حقوق اسرار تجاری در عصر فناوری اطلاعات

مصطفی السان*

چکیده: با ورود به عصر فناوری و امکان دسترسی و پردازش سریع اطلاعات در تمام نقاط جهان، حمایت از اسرار تجاری اهمیت فوق‌العاده‌ای یافته است. مفهوم حقوق اسرار تجاری، با رویکرد وضعیت این حقوق در عصر فناوری اطلاعات و ضمانت‌اجراهای قانونی و عملی برای حمایت همه‌جانبه از اسرار تجاری در عصر ارتباطات نوین، به ندرت در حقوق کشورمان مورد توجه قرار گرفته است. همین امر منجر به بروز مشکلات حقوقی و قضائی گوناگونی در مقام دادرسی اختلافات مطرح شده با ادعای نقض حقوق اسرار و درخواست حمایت قانونی از آنها، شده است. در مقالهٔ حاضر، ضمن تحلیل مباحث مربوط به حقوق اسرار تجاری، مسئولیت ناشی از نقض حقوق اسرار (اعم از قراردادی، قهری و کیفری) و چالشهای فراروی حمایت از اسرار، مورد بحث قرار گرفته و ضمن نگاه تطبیقی به مسئله نقض حقوق اسرار تجاری (به طور خاص در حقوق کامن‌لا)، راهکارهای حقوقی لازم ارائه می‌گردد.

واژگان کلیدی: *اسرار تجاری، فناوری اطلاعات، حقوق کامن‌لا، تجارت الکترونیک و مالکیت معنوی.*

---

* دانشجوی دکتری حقوق خصوصی دانشگاه شهید بهشتی.

مقدمه

پیدایش وسایل الکترونیک ارتباط در عصر حاضر، جابه‌جایی سریع اطلاعات و آگاهیها را از در تمامی جهان امکان‌پذیر ساخته است. آنچه که در تصور بشر نمی‌گنجید، اکنون به واقعیت بدل گردیده و به راحتی می‌توان در کمترین زمان ممکن اصوات، تصاویر، کتابها، اسناد و مدارک ... را با هر کجای دنیا مبادله کرد. این رابطه دو سویه میان فرستنده و گیرنده، اگرچه کارآیی اعجاب‌آوری دارد و بسیاری از مشکلات موجود فراراه صنعت و علم را از میان برداشته، اما در پاره‌ای موارد نیز به حکم طبیعت امور، زیانها و مضراتی را به دنبال داشته است. در میان وسائل گوناگون ارتباط، اینترنت، به‌ویژه گمنامی بی‌خطری را پدیدآورده است که به نسل جدید جاعلان و سارقان هویت، جسارت می‌بخشد.

اگرچه «حقوق اسرار تجاری»[1] پیشینه‌ای طولانی دارد، با این حال اعمال آن در عصر فناوری اطلاعات به دلیل مسائلی چون گمنامی[2]، سرقت شخصیت[3]، وجود شخصیت دیجیتالی و نفوذ هکرها در شبکه با دشواریها و ابهامات گوناگونی روبه‌رو 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. یا اینکه حق حریم[4] شخص نقض شده، حیثیت او با افشای اسرار خصوصی‌اش به گونه جبران‌ناپذیری بر باد رود.

از این رو حفظ اسرار تجاری امروز، یکی از دغدغه‌های مهم به شمار می‌رود. به عنوان نمونه، مطالعه «جمعیت آمریکایی امنیت صنفی»، حاکی از آن است که افشای اسرار تجاری یکی از عوامل عمده زیان شرکتها و

1. Trade Secret Law
2. Anonymity
3. Identity Theft
4. Privacy

مؤسسات صنفی بوده که میزان آن به دو میلیارد دلار در هر ماه بالغ گردیده است. مطالعه مذکور نشان می‌دهد که سرقت اسرار از سال ۱۹۹۲ تا ۱۹۹۵، ۳۲۰ درصد افزایش یافته است. میزان زیانهای ناشی از نقض حقوق مالکیت معنوی، در سال مالی ۲۰۰۱، به ۵۳ تا ۵۹ میلیارد دلار رسیده است.[۱] نمی‌توان سهم توسعه فناوری اطلاعات را در این افزایش نادیده انگاشت.

اسرار تجاری به معنی هر گونه اطلاعاتی است که دارنده مایل به مخفی نگه داشتن آن از دیگران است، علی‌الاصول تحت حمایت قانون قرار می‌گیرد. دزدی اسرار یا هر اقدام مبتنی بر تقصیری که منجر به افشای آن شود، موجب مسئولیت بوده و به همین دلیل در تمام کشورهای دنیا، راه برای طرح دعوی مسئولیت مدنی در چنین مواردی باز است؛ حتی برخی کشورها، این اعمال را جرم و مستوجب کیفر شناخته‌اند.[۲۹۴: ۱۰] دادگاهها جایگاه مسئولیت در حقوق اسرار تجاری را به مثابه «تلاشی برای تحمیل اخلاق به سوداگری» محسوب داشته‌اند.(۱)

در این مقاله، به بررسی جنبه‌های مختلف حقوق اسرار تجاری در عصر فناوری اطلاعات خواهیم پرداخت.

اما ابتدا باید مفهوم «سر» و «حقوق اسرار» مشخص شده، محدوده هر کدام در عصر فناوری اطلاعات تبیین شود. بررسی مختصر پیشینه و تاریخچه حقوق اسرار تجاری نیز از مقدمات بحث به شمار می‌آید.

۱. *اسرار تجاری و تاریخچه حقوقی آن*

۱ـ۱. *مفهوم اسرار تجاری*

سرّ یا راز، عبارت از هر چیزی پنهانی است که مخفی بودن آن برای

---

1. Abbott lab. v.Norse chem. Corp., 33 Wis. 2 d 445, 454 (1967); See: Hill, James W. Trade Secrets, Unjust Enrichment, and the Classification of Obligations, 4 Virginia Journal of Law & Technology, No 2. Spring 1999.

دارنده یا دارندگان موجب امتیاز باشد. راز در مفهوم عام آن شامل تمام واقعیتها، پدیده‌ها، تصورات، دانسته‌ها و حتی تلخ کامیها و خطاهایی است که دارنده متمایل به آگاهی یافتن دیگران از آنها نیست و از افشای آنها متضرر می‌شود.

افشای سر، لزوماً به معنی اطلاع یافتن تمام مردم به محتوای آن نیست؛ بلکه امکان دارد صرفاً با آگاهی یک نفر، افشای سر تحقق یابد. بنابراین، راز و افشا دارای مفهومی دقیق بوده و اصطلاحی فنی به شمار می‌آید. 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 تجاری» در محرمانه بودن مورد مزبور و تعهد کارکنان به عدم افشای آن تردیدی ندارد.

عده‌ای اسرار تجاری را «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.[۸:۱] راز تجاری نسبت به اسرار امنیتی عنوانی منعطف‌تر و جدیدتر است. این عنوان از آن جهت به نوعی استقلال می‌یابد که به ندرت با نظم و منافع عمومی ارتباط پیدا می‌کند و در عین حال، توسعه تجارت الکترونیک در سایه جهانی شدن فناوری اطلاعات منجر به دقیق شدن مباحث مطرح در این حوزه شده است.

در واقع، نباید تردید کرد که تجارت الکترونیک، مخاطرات بیشتری را در راه حفظ اسرار تجاری ایجاد کرده است. شیواترین سخن در تحلیل این وضعیت را یک قاضی استرالیایی اظهار داشته است:[۱]

«در حال حاضر، فناوری امکان ایجاد میلیون‌ها راز ارزشمند را درون

1. Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd [2001] HCA 63 (15 November 2001)

شبکه‌های بی‌شمار الکترونیک فراهم ساخته است. این وضعیت از آن جهت چندان خوشایند نیست که نمی‌توان تشخیص داد که چه کسی می‌تواند به نامه‌های الکترونیک یا شخصی، سابقه پزشکی یا مالی یا مکالمات تلفنی ما دسترسی داشته باشد».

برای اینکه اطلاعات راز تجاری محسوب شوند، سه شرط عمده مورد نیاز است که فقدان هرکدام موجب رد درخواست حمایت می‌گردد. نخست اینکه، اطلاعات مورد ادعا، باید حاوی امتیاز رقابت‌زایی برای دارنده آن باشند. دوم، اطلاعات به نحوی که عرفاً شایسته آنهاست، حفاظت شده باشند. بنابراین، قرار دادن اطلاعات مهم تجاری و مالی در یک پایگاه اینترنتی ناامن یا ارسال آنها به وسیله نامه‌های الکترونیک رایگان که هر لحظه در معرض هَک و Phishing قرار دارد، غیر «متعارف» بوده و دارنده اطلاعات نمی‌تواند تقاضای حمایت از آنها را به عنوان «راز تجاری» مطرح کند. به همین دلیل، در پرونده‌ای، دادگاه اثبات «راز» بودن خواسته را شرط ورود در ماهیت پرونده و صدور حکم دانسته است.[1] لذا عدم رعایت اصول ایمنی در طراحی شبکه و پایگاه اینترنتی که منجر به دسترسی آسان افراد غیر حرفه‌ای به اسرار شود، در خصوص اسرار تجاری اینترنتی، «حفاظت متعارف» محسوب نمی‌گردد. دو شرط یاد شده، با توجه به رویه قضائی، تقریباً اجماعی است.[۱۹:۲۷] برخی از محققین، به استناد آرای قضائی که به ویژه در سالهای اخیر صادر گردیده، قید سومی را نیز به دو شرط فوق افزوده‌اند و آن، اینکه باید اقدامات مؤثری برای حفاظت از اسرار انجام شده باشد.[۱۵] در واقع این شرط در صدد بیان این نکته مهم و ظریف است که حفاظت از اسرار تجاری، امری «مستمر» است و اگر مراتب ایمنی، حتی

1. Electro-Craft Corp. v. Controlled Motion, Inc. 332 N.W.2d 890, 897 (Minn.1983) ("[W] ithout the finding of a trade secret, [the court] can not grant relief..")

برای مدت کوتاهی رعایت نشده و در نتیجه، افشا یا سوء استفاده مستقیم از اسرار روی داده باشد، مالکِ اسرار، به عنوان زیان‌دیده، نمی‌تواند مدعی تحت الحفظ بودن اسرار شود.

اطلاعات را از آن جهت که ارزش پولی دارند، باید جزء دارایی هر فرد به شمار آورد. «دارایی» بهترین واژه برای توصیف «اسرار تجاری»است. زیرا همان گونه که داشتن اسرار «امتیاز» محسوب می‌شود، نداشتن آنها به ویژه در عصر فناوری اطلاعات که مدام در حال تحول است، به طور مستقیم «عیب»و البته نقص یک سیستم و در نتیجه عامل عقب ماندن از نظام گسترده و پر سود تجارت الکترونیک به شمار می‌آید.

۱ـ۲. *تاریخچه حمایت از اسرار تجاری*

حمایت از اسرار تجاری[۱] به نحو عملی به سال ۱۹۵۱ در انگلستان[۲]، و ۱۸۶۸ در ایالات متحده[۳] باز می‌گردد. حقوق کامن‌لا در این زمینه با دو هدف عمده تشویق پژوهش و اختراع و پشتیبانی از استانداردهای اخلاق تجاری شکل گرفته است.[۴]

در آمریکا، برخلاف حقوق بیماران، کپی‌رایت و علائم تجاری، مقرره خاصی در سطح فدرال راجع به اسرار تجاری وجود ندارد. بازنویسی حقوق مسئولیت مدنی[۵] که به وسیله مؤسسه آمریکایی قوانین در سال ۱۹۳۹ انجام گردید،اولین تلاش رسمی برای به رسمیت شناختن حقوق اسرار

۱. چنانچه در مباحث آتی خواهیم دید، به لحاظ تصور سه نوع عمده سوءاستفاده از اسرار تجاری (دستیابی، افشا و بهره‌مندی)، استفاده از عبارت «نقض حقوق اسرار تجاری» با توجه به لحاظ معنایی اعم از سه قسم مذکور، صحیح‌تر به نظر می‌رسد.

2. Morison v. Moat, 68 En. Rep. 492, 9 Hare 241 (1851).

3. Peabody v. Norfolk, 98 Mass. 452 (1868)

4. See. e.g., E.I du Pont deNemours Co.v.Masland, 244 U.S. 100 (1917); E.I du Pont F.Supp. 507 (D.III. 1985); Hill, op cit.

5. Restatement of Torts

تجاری در ایالات متحده بود، به گونه‌ای که هنوز هم به عنوان مرجع قضات در آرای مرتبط به شمار می‌آید.[۲۸-۲۷و۳:۱۲] نویسندگان بازنویسی دوم مسئولیت مدنی، به عمد از پرداختن به حقوق اسرار امتناع کردند، شاید به این دلیل که استنباط مؤسسه از حقوق رقابت که از جمله شامل اسرار تجاری می‌شد، به نوعی متفاوت بود. در سطح ایالتی، تدوین مقررات برای اسرار تجاری تا سال ۱۹۷۹ به کندی صورت می‌گرفت، اما در آن سال کانون وکلای آمریکا،قانون متحد الشکل اسرار تجاری [۲۰] را به عنوان قانون نمونه به تصویب رسانید. علاوه بر آن ویرایش سوم رقابت ناعادلانه[1] که توسط مؤسسه آمریکایی حقوق در سال ۱۹۹۵ انتشار یافت، حاوی مقررات نسبتاً پیش‌رفته‌ای در باب اسرار تجاری است. علی‌رغم سیر قانونی فوق، دادگاهها در تصمیمات خود حسب مورد، علاوه بر تک تک مقررات فوق به رویه قضائی نیز توجه دارند.

در سال ۱۹۶۶، قانون جاسوسی اقتصادی به تصویب رسید که اولین قانون فدرال در زمینه اسرار تجاری به شمار می‌آید. این قانون برای حمایت از اسرار صرفاً به ضمانت اجراهای کیفری متمسک شده است. به این دلیل که راه برای طرح دعاوی حقوقی - اعم از مسئولیت مدنی یا قراردادی - برای زیان‌دیدگان باز است و حقوق مانعی در این مسیر ایجاد نکرده است.

۱-۳. مفهوم «حقوق اسرار تجاری»

اسرار از گذشته عملاً مورد حمایت بوده‌اند. برای نمونه، در چین باستان، مجازات افشای اسرار یک گروه به دیگران، زجرکشی بود.[۸:۱] با اینکه حمایت از اسرار به 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

1. Restatement (Third), of Unfair Competition.

در حال حاضر نیز ناقص است.

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 بیش از توان نظامی تعیین‌کننده استراتژیها و قابلیتهاست، اسرار تجاری نیز مورد حمایت هستند. برای مثال، چنانچه گفته شد، در ایالات متحده قانون جاسوسی اقتصادی[1] که 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.[۱۷]

باید توجه داشت که برخی از استادان در استقلال حقوق اسرار تجاری، تردید کرده و آن را مجموعه‌ای نه چندان مستقل از قواعد قرارداد، کلاهبرداری، سرقت، خیانت و.. دانسته‌اند [۳:۲۴۶] این تحلیل، از آن جهت صحیح به نظر نمی‌رسد که امکان طرح این ادعا، در مورد تمام شاخه‌های فرعی علم حقوق وجود دارد. در واقع، ارتباط بین رشته‌های مختلف غیر قابل انکار و تقسیم‌بندی آنها به اقسام گوناگون، از جمله با هدف تسهیل مطالعه صورت می‌گیرد. البته باید اذعان داشت که حقوق اسرار در مفهوم عام آن، به دلیل ارتباط با امنیت ملی و بین‌المللی، با حقوق عمومی و از جهت ضرورت حمایت از منافع اشخاص، با حقوق خصوصی هم‌خانواده می‌شود. در یک نگاه کلی، با تطبیق حقوق اسرار تجاری و حقوق تجارت می‌توان آنها را در یک دسته‌بندی قرار داد. هرچند، تشخیص جایگاه این رشته در میان سایر شعب علم حقوق، از حیث بررسی اصول و قواعد حاکم بر حقوق اسرار

1. Economic Espionage Act (1996)

تجاری دارای اهمیت است؛ اما پرداختن به آن، تحقیق جامع‌تری را می‌طلبد.

۲. *حقوق اسرار تجاری و حقوق تعهدات*

اسرار تجاری، برای مالک (دارنده) آن ایجاد حق و امتیاز می‌کنند. البته عنوان «تکلیف به حفظ اسرار و رعایت اصول حفظ اسرار» بر مبنای «متعارف» هم از جمله آثار «دارایی» اسرار و بر دوش مالک آن است. در «حقوق تعهدات»، بیشتر جنبه «حق» راز تجاری برای دارنده آن و تعهد یا تکلیفی که برای افراد دیگر ایجاد می‌کند (مانند تعهد به عدم افشای اسرار محیط کار، توسط کارگر؛ یا تکلیف به جبران خسارت ناشی از به کارگیری ناحقِ اسرار دیگران) مورد بررسی قرار می‌گیرد. بعد از پرداختن به جنبه «منصفانه» حقوق اسرار تجاری، به ابعاد قراردادی و قهری آن نیز خواهیم پرداخت.

۲ـ۱. *تعهد به حسن نیت و حقوق اسرار تجاری*

یکی از مبانی منصفانه مطرح برای مسئولیت ناشی از نقض حقوق اسرار تجاری[۱]، که ریشه در سنتهای حقوقی دارد، توجیه این تعهد با حسن نیت است. در واقع، محرمانه بودن اطلاعات اقتضای حسن نیت در حفظ آنها را دارد و خلاف آن (سوء نیت) موجب مسئولیت خواهد بود. بر فرض ثبوت این تعهد، دو پرسش عمده باید پاسخ داده شود: نخست اینکه، آیا اصل بر حسن نیت است و مدعی خلاف، باید آن را علیه کسی که حقوق اسرار تجاری را نقض کرده، اثبات کند یا نه؟ و دوم اینکه، بر فرض اثبات حسن نیتِ شخصی که اسرار تجاریِ تحت اختیار او به هر دلیل و طریق، مورد سوء استفاده قرار گرفته، آیا می‌توان بازهم مسئولیت وی را، ورای حسن نیت و فراتر از این مقوله مطرح کرد؟

---

۱. چنانچه در مباحث آتی خواهیم دید، به لحاظ تصور سه نوع عمده سوء استفاده از اسرار تجاری (دستیابی، افشا و بهره‌مندی)، استفاده از عبارت «نقض حقوق اسرار تجاری»، با توجه به لحاظ معنایی اعم از سه قسم مذکور، صحیح‌تر به نظر می‌رسد.

قبل از پاسخ‌دهی به این سؤالات، باید تذکر داد که تعهد به حسن نیت در حفظ اسرار تجاری، حداقل در حقوق کامن‌لا ثابت است[۱] چنانچه در چند پرونده، دادگاه علاوه بر تمسک به ضابطه قراردادی برای احراز نقض حقوق اسرار تجاری به مبانی «انصاف»، استناد کرده است.[۲] در پاسخ به سؤالات نیز باید قائل به نسبی بودن موضوع و ارجحیت اظهار نظر خاص در هر قضیه با لحاظ اوضاع و احوال آن، شویم. در واقع، نه می‌توان گفت اصل بر حسن نیت نیست (چراکه دوام روابط اجتماعی بر آن استوار است) و نه می‌توان فردی را که از همان ابتدا با قصد افشا یا استعمال غیرمجاز، اسرار تجاری دیگری را در اختیار گرفته، «محسن» شناخت. تصور این امر که شخص، با وجود حسن نیت، به دلایلی همچون سهل‌انگاری، بی‌مبالاتی و.. مسئول شناخته شود نیز هیچ‌گاه منتفی نمی‌باشد.

توسل به انصاف، از جمله در مواردی کارساز خواهد بود که جبران پیش‌بینی شده در قرارداد، نسبت به خسارت وارده کمتر باشد؛ در این صورت دادگاه دستاویزی برای مسئولیت مدنی نخواهد داشت و چاره‌ای جز تمسک به انصاف نیست. فقدان سابقه انصاف در نظام قضائی، جبران پاره‌ای خسارات ـ یا پیش از آن، تصمیم‌گیری در مورد ماهیت قضیه راجع به نقض حقوق اسرار ـ را با دشواری روبه‌رو می‌سازد. به همین دلیل توجه به این مقوله، حداقل در این حوزه ضروری به نظر می‌رسد.

۲ـ۲. اسرار تجاری و حقوق قرارداد

قرارداد، بهترین رابطه قابل تصور از حیث اثبات و جبران خسارت است. آنجا که این ادعا با عقدی صریح پشتیبانی نمی‌شود، تلاش مدعی برای اثبات

1. Coco v.A N Clark (Engineers) Ltd [1969]: Franklin v.Giddins [1978].
2. New Zealand Needle Manufacturers Ltd v.Taylor 1975; Robb v.Green 1895; Nichrotherm Electrical Co Ltd v.JR Perry and G A Harvey & Co London 1956.

وجود «توافق»، *لزوماً قاضی را به وجود چنین رابطه‌ای قانع نمی‌سازد*. هرچند احساس شرط ضمنی یا توافقی در جهت حفظ اسرار با چنین مضمونی، همیشه وجدان قاضی را برمی‌انگیزد و در تصمیم نهایی وی مؤثر می‌افتد. در این گفتار، مبنا را بر این می‌گذاریم که «تعهد به حفظ اسرار شغلی و حرفه‌ای»، لزوماً تعهدی ناشی از قرارداد به شمار نمی‌آید؛ مگر اینکه توافقی در میان یا قابل استنباط باشد.

۲ـ۲ـ۱. *نقش توافق‌نامه استخدامی در پیش‌گیری از نقض حقوق اسرار*

اسرار تجاری اغلب با نقض تعهدات ناشی از روابط کاری ـ استخدامی که در نتیجه آن مستخدمی به افشای اسرار حوزهٔ کاری می‌پردازد، در معرض خطر قرار می‌گیرند. بهترین نوع حمایت از اسرار تجاری در روابط استخدامی، انعقاد توافق‌نامه صریح با موضوع «تعهد به رازداری» است.[۱۹۹:۴] در صورت وجود چنین توافقی، به دلیل مطرح بودن رابطه قراردادی،در اینجا بیش از اینکه تعرض به دارایی کارفرما مطرح باشد، تخلف از قرارداد، مبنای مسئولیت قرار می‌گیرد. زیرا مستخدم به عنوان خوانده می‌تواند مدعی فقدان اوصاف دارایی برای خواسته (راز تجاری) شود، اما قطعاً نمی‌تواند منکر تعهد قراردادی خود به حفظ اسرار شغلی و حرفه‌ای خویش گردد. بنابراین تلاش مستخدم برای دسترسی به اسرار خارج از حرفه خویش ـ ولو اینکه آن اسرار در همان محل کار او باشد ـ تخلف از قرارداد محسوب نمی‌گردد و تنها از باب مسئولیت مدنی یا تعهد به حسن نیت یا انصاف قابل پیگرد می‌باشد. برای مثال، اگر مهندسی که در واحد سیستم عامل یک شرکت تولید نرم‌افزار مشغول به کار است، عمداً یا به طور تصادفی، به اسرار واحد بازی و سرگرمی یا واحد نرم‌افزارهای آموزشی دسترسی پیدا کند و اقدام به افشا یا سوء استفاده از آنها کند، حسب مورد مسئولیت کیفری یا مدنی خواهد داشت و به دلیل فقدان رابطه قراردادی مرتکب با واحد زیان‌دیده، مسئولیتی از این باب متوجه وی نخواهد بود؛ مگر اینکه توافق‌نامه تعهد به رازداری که

وی طرف متعهد آن است، عام بوده و شامل اسرار تمام قسمتها و امور شخص حقوقی مربوط باشد.

۲ـ۲ـ۲. *ماهیت تعهد به حفظ اسرار*

یکی از مسائل مطرح، این است که آیا می‌توان «تعهد به حفظ اسرار» را به توافق طرفین ربط داد؟ به عبارت دیگر، ماهیت این تعهد (اگر قراردادی باشد)، چیست؟

پیش از پاسخ، باید اذعان داشت که همین تردید منجر شد که محاکم کامن‌لا هنگام رویارویی با پرونده‌هایی با موضوع اسرار تجاری، کمتر به دنبال کنکاش در رابطه قراردادی طرفین باشند.[۱] زیرا توافق طرفین (قرارداد اصلی)، در تحمیل التزام به حفظ اسرار به طرفین آن، چندان صریح نیست. به علاوه، افرادی با نقض حقوق اسرار از سوی طرف قرارداد ارتباط می‌یابند که لزوماً طرف عقد نیستند و دادگاهها عملاً با عجز یا غمض عین نسبت به رابطهٔ قراردادی، همه را به یک چوب می‌رانند. در هر حال، تنها راه برای توجیه نحوه انتساب تعهد به حفظ اسرار تجاری به قرارداد طرفین، «شرط یا توافق ضمنی» در این باره است. مگر اینکه قرارداد، حاوی قید چاره‌ساز «تعهد به حفظ اسرار تجاری و حرفه‌ای» به طور صریح باشد. وضعیتی که به ویژه به لحاظ ارتباط شرکتهای درگیر با مسائل فناوری ارتباطات با تولید روزافزون اسرار جدید یا افشای هزینه‌بر اسرار قدیمی، در قراردادهای استخدامی یا همکاری فنی خود درج می‌نمایند. پروانه‌های نمایندگی تولید یا فروش نرم‌افزار، سخت‌افزارهای الکترونیک و وسایل پیشرفته دیگر، اغلب حاوی

---

۱. برای مثال، در پرونده((Electro-Craft Corp.v. Controlled Motion, Inc.(Minn. 1983) دادگاه رأی داد که توافق بر رازداری، در صورتی که محکمه، اطلاعات را «راز» تشخیص ندهد، اجرا نخواهد شد؛ همچنین در پرونده(,American Paper & Packaging prod Inc.v. Kirgan) مقرر گردید که ارائه مفهوم خاص از اسرار تجاری در قرارداد استخدامی، دادگاه را به رعایت همان مفهوم ملتزم نمی‌کند. See: Hill, op cit, Footnote 76

تعهد به حفظ اسرار تجاری برای شخصی هستند که از شرکت مادر، پروانه فعالیت دریافت می‌کند.

وجود قرارداد مستقل در خصوص تعهد به حفظ اسرار تجاری یا شرط صریح این قید در قرارداد اصلی، این امتیاز عمده را دارد که متخلف از قرارداد نمی‌تواند با اثبات اینکه خواسته، «راز» به مفهوم «به کلی سری» نبوده، خود را از مسئولیت مبرا سازد. زیرا حتی افشای اسرار کارخانه‌ای که امکان دارد هزاران مستخدم شرکت از آن آگاهی داشته باشند، در این حالت تخلف از عقد محسوب شده و موجب مسئولیت خواهد بود.

۲ـ۳. اسرار تجاری و مسئولیت مدنی

دنیای مدرن با دو خصیصه «آینده‌نگری» و «نکته‌سنجی»، جایگاه مسئولیت قهری را در دفاع از قلعه‌ی اسرار کمرنگ کرده است. با این وجود، حداقل در عرصه فناوری اطلاعات، این مسئولیت هنوز پابرجاست. گمنامی، بی‌نامی، چندنامی، دیگرنامی (استفاده از نام و مشخصات دیگران) و.. منجر به آن شده که به ویژه در ارتباط با مشتریان، مصرف‌کنندگان و کاربران اینترنتی، یا قراردادی در میان نباشد و یا وقت کاربر با ارزش‌تر از آن باشد که برای پرکردن مُشتی فرم تلف شود. رضایت به قراردادهای استاندارد، با موضوع تعهد کاربر یا مشتری به حفظ اسرار نیز، اغلب بدون مطالعه و با رجوع بی‌درنگ شخص به قسمت انتهایی صفحه برای انتخاب نمایه‌ی «موافقم»[1] اعلام می‌گردد. گاه تعهداتی که از قالب قرارداد خارج می‌ماند نیز بر گستره این حیطه می‌افزاید. آنچه در این مبحث می‌آید، تأملی در مفهوم و محدوده مسئولیت قهری از باب حفظ یا نقض حقوق اسرار تجاری است.

۲ـ۳ـ۱. تحقق مسئولیت مدنی به مفهوم عام

اگر تمام یا قسمتی از سوء استفاده از اسرار، مشمول رابطه قراردادی نباشد،

1. I Agree Submit.

در آن صورت نباید در صدق نهاد مسئولیت مدنی تردید کرد. البته تحصیل نامشروع اسرار تجاری، در همه حال تحت لوای مسئولیت مدنی قرار نمی‌گیرد. در یک پرونده[1]، دادگاه بخش ایالات متحده رأی داد که تحریک مالک از سوی شخصی دیگر برای افشای اسرار به رقیب، اگرچه امکان دارد مشمول عناوینی همچون رقابت ناعادلانه باشد، اما منجر به مسئولیت مدنی ناشی از دسترسی یا افشای اسرار تجاری نیست. نظر دادگاه بر این بود که رقابت ناعادلانه دارای مفهومی گسترده‌تر از نقض اسرار بوده و شامل هر فعالیت غیرمنصفانه در عرصه سوداگری می‌شود.

تحلیل فوق صحیح به نظر می‌رسد؛ زیرا عدم پذیرش آن منجر به این نتیجه غیرمنطقی خواهد بود که باب محصولات فکری (غیرمادی)، تنها با هراس از اینکه مبادا شخصی مدعی سوء استفاده از دانسته‌های او برای تولید آن محصولات باشد، مسدود گردد. در واقع با ارائه محصول (به طور نمونه، نرم‌افزار) در بازار، متخصصین امر به راحتی می‌توانند فناوری به‌کار رفته در آن را ـ حتی اگر برای آنها سابقه‌ای نداشته باشد ـ کشف کنند و نمی‌توان انتقال نامحسوس یا قهری فناوری را در همه موارد، نقض حق اسرار تجاری محسوب داشت. در مثال فوق، همان‌گونه که در روابط بازرگانی نیز ملاحظه می‌شود، بحث رقابت غیرمنصفانه نیز مطرح نمی‌گردد: کشف و طراحی «سیستم ارتباط کوتاه بی‌سیم»[2] از سوی یک شرکت، برای نخستین بار در جهان، نباید این حق را برای شرکت مذکور ایجاد کند که مدعی «انحصار» بر این فناوری یا «راز» بودن آن شود و در نتیجه اطلاع دیگران از شیوه علمی

1. Filmways Pictures, Inc. v. Marks Polaroid Corp., 552 F. Supp. 863, 867 S.D.N.Y. 1982.
quotiong Roy Export Co. v. Columbia Broad. SYs., Inc., 672 F. 2 d 1095, 2205 2d Cir. 1982.

2. Bluetooth or Infrared System

طرح مذکور ـ و لو با بررسی دستگاههای شرکت طراح ـ را منع کند. در واقع، پذیرش چنین تهدیدها و تحدیدهایی در عصر فناوری اطلاعات نه امکان‌پذیر است و نه به صلاح رشد روزافزون علم و دانش بشری.

۲ـ۳ـ۲. *دارا شدن ناعادلانه و نقض حقوق اسرار*

جایی که مسئولیت قهری صدق کند، یکی از مبانی مطرح برای مسئولیت شخصی که به اسرار تجاری دست یافته، آن را فاش کرده یا به کار گرفته است، نهاد «دارا شدن ناعادلانه» می‌باشد. بر مبنای این تأسیس که سابقه‌ای به قدمت حقوق مسئولیت مدنی دارد، شخصی که به ناحق رازی را دارا شده، در مقابل مالک آن مسئول است.

دقت در مسئله بیانگر آن است که توسل به نهاد دارا شدن ناعادلانه در زمینه اسرار تجاری، چندان ساده نیست. در واقع، تفکیک بین نحوه سوء استفاده از اسرار، مبین تحقق ارکان نهاد دارا شدن، تنها در برخی از مصادیق نقض حقوق اسرار می‌باشد. به عبارت دیگر، نقض این دسته از حقوق، به یکی از سه شکل زیر متصور است:

نخست، شخصی که حق دسترسی به اسرار تجاری نداشته، بدانها دسترسی پیدا کند. در این حالت نیز، ممکن است دسترسی شخص با علم و آگاهی بوده یا کاملاً تصادفی باشد (دستیابی).

دوم، شخصی که به نحو مشروع یا نامشروع بر اسرار تجاری دسترسی داشته، اعم از اینکه حق به کارگیری آنها را داشته باشد یا نه، اسرار را نزد شخصی که حق دسترسی به آنها را ندارد، افشا کند (افشا).

سوم، شخصی که به اسرار دسترسی مشروع داشته و در هر حال حق بهره‌گیری از آنها را دارا نبوده است؛ اقدام به استفاده از آنها (به‌کارگیری) برای منافع تجاری خویش (مثبت) یا به زیان رقیب (منفی) نماید.

برای مثال، (الف) مهندس واحد تولید سخت‌افزار یک کارخانه سازنده تلویزیون است. واحد تحقیقات کارخانه، اخیراً به فناوری ساخت صفحه‌های

مسطح با کوچک‌ترین ابعاد ممکن دست یافته است؛ چون اطلاعات واحد تحقیق، در اختیار واحد تولید قرار نگرفته و ساخت از روی نمونه صورت می‌گیرد، اقدام (الف) برای دسترسی به اسرار «دستیابی»؛ ارائه اطلاعات مذکور به شخص غیرمجاز (ب)، «افشا» و استفاده یا سوء استفاده از اسرار توسط (ج) که آنها را از «ب» تحصیل کرده، تحت عنوان «به‌کارگیری» مطرح می‌شود. در تمام حالات فوق، ممکن است اقدام هریک از دستیابنده، افشاگر یا کاربر، یا تمام یا بعضی از ایشان، عالمانه و عامدانه بوده یا توأم با جهل باشد. همچنین امکان دارد، دو عنوان دستیابنده و کاربر در شخص واحد جمع شود که در این حالت، «افشا» قابل تصور نخواهد بود.

هرچند جهل هر سه شخص (دستیابنده، افشاگر و کاربر)، به «راز تجاری» بودن یک امر کاملاً نادر است؛ اما تصور آن محال نیست. برای مثال، (الف)، زمانی به راز بودن جزئیات فعالیت یک شرکت، که به طور اتفاقی در اینترنت بدانها دست یافته، آگاهی می‌یابد که اطلاعات مذکور را از طریق نامه الکترونیکی یا تبادل الکترونیکی داده به صدها نفر ارسال کرده و برخی از ایشان نیز با پخش این پیام در سطح اینترنت، زمینه بهره‌مندی رقبای جاهل به راز بودن پیام را فراهم ساخته‌اند. در واقع، توسعه و تنوع فناوریهای ارتباطات و اطلاعات، تصور چنین فرضی را آسان کرده است. جدای از این وضعیت نادر که عملاً نمی‌توان مسئولیت را بر شخص خاصی تحمیل کرد؛ در حالت علم و عمد، قواعد حقوق مسئولیت اجرا می‌شود. البته در صورت علم عده‌ای و جهل برخی دیگر، باید بر مبنای «تحمیل مسئولیت بیشتر به دارندهٔ نیت سوء» بین ایشان قائل به تفکیک شد.

در ارتباط با تطبیق عنوان دارا شدن ناعادلانه به هر یک از سه فرض فوق‌الذکر، باید توجه داشت که این نهاد در حالتی که دستیاب، اقدام به افشای اطلاعات نکرده یا شخصاً از آنها بهره‌مند نشده، صادق نیست. زیرا دارا شدن به مفهوم عرفی و حقوقی آن، تنها زمانی تحقق می‌یابد که موجد نفع مادی یا

معنوی برای دارنده باشد و صرف تحصیل، اگرچه امکان دارد واجد عنوان مدنی یا کیفری به لحاظ رکن علم و عمد باشد، اما «دارا شدن» به شمار نمی‌آید. البته، افشای اسرار از سوی دستیابنده، حتی در فرضی که متضمن نفع مادی مستقیم برای افشاکننده نباشد، دارا شدن ناعادلانه محسوب می‌شود؛ چراکه مقصود از دارا شدن، بالضروره «ارتباط مستقیم فعل و شیء» نیست. بهره‌مندی از اسرار تجاری، از آن جهت که منجر به نفع مادی می‌شود، مشمول «دارا شدن ناعادلانه» بوده و محکوم به ارکان و آثار آن است.

از این حیث، می‌توان «دارا شدن ناعادلانه» را با جرم سرقت در حقوق کامن‌لا مقایسه کرد. در کامن‌لا، یکی از ارکان لازم برای تحقق سرقت، «تصاحب» یا منظور کردن مال مسروقه برای خویش است. هرچند تحقق این رکن در حد قصد نیز برای اطلاق جرم کافی است، اما فی‌نفسه بیانگر آن است که هدف باید استفاده یا سوء استفاده (که به نوعی همان مفهوم استفاده را دارد)، باشد و صرف در اختیار داشتن کافی نیست. بر مبنای همین تحلیل، در گزارش تفسیری بخش سوم «قانون متحدالشکل اسرار تجاری»، اصلاحی قانون مصوب ۱۹۸۵ «کنفرانس نمایندگان رسمی برای تصویب قوانین متحدالشکل ایالات متحده»[1]، «تصاحب ناحق»[2] شرط تحقق «دارا شدن ناعادلانه» محسوب شده است.

در این خصوص که صرف در اختیار داشتن، دارا شدن به شمار نمی‌آید، می‌توان به پرونده دو پونت[3]، استناد کرد. شرح پرونده اینکه، خوانده، به هنگام نصب تجهیزات کارخانه تولید الکل متیلیک (متانول) خواهان، اقدام به عکس‌برداری هوائی از آن کرده بود. وضعیتی که عکسها نشان می‌داد، تنها از

1. National Conference of Commissioners on Uniform State Laws.
2. Misappropriation.
3. E.I du Pont deNemours Co.v. Christopher, 431 F. 2d 1012, 1017 5th Cir. 1970.

آسمان قابل مشاهده بود و به همین دلیل، این اشکال در تصمیم‌گیری دادگاه بروز کرد که هیچ یک از عناوین مجرمانه یا مسئولیت همچون خیانت، تخلف از قرارداد یا نقض اصول حقوقی، مثل تعهد به رازداری محقق نبود. با این‌حال، دادگاه خوانده را به دلیل تحصیل نامشروع اسرار دیگری (در قالب عکس) مسئول شناخت. به زعم محکمه، تصاویر هوایی می‌توانستند مقدمه نامشروع استفاده از اسرار تجاری باشند. این مثال، همچنین به استقلال حقوق اسرار تجاری از سایر شاخه‌های حقوق، دلالت دارد.

نقض حقوق اسرار، در مورد افرادی که اسرار حرفه‌ای و شغلی در اختیار دارند، به طور قطع منجر به مسئولیت حرفه‌ای ایشان است. از آن جهت که نمی‌توان رابطهٔ قراردادی میان شخص و تعهد او به حفظ اسرار مشتریان برقرار کرد. بنابراین تعهد مذکور نیز بر مبنای مسئولیت مدنی و در کشورهایی که «انصاف» را پذیرفته‌اند، گاه بر همین مبنا استوار می‌شود.[1] سه نکته مهم در مورد مسئولیت حرفه‌ای و حقوق اسرار تجاری قابل یادآوری است:

نخست اینکه، به دلیل تنوع مشاغل، مسئولیت حرفه‌ای به حفظ اسرار شغلی نیز حیطه گسترده‌ای دارد و برای مثال تعهد پزشکان، وکلا، تجار، قضات، کارمندان اداری، خادمان، قائم مقام تجاری، نماینده، سرویس‌دهنده امضا و ارتباط اینترنتی و.. را شامل می‌شود. که البته نمی‌توان همه آنها را با مبنایی واحد مورد بررسی قرار داد. دوم اینکه، تعهد به حفظ اسرار حرفه‌ای،

---

۱. البته این ادعا نیز قابل بررسی است که «تعهد به حفظ اسرار حرفه‌ای» بر مبنای «قرارداد» تحلیل گردد. در آن صورت مباحث مهمی مطرح می‌شود که باید درصدد یافتن پاسخ آنها و اقناع منتقدین بود. از جمله اینکه، این قرارداد به کدام «ارادهٔ تعهدزا» منتسب می‌شود؟ آیا واقعاً کسی که حرفه‌ای را شروع می‌کند، ملتزم به حفظ اسرار حرفه‌ای خویش می‌شود (ارادهٔ تحمیلی)؟ ماهیت «قرارداد» مذکور چیست؛ توافق تک تک مشتریان (طرف مقابل) که ممکن است تعدادشان در طول سالهای اشتغال شخص به آن حرفه، از هزاران نفر فراتر رود؛ یا «قرارداد جمعی» افراد ناشناسی که جدای از هم ارادهٔ خویش را به ملتزم ساختن شخصی که او را فقط به کارش می‌شناسند، ابراز داشته‌اند؟

در اکثر موارد همراه با «سوگندی» است که شخص قبل از شروع به کار یاد می‌کند و از جمله خود را ملزم به حفظ اسراری می‌کند که در محدوده شغل او در اختیار وی قرار می‌گیرند. در سایر موارد، این تعهد ناشی از عرف و رسم تجاری و شرایط و اوضاع و احوال می‌باشد. به همین دلیل است که دفاع یک پزشک در افشای اسرار در مقایسه با قائم مقام تجاری، دشوارتر پذیرفته می‌شود. زیرا شخص اول (پزشک)، ملتزم با قید قسم است. سوم اینکه، تعهد به حفظ اسرار حرفه‌ای، تنها در آن بخش از اسرار که به «حرفه» و «شغل» شخص ارتباط دارند، مطرح بوده و در خارج از آن مشمول قواعد عام می‌شود.

۲ـ۳ـ۳. نقض حقوق اسرار تجاری و شبه عقد

پرسشی که می‌توان مطرح ساخت، این است که آیا می‌توان رابطه تعهد به حفظ اسرار را با شبه عقدی چون «اداره فضولی امور غیر»، مقایسه کرد؟ صدق این عنوان، از جمله در مواردی است که شخص ناخواسته به اسراری دست یابد که مالک، قدرت حفظ آن را نداشته و یا به هر دلیل از حیطه تسلط وی خارج شده و در عین حال دارای ارزش تجاری و اقتصادی فوق‌العاده‌ای برای اوست. در حالاتی از این قبیل، به نظر می‌رسد که بتوان نوعی تعهد مبتنی بر شبه عقد را به دارنده اسرار تحمیل کرد که البته دارای تمام آثار شبه عقد (نظیر استحقاق دریافتِ هزینهٔ حفظ اسرار و..)، خواهد بود.

۳. *اسرار تجاری و حقوق کیفری*

تعیین مجازات برای افشای اسرار، سابقه‌ای طولانی‌تر از مسئولیت قراردادی یا غیرقراردادی دارد. علت این امر، بیش از اینکه با حقوق اسرار در ارتباط باشد، با فلسفهٔ مجازات و تاریخ تحول اندیشه‌های بشر در زمینه ضمانت‌اجرا بستگی دارد. البته کیفرهایی همچون زجرکشی برای افشاکننده، در طول زمان تعدیل یافته‌اند. در این مبحث، روند این تحول، قوانین و مقررات مرتبط و

ارتباط جرائم علیه اسرار را با سایر جرائم مورد بررسی قرار می‌دهیم.

۳ـ۱. جرم‌انگاری نقض حقوق اسرار تجاری

در حقوق ایران، چنانچه بررسی می‌شود، قانون تجارت الکترونیکی، مواد خاصی (۶۴، ۶۵ و ۷۵) را به حقوق اسرار تجاری و حمایت از آنها اختصاص داده است. جز این قانون، پاره‌ای از مواد لایحه جرائم رایانه‌ای نیز به نوعی متعرض بحث شده‌اند. بررسی لایحه، بیانگر آن است که وجود قانون سابق (قانون تجارت الکترونیکی) و اجتناب از تداخل مواد دو مقرره، به ندرت مدنظر بوده است. در این بند، تنها تا حدی در صدد طرح بحث هستیم که با «اسرار تجاری الکترونیکی» ارتباط دارد. برای مثال، ماده ۱۳ لایحه مقرر می‌دارد: «هر کس به وسیله سیستم رایانه‌ای یا مخابراتی صوت یا تصویر و یا فیلم خصوصی و یا خانوادگی یا اسرار دیگری را، به جز موارد قانونی، بدون رضایت او منتشر کند یا در دسترس دیگران قرار دهد به گونه‌ای که منجر به ضرر وی شود یا به طور عرفی موجب هتک حیثیت او تلقی شود به مجازات مقرر برای افشای سر محکوم خواهد شد». ایرادات عمده‌ای به این ماده وارد است: نخست اینکه، ماده مذکور در بیان «افشای سر»، مفهوم عامی را از «سر» مدنظر داشته و از بیان صریح مقصود امتناع کرده است. حال آنکه بهتر بود که معنی دقیق واژه مذکور ـ به دلیل اینکه در حقوق کشورمان چندان مورد بررسی قرار نگرفته ـ مشخص می‌گردید. دوم اینکه، مجازات افشای سر در ماده ۶۴۸ قانون مجازات اسلامی معین شده که عبارت از سه ماه و یک روز تا یک سال حبس و یا یک میلیون و پانصدهزار تا شش میلیون ریال جزای نقدی می‌باشد؛ معلوم نیست در شرایطی که شمای کلی لایحه بر استقلال از سایر مقررات و تعیین کیفر مستقل بر مدار حبس‌زدایی می‌باشد، چرا حکم مسئله به قانون مجازات اسلامی واگذار شده است. نیز، می‌توان تداخل ماده ۱۳ لایحه با مواد ۵۸ و ۶۴ قانون تجارت الکترونیکی و عدم کفایت کیفر تعیین

شده برای اسرار تجاری را به اشکالات ماده مذکور افزود.[۱]

از بعد تطبیقی، در حقوق آمریکا «قانون جاسوسی اقتصادی»، تنها به دنبال جرم‌انگاری نقض حقوق اسرار است و در آن سخنی از سایر تضمینها به میان نمی‌آید. مجازات مقرر برای سرقت اسرار در ماده ۱۸۳۲ این قانون، ۲۵۰ هزار دلار و ده سال حبس برای اشخاص حقیقی و جزای نقدی به میزان بیش از پنج میلیون دلار برای اشخاص حقوقی است. مطابق همین قانون، در صورتی که جاسوسی اقتصادی به قصد منتفع ساختن دولت بیگانه‌ای انجام گیرد، فاعل آن اگر شخص حقیقی باشد، به بیش از پانصدهزار دلار و پانزده سال حبس محکوم می‌گردد و اگر شخص حقوقی باشد، جزای نقدی وی بیش از ده میلیون دلار خواهد بود.

شدت مجازاتها در قانون جاسوسی اقتصادی، با احتیاطهایی که در ایالتهای مختلف در قالب مقررات مسئولیت، ایمنی و حفاظت اسرار تجاری

---

۱. حتی اگر مبنای لایحه، تأکید بر استقلال از سایر مقررات و تعیین کیفر مستقل بر مدار حبس‌زدایی باشد، نمی‌توان با لحاظ بی‌منطق بودن اولی و کلی بودن دومی، از چنین مبانی و اهدافی که ابداع لایحه می‌باشد، حمایت کرد. ایرادات را به نحو دیگری نیز می‌توان مطرح ساخت: از یک سو، مجازات افشای اسرار تجاری، در صورتی که با اقتصاد ملی ارتباط یابد، در زمره «جرائم علیه امنیت اقتصادی» قرار می‌گیرد که مقنن توجه خاصی بدان مبذول نداشته است. از سوی دیگر، تصریح لایحه جرائم رایانه‌ای مبنی بر ملغی بودن قوانین مغایر با آن، در ماده ۴۲۷ در اکثر موارد راهگشا نیست. زیرا قاضی در مقام رسیدگی، ممکن است با تفسیر عامی که از خواسته می‌نماید، آن را در شمول قانون مجازات دانسته و خارج از حیطه لایحه (قانون) جرائم رایانه‌ای محسوب دارد. جالب‌تر آنکه، لایحه در ماده (۴)، برای «جرائم علیه امنیت» از مجازات سنگین‌تری غیر از جزای نقدی از ده میلیون ریال تا یکصد میلیون ریال، استفاده نکرده است. تدقیق در لایحه مبین آن است که تدوین‌کنندگان آن، به هر قیمتی درصدد «حبس‌زدایی» بوده‌اند، ولو این رویه، امنیت ملی و منافع عمومی (برای مثال، در نقض حقوق اسرار تجاری الکترونیکی، منافع کلان اقتصادی) را در معرض مخاطره قرار دهد. سرانجام اینکه، از حیث تعیین مجازات برای معاونت، تبصره مادهٔ ۱۸، با این ایراد روبه‌رو است که اقدام به ابداع نسبت جدید از مجازات (نصف حداکثر مجازات قانونی)، کرده است که در مواردی امکان دارد بیشتر از مجازات مرتکب (مباشر) جرم باشد!

وضع گردیده تکمیل شده است. ماده یک این قانون، مفهوم عامی از «اسرار» ارائه می‌دهد و به طور صریح آن را شامل اطلاعاتی که به وسیلهٔ سیستمهای الکترونیکی ایجاد یا مبادله می‌شود، می‌داند. البته باید اذعان داشت که قانون، تمام مخاطراتی که اسرار تجاری را تهدید می‌کند، شامل نمی‌شود.[۱۸] به همین دلیل هنوز هم توجه محاکم به رویه قضائی و قرارهای تأمینی معطوف است.(۱)

مطالعه در پیشینه قانون جاسوسی اقتصادی بیانگر تهدیدهای عمده‌ای است که همواره اقتصاد آمریکا با آن مواجه بوده است. به گونه‌ای که در سال ۱۹۹۶، تنها صنعت با فناوری پیشرفته(۲) نوزده میلیون دلار از بابت سرقت و جاسوسی خسارت‌دیده است. فناوری زیستی به عنوان یکی از فناوریهایی که با توسعه فناوری اطلاعات به سرعت گسترش یافته نیز، از قربانیان عمده نقض حقوق اسرار بوده است. گزارش سازمان بازرسی فدرال نشان می‌دهد که حدود ۲۰ درصد جاسوسی توسط نمایندگان دولتهای خارجی انجام گرفته است.[۱۴:۴]

نگاه تحلیلی‌تر به جرائم علیه اسرار تجاری مبین نقطه ضعفهای قوانین داخلی آمریکا در این باب و خلأهای عمده حقوق کشورمان در زمینه «اسرار تجاری» می‌باشد. حقوق اسرار تجاری از منظر حقوق کیفری با دو دسته از جرائم ارتباط تنگاتنگی دارد که بدون در نظر گرفتن آنها نمی‌توان به قانون‌گذاری و ارائه راهکارهای اجرائی دقیق و قابل اعمال دست یافت. از یک سو، حقوق اسرار به عنوان یکی از شاخه‌های حقوق مالکیت معنوی، با جرائمی که در این رشته ارتکاب می‌یابد، ارتباط دارد و از سوی دیگر، حقوق

---

۱. برای دیدن حدود ۴۰۰ پرونده در خصوص «حقوق اسرار تجاری» به پایگاه داده زیر مراجعه شود:

Trade Secerts Case Law Database, at:www.asksam.com/halligan/

2. High-Tech Industry

اسرار با جرائم علیه اموال و مالکیت ارتباط پیدا می‌کند که شرح جداگانه آنها ضرورت دارد.

۳ـ۲. جرائم علیه مالکیت معنوی و جرائم علیه اسرار تجاری

خصیصه مشترک مالکیت معنوی و اسرار تجاری که آنها را در یک دسته‌بندی قرار می‌دهد، توصیف «مالی بودن حق ناشی از این دو» می‌باشد.[۱] به عبارت دیگر، هر دو مفهوم مالکیت معنوی و اسرار تجاری در بادی امر، از آن جهت ارزش بحث دارند که به طور مستقیم برای مالک «حق مالی» ایجاد می‌کنند. لذا نقض حق مالکیت معنوی یا حق اسرار تجاری از طریق افعال مجرمانه، تعرض به «حق مالکیت» به شمار می‌آید. بنابراین، قواعد حقوق مالکیت معنوی را که در مقایسه با حقوق اسرار تجاری، به دلیل تصدی سازمان جهانی مالکیت معنوی و توجه تضمینی کشورها به آن، به ویژه در عصر فناوری اطلاعات، توسعه فراوانی یافته است، می‌توان به طور خاص در باب جرائم علیه «حق مالی» ناشی از اسرار تجاری نیز اعمال کرد.

باید تذکر داد که حقوق اسرار، از شاخه‌های نسبتاً مهجور حقوق محسوب می‌گردد که مع‌الأسف گاه با این تصور که با شرایطی که اینترنت و سایر وسایل ارتباط الکترونیکی از حیث ایمنی و گمنامی به وجود آورده نمی‌توان اصول استانداردی برای آن توصیف کرد، فراموش شده است. بررسی حقوق مالکیت معنوی و حقوق اسرار در قالبی واحد، نه تنها از مشکلات تحلیلی حقوق اسرار تجاری می‌کاهد، بلکه زمینه تضمین مالکیتهای معنوی را از طریق حمایت قانونی از اسرار ناشی از این نوع مالکیتها فراهم می‌آورد.

شاید با لحاظ تحلیل فوق است که قانون جاسوسی اقتصادی آمریکا،

۱. البته حقوق مالکیت معنوی (Intellectual Property Law)، به دلیل همراه داشتن عبارت «معنوی»، تقریباً در تمام موارد واجد حق معنوی برای مالک نیز می‌باشد. اما واقعیت این است که به ویژه در حیطه فناوری اطلاعات، نگاه نهایی به این حق بیشتر از باب مزایای مادی می‌باشد که در بردارنده آن است.

تعریف عام ـ و البته قابل انتقادی ـ از اسرار تجاری ارائه می‌دهد و آنها را از جمله شامل کلیه اسرار مالی، تجاری، علمی، ناشی از فناوری، اقتصادی یا اطلاعات مهندسی می‌داند.[۱] در عصر فناوری به مفهوم عام، «اطلاعات» علاوه بر اینکه واجد ارزش مالی فراوان برای دارنده آن است، به دلیل نداشتن تجسم مادی در اکثر موارد، تنها با توجیه «مالکیت معنوی» به مالک منسوب می‌شود. برای مثال، مالکیت شرکت «یاهو» نسبت به شکل ظاهری، امکانات، نحوه فعالیت، نام دامنه و سایر مزایای پایگاه اینترنتی خود، علاوه بر اینکه همواره «رازهایی تجاری» با خود به همراه دارد؛ در عین حال «مالکیت معنوی» به شمار می‌آید. در ظرافت و صحت این توصیف نباید تردید کرد.

۳ـ۳. *جرائم علیه اسرار تجاری و جرائم علیه مالکیت*

با توسعه فناوری اطلاعات که امکان تجارت مستقیم الکترونیک را فراهم آورده است، اکنون می‌توان از اموالی سخن گفت که در عین داشتن وجهه مادی، به هر دلیل، از جمله به منظور آسان کردن مبادله، ارزان کردن محصول و... به صورت «الکترونیک» در آمده‌اند. برای مثال، کتاب «حقوق تجارت الکترونیک» وین و رایت[۲] علاوه بر اینکه نسخه کاغذی دارد، می‌توان نسخه «بر خط» آن را که شامل تصویر الکترونیک کتاب می‌شود، از پایگاه اینترنتی ناشر یا آمازون خریداری کرد. اگر بتوان پیش از پرداخت قیمت و طی تشریفات اینترنتی سفارشی و خرید عنوان راز «افشا نشده» را به کتاب مذکور اطلاق کرد، حالت جالبی اتفاق می‌افتد که در آن عنوان «راز تجاری» و «مال» در مورد یک مدرک الکترونیک با هم جمع می‌شود. طرح مثال نرم‌افزاری که

۱. بند (۳) ماده ۱۸۳۹ از مقرره شماره (۱۸ـ قانون جاسوسی اقتصادی)، مجموعه قوانین و مقررات ایالات متحده.

2. Winn, Jane K. & Wright Benjamin, Law of Electronic Commerce, Forth Edition, Aspen Law & Business supplement 2002.

به هیچ وجه نسخه غیر اینترنتی آن ارائه نمی‌شود، شاید برای فهم بهتر این تلفیق، گویاتر باشد. شرکت Learnkey[1] سالهاست که به تولید، توزیع و فروش اینترنتی نرم‌افزارهای آموزشی خود در سراسر دنیا می‌پردازد. حال، آیا نمی‌توان ادعا کرد که سرقت، تکثیر و توزیع غیرمجاز یکی از نرم‌افزارهای شرکت در نخستین عرضهٔ اینترنتی آن، عملاً «نقض حقوق اسرار تجاری» نیز محسوب می‌گردد؟

این ادعا، از جهاتی قابل دفاع و به دلایلی دیگر مردود است: در حقوق داخلی کشورها، عملاً برای اسرار تجاری ارزش مادی شناخته‌اند و در مقام ارائه مصادیق اسرار، مواردی ذکر شده که موجب نوعی سردرگمی در تشخیص «مال» و «راز» از همدیگر می‌شود. ماده ۶۵ قانون تجارت الکترونیک کشورمان (مصوب ۱۳۸۲/۱۰/۱۷) با همین طرز تفکر مقرر می‌دارد: «اسرار تجاری الکترونیکی «داده پیام»ی است که شامل اطلاعات، فرمولها، الگوها، نرم‌افزارها و برنامه‌ها، ابزار و روشها، تکنیکها و فرایندها، تألیفات منتشرنشده، روشهای انجام تجارت و داد و ستد، فنون، نقشه‌ها و فراگردها، اطلاعات مالی، فهرست مشتریان، طرحهای تجاری و امثال اینهاست، که به طور مستقل دارای ارزش اقتصادی بوده و در دسترس عموم قرار ندارد و تلاشهای معقولانه‌ای برای حفظ و حراست از آنها انجام شده است». قانون جاسوسی اقتصادی آمریکا، که پیشتر مورد بررسی قرار گرفت نیز، وضعیت مشابهی مقرر می‌دارد.

با وجود تصور غلط فوق، که وارد قانون داخلی برخی کشورها ـ از جمله ایران و آمریکا ـ هم شده است؛ باید اذعان داشت که راز تجاری با مال تجاری و این دو با حق تألیف و حریم خصوصی تفاوت دارند. راز و مال هر دو ممکن است در قالب الکترونیک یا سنتی باشند، اما تفاوتهای عمده به شرح زیر

1. www.learnkey.com/elearning/

منجر به تمایزی آشکار بین آنها می‌شود.

- ارزش مادی مال (اعم از مالکیت مادی و معنوی)، عرفاً مشخص و معادل با ارزش اقتصادی و قدرت پایاپایی در مقایسه با سایر کالاهاست. در مقابل، ارزش «اسرار تجاری»، صرفاً با قالب مادی آن سنجیده نمی‌شود و امکان دارد ارزش اقتصادی یک سیستم عامل که توسط شرکتی رقیب در مقابل محصولات یک شرکت طراحی شده است، میلیونها برابر قیمت لوح فشرده‌ای باشد که در آن پیاده شده است.

- جرائم علیه اسرار و جرائم علیه اموال، حتی اگر نام واحدی همچون سرقت، خیانت، کلاهبرداری یا .. برای تحصیل و بهره‌مندی از آنها، اطلاق شود؛ به لحاظ ماهوی با همدیگر تفاوت دارند. جرائم علیه اموال و مالکیت، در اکثر موارد به طور مستقیم با مال یا مالکیت ارتباط می‌یابند و از دو حالت عام «انتفاع مجرم» یا «تضرر بزه‌دیده (یا فرد دلخواه او) به سود مجرم یا بدون انگیزه سودبری» خارج نیستند. اما جرائم علیه اسرار تجاری امکان دارد که ارتکاب یابند، حال آنکه سود و زیانی در میان نباشد.[1] برای مثال، دسترسی (الف) به نرم‌افزار نحوه به کارگیری افزارهای پیشرفته (اینترنتی، پزشکی، جنگی و..)، اگر افشا نشده یا به کار گرفته نشود و پیش از آن به مالک مسترد گردد، عرفاً زیانی به مالک نرم‌افزار وارد نمی‌سازد. با این حال، در اکثر

۱. اگرچه همان‌گونه که ماده ۶۵ قانون تجارت الکترونیکی نیز اشاره کرده، اسرار تجاری «به طور مستقل دارای ارزش اقتصادی» هستند، اما تعرض یا اختلال در ارزش اقتصادی آنها، رکن ضروری ارتکاب تمام جرائم علیه این دسته از حقوق مالی به شمار نمی‌آید. به علاوه، برای تحقق این جرائم، نیازی به منتفع شدن مجرم در تمام اقسام نقض حقوق اسرار (دستیابی، افشا و به کارگیری)، وجود ندارد. چراکه برای مثال ممکن است افشای اسرار از روی کنجکاوی، برای مشهور شدن، انتقام و... بوده و منجر به نفع مادی ملموسی برای مرتکب نباشد از این حیث می‌توان جرائم علیه اسرار را با جرائم علیه امنیت مقایسه کرد. دلیل عمده این امر، ارتباط ضمنی حقوق اسرار تجاری با منافع اقتصادی کلان ملی هر یک از کشورها می‌باشد؛ چنانچه آمریکا، نام «جاسوسی» را بر قانونی که در باب جرائم علیه اسرار اقتصادی وضع شده، نهاده است.

کشورها، عنوان مجرمانه مستقل دارد. نه شروع به جرم است و نه در قالب سرقت یا کلاهبرداری قابل تحلیل است. هرچند می‌توان صدق شروع یا تحقق هر یک از جرائم مذکور و نیز تحقق خیانت در امانت را در پاره‌ای از مصادیق به نوعی پذیرفت.

۳ـ۴. حمایت از اسرار تجاری در قانون تجارت الکترونیکی

مواد ۶۴ و ۷۵ قانون تجارت الکترونیکی، در مقام جرم‌انگاری «نقض حقوق اسرار تجاری» وضع شده‌اند که بعد از ذکر کامل متن مواد، به ذکر نکاتی چند در مورد آنها خواهیم پرداخت.

ماده ۶۴، «به منظور حمایت از رقابتهای مشروع و عادلانه در بستر مبادلات الکترونیکی، تحصیل غیرقانونی اسرار تجاری و اقتصادی بنگاهها و مؤسسات برای خود و یا افشای آن برای اشخاص ثالث در محیط الکترونیکی جرم محسوب و مرتکب به مجازات مقرر در این قانون خواهد رسید».

ماده ۷۵، «متخلفین از ماده (۶۴) این قانون و 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 و یا برای اشخاص ثالث افشا نماید به حبس از شش ماه تا دو سال و نیم، و جزای نقدی معادل پنجاه میلیون ریال محکوم خواهد شد».

ایراداتی به این دو ماده به شرح زیر وارد است:

۱. ماده ۶۴ باید پس از ماده ۷۵ ذکر می‌گردید. به عبارت دیگر، با توجه به آیین تدوین قانون که ابتدا تعریف و سپس مباحث ماهوی و تکلیف‌زا ذکر می‌شوند؛ متن ماده ۷۵ که به تعریف و توصیف «اسرار تجاری» اختصاص دارد، باید پیش از ماده ۶۴ که به ذکر مقررات حمایتی می‌پردازد،

ذکر می‌گردید.

۲. دلیل ذکر جداگانه مجازات مقرر برای مفاد ماده ۶۴، مشخص نیست. جز اینکه معتقد شویم، مقنن با ماده ۷۵، علاوه بر جرم‌انگاری «نقض حقوق اسرار تجاری»، در صدد افزودن موارد دیگری غیر از «اسرار تجاری» بوده است. این تفسیر با ظاهر ماده ۷۵ انطباق نداشته و به هیچ وجه منطقی نیست. زیرا به نظر می‌رسد که مقصود از «نقض حقوق قراردادهای استخدام مبنی بر عدم افشای اسرار شغلی»، در متن ماده، باز هم ارتباط آن با اسرار تجاری بوده است. چنانچه در ادامه ماده همین امر مورد تصریح قرار گرفته است. بهترین روش برای حل مشکل، ادغام مواد ۶۴ و ۷۵ و حذف مفاد تکراری این دو می‌باشد.

۳. هیچ‌کدام از دو ماده، به صراحت از «نقض حقوق اسرار» سخن نمی‌گویند و همین امر منجر شده، که جرم‌انگاری تمام اقسام متصور برای نقض این حقوق، به دقت انجام نشود. برای مثال، هر دو ماده به طور صریح، شامل «به‌کارگیری» اسرار تجاری دیگران در جهت منافع خویش یا زیان رساندن به مالک اسرار نمی‌شود.

۴. *چالشهای حقوق اسرار در عصر فناوری اطلاعات*

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

بر همین اساس باید مدعی شد که جز در صورت وجود یک نظام

قدرتمند و علمی برای حمایت از اسرار، نمی‌توان از دست‌یازیهای دیگران به دور بود. بین‌المللی شدن مسئله و افشای اسرار نظامی و امنیتی در اینترنت نیز بر این واقعیت دلالت دارد. بر خلاف نظر نویسنده‌ای که اختراع دوربین، تلفنهای تصویری، دستگاههای دیده‌بانی، پیگردی الکترونیک، انواع میکروفونها، گوشیها، وسایل هوشمند شنیداری و دیداری، نامه الکترونیک، *مبادله الکترونیک داده و... را موجب تضعیف حق حریم دانسته [۱۴۶۳: ۷/۱] با* وضع ضوابط فنی و حقوقی به‌راحتی می‌توان از مشکلات ناشی از ظهور فناوری جدید کاست و آن را به حداقل ممکن رسانید. چالشهای حقوق اسرار در عصر فناوری اطلاعات را که منحصر به اسرار تجاری نبوده و اسرار امنیتی و حق حریم نیز با آنها مواجه‌اند، به شرح زیر می‌توان برشمرد.

۴ـ۱. گمنامی

عده‌ای فکر می‌کردند، فضای مجازی[1] بهشت بی‌قانونی است که در آن مقنن داخلی یا بین‌المللی توان وضع قاعده ندارد و حتی اگر چنین نماید، ضمانت اجرائی 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 می‌دهد به عالم خیال تعلق نداشته و به وقایع عالم حقیقی شباهت دارد.[۱۶] گمنامی اینترنتی به معنی نامعلوم بودن هویت افرادی است که از طریق این شبکه با یکدیگر ارتباط برقرار می‌کنند. واضح است که اگر این گمنامی به مفهوم عرفی آن محقق باشد، در آن صورت هر قانونی برای کنترل فعالیتهای اینترنتی محکوم به بی‌اعتباری خواهد بود. حال آنکه در اکثر موارد با رهگیریهای دقیق علمی، ردپای افراد و در نتیجه هویت ایشان شناسایی می‌شود و بر همین اساس اعمال مجازات برای یاغیان شبکه (هکرها) و افشاکنندگان اسرار امکان‌پذیر است.

1. Cyberspace

۴ـ۲. 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: عده‌ای به‌راحتی مسائل خصوصی مردم را به تصویر می‌کشند و به طور برخط (آن‌لاین) در اینترنت ارائه می‌کنند؛ مشخصات تأسیسات نظامی و امنیتی دولتهای دیگر را فاش می‌کنند؛ با افشای اسرار یک شرکت فراملی، آن را تا ورطه ورشکستگی پیش می‌برند؛ با ارائه تصاویر ساختگی و مستهجن منجر به هتک حیثیت افراد می‌شوند و.. بدون آنکه مورد پیگرد قرار گرفته و مجازات شوند.

این ادعا تنها در روابط بین‌المللی صحیح می‌نماید، چرا که دولتها حقیقتاً خود را ملزم به رعایت حقوق اسرار امنیتی نمی‌دانند 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، بدون تردید امکان‌پذیر است و حتی برخی کشورها، مقررات صریحی در منع افشای الکترونیکی اسرار وضع کرده‌اند.

بنابر گزارش روزنامه خلق، وزارت امنیت داخلی چین در ژوئن ۲۰۰۰ بخشنامه‌ای صادر کرد که تمام سازمانها و اشخاص را از افشا، طرح یا انتقال اسرار دولتی در پایگاههای اینترنتی، تابلوهای اعلان عمومی، واحدهای گپ‌زنی (چت) و از طریق نامه الکترونیک منع کرده است.[۶] به علاوه، به موجب قانون خاص[۱] در این کشور تصریح شده که از اینترنت نمی‌توان برای صدمه به امنیت داخلی، افشای اسرار دولتی، متضرر ساختن جامعه، آسیب

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

رساندن به منافع ملی، جامعه یا گروه، حقوق شهروندان یا شرکت در افعال مجرمانه، استفاده کرد. در انگلیس، قانون اسرار رسمی[1] افشای اسرار به اشخاص غیر مجاز را ممنوع و مستوجب کیفر دانسته است. در مورد سایر اسرار در اغلب موارد مسئولیت مبتنی بر انصاف یا قواعد عام حقوق مدنی خواهد بود.

۴ـ۳. 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 الکترونیک منع کرد؟ اگر دولتی به طور خودسرانه اطلاعات سری متعلق به تجهیزات نظامی و استراتژیک کشوری را در اینترنت منتشر کند، چه ضمانت اجرائی علیه آن دولت وجود خواهد داشت؟ آیا می‌توان علیه آن دولت در محاکم صالح بین‌المللی طرح دعوی کرد؟ 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 تجاری در سطح بین‌المللی، تقریباً ناموجود است. شاید زمانی تحولات حقوق مالکیت، معنوی که اکنون حمایت از اسرار و علائم تجاری را نیز پوشش داده، به این عرصه کشیده شود و بتوان راه‌حلهای آن را اعمال کرد. 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 هکرها (چه حرفه‌ای و چه تازه‌کار) همواره برای دسترسی به اطلاعات دولتی و محرمانه تلاش کرده‌اند؛

1. Offcial Secrets Act 1989.

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 الکترونیک برای مقاصد دفاعی، نظامی و استراتژیک دخالت داشته‌اند.[۱۵] تشریح این وضعیت در ایالات متحده نشان از دوراندیشی محققان این کشور دارد، وگرنه امکان چنین سوء استفاده‌ای 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 به شمار می‌آید. با این‌حال می‌توان مواردی را تصور کرد 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 کند. چنانکه بعد از انفجار یک بمب در ساختمان فدرال اوکلاهاما سیتی، سازمان بازرسی فدرال آمریکا احضاریه‌ای به تمام دارندگان دوربینهای تصویربرداری، عکاسی، وسایل دیداری و شنیداری و ویدئوها و به طور کلی همه مالکین وسایل تجسس الکترونیک ارسال داشت.[۱۱:۱۹۵] این وضعیت نمود تحول در مفهوم حق حریم و حق بر داشتن راز می‌باشد که نیازهای امنیتی و اجتماعی آن را تحمیل می‌کند.

۵. ایمنی اسرار و عوامل توجیه‌کننده افشای اسرار

با ظهور فناوریهای جدید شنیداری و دیداری، گوشیها 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 می‌کنند 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 الکترونیک پیشرفته، جدیدترین امکانات و دستاوردهای علمی و فناوری نیز بهره گرفت. از سوی دیگر، در مواردی به هیچ وجه نمی‌توان از افشای اطلاعات جلوگیری کرد و یا حتی افشای اسرار توجیه پذیر است که این موضوع را به طور جداگانه تشریح خواهیم کرد.

۵-۱. ایمنی اسرار در عصر فناوری اطلاعات

امنیت اطلاعات در عصر روابط الکترونیک در اکثر موارد بعد حقوقی نداشته و بیشتر به مسائل علمی و فنی ارتباط می‌یابد. تحقیقات زیادی در زمینه ایمنی داده‌های رایانه‌ای از حیث عدم امکان نفوذ اشخاص غیرمجاز انجام و نتایج آن ارائه شده،[۱۳:۲۱] که می‌توان به آنها مراجعه کرد. برخی از نویسندگان تقویت سیستمهای الگوریتمی را پیشنهاد می‌کنند؛ به گونه‌ای که حتی معروف‌ترین سرویسهای جاسوسی نیز توان شکستن (یافتن رمز ورود) آن را نداشته باشند.[۱۱:۱۹۰]

میزان ایمنی اطلاعات محرمانه و سری در برابر نفوذ هکرها و جاسوسان حرفه‌ای و متخصص در سیستمهای الکترونیک، از نظر حقوقی دارای آثار زیر است:

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

دوم: نفوذ به اطلاعاتی که درجه معقول و متعارفی از ایمنی را دارا

می‌باشند در هر صورت موجب مسئولیت است؛ زیرا با این اقدام «سوءنیت» مرتکب آشکار می‌گردد. چنانچه در پرونده‌ای[1] قاضی پرونده[2] اظهار داشت که تعهد به عدم افشا، محدود به مواردی که در آن اشخاص دارای رابطه قراردادی هستند نیست، بلکه سوء استفاده یک نفر از موقعیتی که برای تحصیل اطلاعات سری داشته نیز، می‌تواند منجر به مسئولیت شود.|۲:۲۸۷| دلیل این وضعیت آشکار است: از یک سو، همواره عده‌ای معین 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 الکترونیک روز به روز در حال پیشرفت و تحول است و چه بسا قبل از آگاهی و بهره‌گیری از جدیدترین فناوری، شخصی با دست یافتن به آن، نسبت به افشای اسرار اقدام کند که در این صورت نیز نمی‌توان راه را بر او بست.

۵-۲. عوامل توجیه‌کننده افشای اسرار در عصر فناوری اطلاعات

اگر محرمانه بودن اسرار در فضای مجازی اثبات شد، اصل بر این است که نمی‌توان آنها را افشا کرد. مگر اینکه همان مصلحتی که ایجاب کرده آن اطلاعات مخفی بماند، افشای آنها را اقتضا کند. به عبارت دیگر تنها با حکم قانون یا دادگاه می‌توان اسرار را فاش کرد. مقررات موجود نیز بر این واقعیت تصریح دارند.

به عنوان استثنائی بر اصل عدم امکان افشای اسرار، دادگاه می‌تواند دستور رمزگشایی الکترونیک را صادر کند. به‌موجب ماده ۱۰۴ قانون آیین دادرسی دادگاههای عمومی و انقلاب در امور کیفری مصوب ۱۳۷۸، «در مواردی که ملاحظه، تفتیش و بازرسی مراسلات پستی، مخابراتی، صوتی و

1. Saltman Engineering Co v. Campbell Engineering Co Ltd 1963.
2. Lord Green.

تصویری مربوط به متهم برای کشف جرم لازم باشد، قاضی به مراجع ذی‌ربط اطلاع می‌دهد که اشیای فوق را توقیف کرده و نزد او بفرستند...» 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 کرده که اسناد سری دولتی نیز در صورت ضرورت با اجازه رئیس قوه قضائیه برای کشف جرائم و تحقیقات کیفری قابل ارائه می‌باشد.

از بعد تطبیقی، افشای اسرار و اطلاعات محرمانه به دست آمده از طریق وسایل الکترونیک در حقوق خارجی نیز در موارد خاصی مجاز شناخته شده است. چنانچه در پرونده‌ای[1]، خواهان ادعا کرد که پلیس یک کپی از عکسهای او را به متصدیان فروشگاه محلی ارائه کرده، که آن عکس او را در حال سرقت از اشیای فروشگاه نشان می‌دهد. در آن پرونده خواهان متهم به سرقت بود، ولی بدان محکوم نشد (البته بعدها محکوم گردید). قاضی اظهار داشت که پلیس در استفاده از عکسها که امکان داشت به عنوان جزئی از اسرار محرمانه به شمار آیند، به هر شیوه‌ای که تمایل داشت، آزاد نبوده است. البته به استناد محکومیتهای مکرر خواهان و اینکه عکسها فقط به متصدیان فروش داده شده بود، چنین حکم داده شد که عمل پلیس ـ بدون هیچگونه شک وشبهه‌ای ـ در جهت حفظ منافع عمومی بوده و پلیس با حسن‌نیت برای مقابله با جرائم و کاهش سرقت اقدام کرده است.|۲:۲۹۶|

ادعای اشتباه در ارائه اطلاعات الکترونیک محرمانه به اشخاص غیر مجاز نیز اصولاً پذیرفته نیست. مگر اینکه مدعی با دلائل قابل قبول اثبات کند که خطای رایانه‌ای منجر به رسوخ اسرار در شبکه شده و اقدامات معمول را برای جلوگیری از این کار انجام داده است.

1. Hellwell v. Chief Constable of Derbyshire 1984.

به نظر می‌رسد در مورد کلیه اسرار بتوان «اجبار» و «قوه قاهره» را از عوامل توجیه‌کننده ارائه 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 نیاورده‌اند، ولی از قواعد عام می‌توان آن را استنباط کرد.

نتیجه

فناوری اطلاعات، تعرض به حریم اسرار تجاری را آسان و حفاظت از آنها را دشوار کرده است. این مسئله همراه با شکل‌گیری اقسام جدیدی از اسرار است که تنها در محیط الکترونیک قابل تصور بوده و در عین حال، گاه ارزش مادی آنها از اسرار سنتی بیشتر است. فناوری موجب مسئله جالب‌تری نیز شده است: برخی از اسرار به هیچ وجه قابلیت بقا ندارند و با افشا شدن در محیط اینترنت، به سرعت ویژگی «راز» بودن را از دست می‌دهند. شاید به این دلیل مهم که «هرچه راز در میان افراد بیشتری مطرح باشد، احتمال برملا شدن آن نیز بیشتر است». این وضعیت به معنی مرگ حق حریم یا افول حقوق اسرار نیست: می‌توان از ورود اسرار به محیطی که دیگر حمایت از آنها امکان‌پذیر نیست، جلوگیری کرد. البته این پیش‌گیری، بیش از آنکه صبغه حقوقی داشته باشد، جنبه علمی و فنی دارد.

از منظر حقوقی، قانون‌گذاری برای حمایت از اسرار تجاری باید با لحاظ دو نکته مهم «ضرورت حمایت همه‌جانبه از حقوق و منافع تجار و لو در فضای مجازی» و «وضع قاعده برای صیانت از منافع کلان ملی» صورت گیرد. قانون تجارت الکترونیک و لایحه جرائم رایانه‌ای، بدون توجه به این دو نکته مهم، سکوت نسبت به «اسرار تجاری بین‌المللی» که در عصر ارتباطات تردیدی در طرح آنها وجود ندارد، تداخل مقرراتی و اختلاط نامربوط اسرار تجاری با سایر اسرار (خانوادگی، علمی و..) و حق حریم، فاقد جامعیت هستند. این نقص را می‌توان در تدوین نهایی «قانون جرائم رایانه‌ای» جبران

کرد. نکته مهم، یکپارچگی مقررات و توجه به تمام ابعاد قضیه، با صرف‌نظر از مسائل نامرتبط است.

سرانجام، در بررسی حقوق اسرار تجاری باید به چند نکته مهم توجه داشت:

اول: ارتباط تنگاتنگ حقوق اسرار با اقتصاد و منافع ملی و بین‌المللی؛ از آن جهت که افشای اسرار می‌تواند در دراز مدت این تصور را مطرح سازد که قانون و مجری از تضمین این اسرار عاجز هستند و همین امر ابعاد وخیم اقتصادی در پی خواهد داشت. به خصوص در زمینه اسرار تجاری که در محیط الکترونیک شکل می‌گیرند، وظیفه دولت به‌روز کردن وسایل علمی و فنی لازم برای تولید، حفظ و بازبینی اسرار است. ضعف در این عرصه ممکن است افشای اسرار را آسان ساخته یا زمینه سوء استفاده‌های دیگر را فراهم سازد.

دوم: اوصاف خاص جرائم علیه اسرار تجاری از حیث تاکتیکهای منحصر ارتکاب جرم، نبوغ مجرمین در محیط الکترونیک، ارزش مالی بسیار این اسرار، تنوع شیوه‌های سوء استفاده (افشا، به‌کارگیری و رقابت غیرمنصفانه)، اقتضا دارد تا روشهای نوین پی‌گرد و پیش‌گیری از این جرائم به موجب مقررات خاص پیش‌بینی شده و به کار گرفته شود.

آخرین نکته: استقلال حقوق اسرار تجاری و ضرورت لحاظ این واقعیت در تمام مطالعات و پژوهشهای حقوقی در این شاخه می‌باشد که خود مقتضی معرفی اصول و قواعد خاص آن و دقت در تفکیک شباهتها و تفاوتهای این رشته با سایر شاخه‌های علم حقوق می‌باشد.

فهرست منابع

1. American Society for Industrial Security [ASIS] International advancing security worldwide. Trends in Proprietary Information Loss, Survey Report. September 2002. Available at:
http://banners.noticiasdot.com/termometro/boletines/docs/consultoras/pwc/2002/pwc-spi2 .pdf
2. Bainbridge (David), Intellectual Property. Fourth Edition, Financial Times, Pitman Publishing, Harlow, England 1999.
3. Bone (Robert G), A New Look at Trade Secret Law: Doctrine in Search of Justification, 86 California Law Review. March 1998.
4. Bouchoux (Deforah E.). Protecting your Company's Intellectual Property:A Practical Guide to Trademarks, Copyrights, patents e Trade Secrets, Saranac Lake, Amacom, New York 2001.
5. 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
www.fas.org/irp/congress/2002-rpt/jec sec.pdf
6. 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.
www.public.asu.edu /wfostel/chinainternet.pdf
7. Froomkin (A. Michael),The Death of Privacy? Stanford Law Review, Vol. 52 May 2000.
8. Gesmer (Lee.T), Protection of Trade Secrets in the Computer Industry, Available at:
www.gesmer.com/publications/tradesecrets/4. php
9. Hill (James W.), Trade Secrets, Unjust Enrichment, and the Classification of Obligations,4 Virginia Journal of Law & Technology, No 2, Spring 1999.

10. Hilton (William E.), What Sort of Conduct Constitutes Misappropriation of a Trade Secret, 30 IDEA:The Journal of Law and Technology 1990.
11. Huber (Peter), Law and Disorder in Cyberspace, Oxford University Press, New York 1997.
12. Jager (Melvin, F.), Trade secret laws, Thompson Information Services, Inc.West Group, St. Paul, Minn 1998, Section 1.05, 1996.
13. 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 2002.
14. Matthews (Robert), Post Cold War Spies Will Stop at Nothing to Trade in Secrets, Sunday Telegraph, Dec.14, 1997.
15. Post (Jeffrey, W.), The Secrets of Trade Secrets: Protecting Your Company's Trade Secrets and Protecting Your Company Against Trade-Secret Claims, Privacy & Data Security Law Journal, November 2005.
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.
17. Scott (Charney), Transition Between Law Enforcement and National Defense,Security in the Information Age: New Challenges, New Strategies,Joint Economic Committee G01 Available at: www.house.gov/jec http://www.fas.org/irp/congress/2002-rpt/jec-sec.pdf
18. Seltzer (Mark D.) & Burns (Angela A.), Criminal Consequences of Trade Secret Misappropriation: Does the Economic Espionage Act Insulate Trade Secrets from Theft and Render Civil Remedies Obsolete? Boston College Intellectual Property & Technology Forum 1999.
19. Simon (David W.) & Jones (Richard L.), Crimes and Criminals: How to Avoid Being a Victim or Perpetrator, The Computer & Internet Lawyer, Volume 22,

Number 6, June 2005.

20. Uniform Trade Secrets Act with 1985 Amendments, Drafted by National Conference of Commissioners on Uniform State Laws, Annual Conference Meeting in its Ninety-Fourth Year in Minneapolis, Minnesota. August 2-9, 1985. at:
www.law.upenn.edu/bll/ulc/fnact99/1980s/utsa85.pdf
21. 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
22. Winn (Jane K.) & Wright (Benjamin), Law of Electronic Commerce, Forth Edition, Aspen Law & Business Supplement 2002.