه قاهره» را از عوامل توجیه‌کنندهٔ ارائهٔ اسرار به اشخاص غیرمجاز یا نشر آنها در شبکه به شمار آورد؛ زیرا اگرچه قوانین و مقرّرات در این موارد بحث زیادی به عمل نیاورده‌اند ولی از قواعد عام می‌توان آن را استنباط نمود.

نتیجه

حقوق اسرار هنوز به طور کامل شکل نگرفته است. اگر برخی از قواعد عام را می‌توان برای طرح بعضی از مباحث از رشته‌های دیگر به عاریت گرفت در این حیطه باید از اصول خاصی بحث کرد که تنها در حقوق اسرار جاری‌اند. تعهّد به عدم افشای اطلاعات مربوط به دیگران یا مرتبط با نظم عمومی و ملّی، در فضای مجازی، تقریباً در رویه قضایی پذیرفته شده است؛ با این حال 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 امّا 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 متعلّق به اتباع یا نهادهای دولتی دیگر دول و حقّ آنها به تعقیب در دادگاه‌های بین‌المللی 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 شکل‌گیری این روند دارند.

به دلیل فقدان یا نقص ضوابط یا کنترل موجود، اینترنت به محلّی برای ردّ و بدل کردن اطلاعات خصوصی، اقتصادی و تجاری (و در برخی از موارد حتّی دستکاری شدهٔ دیگران) بدل شده است. این بی‌قانونی ناشی از گمنامی را چنانکه گفته شد می‌توان با ایمن‌کردن سیستم‌های اطلاعاتی یا تعیین کیفر برای متخلّفین، جبران نمود. در زمینهٔ جاسوسی الکترونیکی، اعم از اینترنتی، ماهواره‌ای و یا با استفاده از سایر وسایل ارتباط، کشورمان می‌تواند به عنوان پیشگام در این زمینه در سطح جهانی عمل نموده و با طرح آن در مراجع ذی‌صلاح بین‌المللی زمینهٔ تصویب کنوانسیون‌ها و مقرّرات دقیق جهانی را برای ضابطه‌مندکردن ارائهٔ اطلاعات، جلوگیری از جاسوسی و دروغ‌پردازی از طریق وسایل ارتباطی جدید و اِعمال ضمانت اجراهای متناسب برای متخلّفین، فراهم آورد.

فهرست منابع

الف) قوانین و آیین‌نامه‌ها

۱-آیین‌نامهٔ طرز نگهداری اسناد سرّی و محرمانهٔ دولتی و طبقه‌بندی و نحوهٔ مشخص نمودن نوع اسناد و اطلاعات، مصوب جلسهٔ یکم دی ماه ۱۳۵۴ هیأت وزیران، به نقل از روزنامه رسمی شماره ۹۰۵۶ مورخ ۱۳۵۴/۱۱/۱۳.

۲-قانون (لایحه) تأسیس نهاد ملّی دفاع از حقوق شهروندی، مطروحه در کمیسیون لوایح دولت. برای دیدن متن لایحه، به سایت سخنگوی دولت رجوع شود.

۳-قانون تجارت الکترونیکی (ایران)، مصوّب ۱۳۸۲/۱۰/۱۷، روزنامه رسمی، سال ۵۹، شماره ۱۷۱۶۷، مورخ ۱۳۸۲/۱۱/۱۱.

۴-قانون مجازات انتشار و افشای اسناد محرمانه و سرّی دولتی، مصوّب ۲۹ بهمن ماه ۱۳۵۳، به نقل از روزنامه رسمی شماره ۸۷۹۴ مورخ ۱۳۵۳/۱۲/۲۴.

۵-قانون مجازات جرایم نیروهای مسلّح جمهوری اسلامی ایران، مصوّب ۱۸ مرداد ۱۳۷۱ کمیسون امور قضایی و حقوقی مجلس شورای اسلامی، به نقل از روزنامه رسمی شماره ۱۳۸۴۸ مورخ ۱۳۷۱/۷/۲.

۶-مجموعه قوانین و مقرّرات جزایی، تدوین غلامرضا حجتی اشرفی، زیر نظر غلامعلی امیری، انتشارات گنج دانش، چاپ اوّل، تهران، ۱۳۸۱.

ب) منابع خارجی

7- Bainbridge, David, *Intellectual Property*, Fourth Edition, Financial Times, Pitman Publishing, Harlow, England, 1999.

8- Charney, Scott, *Transition Between Law Enforcement and National Defence, 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 Politicistation 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. In: 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*, 2004, in: 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 & Bengtsson, Henrik, *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. Swedish Government Official Reports, 2002. 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. Swedish Government Official Reports, 2002. http://www.itkommissionen.se/dynamaster/file_archive/030116/7e0e41f75b311025949bac25873c241e/Swedish%20Views%20antalogi%20rapport.pdf.
17- San, Wai & Wong, Mary, *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.

Legal Protection of Secrets and Privacy in Information Technology Age

Mashaallah Banae Niasari*
Mohammadreza Manouchehri**

Received:20/4/2015 *Accepted:16/9/2015*

Abstract:
Protecting economic, trade and national secrets and privacy is an important matter of information age worldwide. Legal protections include non-disclosure agreements and work-for-hire and non-compete clauses. The concept of privacy is the ability of an individual or group to seclude themselves, or information about themselves, and thereby express them selectively. The boundaries and content of what is considered private differ among cultures and individuals, but share common themes. When something is private to a person, it usually means that something is inherently special or sensitive to them. The domain of privacy partially overlaps security (confidentiality), which can include the concepts of appropriate use, as well as protection of information. Privacy may also take the form of bodily integrity. This paper discusses the importance and necessity of protecting these kinds of secrets. Obligation to non-disclosure is one of the main factors in this field which should be discussed.

Key words: Trade Secrets, State Secrets, Security Secrets, rights and Obligations.

*Assistant Professor of Law Faculty at Shahid Beheshti University.
Niasari@gmail.com
**Ph.d student of Private Law at Shahid Beheshti University.
mr.manouchehri19@yahoo.com