حقوق خصوصی
دورهٔ ۱۰، شمارهٔ ۲، پاییز و زمستان ۱۳۹۲
صفحات ۲۰۹ ـ ۱۸۳

مطالعهٔ تطبیقی تزاحم حقوق اشخاص ثالث با اعمال مالکیت فکری در محیط مجازی

جلیل قنواتی[۱*]، حسین جاور[۲]، علی‌تقی خانی[۳]

۱. دانشیارگروه حقوق خصوصی، دانشکدهٔ حقوق، پردیس فارابی، دانشگاه تهران
۲. استادیارگروه حقوق خصوصی، دانشگاه حضرت معصومه (س)
۳.دانشجوی دکتری حقوق خصوصی، پردیس فارابی دانشگاه تهران
(تاریخ دریافت: ۱۳۹۲/۵/۲؛ تاریخ پذیرش: ۱۳۹۲/۱۲/۱۵)

چکیده

اعمال حق مالکیت فکری و حق تحقیق دربارهٔ ادعای نقض آن و تسهیل احقاق حق خواهان، به صدور قرارهای حمایتی نیاز دارد. این کار، بیشتر برای جلوگیری از نابودی ادله و شواهدی است که می‌تواند در اثبات حق خواهان مؤثر باشد. این امر به وضوح، حریم خصوصی اشخاص موضوع تحقیق و اشخاص ثالث را در مخاطره قرار می‌دهد. بنابراین، مسئله‌این است که در جریان اجرای حق اعمال مالکیت فکری، چگونه می‌توان از حق حریم خصوصی اشخاص ثالث حمایت کرد. به نظر می‌رسد دادگاه‌ها هنگام تحقیقات قضایی، ضمن اهتمام به احقاق حق مالکیت فکری و اجرای آن در محیط مجازی، باید هم زمان، آثار ضمنی آن را بر حریم خصوصی اشخاص ثالث و غیرمرتبط به پرونده بررسی کنند، سپس، قرار مقتضی را صادر کنند. در حقوق کامن‌لا، در این زمینه دو قاعدهٔ بسیار مهم و متمایز وجود دارد، اول، قراری با ماهیت دستور موقت، معروف به «قرار آنتون پیلر»، برای «کشف هویت»، و دوم، قاعدهٔ مندرج در پروندهٔ «نورویچ فارماکال» که دربارهٔ «افشای هویت» به‌کار می‌رود. بازنگری در معیارها و شرایط صدور دستور تحقیقات مقدماتی، تمایز بین افشای هویت و اطلاعات، محدودکردن دامنهٔ کشف هویت و اطلاعات و احتیاط در صدور دستورهای سیار از جمله تلاش‌هایی است که برای حفظ حریم خصوصی و تعدیل قواعد یادشده انجام گرفته است. در حقوق ایران نیز، گردآوری اطلاعاتی که در اختیار واسطه‌ها قرار دارد، بدون به‌کارگیری دستورهای قضایی، در زمرهٔ جرایم مرتبط با رهگیری ارتباطات به‌شمار می‌رود و رهگیری، افشا یا به‌کارگیری محتوای ارتباطات، خلاف اصل در شرایط خاص و محدود مجاز تلقی شده است.

واژگان کلیدی

افشای هویت، دستور آنتون پیلر، حریم خصوصی، کشف اطلاعات، مالکیت فکری.

* نویسندهٔ مسئول تلفن: ۰۹۱۲۱۵۹٤۳۲۸ پست الکترونیک: ghanavaty@ut.ac.ir

مقدمه

اگرچه اعمال حقوق مالکیت فکری، به اقتضای خود، در تمام زمینه‌های تحقق مالکیت فکری ممکن است، اجرای این حقوق در محیط برخط، تهدیدهای خطرناکی را برای حریم خصوصی کاربرانی دارد که عموماً از فرآیند اعمال حق مالکیت فکری بی‌اطلاع‌اند و فرصت کافی برای پاسخ‌گویی نیز ندارند، زیرا با طرح دعوای صاحبان مالکیت فکری و گردآوری اطلاعات از واسطه‌های اینترنتی (عرضه‌کنندگان خدمات به افراد، ISP)، به راحتی زمینهٔ نقض حریم خصوصی اشخاص ثالث فراهم می‌شود. به دیگر سخن، از یک سو، سرعت، قدرت، قابلیت و راحتی دسترسی به اطلاعات شخصی، بازیابی ظرفیت ذخیره‌سازی اطلاعات، پایداربودن روش‌های ذخیره‌سازی اطلاعات و تحولات گستردهٔ فناورانه، امکان نقض حقوق کپی رایت را فراهم می‌کند و از سوی دیگر، به دلیل نوع دسترسی اشخاص ثالث به اطلاعات محرمانهٔ قابل برداشت، حمایت از مالکیت فکری در تحقیقات، حریم خصوصی را به مخاطره می‌اندازد.

با توجه به مشکل یادشده، مسئله این است که اگر بین اجرای حقوق مرتبط با مالکیت فکری و تحقیقات مقدماتی مرتبط به نقض آن و حریم خصوصی اشخاص در محیط مجازی، تزاحم به وجود آید، چگونه می‌توان بین این دو حق، تعادل برقرار کرد.

در پاسخ به این پرسش، در حقوق کامن‌لا، به بازنگری در معیارها و شرایط صدور دستور تحقیقات مقدماتی، گسست افشای هویت از افشای اطلاعات، محدودکردن دامنهٔ کشف هویت و اطلاعات و احتیاط در صدور دستورهای سیار توجه شده است. در حقوق ایران نیز، گردآوری اطلاعاتی که در اختیار واسطه‌ها قرار دارد، بدون به‌کارگیری دستورهای قضایی، در زمرهٔ جرائم مرتبط با رهگیری ارتباطات به شمار می‌رود. بنابراین، هم در حقوق کامن‌لا و هم در حقوق ایران، واسطه‌های اینترنتی بدون مجوز قانونی و دستور مقامات قضایی رهگیری، حق افشا یا به‌کارگیری محتوای ارتباطات را نخواهند داشت. به علاوه، دادگاه‌ها هنگام بررسی درخواست افشای اطلاعات محرمانهٔ واسطه‌ها باید حق حریم خصوصی افراد مورد نظر را به‌طور هم‌زمان و با توجه به آثار ضمنی افشای اطلاعات بر آن افراد، بررسی کنند.

میان‌کنش اعمال حق مالکیت فکری در محیط مجازی و حریم خصوصی ثالث در کامن‌لا

حقوق کامن‌لا، از حریم خصوصی کاربران، در هنگام تحقیقات مقدماتی مربوط به مالکیت فکری، به شیوه‌های مختلفی حمایت می‌کند. این شیوه‌ها که در قالب چند قاعده تجلی یافته است، به ترتیب، بررسی خواهد شد.

قاعدهٔ «آنتون پیلر»

این دستور که با عنوان «قرار تحقیق مدنی[1]» و «تسلیحات هسته‌ای قانون[2]» توصیف شده‌اند (Bank Mellat v Nikpour, 1985, p.92). در حقیقت، به سبب پروندهٔ «آنتون پیلر.کی.جی[3]» علیه شرکت «مانیو فکچرینگ پروس[4]» در دادگاه تجدیدنظر، به قرار آنتون پیلر معروف شد.[5] براساس دیدگاه قاضی «دنینگ[6]» این دستور بدون اطلاع خوانده و به منظور احقاق حق تحقیق خواهان در جلوگیری از نابودی شواهد اصلی پرونده یا خارج شدن شواهد از حوزهٔ صلاحیت دادگاه و تحقق عدالت بین دو طرف صادر می‌شود (Mellat v Nikpour, 1985, p.61). در عین حال، این دستور پیش‌شرط‌هایی دارد که باید مطالعه شود.

پیش‌شرط‌های دستورهای آنتون پیلر

دستورهای آنتون پیلر بر پیش‌شرط‌های اساسی و مهم زیر استوار است:

۱. خواهان، قبل از صدور دستور باید ثابت کند دلایل و شواهد محکمی علیه خوانده در اختیار دارد. بنابراین، در همان ابتدای امر، خواهان باید اتهامات و مبنای آن را به وضوح معلوم کند.[7] دستورهای آنتون پیلر به خواهان اجازه نمی‌دهد تا از لابه‌لای مدارک به دنبال شناسایی

1. Civil Search Warrants
2. Nuclear Weapons Of The Law
3. Anton Piller K.G
4. Manufacturing Processes Ltd.
5. [1976] Ch 55; [1976] 1 All ER 779.
6. Dening
7. [1982] 3 All ER 415 at 418 per Lawton J.

«موارد احتمالی نقض» و یا «خوانده‌های احتمالی» باشد و دستورهای یادشده نمی‌تواند به منظور ابزاری برای فهم «نوع اتهامات» قابل طرح و پیداکردن «اسباب جدید» اقامهٔ دعوی به‌کار گرفته شود؛ بلکه اطلاعات، صرفاً باید برای تقویت یا تسهیل دعاوی پیچیده به‌کار گرفته شود.

۲. دستور آنتون پیلر در صورتی صادر خواهد شد که خسارت‌های بالقوه و بالفعل خواهان، بسیار جدی باشد.

۳. در صورت ابلاغ اخطاریهٔ طرح دعوی به خوانده، واقعاً نابودی اطلاعاتی که در اختیار خوانده است، ممکن باشد (Universal Music Australia Pty Ltd v Sharman License Holdings Ltd, 2004 ,p. 319). بنابراین، خواهان، باید اثبات کند که خوانده، در صورت اطلاع از شکایت، مدارک وی را از بین خواهد برد.

٤. اطلاعات درخواستی باید با نقض حق مالکیت فکری مرتبط باشد (*Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* 2004 ,p. 319).

دامنهٔ دستورهای آنتون پیلر

دستورهای آنتون پیلر، اجازه می‌دهد اطلاعات مرتبط فراوانی گردآوری شود و در صورت نیاز، اجازه می‌دهد اطلاعات مرتبط، از منابع الکترونیکی، برداشت، کپی‌برداری و به داخل پروندهٔ وکلای خواهان منتقل شود.

دستورهای آنتون پیلر دربارهٔ اطلاعات ایستا[۱] و اطلاعات پویا[۲] نیز، به‌کار گرفته می‌شود. از این رو، اطلاعاتی که براساس دستور یادشده گردآوری می‌شود، به‌طور طبیعی، گزارش ارتباطات تعداد

---

۱. اطلاعات ایستا آن دسته اطلاعاتی است که واسطه یا سیستم‌های آن ضبط کرده‌اند و باید به نحوی کنترل شود تا به حریم خصوصی کاربران آسیبی نرسد.

۲. اطلاعات پویا، آن دسته اطلاعاتی است که از راه سیستم ارتباطی رد و بدل می‌شود و الزاماً، تمامی فعالیت کاربران سیستم را در زمان انتقال اطلاعات در داخل شبکه از جمله جستجو، به اشتراک گذاشتن مجاز پرونده‌ها و امثال آن دربرمی‌گردد.

زیادی از کاربران شخصی را در بردارد. «کشف هویت»، «افشای هویت» و «کشف اطلاعات» از جمله مواردی است که می‌تواند در تحقیقات مقدماتی، حریم خصوصی اشخاص ثالث را نقض کند. از این رو، قاعدهٔ «نورویچ فارماکال» هویت و موارد جواز کشف هویت را تشخیص می‌دهد.

ضوابط کشف هویت در قاعدهٔ «نورویچ فارماکال»

مجلس لردها، در سال ۱۹۷۳، در پروندهٔ شکایت «نورویچ فارماکال علیه مأموران گمرک و مالیات» (Norwich Pharmacal v. Commissions Of Customs And Excise,1974, p.133)[1] جبران خسارت منصفانه را به سبب «کشف هویت» شخص بی‌گناهی که هویت وی، هنگام تشخیص هویت خواندگان اصلی در دعوی افسا شده بود، خواستار شدند. این رأی برای کشف هویت ضوابط مختلفی را به شرح ذیل مطرح کرده است.

۱. وجود دلیل قابل کشف برای اقامهٔ دعوی علیه فرد خاطی: برای حمایت از حریم خصوصی افراد بی‌گناه در برابر تحقیقات ناروا، دادگاه‌ها در هنگام صدور حکم «تشخیص هویت»، قوت استدلال خواهان را علیه متهم ادعایی بررسی می‌کنند (See Glaxo Welcome PLC v Canada 1998, p.387). بنابراین، دستور تشخیص هویت، هیچ‌گاه برای ارضای حس کنجکاوی افراد صادر نمی‌شود. بنابراین، اگر صرف‌نظر از محتوای درخواست کشف هویت، دعوای مطرح‌شده صحیح دانسته شود، دادگاه، به دلیل وجود ادلهٔ دیگر و کافی‌بودن آن برای اثبات مدعای خواهان، از صدور آن خودداری خواهد کرد.

۲. دخالت نداشتن شخص ثالث در اجرای فعل زیان‌بار: کشف هویت، صرفاً علیه کسانی به‌کار گرفته می‌شود که تا حدودی در انجام‌دادن فعل زیان‌بار نقش داشته‌اند، یا انجام‌دادن آن را، اگرچه سهواً و بدون تقصیر، تسهیل کرده باشند (See Glaxo Welcome PLC v Canada 1998, p.387).

1. [1974] AC 133; [1973] 2 All ER 943.

۳. **نبود شیوهٔ معقول دیگر برای کسب اطلاعات**: اگر راه دیگری، غیر از دستور کشف هویت باشد، دادگاه‌ها خوانده را در معضل کشف هویت قرار نمی‌دهند (Norwich Pharmacal Co v. Commissioners of Customs and Excise , 1974, p.174A).

٤. **مخالفت نکردن با مسائل مربوط به نظم عمومی**: دادگاه‌ها، به‌ویژه در مرحلهٔ تجدید نظر، در احکامی که افشای هویت علیه خواندگان را در بر دارد، به مصونیت منافع عمومی و نیز تأثیر منفی احکام بر فعالیت‌های تجاری خوانده توجه می‌کنند.

۵. **بی‌توجهی به ادعاهای کلی یا اغراق آمیز**: هدف خواهان فقط باید کشف هویت فرد خاطی باشد، به‌طوری که اگر خواهان هویت مجرم را کشف نکند، قادر به شروع مراحل دادرسی نباشد؛ زیرا تا زمانی که کشف هویت انجام نگیرد، خواهان، نمی‌تواند آن را ادامه دهد و به مرحلهٔ محاکمه برساند.[1]

افشای هویت

براساس مادهٔ ۱۵ (الف) (ر) (۳) از قواعد دادگاه فدرال استرالیا، «افشای هویت» جایی است که خواهان، برای شروع دادرسی، حتی با انجام‌دادن تحقیقات متعارف هم نتواند به مشخصات کامل خوانده دعوی دست یابد. در این صورت، با دستور افشای هویتی که از طرف دادگاه صادر می‌شود، هرگونه افشای هویت علیه هر فردی در اینترنت که در جایگاه تشخیص هویت خطاکار ادعایی قرار دارد، مجاز دانسته می‌شود. در حقیقت، اگر ظاهراً به نظر برسد، اطلاعات یا اسنادی از شخص خطاکار، در اختیار اشخاص ثالث قرار دارد به‌طوری که اگر این اطلاعات یا اسناد، در اختیار خواهان قرار گیرد، وی را در طرح دعوی یاری می‌کند، افشای هویت مجاز خواهد بود.

اگرچه، دستور افشای هویت طوری صادر نمی‌شود که خواهان بتواند دادرسی صرفاً احتمالی را شروع کند، در مقایسه با دستور کشف هویت (قاعدهٔ نورویچ فارماکال)، سطح ادلهٔ الزامی و مورد نیاز، اهمیت کم‌تری دارد، به‌طوری که نباید خواهان، دعوایی با ادله و شواهد قوی علیه خواندهٔ

1. [1992] 2 All ER 911 at 914B

آتی مطرح کند (Levis v McDonald, 1997, 75 FCR 36, p.41). همچنین، مشابه دستور کشف هویت در اعمال این دستور نیز، دادگاه‌ها قبل از صدور دستور، احتمال موفقیت خواهان را بررسی می‌کنند (John Fairfax & Sons Ltd v Cojuangco ,1988, p.357). همچنین، نوع اطلاعاتی که در چارچوب دستور افشای هویت، قابل کشف و افشا است، فقط شامل «توصیف فرد» به منظور شروع دادرسی خواهد بود.[1] بنابراین، اطلاعات به‌دست‌آمده از «هویت خوانده» نباید برای «کشف اطلاعات» به‌کار گرفته شود.

کشف اطلاعات

برخلاف آنچه گفته شد، در دادگاه‌های فدرال و در قانون دادگاه عالی استرالیا، دستور کشف هویت طوری صادر می‌شود که به‌طور معمول، قلمرو اطلاعات کشف‌شده را نیز شامل شود. برای مثال، می‌توان به قواعد مربوط به «کشف اطلاعات از خواندهٔ آتی» و «بازرسی و توقیف اموال» اشاره کرد.

کشف اطلاعات از خواندهٔ آتی

براساس مادهٔ ٦ قواعد دادگاه فدرال استرالیا، جایی که: الف) دلیل منطقی وجود داشته باشد که خواهان می‌تواند یا ممکن است بتواند حکم جبران خسارت را در دادگاه از شخصی که مشخصاتش محرز شده، به دست آورد؛ ب) بعد از انجام‌دادن همهٔ تحقیقات متعارف، خواهان، اطلاعات کافی را برای تصمیم‌گیری دربارهٔ شروع دادرسی و جبران خسارت، به دست نیاورده باشد؛ ج) دلیل منطقی وجود داشته باشد که فرد مورد نظر، اسنادی را حتماً یا احتمالاً در اختیار داشته و یا دارد و بازرسی خواهان دربارهٔ اسناد وی، به حق خواهان برای جبران خسارت کمک می‌کند. پس دادگاه می‌تواند دستور دهد این فرد باید هرگونه سندی را که در بند (ج) گفته شده، برای خواهان افشا کند.[2]

1. FCR O 15A r 1; NSWPt 4 r 1 (3); Vic r 32.01; ACT O 34A r 1; NT r 32.01.
2. ACT O 34A r 6 (a) , ACT O 34A r 6 (b), 138 Order 15A r 12 (a)

بنابراین، کشف اطلاعات فقط دربارهٔ فردی به‌کار گرفته می‌شود که دلیل معقولی برای حق جبران خسارت خواهان علیه وی وجود داشته باشد. اگرچه، این قواعد، برای گردآوری اطلاعات از شخص ثالث به‌کار گرفته نمی‌شود، در صورت دخالت شخص ثالث در فعل زیان‌بار و احتمال مسئولیت، کشف اطلاعات دربارهٔ وی هم مجاز خواهد بود. این امکان، کشف همهٔ اطلاعات مربوط به کاربرانی را که در اختیار اشخاص ثالث قرار گرفته، یا از سیستم آن‌ها عبور کرده است، شامل می‌شود. بنابراین، ترکیب کشف هویت و کشف اطلاعات می‌تواند علیه افرادی که شبه‌جرم را به‌طور مشترک انجام داده‌اند، صورت پذیرد. به دیگر سخن، کشف هویت یا افشای اطلاعات دربارهٔ فرد خطاکار نامرتبط به‌کار گرفته می‌شود.

کشف اطلاعات در ضمن بازرسی و توقیف اموال

مورد دیگری که کشف هویت در کنار اطلاعات مطرح می‌شود، هنگام بازرسی و توقیف اموال است. براساس مواد ۱۲ و ۱۵ (الف) (و) (ر) قواعد دادگاه فدرال و مواد ۳٤ (الف) (و) و ۸ (ر) قواعد دیوان عالی استرالیا، دادگاه می‌تواند حکم بازرسی، اندازه‌گیری، کپی‌کردن، حفظ، ضبط و بازداشت اموال مرتبط با جریان دادرسی، یا دستور نمونه‌گیری، معاینه، انجام‌دادن هرگونه آزمایش، شنیدن و دیدن نوارهای صوتی و ویدیویی، و فیلم‌ها و ابزارهای ضبط تصویر یا صدا یا تولید و بازتولید و ابزارهای دیگر ضبط و پی‌گیری مرتبط با این اموال را صادر کند.[1]

عمده‌ترین نگرانی دربارهٔ این گونه مقررات این است که به موجب آن، اجازهٔ دسترسی به سطح گسترده‌ای از اطلاعات، بیش از حد لازم و قانونی، فراهم می‌شود. اگرچه گاهی، بازرسی یا توقیف اموال، برای شناسایی خوانده ضروری می‌شود، به نظر می‌رسد، اطلاعات افشاشده نباید از مقدار معقول و ضروری برای تعیین وصف واقعی فردی که قرار است علیه وی دعوایی اقامه شود، فراتر رود و به حد کشف اطلاعات برسد (John Fairfax & Sons Ltd v Cojuangco ,1988, p.64).

دادگاه‌ها هنگام بررسی درخواست افشای اطلاعات محرمانهٔواسطه‌ها باید حق حریم خصوصی

1. Order 15A r 12 (a).

افراد مورد نظر را به‌طور هم‌زمان و با توجه به آثار ضمنی افشای اطلاعات بر آن افراد، بررسی کنند، زیرا واسطه‌ای که به افشای اطلاعات وادار می‌شود، به‌طور اساسی، نفعی در حفظ و حمایت از حریم خصوصی افراد در خود احساس نمی‌کند. به‌ناچار بعد از افشای اطلاعات و ایجاد خسارت، افرادی که حریم خصوصی آن‌ها نقض شده، مجبور می‌شوند در روندی پرهزینه و پیچیده، برای جبران خسارت خود اقدام‌های حقوقی انجام دهند. بنابراین، دادگاه‌ها باید فرآیند کشف اطلاعات را طوری هدایت کنند که به سود افرادی باشد که حریم خصوصی آن‌ها به احتمال زیاد نقض می‌شود و دادن اجازهٔ تحقیقات وسیع، فقط به دلیل دردسترس‌بودن اطلاعات یا جدید و نامأنوس بودن فناوری به‌کارگرفته‌شده، برخلاف هدف یادشده خواهد بود.[1]

توجه به حریم خصوصی کاربران در هنگام تحقیقات مقدماتی

برای ایجاد توازن و حفظ حریم خصوصی دو طرف ذی‌ربط، پیشنهادهایی به شرح ذیل مطرح شده که به ترتیب بررسی خواهد شد.

بازنگری معیارهای لازم برای صدور دستور تحقیقات مقدماتی

در صورت نیاز به مطرح‌شدن اطلاعات محرمانهٔ مهم کاربران واسطه، خواهان باید قبل از ضبط و توقیف سابقهٔ ارتباطات کاربران، دعوایی همراه با شواهد و ادلهٔ محکم علیه هر کاربر یا دست‌کم علیه تعداد زیادی از کاربران، اقامه کند. بنابراین، قاضی نباید بر پایهٔ دلایلی که «تخمین صرف» محسوب می‌شوند، و به بهانهٔ جلوگیری از سکوت خواندهٔ احتمالی یا گریز وی از مسئولیت، مجوز کشف اسناد را صادر کند. معمولاً در دعاوی تحقیق مقدماتی، به خوانده فرصت پاسخ‌گویی داده می‌شود. به علاوه، خواهان نیز فرصت پیدا می‌کند تا با استدلال ثابت کند درخواستش خودسرانه و فقط برای تجسس در امور شخصی دیگران نیست (C7 Pty Ltd v Foxtel Management Pty Ltd, 2001; 1864, p.50). بنابراین، هنگام درخواست دستوری که باعث مداخله

1. (2003) 198 ALR 367 at [64].

در حریم خصوصی افراد غیرمرتبط با فرآیند دادرسی می‌شود، نباید امکان «فیشینگ»[1] را بـه عنـون ابزار بی‌عدالتی درآورد. به علاوه، خواهان باید ثابت کند براساس واقع و منطق (و نه به طور واهـی و براساس تخمین صرف)، سـبب معقـول و مقبـولی بـرای طـرح دعـوی وجـود دارد. همچنـین، اطلاعات درخواستی نباید از میزان مورد نیاز برای افشای هویت متهمان ادعایی بیشتر باشد.

گسست افشای هویت از افشای اطلاعات

گسست دستور افشای هویت از دستور افشای اطلاعات از بایسته‌های حفظ بیشتر حریم خصوصی در حوزهٔ تحقیقات قضایی در نظر گرفته شده است. بنابراین، تفاوت در مـوارد زیـر شـایان توجـه است.

فرض اول، زمانی است که خواهان می‌تواند «سـبب طـرح دعـوی» را اثبـات کنـد ولـی «فـرد خاطی» را نمی‌شناسد، در این صورت، برای اینکه زمینهٔ کـافی بـرای اقامـهٔ دعـوی خواهـان علیـه خواندهٔ واقعی فراهم شود، »دستور کشف هویت» صادر می‌شود.

فرض دوم، وقتی است که خواهان از «هویت واقعی» متهم ادعایی باخبر اسـت امـا «اطلاعـات کافی» برای اثبات سبب طرح دعوی ندارد، در این صورت، به صلاحدید دادگـاه، «دسـتور کشـف اطلاعات» صادر می‌شود تا سبب طرح دعوی را تعیین کند.

در بیان تفاوت این دو فرض باید گفت، این دو، در حقیقت، دو نقـش متفـاوت دارنـد و نبایـد افشای هویت و افشای اطلاعات را یکسان دانست و با توجه به کارکرد مختلف هر یک از این دو، دادگاه نمی‌تواند این دو دستور را به‌طور هم‌زمان، صادر کند.

فرض سوم، وقتی است که خواهان، نه اطلاعات کافی برای پیداکردن «سبب طـرح دعـوی» را دارد و نه توان شناسایی «فرد خاطی» را ، در این صورت، نباید دستور کشف صادر شـود، زیـرا در صورت صدور دستور کشف، در حقیقت، این دستور، به صرف درخواست و بـا اتکـا بـه ماهیـت

1. Fishing

خود صادر شده است که متضمن نوعی «دور» است، زیرا کشف هویت نباید براساس اطلاعاتی باشد که قرار است به کمک کشف به آن برسیم (SmithKline Beecham plc v Alphapharm Pty Ltd ,2001, p.19).

محدودکردن گسترهٔ کشف هویت

پس از صدور دستور کشف هویت علیه واسطهٔ اینترنتی، اغلب، این احتمال هست که هویت افراد بسیاری که ممکن است ارتباطی به پروندهٔ نقض مالکیت فکری خواهان نداشته باشند، افشا شود. همچنین، تضمینی وجود ندارد که نتیجهٔ کشف فقط شامل هویت افراد مرتبط با پرونده باشد. از یک سو، نفع خواهان در این است که برای تشخیص نوع به‌کارگیری (تجاری یا غیرتجاری)، فهرست افرادی را که این ابزارها برای آن‌ها تهیه شده است، در اختیار بگیرد و از سوی دیگر، به سود نفع عمومی است که هویت افراد نامرتبط با دعوی، بدون ضرورت، افشا نشود. بنابراین، دادگاه در زمان اعمال صلاحدید برای اعطای دستور کشف، باید به تأثیر واقعی کشف بر تمامی افراد مربوط به پرونده توجه کند. بنابراین، در صورت زیادبودن خسارت ادعاشده و یا کم‌بودن احتمال خطاکاربودن افراد مورد تحقیق، شرایط برای صدور دستور کشف هویت فراهم است. به علاوه، جایی که حریم خصوصی و گمنامی شمار زیادی از افراد نامرتبط با پرونده به خطر می‌افتد، حمایت از حریم خصوصی افراد از دست‌یابی خواهان به اطلاعات خوانده مهم‌تر است و در مواردی که دستور افشای هویت صادر می‌شود، این دستور، تا حد ممکن باید خاص و موردی باشد، به‌طوری که فرد واسطه فقط هویت افرادی را که خواهان، دعوایی با ادله و شواهد محکم علیه آن‌ها اقامه کرده است، افشا کند (Sony Music Entertainment (Australia) Limited & others v University of Tasmania & others,2003, p.19).

گسست حفظ اطلاعات از تحقیقات مقدماتی

گاهی خواهان می‌خواهد اطلاعات ضروری برای محاکمه را از گزند نابودسازی خوانده در امان نگه دارد. این امر نیازمند آن است که اطلاعات مورد نیاز خواهان، بدون بررسی، حفظ و در اختیار

قرار گیرد. در این صورت، دستور آنتون پیلر مناسب وضعیت پرونده است و چون در صدد حفظ اطلاعات است و اطلاع خوانده، به این هدف ضرر می‌رساند، این درخواست، به‌طور «یک‌جانبه» مطرح می‌شود. اما اگر خواهان بخواهد اطلاعات مورد نیاز را برای شروع دادرسی و با فرض معلوم‌بودن هویت خوانده به دست آورد، در این صورت، خطر نابودی اطلاعات اندک است. بنابراین، می‌تواند در قالب دستوری با ماهیت «دوجانبه» و همانند یک درخواست عادی تحقیقات مقدماتی مطرح شود.

محدودکردن گسترهٔ کشف اطلاعات الکترونیکی

دامنه و گسترهٔ اطلاعات موجود در سیستم‌های رایانه‌ای، نامحدود و تعیین دقیق دامنهٔ واقعی اطلاعاتی که قبل از صدور دستور باید افشا شود، بسیار دشوار است. بنابراین، دادگاه‌ها دوست دارند برای تضمین حفظ اطلاعات و ازبین‌نرفتن آن‌ها دستورهای کشف اطلاعات را طوری صادر کنند که امکان دسترسی به هرگونه اطلاعات ذخیره‌شده یا در دسترس را فراهم کنند. این خواسته به وضوح، به زیان حریم خصوصی تمام می‌شود[1] (Sony Music Entertainment (Australia) Limited & others v University of Tasmania & others, 2003, p.26). بنابراین، در هنگام صدور دستور تحقیقات مقدماتی و برای محدودکردن دامنهٔ اطلاعات افشاشده، در پرونده‌های مربوط به گزارش‌های الکترونیکی، حداقل‌های زیر باید در نظر گرفته شوند:

- پرونده‌های الکترونیکی ذخیره‌شدهٔ افراد، باید اسناد و مدارک شخصی محسوب شوند؛
- نباید افراد برای دسترسی گسترده به اطلاعات انتقالی (موقتی) تشویق شوند؛
- به افراد نامرتبط به پرونده توجه شود.

جداسازی اسناد مرتبط از پرونده‌های الکترونیکی(شخصی)

چون نیازی نیست فقط برای دسترسی به یک پرونده، همهٔ سرور رایانه بررسی شود و گزارش‌کار

1. [2001] FCA 271

تمام اشخاصی که در رایانه ذخیره شده شناسایی و منتقل شود، کاملاً منطقی است که دسترسی به سرور، برای دستیابی به انواع خاصی از گزارش‌ها یا اسناد، محدود شود و اطلاعات شخصی، قبل از دسترسی و افشای نسخه‌هایی که از دستگاه‌های ذخیرهٔ سرور تهیه شده، حذف شود. این روند الکترونیکی، تقریباً، شبیه کنار گذاشتن اطلاعات نامرتبط در نسخه‌های چاپی و یا شبیه تحویل چندین پروندهٔ یک قفسه، به‌جای تحویل پرونده‌های کل قفسه است.

محدودکردن دسترسی به اطلاعات موقتی (انتقالی)

اطلاعات از یک دیدگاه، به اطلاعات ایستا (پایدار) و اطلاعات پویا (ناپایدار) تقسیم می‌شود. دستورهای آنتون‌پیلر، دسترسی به هر دو نوع اطلاعات را ممکن می‌کند، با این تفاوت که دربارهٔ اطلاعات پایدار (ایستا)، اعطای دستور، هنگامی است که گزارش‌ها در حال نابودی باشند.[1] بسط این قاعده باعث می‌شود که یک طرف دعوی، اجازهٔ دست‌اندازی به تمامی ارتباطات بین کاربران و مراکز خدماتی را برای جلوگیری از گم‌شدن اطلاعات پیدا کند. در حالی که در ابزارهای دیگر به‌کارگرفته‌شده در ارتباطات، دارندهٔ حق کپی‌رایت به راحتی نمی‌تواند اطلاعات مشابهی را در دنیای «آنالوگ» و برای مثال، از راه به دست آوردن دستوری مبنی بر ضبط همهٔ مکالمه‌های تلفنی بین یک موسسهٔ بزرگ و افراد مرتبط با آن، به دست آورد. این تفاوت، هیچ توجیه منطقی ندارد و یکی‌نبودن ابزارهای به‌کارگرفته‌شده در ارتباطات نباید بر روش حمایت قانونی از حریم خصوصی ارتباطات تأثیر بگذارد. به بیان دیگر، پویایی اطلاعات و سهولت دسترسی انبوه به آن، نباید مجوزی برای نقض حریم خصوصی کاربران باشد و مشابه دنیای آنالوگ، دسترسی به اطلاعات الکترونیکی نیز باید محدود شود.

توجه به افراد نامرتبط با پرونده

زمانی که دستور تحقیقات مقدماتی یا انواع دیگر افشا صادر می‌شود، باید این دستور دربارهٔ

1. (2004) 205 ALR 319; 59 IPR 299.

اطلاعاتی باشد که به‌طور معمول، در دادگاه به آن‌ها نیاز است. بنابراین، اطلاعات نامرتبط نباید فقط به دلیل آنکه خوانده به آن‌ها دسترسی داشته، افشا شود. همچنین، ضرورتی هم ندارد که همهٔ اطلاعات کاربران سرورها، که اغلب با دادرسی نامرتبط است، افشا شود.

تعهد ضمنی به استفاده نکردن نادرست از اطلاعات

اطلاعات تهیه‌شده یا به‌دست‌آمده در طی دادرسی قانونی، موضوع تعهدی ضمنی در قبال دادگاه به شمار می‌رود (Home Office v Harman , 1983, p.280) تا اطلاعات افشاشده، بدون اجازهٔ دادگاه، برای اهداف پنهانی و جانبی، به‌کار گرفته نشود (Citing Cobra Gold Inc v Rata, 1996, p.819).

براساس این تعهد ضمنی، دستور کشف، فقط باید برای هدفی که دستور کشف به سبب آن صادر شده، به‌کار گرفته شود، و چون هدف از صدور فرمان کشف هویت، اغلب، شناسایی درست افرادی است که دعوی باید علیه آنان اقامه شود، اطلاعات افشاشده را فقط می‌توان برای شناسایی افراد ذی‌ربط به‌کار گرفت (Northrop J in Autodesk Australia Pty *Ltd v Dyason* , 1994, p.471).

احتیاط در صدور دستورهای سیار (دوره‌ای) علیه خواندگان ناشناس

در برخی پرونده‌ها، وضعیت نقض حقوق مالکیت فکری، به صدور دستور کشف علیه خواندگان ناشناس نیاز دارد، به‌طوری‌که خواهان بتواند کالاهای قاچاق، که برای مثال، با نقض علامت تجاری خواهان تولید شده است، یا اسناد مربوط را از افراد، «در هر جایی که آن‌ها را بیابد» (سیار) ضبط کند. این اطلاعات را می‌توان برای کشف موارد بیشتر نقض و نیز کشف خواندگان جدید به‌کار گرفت. دستورهای سیار، به خواهان اجازه می‌دهد دربارهٔ هر رابطی در زنجیرهٔ نقض بررسی و تحقیق کند. این دستورها خواهان را قادر می‌کند تا به دنبال ناقضان احتمالی بگردد و اطلاعات و اموال را ضبط کند. در حالی که این گونه دستورها، به وضوح، مداخله در حق افرادی است که باید خلوت و امنیت مالی و تجاری آن‌ها محترم شمرده شود. بنابراین، شایسته است دادگاه‌ها احتیاط بیشتری را در صدور دستورهای سیار داشته باشند.

تضمین‌های موجود در درخواست‌های یک‌جانبه

احکام یک‌جانبهٔ مربوط به کشف یا تحویل، تنها باید زمانی صادر شوند که یا برای نابودی اطلاعات مورد نظر، تهدیدی فوری و یا احتمال واردآمدن خسارت جبران‌ناپذیر به خواهان وجود دارد. با این حال، خواهان، از یک سو تلاش می‌کند با به‌کارگیری انواع ترفندها، دربارهٔ ترس از آسیب، اغراق کند و از سوی دیگر، تعیین خطر آسیب احتمالی، به دلیل نبود خوانده، برای دادگاه دشوار است. به علاوه، گاهی خطر نابودی اطلاعات، ضمنی و غیرمستقیم است. برای مثال، وقتی شواهد محکمی در دست است که خواندگان از نقض حق خواهان آگاهی داشته‌اند (Northrop J in Autodesk Australia Pty *Ltd v Dyason* ,1994, p.7). براساس قاعده‌ای که قاضی «آلسوپ» در پروندهٔ شکایت «اسکای چنل علیه یاموک»[1] بیان کرده است، حکم آنتون پیلر باید زمانی صادر شود که خطر، فوری است، یعنی اگر خوانده آگاه شود، مدارک را نابود می‌کند و خواهان باید شواهد محکمی را دربارهٔ نقض آگاهانهٔ حقوق خود به دست خوانده به دادگاه دهد. بنابراین، مشکل مهم در فرآیند دادرسی این است که اگر دادگاه در برابر درخواست‌های یک‌جانبه تسلیم شود، ممکن است خواهان دربارهٔ ترس از آسیب احتمالی و نابودی اطلاعات، اغراق کرده باشد و اگر این درخواست را نپذیرد، به این معنی است که نتیجه را بدون دفاع خوانده و استدلال متقابل وی و وکیل او به سود او تغییر داده است که در هر حال، خروج از بی‌طرفی و عدالت به شمار می‌رود. از این **رو**، در فرآیند دادرسی و برای ایجاد تعادل بین این دو امر متضاد، به دو نکتهٔ اساسی باید توجه کرد:

نخست، مکلف ساختن خواهان به صداقت در رفتار، خواهان‌ها، در دادرسی‌های یک‌جانبه، باید در مقابل دادگاه، با صداقت رفتار کنند (Sega Enterprises Ltd v Alca Electronics, 1982, p.525)[2]؛

1. (2003) 58 IPR 63.
2. Sega Enterprises Ltd v Alca Electronics (1982) FSR 516 at 525 per Templeman LJ.

دوم، با مطرح‌شدن درخواست‌های یک‌جانبه، به فراخور حال، دادگاه برای جلوگیری از بی‌عدالتی و حمایت از طرف غایب، درخواست کند به‌جای فرد غایب، یک نفر (دوست دادگاه)[1] در دادگاه حضور یابد.[2]

ضوابط توقیف و تفتیش داده‌ها در حقوق ایران

دربارهٔ رعایت حق حریم خصوصی در انجام‌دادن تحقیقات و اجرای حق مالکیت در محیط مجازی در حقوق ایران، دو حوزهٔ مهم به شرح زیر بررسی می‌شود:

ضوابط توقیف داده‌ها

تعرض نکردن به موارد نامرتبط

براساس مادهٔ ۱۰۳ قانون آیین دادرسی دادگاه‌های عمومی و انقلاب در امور کیفری، «از اوراق و نوشته‌ها و سایر اشیای متعلق به متهم، فقط آنچه که راجع به واقعهٔ جرم است، تحصیل و در صورت لزوم به شهود تحقیق ارائه می‌شود و قاضی، مکلف است در مورد سایر نوشته‌ها و اشیا متعلق به متهم با کمال احتیاط رفتار نموده و موجب افشای مضمون و محتوای آن‌ها که ارتباط به جرم ندارد، نشود.» (بخشنده، ۱۳۸۲، ص۱۱۰؛ گاتن، ۱۳۸۳، ص۱۵٤). اما در حال حاضر، محدودبودن امکانات بازرسی پلیس در صحنهٔ اجرای توقیف و زمان‌بربودن جداسازی داده‌ها و دیگر محدودیت‌های فنی صحنهٔ توقیف، امکان جداسازی داده‌ها را در صحنهٔ توقیف فراهم نمی‌کند (وزارت دادگستری آمریکا، ۲۰۰۲، ص ۵۲).

تصریح به توقیف داده‌ها

داده‌ها ممکن است سه شکل باشند:

- ذخیره‌شده در حامل‌های انتقال‌پذیر، مانند لوح فشرده و دیسکت؛

1. Amicus curiae
2. Ex parte Island Records Ltd [1978] Ch 122; [1978] 3 All ER 824.

- ذخیره‌شده در حامل‌های غیرقابل انتقال، مانند حافظهٔ دیسک سخت رایانه یا پایگاه دادهٔ بزرگ؛
- در حال انتقال در شبکه‌های رایانه‌ای.

دربارهٔ مورد اول، چون داده‌ها در حامل فیزیکی ذخیره شده‌اند و اختیارات تفتیش و توقیف به طور سنتی، کلیهٔ اشیای فیزیکی موجود در محل اجرای حکم را دربرمی‌گیرد، لذا مشکلی در توقیف آن‌ها نخواهد بود. اما دربارهٔ دو مورد دیگر، توسعهٔ اختیارات تفتیش و توقیف به محیط‌های مجازی و داده‌های موجود در آن‌ها که اشیای غیرمادی محسوب می‌شوند، پذیرفته نیست، و در صورت امکان وجود چنین داده‌هایی در محل، مأموران باید اجازهٔ مخصوص مقام قضایی را بگیرند. البته این امر مانع نمی‌شود که اگر مأموران در هنگام تفتیش، به چنین مواردی برخوردند، به‌دلیل بیم از نابودسازی دلایل، خود اقدام کرده و مراتب را سریعاً به مقام قضایی اطلاع دهند (مفاد مادهٔ ٢٦ لایحهٔ جرایم رایانه‌ای و مادهٔ ۲۸ اصلاحیهٔ آن)[1] (بخشنده، ۱۳۸۲، ص۱۰۵).

همچنین، براساس مادهٔ ۳۲ لایحهٔ جرایم رایانه‌ای، «چنانچه در حین اجرای دستور تفتیش و توقیف، تفتیش داده‌های مرتبط با جرم ارتکابی در سایر سیستم‌های رایانه‌ای یا مخابراتی که تحت کنترل و یا تصرف متهم قرار دارند، ضروری باشد، «ضابطان» با «دستور مقام قضایی» دامنهٔ تفتیش و توقیف را به سیستم‌های دیگر گسترش داده و داده‌های موردنظر را تفتیش و یا توقیف خواهند نمود»[2]. البته، براساس اصلاحیهٔ لایحهٔ جرایم رایانه‌ای (مادهٔ ۳۵)، اجازهٔ مقام قضایی ضرورت دارد و عبارت «ضابطان» نیز به «مأموران» تبدیل شده تا کارشناسان هم جزء آن‌ها شمرده شوند.[3]

---

۱. همچنین، ر.ک. مجلس شورای اسلامی، دورهٔ هفتم، لایحهٔ جرایم رایانه‌ای؛ اداره کل قوانین، شماره ثبت: ٤٢٩، شماره چاپ ٩٣٦، ١٣٨٤. مجلس شورای اسلامی، مرکز پژوهش‌ها؛ اظهار نظر کارشناسی دربارهٔ لایحهٔ «جرایم رایانه‌ای»؛ کد موضوعی ۲۰۰، شماره مسلسل ۷۵۵۲، آبان ١٣٨٤

۲. مجلس شورای اسلامی، دورهٔ هفتم، لایحهٔ جرایم رایانه‌ای؛ همان.

۳. مجلس شورای اسلامی، مرکز پژوهش‌ها؛ اظهار نظر کارشناسی دربارهٔ لایحهٔ «جرایم رایانه‌ای» همان.

تعیین سقف زمانی برای توقیف داده‌ها

در اصلاحیهٔ لایحهٔ جرایم رایانه‌ای و الحاق مادهٔ ۳۸ به آن بیان شده است «در مواردی که اصل داده‌ها یا سیستم‌های رایانه‌ای یا مخابراتی توقیف می‌شوند، قاضی، موظف است با لحاظ نوع و میزان داده‌ها و نوع و تعداد سخت‌افزارها و نرم‌افزارهای مورد نظر و نقش آن‌ها در جرم ارتکابی، در مهلت متناسب و متعارف نسبت به آن‌ها تعیین تکلیف کند[1]». اما ضمانت اجرایی رعایت‌نکردن این موارد، معلوم نشده است.

رعایت گسترهٔ بازرسی شعبه‌های شبکه‌های رایانه‌ای

در صورت لزوم، شبکهٔ رایانه‌ای از چند نقطه بازرسی و داده‌های موجود در آن توقیف می‌شود، برای مثال، دربارهٔ شبکهٔ رایانه‌ای شرکتی که چند شعبه دارد و باید همهٔ شعبه‌های آن به‌طور هم‌زمان بازرسی شود، داشتن حکم کلی برای بازرسی این شبکه کافی نیست، بلکه باید نام مکان‌های مختلفی که باید بازرسی شود، در حکم آمده باشد (قاجار قیونلو، ۱۳۷٤، ص ۵۷).

توجه به حقوق اشخاص ثالث

بحث توقیف داده‌ها و سیستم‌های رایانه‌ای، بیشتر مقدمه‌ای برای حفظ حقوق اشخاص و دفاع و حفاظت از منافع عمومی دانسته می‌شود. در نتیجه، اگر حقوق خواهان (شاکی) در تزاحم با حقوق مهم‌تری قرار گیرد، این حق در هنگام توقیف داده‌ها و سیستم‌های رایانه‌ای اعمال نخواهد شد. یکی از این موارد، تزاحم حق خواهان (شاکی) با حقوق اشخاص ثالث است. البته باید توجه داشت فقط زمانی می‌توان حقوق اشخاص ثالث را مقدم دانست که احتمال لطمهٔ شدید به حقوق اشخاص ثالث وجود داشته باشد.

البته مادهٔ ۳٦ اصلاحیهٔ لایحهٔ جرایم رایانه‌ای هیچ اشاره‌ای به ضررهای حیثیتی نکرده است که از این جهت، می‌توان به آن انتقاد کرد مگر اینکه در توجیه نگفتن این موضوع مهم، آن را سهو قلم

---

۱. مجلس شورای اسلامی، مرکز پژوهش‌ها؛ اظهار نظر کارشناسی دربارهٔ لایحهٔ «جرائم رایانه‌ای»؛ همان.

در قانون‌گذاری دانست و یا با تمسک به قیاس اولویت و اهمیت بیشتر «آبرو» بر جسم و مال، حیثیت‌های معنوی را هم مشمول این ماده دانست. همچنین، می‌توان گفت، چون قانون‌گذار از «ضرر شدید» سخن گفته است، آن را به دو جنبهٔ مالی و جسمانی محدود کرده است وگرنه دربارهٔ حیثیت‌های معنوی، هر نوع ضرری در برابر حق توقیف یادشده، شدید و مهم محسوب می‌شود. همچنین، اگر این حقوق در تزاحم با منافع عمومی یا مسئلهٔ امنیت ملی قرار گیرد، با توجه به تقدم حقوق و منافع عمومی و امنیت ملی بر منافع فردی، باز هم امکان اعمال حق یادشده نخواهد بود.

حق دریافت کپی از اصل داده‌ها

در این زمینه مادهٔ ۳۷ لایحهٔ جرائم رایانهٔ مقرر می‌دارد «در جایی که اصل داده‌ها توقیف می‌شود، ذی‌نفع حق دارد پس از پرداخت هزینه، از آن‌ها کپی دریافت کند، مشروط به اینکه ارائهٔ داده‌های توقیف‌شده منافی با محرمانه‌بودن تحقیقات نباشد و به روند تحقیقات لطمه‌ای وارد نسازد و داده‌ها غیرقانونی نباشند». اگرچه در این ماده به اشخاص ثالث اشاره نشده است، براساس ظاهر ماده و اصطلاح «هر ذینفع» می‌توان گفت، اشخاص ثالث هم می‌توانند با هزینهٔ خود تهیهٔ رونوشت از اصول داده‌های توقیف‌شده را بخواهند (بخشنده، ۱۳۸۲، ص ۱۰۵؛ زیبر، ۱۳۸۳، ص۲۳۹).

ضوابط تفتیش داده‌های ارتباطی

ضوابط تفتیش داده را در دو قسمت می‌توان بیان کرد؛ نخست، ضوابط کلی تفتیش و دوم، ضوابط اختصاصی تفتیش داده‌های ارتباطی و رهگیری ارتباطات اشخاص.

ضوابط کلی صدور دستور تفتیش

ضوابط کلی صدور دستور تفتیش در چهار قسمت به شرح زیر بررسی خواهد شد.

الف) تعیین محل یا شیء مورد تفتیش: در مجوز صادرشده باید آدرس دقیق محل مورد تفتیش نوشته شود. پیش‌نویس لایحهٔ آیین دادرسی کیفری در مواد ۱۹-۱۲٤، علاوه بر اشاره به ضرورت موردی‌بودن مجوز، به ضرورت درج نشانی اماکن در آن نیز اشاره کرده است.

ب) تعیین اقدام‌های مورد نیاز: در مجوز تفتیش باید حدود اقدام‌های ضابط نوشته شود. اگر

تعیین دقیق اشیایی که در تفتیش، به دنبال آن هستند، ممکن باشد، باید در مجوز نوشته شود که فقط ضبط این اشیا ممکن است و در غیر این صورت، باید مشخص شود که با توجه به اتهام واردشده، اشیا مربوط می‌توانند چگونه باشند، تا فقط ضبط آن‌ها ممکن باشد. چنانچه در محل بازرسی، اسناد و مدارکی یافت شود که مربوط به جرم متهم نیست ولی بر ارتکاب جرم دیگری دلالت دارد، موضوع، مشمول مادهٔ ۷۷ قانون آیین دادرسی‌کیفری است» (زراعت، ۱۳۸۳، ص۳۵۴).

ج) زمان تفتیش: جز در موارد ضروری (به تشخیص مقام قضایی) و جز در مورد جرائم مشهود، «مصونیت مطلق اقامتگاه از بازرسی‌های شبانه» اصل، دانسته شده است (مادهٔ۱۰۰ قانون آیین دادرسی دادگاه‌های عمومی و انقلاب).

د) مدت اعتبار مجوز و دفعات اقدام: مقام صالح صدور مجوز باید مدت اعتبار مجوز را در آن بنویسد. بند سوم مادهٔ ۲۱ لایحهٔ[1] (طرح)[2] حمایت از حریم خصوصی، از جمله موارد بی‌اثربودن حکم برای ورود به اماکن خصوصی و منازل را گذشتن ۱۵ روز از تاریخ صدور مجوز و اجرانکردن آن دانسته است. مواد ۱۹-۱۲٤ پیش‌نویس لایحهٔ آیین دادرسی کیفری به مدت اعتبار مجوز تفتیش اشاره نکرده است و نوشتن زمان تفتیش را در مجوز، کافی دانسته است.

ضوابط اختصاصی دستور شنود و رهگیری ارتباطات

مادهٔ ٦١ لایحهٔ حمایت از حریم خصوصی به مجموعه ضوابطی برای صدور مجوز رهگیری اشاره کرده است که به‌طور مختصر نقل می‌شود.

---

۱. مجلس شورای اسلامی، دورهٔ ششم، لایحهٔ حمایت از حریم خصوصی، ادارهٔ کل قوانین، شماره ثبت:٤٥٥، شمارهٔ چاپ ۹۸۵، ۱۳۸٤/٥/١٦.

۲. مجلس شورای اسلامی،دورهٔ هفتم، طرح حمایت از حریم خصوصی، ادارهٔ کل قوانین، شمارهٔ ثبت ٥٦٠،شمارهٔ چاپ ۱٤۸۳، ۱۳۸٥/٤/۸.

مشخصات افرادی که ارتباطات آن‌ها باید رهگیری یا کنترل شود

افرادی که ارتباط تلفنی آن‌ها رهگیری یا کنترل می‌شود، باید به‌طور دقیق مشخص شوند. گاه فقط یک طرف ارتباط، مشخص است و مشخصات طرف دیگر در دست نیست. در این‌موارد، بهتر است به نوشتن مشخصات دقیق یک طرف، و نوشتن مشخصات کلی، مانند مرد یا زن‌بودن، موضوع گفتگو، رابطه و جز آن بسنده شود. بنابراین، شنود و رهگیری ارتباطات افراد نامرتبط با پرونده مجاز نیست. البته باید توجه کرد براساس مواد ٤٥، ٦٩ و ٧٠ ق. آ. د.ک، توقف تحقیقات به عذر معین‌نبودن متهم، ممنوع است. این مواد در واقع، اصل لازم‌نبودن تعیین متهم و ضرورت انجام‌دادن تحقیقات مراجع قضایی را بیان می‌کند. بنابراین، شناخت هویت متهم، برای شروع تحقیقات، ضروری نیست و قاضی باید تحقیقات خود را دربارهٔ موضوع و نه شخص معین شروع کند، و اگر نام کسی در شکواییه یا کیفرخواست نیامده باشد (طرح دعوی علیه شخص ناشناس)، قاضی تحقیق مکلف است دربارهٔ موضوع مطرح‌شده تحقیق کند (آشوری، ۱۳۸۳، ص۲۸).

تعیین نحوهٔ اجرای قرار

بر حسب اوضاع و احوال هر مورد، مقام قضایی صادرکنندهٔ مجوز باید نوع اقدام‌های ضروری دربارهٔ آن مورد را در مجوز قید کند که ممکن است «رهگیری و شنود مکالمه‌ها»، «اطلاع از تماس‌های برقرارشده با افراد خاص» یا «رهگیری حضوری و ضبط مکالمه‌های در مکان‌های عمومی و خصوصی» و نظایر آن را شامل شود. همچنین، مقام قضایی باید نوع اقدام‌های ضابطین را در شنود مکالمه‌های افراد موضوع قرار روشن کند، به‌طوری که تا حد ممکن، ضبط مکالمه‌ها و استخراج مفاد ارتباطات الکترونیکی و نظایر آن، به موارد ضروری و به موضوع خاص مورد نظر محدود شود (شهشهانی، ١٣٨٦، ص١١٤).

موضوع مورد رهگیری

مجوز شنود مکالمه‌های افراد نباید وسیله‌ای برای سوء استفادهٔ مأموران اجراکنندهٔ دستور شود؛ به طوری که آن‌ها به بهانهٔ کشف حقیقت، اختیار داشته باشند که همهٔ مکالمه‌های فرد موضوع قرار را

دربارهٔ هر موضوعی ضبط کنند (شهشهانی، ۱۳۸٦، ص۱۱٦). در رعایت حریم خصوصی باید حوزهٔ عملکرد مأموران در این زمینه به‌طور دقیق معلوم شود.

ضرورت‌هایی که اجازهٔ رهگیری می‌دهند، یکسان نیستند. بنابراین، در هر مورد باید به قدر متیقن بسنده کرد. گاه، ضرورتی برای «شنود مکالمات» یا «افشای مفاد نامه‌های الکترونیکی» افراد و مانند آن وجود ندارد. در چنین مواردی، مجوز «رهگیری» صادر نخواهد شد. در این صورت، فقط این مسئله بررسی خواهد شد که فرد موضوع قرار با کجا ارتباط داشته و یا با وی ارتباط برقرار شده است یا نه، و در صورت لزوم، شماره یا IP مورد نظر متعلق به چه کسی بوده و از چه محلی، تماس انجام گرفته است.

مدت زمان اعتبار مجوز

براساس نظریهٔ شمارهٔ ۷/۱٤٦٥–۱۳۷۱/۲/۲۰ ادارهٔ حقوقی دادگستری: «مطابق اصل ۲۵ قانون اساسی جمهوری اسلامی ایران، ضبط و افشاکردن مکالمات تلفنی و استراق سمع، ممنوع است مگر به حکم قانون. بنابراین، چنانچه منحصراً از طریق استراق سمع، کشف جرم امکان‌پذیر باشد، دادستان با توجه به مادهٔ ٤۸ قانون آیین دادرسی کیفری ۱۱ شهریور ۱۲۹۰ [فعلاً تبصرهٔ مادهٔ ۱۰٤ قانون آیین دادرسی دادگاه‌های عمومی و انقلاب در امور کیفری] مجاز به صدور دستور استراق سمع مکالمات تلفنی متهم، آن هم در مدت معین، به ضابطین دادگستری می‌باشد.» (حسینی، ۱۳۸۲، ص۲۹۱). قوانین فعلی چنین ضابطه‌ای را مقرر نکرده‌اند؛ ولی در مادهٔ ۲۸–۱۲٤پیش‌نویس لایحهٔ آیین دادرسی کیفری به تعیین مدت و دفعات کنترل اشاره شده است. به‌کارگیری این ضابطه در ارتباطات الکترونیکی هم ممکن است.

تعیین استفاده‌کننده از اطلاعات به‌دست‌آمده

مقام قضایی صالح باید در مجوز صادره شده، علاوه بر تعیین مقام اجراکنندهٔ قرار، افرادی را که حق دسترسی به مکالمات ضبط‌شده یا اطلاعات به‌دست‌آمده از آن را دارند، نیز مشخص کند. مادهٔ ٦۲ لایحهٔ (طرح) حمایت از حریم خصوصی نیز هرگونه افشای اطلاعات به‌دست‌آمده از رهگیری

قانونی را به اشخاص و مراجع غیرقانونی، جرم می‌داند و مادهٔ ٦٣ این لایحه مقرر می‌دارد که خدمات‌دهندگان از راه دور و کارمندان و کارگران و متخصصان فنی آنان که در اجرای قانون مادهٔ ٦٢ لایحه با مأموران دوست همکاری می‌کنند، حق افشای وسایل به‌کار گرفته شده برای رهگیری، ارتباطات رهگیری‌شده و اطلاعات گردآوری شده را ندارند. به هر حال، مقام اجراکنندهٔ قرار موظف است با تمام‌شدن اجرا اقدام‌های خود را به مقام قضایی صادرکنندهٔ دستور گزارش دهد.

تطبیق و نتیجه

در حقوق ایران و کامن‌لا، اگر معلوم شود که شواهدی مبنی بر صحت ادعای خواهان (شاکی) وجود دارد، مقام قضایی، دستور تحقیقات مقدماتی را برای احقاق حق خواهان (شاکی) صادر می‌کند. در هر دو، اولاً، صدور قرار در گرو طرح دعوی نیست و ثانیاً، برای جلوگیری از نابودی شواهد و ادله، ابلاغ مفاد قرار به خواندهٔ (متهم) احتمالی ضرورتی ندارد.

در کامن‌لا، برای حفظ حریم خصوصی اشخاص در تحقیقات مقدماتی، به‌ویژه برای جلوگیری از خطراتی که برای اشخاص ثالث و نامرتبط پیش می‌آید، بین موارد مختلفی که ممکن است به کشف دلیل، کشف هویت و افشای هویت بینجامد، فرق می‌گذارند. در هر مورد، شرایط و مقدمات خاصی لازم است و رویهٔ قضایی هم میل دارد که دامنهٔ قرارهای تحقیق بیشتر، محدود و منطبق با قوت استدلال خواهان (شاکی) و محدودهٔ نیاز وی در پیش‌برد دعوی، با حفظ بیشتر حقوق اشخاص ثالث و نامرتبط با دعوی، باشد. در حقوق ایران، براساس اصل لازم‌نبودن تعیین متهم، شناخت هویت متهم، برای شروع تحقیقات ضروری نیست و قاضی تحقیق باید تحقیقات خود را دربارهٔ موضوع، و نه الزاماً دربارهٔ شخص معینی شروع کند. حتی در جایی که دستور تحقیقات مقدماتی، به کشف و افشای هویت هم بینجامد، قاضی، باید اقدام‌های لازم را در این زمینه انجام دهد. بنابراین، در حقوق ایران، این دستور می‌تواند بدون جداسازی و در همهٔ زمینه‌ها، از جمله «وجود دلیل قابل کشف برای اقامهٔ دعوی»، «کشف هویت»، «افشای هویت» و «کشف اطلاعات» صادر شود. در حالی که به نظر می‌رسد، توجه نکردن به جداسازی، در موارد بسیاری به نقض حریم خصوصی اشخاص ثالث می‌انجامد.

بنابراین، باید در تنظیم لایحهٔ حریم خصوصی و قوانین دیگر مرتبط با حریم خصوصی به این مسئلهٔ مهم توجه شود. به علاوه، در صدور قرارهای تحقیق نیز به گونه‌ای عمل شود که در هر مورد، به قدر متیقن از موارد مورد نیاز بسنده شود. جداسازی کشف هویت، افشای هویت و کشف اطلاعات و مشروط‌کردن هر یک به وضعیت خاص خواهان و قوت استدلال وی، مناسب به نظر می‌رسد.

در حقوق کامن‌لا و حقوق ایران، هنگام صدور قراری که برای کشف دلیل یا کشف و افشای هویت صادر می‌شود، گرفتن «خسارت احتمالی» برای دادگاه‌ها التزامی نیست؛ در حالی که به نظر می‌رسد، حداقل در مواردی که بیم ورود زیان جبران‌ناپذیر به حریم خصوصی هست، یا قوت دلایل خواهان بسیار ضعیف است، این کار باید اجباری شود و گرفتن این خسارت می‌تواند در جبران خسارت‌های واردشده و انصراف کسانی که درصدد طرح دعوی واهی و کشف اطلاعات از افراد نامرتبط‌اند، مفید باشد.

منابع و مآخذ

۱. آخوندی، محمود (۱۳۸۰). *آیین دادرسی کیفری*. جلد دوم، تهران، سازمان چاپ و انتشارات.

۲. آشوری، محمد (۱۳۸۳). *آیین دادرسی کیفری*. جلد دوم، تهران، سازمان مطالعه و تدوین کتب علوم انسانی دانشگاه‌ها.

۳. بخشنده، مسعود (۱۳۸۲). *بررسی پیش‌نویس لایحهٔ قانونی جرایم کامپیوتری ایران و مطالعهٔ تطبیقی آن (بلژیک و انگلیس)*. پایان‌نامهٔ کارشناسی ارشد حقوق جزا و جرم‌شناسی، دانشگاه تهران.

٤. حسینی، سیدمحمدرضا (۱۳۸۲). *قانون مجازات اسلامی در رویهٔ قضایی*. تهران، انتشارات مجد.

۵. زراعت، عباس (۱۳۸۳). *قانون آیین دادرسی در نظم حقوقی کنونی*. تهران، انتشارات خط سوم.

٦. زیبر، اولریش (۱۳۸۳). *جرائم رایانه‌ای*. ترجمهٔ محمدعلی نوری و همکاران، تهران، گنج دانش.

۷. میرشمس شهشهانی، مائده (۱۳۸٦). *حمایت از حریم خصوصی در تحقیقات مقدماتی*. پایان‌نامهٔ کارشناس ارشد جزا و جرم‌شناسی، دانشگاه تهران.

۸. قاجار قیونلو، سیامک (۱۳۷٤). *مطالعهٔ تطبیقی ادلهٔ اثبات در محیط‌های دیجیتال و ادلهٔ کامپیوتری با توجه به حقوق ایران*. تهران، سازمان برنامه و بودجه، شورای عالی انفورماتیک.

۹. گاتن، آلن اِم (۱۳۸۳). *ادلهٔ الکترونیکی*. ترجمهٔ مصیب رمضانی، تهران، دبیرخانهٔ شورای عالی اطلاع‌رسانی.

۱۰. مجلس شورای اسلامی، دورهٔ ششم، *لایحهٔ حمایت از حریم خصوصی*، ادارهٔ کل قوانین، شمارهٔ ثبت: ٤۵۵، شمارهٔ چاپ: ۹۸۵، ۱۳۸٤/۵/۱٦.

۱۱. مجلس شورای اسلامی، دورهٔ هفتم، *لایحهٔ جرایم رایانه‌ای*، ادارهٔ کل قوانین، شمارهٔ ثبت: ٤۲۹، شمارهٔ چاپ: ۹۳٦، ۱۳۸٤.

۱۲. مرکز پژوهش‌های مجلس شورای اسلامی، اظهار نظر کارشناسی دربارهٔ لایحهٔ «جرایم رایانه‌ای»، کد موضوعی: ۲۰۰، شمارهٔ مسلسل: ۷۵۵۲، آبان ۱۳۸٤.

۱۳. مجلس شورای اسلامی، دورهٔ هفتم، *طرح حمایت از حریم خصوصی*، ادارهٔ کل قوانین، شمارهٔ ثبت: ۵۶۰، شمارهٔ چاپ: ۱۴۸۳، ۱۳۸۵/٤/۸.

۱٤. وزارت دادگستری آمریکا، بخش کیفری، دایرهٔ جرم رایانه‌ای و مالکیت صنعتی (۲۰۰۲). *تفتیش و توقیف و تحصیل دلایل الکترونیکی در تحقیقات کیفری*. ترجمهٔ امیرحسین جلالی، تهران، شورای عالی توسعهٔ قضایی، کمیتهٔ مبارزه با جرایم رایانه‌ای.

15. Greenleaf, G. (*2002*). "IP, Phone Home: Privacy as Part of Copyright's Digital Commons". *Hong Kong and Australian law*' in L Lessig, Hochelaga Lectures.
16. Australian Privacy Charter Council (1995). "The Australian Privacy Charter" *PLPR,* 31.
17. Kirby, M.D. (1998). "Privacy in Cyberspace". *UNSWLJ*, 21(2), 323- 325.

پرونده‌های قضایی در کامن‌لا

1. *A v B plc* [2003] QB 195 at 202.
2. *A v B plc* [2003] QB 195 at 202; [2002] 2 All ER 545.
3. *Attorney-General v Guardian Newspapers Ltd (No 2)* [1990] 1 AC 109 at 281.
4. *Attorney-General v Guardian Newspapers Ltd (No 2)* [1990] 1 AC 109 at 281.
5. *Axa Equity and Law Life Assurance Society v National Westminster Bank.* (unreported, Ch Div, Rimer J, 2 February 1998, Transcript: B F Nunnery).
6. *Bank Mellat v Nikpour* [1985] FSR 87 at 92 (CA) per Donaldson LJ.
7. C7 Pty Ltd v Foxtel Management Pty Ltd [2001] FCA 1864 at [50].
8. *Coco v AN Clark (Engineers) Ltd* [1969] RPC 41 at 48 per Megarry J.
9. *Glaxo Welcome PLC v Canada (Minister of National Revenue)* (1998) 81 CPR (3rd)372 at 387 per Stone.
10. *Home Office v Harman* [1983] AC 280; [1982] 1 All ER 532.
11. *ohn Fairfax & Sons Ltd v Cojuangco* (1988) 165 CLR 346 at 357.
12. *Kalaba v Commonwealth of Australia* [2004] FCA 763 (unreported, Heerey J, 8 June 2004,BC200403700) at [6].
13. *Levis v McDonald* (1997) 75 FCR 36 at 41, 44; 155 ALR 300; approved of in *Hooper v Kirella Pty Ltd* (1999) 96 FCR 1; 167 ALR 358 at [33].
14. Northrop J in *Autodesk Australia Pty Ltd v Dyason* (1994) 30 IPR 469 at 471.
15. *Norwich Pharmacal Co v Commissioners of Customs and Excise* [1974] AC 133 at 74A; [1973] 2 All ER 943 at 947 per Lord Reid.
16. S*altman Engineering Co Ltd v Campbell Engineering Co Ltd* [1963] 3 All ER 413 at 414 perLord Greene MR.
17. *Sega Enterprises Ltd v Alca Electronics* (1982) FSR 516 at 525.
18. *Sony Music Entertainment (Australia) Limited & others v University of Tasmania & others* [2003]FCA 532' (September 2003) 53 *Computers & Law* 16 at 19.

19. *Stephens v Avery* [1988] Ch 449; [1988] 2 All ER 477.
20. Universal Music Australia Pty Ltd v Sharman License Holdings Ltd (2004) 205 ALR 319.

قواعد و مقررات دادرسی در کامن‌لا

1. [2003] 23 *Aust Bar Rev* 314 at 320.
2. [2003] 58 IPR 63.
3. [2001] FCA 271 [1976] 1 All ER 779.
4. [1976] Ch 55.
5. [1978] 3 All ER 824.
6. [1982] 1 All ER 532.
7. [1982] 3 All ER 415 at 418 per Lawton J.
8. [1988] All ER 545 at 658.
9. [1988] 2 All ER 477.
10. [1988] 3 All.
11. [1992] 2 All ER 911 at 914B [2002] 2 All ER 545.
12. [2004] 205 ALR 319; 59 IPR 299.
13. [1992] 2 All ER 911 at 914B.