

## تحلیل کیفری نقض محرمانگی اسرار تجاری

### در مراودات و مبادلات الکترونیکی

(تاریخ دریافت ۱۴۰۴/۰۹/۱۷، تاریخ تصویب ۱۴۰۴/۱۱/۰۲)

روح الله شیرزادی

#### چکیده

گسترش تجارت الکترونیکی و تکیه روزافزون بنگاه‌ها بر داده‌ها، الگوریتم‌ها، فهرست مشتریان، روش‌های تولید، برنامه‌های بازاریابی و سایر اطلاعات غیرعلنی، جایگاه «اسرار تجاری» را از یک دارایی مکمل به یک مزیت رقابتی تعیین‌کننده ارتقا داده است. هم‌زمان، ماهیت شبکه‌ای ارتباطات و سرعت تکثیر و انتقال داده‌ها، احتمال نقض محرمانگی را افزایش داده و اثبات و انتساب رفتار مجرمانه را پیچیده‌تر کرده است. این مقاله با رویکرد تحلیلی و تطبیقی، نخست مفهوم و عناصر اسرار تجاری و محرمانگی آن را در محیط الکترونیکی بازخوانی می‌کند و سپس ابعاد کیفری نقض محرمانگی را از منظر ارکان جرم، شیوه‌های تحقق در مبادلات الکترونیکی، چالش‌های ادله دیجیتال و ملاحظات سیاست جنایی واکاوی می‌نماید. در نظام حقوقی ایران، حمایت کیفری از اسرار تجاری به‌صورت پراکنده و در قالب عناوین متعدد از جمله دسترسی غیرمجاز، شنود، سرقت داده، افشای غیرمجاز، نقض تعهدات قراردادی و سوءاستفاده از اعتماد قابل پیگیری است، اما نبود تعریف جامع و معیار روشن برای تشخیص «راز تجاری» و نیز فقدان جرم‌انگاری اختصاصی برای افشاء و بهره‌برداری غیرمجاز در بستر مبادلات الکترونیکی، به ناهمسانی رویه و کاهش پیش‌بینی‌پذیری منتهی می‌شود. مقاله در ادامه نشان می‌دهد که تبیین دقیق «موضوع جرم» و تفکیک میان دسترسی، تحصیل، افشاء و بهره‌برداری، همراه با توجه به استانداردهای بین‌المللی، می‌تواند هم از تورم کیفری جلوگیری کند و هم حمایت مؤثرتری برای اقتصاد دانش‌بنیان فراهم آورد. در پایان، مجموعه‌ای از راهکارهای تقنینی و اجرایی برای بهبود حمایت کیفری، ارتقای سازوکارهای اثبات و کاهش ریسک نقض محرمانگی در مراودات الکترونیکی پیشنهاد می‌شود.

**واژگان کلیدی:** اسرار تجاری، محرمانگی، تجارت الکترونیکی، جرم رایانه‌ای، ادله دیجیتال

## مقدمه

در اقتصاد مبتنی بر دانش، ارزش بسیاری از شرکت‌ها در دارایی‌های نامشهودی نهفته است که الزاماً در قالب اختراع ثبت‌شده یا حق مؤلف ظاهر نمی‌شوند. فرمول‌ها، نقشه‌های مهندسی، الگوریتم‌ها، رویه‌های داخلی، برنامه‌های قیمت‌گذاری، داده‌های مشتریان و نتایج پژوهش، نمونه‌هایی از اطلاعاتی هستند که اگر در معرض رقبا قرار گیرند، مزیت رقابتی بنگاه را کاهش می‌دهند یا به کلی از میان می‌برند. ویژگی مهم این اطلاعات آن است که ارزششان به «محرمانه بودن» وابسته است و به محض افشاء یا دسترسی غیرمجاز، امکان جبران کامل خسارت کاهش می‌یابد.

تحول دیجیتال، در کنار فرصت‌های بی‌سابقه برای رشد تجارت، سطح تهدیدات را نیز دگرگون کرده است. نقض محرمانگی دیگر صرفاً به برداشتن یک پرونده کاغذی یا عکس‌برداری محدود نمی‌شود، بلکه می‌تواند با یک کلیک، استخراج پایگاه‌داده، ارسال فایل رمزگذاری‌شده، یا حتی کپی بی‌صدا از مخزن کد انجام گیرد. از سوی دیگر، تقسیم کار در پروژه‌های مشترک، برون‌سپاری خدمات، رایانش ابری و استفاده از پلتفرم‌های همکاری آنلاین، مرزهای سازمانی را کمرنگ کرده و زنجیره دسترسی به اطلاعات را طولانی‌تر ساخته است. همین امر پرسش‌های کیفی مهمی را به میان می‌آورد: نقض محرمانگی اسرار تجاری در مبادلات الکترونیکی دقیقاً چه «موضوعی» دارد، با چه «رفتارهایی» تحقق می‌یابد، عنصر روانی آن چگونه احراز می‌شود و ادله دیجیتال تا چه حد می‌توانند انتساب را تقویت یا تضعیف کنند.

در حقوق ایران، هرچند عنوان «اسرار تجاری» به صورت یک نهاد مستقل و منسجم کمتر صورت‌بندی شده است، اما قواعد متعددی در قوانین مختلف وجود دارد که می‌تواند در مقام حمایت از محرمانگی اطلاعات تجاری به کار آید. علاوه بر آن، تجربه‌های تطبیقی در اسناد بین‌المللی و قوانین برخی کشورها مسیرهای مختلفی را برای جرم‌انگاری و تنظیم رابطه میان حمایت کیفی و آزادی رقابت نشان می‌دهد. این مقاله تلاش دارد با تمرکز بر محیط الکترونیکی، تصویری نظام‌مند از وضعیت حمایت کیفی ارائه کند و از منظر کارآمدی و تناسب، پیشنهادهایی برای ارتقا ارائه دهد.

## بخش اول: کلیات

مسئله اصلی این پژوهش آن است که نقض محرمانگی اسرار تجاری در مراودات و مبادلات الکترونیکی، به سبب ویژگی‌های فنی و ساختاری فضای دیجیتال، با ابهام‌های مفهومی و عملی مواجه است و نظام حقوقی نیز در پاسخ‌دهی کیفری با چالش‌هایی روبه‌روست.

نخست، در سطح مفهومی، تشخیص اینکه یک داده یا مجموعه اطلاعات، «راز تجاری» محسوب می‌شود یا خیر، وابسته به معیارهایی نظیر ارزش اقتصادی، محرمانگی، و اتخاذ تدابیر معقول برای حفاظت است. در عمل، بنگاه‌ها برخی اطلاعات را بدون طبقه‌بندی و سیاست امنیتی روشن نگه می‌دارند، اما پس از وقوع نقض محرمانگی، انتظار حمایت کیفری حداکثری دارند. از سوی دیگر، اگر معیارها بیش از حد سهل‌گیرانه باشد، هر اطلاعاتی ممکن است به عنوان راز معرفی شود و این امر به ابزارسازی کیفری در رقابت‌های تجاری منجر می‌گردد.

دوم، در سطح رفتاری، نقض محرمانگی در بستر الکترونیکی طیفی از رفتارها را دربر می‌گیرد: دسترسی غیرمجاز به سامانه یا حساب کاربری، استخراج داده از پایگاه داده، کپی‌برداری از کد منبع، ارسال یا بارگذاری در فضای ابری، افشای مستقیم به رقیب، یا استفاده غیرمجاز در محصول جدید. هر یک از این رفتارها ممکن است با عناوین کیفری متفاوتی قابل انطباق باشد. نبود جرم‌انگاری اختصاصی برای «تحصیل و افشاء و بهره‌برداری غیرمجاز از راز تجاری» موجب می‌شود برخی پرونده‌ها میان عناوین پراکنده سرگردان شوند و در نتیجه، پیش‌بینی‌پذیری کاهش یابد.

سوم، در سطح اثبات و انتساب، داده‌های دیجیتال به‌رغم قابلیت ثبت و بازسازی، آسیب‌پذیر و قابل دستکاری‌اند. علاوه بر آن، استفاده از VPN، هویت‌های جعلی، رمزنگاری، ذخیره‌سازی توزیع‌شده و سرویس‌های خارجی، مسیر کشف جرم را دشوار می‌کند. در این میان، قواعد ادله الکترونیکی، صلاحیت قضایی و همکاری بین‌المللی نقش تعیین‌کننده دارد.

چهارم، در سطح سیاست جنایی، پرسش از «حد و مرز کیفری‌سازی» مطرح است. حمایت کیفری باید از یک سو بازدارنده و حامی سرمایه‌گذاری و نوآوری باشد و از سوی دیگر، آزادی رقابت، گردش اطلاعات و جابه‌جایی نیروی انسانی را به نحو نامتناسب محدود نکند. بنابراین مسئله، صرفاً یافتن عنوان مجرمانه نیست، بلکه طراحی پاسخ کیفری متناسب،

دقیق و قابل اجراست.

بر این اساس، پرسش محوری مقاله چنین صورت‌بندی می‌شود: در نظام حقوقی ایران، نقض محرمانگی اسرار تجاری در مبادلات الکترونیکی چگونه از منظر کیفری قابل تحلیل است، چه خلأها و چالش‌هایی دارد، و چه راهکارهایی برای تقویت کارآمدی و تناسب حمایت کیفری می‌توان پیشنهاد کرد.

### بخش دوم: مرور ادبیات

ادبیات حقوقی پیرامون اسرار تجاری و حمایت کیفری از آن، در دو مسیر عمده شکل گرفته است: مسیر نخست، مطالعات نظری و اقتصادی که بر نقش اسرار تجاری در نوآوری، رقابت و انگیزه سرمایه‌گذاری تأکید می‌کند و مسیر دوم، پژوهش‌های حقوق کیفری و آیین دادرسی که بر جرم‌انگاری، عناصر جرم، ادله دیجیتال و صلاحیت تمرکز دارد.

در ادبیات بین‌المللی، معیارهای کلاسیک راز تجاری عمدتاً متأثر از قواعد رقابت منصفانه و همچنین استانداردهای موافقت‌نامه تریپس است. پژوهشگران، راز تجاری را اطلاعاتی می‌دانند که به سبب محرمانگی، ارزش اقتصادی دارد و دارنده آن اقدامات معقولی برای حفظ محرمانگی انجام داده است. این معیارها در بسیاری از نظام‌ها پذیرفته شده و سپس در قوانین خاص، مانند قانون فدرال آمریکا درباره دفاع از اسرار تجاری و نیز دستورالعمل اتحادیه اروپا، بازتاب یافته است. در این حوزه، بحث‌های مهمی درباره تمایز میان تحصیل غیرمجاز و بهره‌برداری، و نیز مرزبندی میان یادگیری مشروع از طریق مهندسی معکوس و نقض محرمانگی مطرح می‌شود.

در ادبیات کیفری، یکی از محورهای اصلی، خطر «تورم جرم‌انگاری» است. برخی نویسندگان هشدار می‌دهند که گسترش حمایت کیفری بدون معیار روشن، به استفاده ابزاری از نظام کیفری برای حذف رقبا یا محدود کردن کارکنان سابق می‌انجامد. در مقابل، دیدگاه دیگری تأکید می‌کند که در عصر دیجیتال، ابزارهای مدنی برای جبران خسارت کافی نیستند، زیرا افشاء یا تکثیر داده‌ها غالباً برگشت‌ناپذیر است و تنها ضمانت اجرای کیفری می‌تواند بازدارندگی لازم را فراهم کند. نتیجه عملی این مناظره، حرکت بسیاری از نظام‌ها به سمت جرم‌انگاری دقیق‌تر، تعریف روشن‌تر موضوع جرم، و پیش‌بینی استثناهایی مانند افشاء به‌منظور گزارش فساد یا تهدیدات عمومی بوده است.

در ایران، پژوهش‌های متعددی درباره جرایم رایانه‌ای، ادله الکترونیکی و نیز حمایت از اسرار

حرفه‌ای و شغلی وجود دارد. بخشی از ادبیات، به تفسیر مواد مربوط به دسترسی غیرمجاز، شنود، سرقت داده و افشای اسرار پرداخته و تلاش کرده است نسبت این عناوین را با حفاظت از داده‌های تجاری تبیین کند. در عین حال، ادبیات تخصصی «اسرار تجاری» به معنای دقیق آن، نسبت به حقوق اختراعات و علائم تجاری کمتر توسعه یافته است. برخی نویسندگان، خلأ تعریف قانونی و پراکندگی مقررات را نقطه ضعف دانسته‌اند و پیشنهاد داده‌اند که قانون‌گذار با الهام از استانداردهای بین‌المللی، نهاد اسرار تجاری را شفاف‌تر کند. از منظر آیین دادرسی، پژوهش‌هایی نیز درباره اعتبار امضای دیجیتالی، ارزش ادله الکترونیکی، و شیوه‌های جمع‌آوری و نگهداری داده‌ها صورت گرفته است که برای پرونده‌های نقض محرمانگی اهمیت مستقیم دارد.

جمع‌بندی مرور ادبیات نشان می‌دهد که اگرچه ابزارهای تحلیلی برای بررسی جرایم رایانه‌ای در ایران فراهم است، اما پیوند منسجم میان آن ابزارها و مفهوم راز تجاری، و نیز تحلیل اختصاصی از «نقض محرمانگی در مراودات الکترونیکی» همچنان نیازمند توسعه است. این مقاله می‌کوشد این پیوند را با چارچوب‌بندی موضوع جرم، تفکیک رفتارها و ارائه پیشنهاد‌های سیاست جنایی تقویت کند.

### بخش سوم: روش‌شناسی

این پژوهش از روش توصیفی تحلیلی بهره می‌گیرد و در کنار آن، رویکرد تطبیقی محدود برای غنی‌سازی تحلیل به کار رفته است. بدین معنا که ابتدا مفاهیم و عناصر اسرار تجاری و محرمانگی در محیط الکترونیکی به صورت نظری تبیین می‌شود، سپس عناوین کیفری مرتبط در حقوق ایران به عنوان چارچوب تحلیل انتخاب و نسبت آن‌ها با مصادیق نقض محرمانگی بررسی می‌گردد. در مرحله بعد، با استفاده از منابع معتبر فارسی و انگلیسی در حوزه حقوق مالکیت فکری، حقوق کیفری رایانه‌ای و سیاست جنایی، تجربه‌های منتخب برخی نظام‌ها و اسناد بین‌المللی برای مقایسه معیارها و راهکارها مرور می‌شود.

واحد تحلیل در این مقاله «رفتارهای نقض محرمانگی در بستر الکترونیکی» است. برای افزایش دقت، رفتارها به چهار دسته اصلی تفکیک می‌شوند: دسترسی غیرمجاز، تحصیل، استخراج داده، افشاء، و بهره‌برداری. سپس برای هر دسته، عناصر مادی و روانی، چالش‌های اثبات، و پاسخ‌های کیفری ممکن بررسی می‌شود. در نهایت، بر پایه نتایج تحلیل، پیشنهاد‌های تقنینی و اجرایی ارائه می‌شود که هم با اصول تناسب و ضرورت در حقوق

کیفری سازگار باشد و هم نیازهای اقتصاد دیجیتال را پاسخ دهد.

### بخش چهارم: مفهوم و ماهیت اسرار تجاری در بستر الکترونیکی

اسرار تجاری در ساده‌ترین بیان، اطلاعاتی است که برای یک بنگاه ارزش اقتصادی ایجاد می‌کند و به دلیل محرمانه بودن، از دسترس عمومی خارج است. تفاوت اساسی راز تجاری با بسیاری از حقوق مالکیت فکری آن است که موضوع آن با ثبت یا اعلام عمومی شکل نمی‌گیرد، بلکه دقیقاً با «پنهان ماندن» ارزش خود را حفظ می‌کند. از همین رو، رابطه میان دارنده راز و دیگران بیش از آنکه مبتنی بر اعلام حق باشد، مبتنی بر «تعهد به عدم افشاء» و «ممنوعیت تحصیل و استفاده غیرمجاز» است.

در محیط الکترونیکی، ماهیت راز تجاری پیچیده‌تر می‌شود، زیرا اطلاعات می‌تواند در قالب‌های متعدد و در زنجیره‌ای از سامانه‌ها توزیع گردد. راز تجاری ممکن است یک فایل واحد نباشد، بلکه ترکیبی از داده‌ها باشد که تنها با کنار هم قرار گرفتن ارزش پیدا می‌کند. برای مثال، یک مدل قیمت‌گذاری ممکن است در کد نرم‌افزار، جدول‌های داده و مستندات پراکنده باشد. همین پراکندگی سبب می‌شود که تشخیص «موضوع جرم» در پرونده‌های کیفری دشوارتر شود و دادگاه ناگزیر از ارزیابی دقیق فنی و اقتصادی گردد.

معیارهای رایج برای شناسایی راز تجاری، معمولاً سه عنصر را در کنار هم می‌نشانند. عنصر نخست، محرمانگی نسبی است، یعنی اطلاعات برای عموم یا برای اشخاص فعال در آن صنعت به سادگی قابل دسترسی نباشد. عنصر دوم، ارزش اقتصادی ناشی از محرمانگی است، به این معنا که اگر اطلاعات افشاء شود، دارنده آن مزیت رقابتی خود را از دست می‌دهد یا دست‌کم ارزش آن کاهش می‌یابد. عنصر سوم، اقدامات معقول حفاظتی است، یعنی دارنده راز به صورت متعارف تدابیری مانند کنترل دسترسی، طبقه‌بندی اطلاعات، قراردادهای عدم افشاء، و سیاست‌های امنیت اطلاعات را اعمال کرده باشد. در فضای الکترونیکی، این اقدامات معقول، غالباً شکل فنی‌تری می‌یابد، مانند احراز هویت چندمرحله‌ای، ثبت لاگ، رمزنگاری، تفکیک سطح دسترسی و نظارت مستمر.

نکته مهم آن است که محرمانگی به معنای «پنهان‌سازی مطلق» نیست. بسیاری از اسرار تجاری در فرآیند همکاری با پیمانکاران، توسعه‌دهندگان، یا سرمایه‌گذاران ناگزیر از اشتراک‌گذاری محدود هستند. بنابراین محرمانگی بیشتر به معنای «کنترل‌شده بودن دسترسی» است. همین ویژگی، پیوند مستقیمی با تحلیل کیفری دارد، زیرا هرگاه کنترل

دسترسی به طور مستند تعریف شده باشد، اثبات اینکه فرد از مرز مجاز عبور کرده و به اطلاعات محرمانه دسترسی یافته، آسان تر می شود.

از منظر جرم شناختی نیز، دیجیتالی شدن اسرار تجاری سه اثر اصلی دارد. نخست، هزینه ارتکاب را کاهش می دهد، زیرا کپی برداری سریع و کم ریسک تر به نظر می رسد. دوم، دامنه آسیب را افزایش می دهد، زیرا افشاء می تواند به انتشار گسترده یا فروش چندباره منجر شود. سوم، پنهان کاری و ناشناس سازی را تقویت می کند، زیرا مهاجم می تواند با ابزارهای فنی، ردپا را کم رنگ کند. این سه اثر، توجیهی برای تقویت واکنش کیفری ارائه می دهند، اما در عین حال هشدار می دهند که واکنش باید متناسب و دقیق باشد تا از سرایت کیفری به تعارضات قراردادی یا رقابت مشروع جلوگیری شود.

### بخش پنجم: گونه های نقض محرمانگی در مراودات و مبادلات الکترونیکی

نقض محرمانگی در فضای الکترونیکی، بسته به نقش مرتکب و مسیر دسترسی، شکل های متنوعی پیدا می کند. یک دسته مهم، نقض توسط اشخاص داخلی است، مانند کارمند یا مدیر یا پیمانکاری که دسترسی مجاز دارد اما از آن سوءاستفاده می کند. دسته دیگر، نقض توسط اشخاص خارجی است، مانند هکر یا رقیبی که از طریق نفوذ به سامانه یا فیشینگ، دسترسی غیرمجاز به دست می آورد. در عمل، بسیاری از پرونده ها ترکیبی اند، یعنی نفوذ خارجی با همکاری داخلی یا سهل انگاری داخلی همراه است.

در مراودات الکترونیکی، چهار مرحله رفتاری قابل تفکیک است. مرحله نخست، دسترسی است. دسترسی ممکن است غیرمجاز باشد، مانند ورود به سامانه با رمز عبور سرقت شده، یا فراتر از مجوز باشد، مانند کاربری که برای هدفی مشخص مجاز بوده اما به بخش دیگری می رود که به او مربوط نیست. مرحله دوم، تحصیل و استخراج است. در این مرحله، مرتکب داده را کپی می کند، دانلود می کند، اسکرینشات می گیرد، یا با ابزارهای پایگاه داده آن را استخراج می کند. مرحله سوم، افشاء است. افشاء می تواند مستقیم باشد، مانند ارسال ایمیل به رقیب یا بارگذاری در فضای ابری مشترک، یا غیرمستقیم باشد، مانند قرار دادن در مخزن عمومی یا ارائه در جلسه تجاری. مرحله چهارم، بهره برداری است. بهره برداری زمانی رخ می دهد که مرتکب با استفاده از راز، محصول یا خدمت رقابتی تولید کند، یا در مذاکره تجاری از آن به عنوان اهرم استفاده کند، یا به دیگری مجوز بهره برداری بدهد.

این تفکیک چهار مرحله ای از جهت کیفری اهمیت دارد، زیرا همیشه همه مراحل رخ

نمی‌دهد. گاه جرم در همان دسترسی غیرمجاز متوقف می‌شود و گاه دسترسی مجاز بوده اما افشاء رخ داده است. بنابراین تحلیل حقوقی باید به‌جای تمرکز صرف بر «افشاء»، همه حلقه‌های زنجیره را ببیند. همچنین از منظر اثبات، ادله هر مرحله متفاوت است. برای دسترسی، لاگ ورود، آدرس‌های IP، نشانه‌های احراز هویت و شواهد نفوذ اهمیت دارد. برای استخراج، آثار دانلود، انتقال فایل، اتصال حافظه جانبی، یا کوئری‌های پایگاه داده مهم می‌شود. برای افشاء، ردپای پیام‌رسان، ایمیل، لینک اشتراک، یا سوابق آپلود قابل توجه است. برای بهره‌برداری، شباهت‌های فنی، تحلیل تطبیقی محصول و نیز مسیر توسعه کسب‌وکار اهمیت می‌یابد.

در مبادلات الکترونیکی، برخی مصادیق خاص نیز برجسته‌اند. استفاده از ابزارهای همکاری تیمی می‌تواند سبب شود فایل مجرمانه به‌صورت ناخواسته یا با تنظیمات اشتباه اشتراک‌گذاری شود. این وضعیت، مرز میان تفصیر سازمانی و رفتار مجرمانه را برجسته می‌کند. همچنین در محیط‌های ابری، مسئله صلاحیت و محل داده‌ها مطرح می‌شود، زیرا سرور در کشور دیگری قرار دارد و دسترسی به داده‌ها مستلزم همکاری بین‌المللی است. در تجارت الکترونیکی بین بنگاه‌ها، تبادل قراردادهای و اسناد مجرمانه از طریق ایمیل یا پلتفرم‌ها انجام می‌شود و اگر استانداردهای امنیتی رعایت نشود، احتمال رهگیری یا افشاء افزایش می‌یابد. این موارد نشان می‌دهد که تحلیل کیفی باید با شناخت فنی همراه باشد و دادگاه و ضابطان تخصص لازم را داشته باشند.

### بخش ششم: ارکان کیفری نقض محرمانگی اسرار تجاری در حقوق ایران

برای تحلیل کیفری، باید موضوع، رفتار، نتیجه و رابطه علیت، و نیز عنصر روانی بررسی شود. در پرونده‌های اسرار تجاری، حساس‌ترین بخش، تعیین «موضوع جرم» است. اگر نتوان ثابت کرد اطلاعات واقعاً مجرمانه و دارای ارزش اقتصادی بوده و تدابیر معقول برای حفاظت از آن اتخاذ شده است، حمایت کیفری سست می‌شود یا به اختلاف مدنی فروکاسته می‌گردد. بنابراین در تحلیل حقوقی، معمولاً نیاز به کارشناس فنی و اقتصادی وجود دارد تا توضیح دهد چرا اطلاعات مورد ادعا راز تجاری است و افشاء یا تحصیل آن چه زبانی ایجاد می‌کند.

از منظر رفتار مجرمانه، در نظام ایران مجموعه‌ای از عناوین کیفری می‌تواند مورد استفاده قرار گیرد. در سطح جرایم رایانه‌ای، دسترسی غیرمجاز به سامانه‌ها و داده‌ها، شهود غیرمجاز

داده‌ها در حال انتقال، و سرقت یا ربایش داده می‌تواند در برخی پرونده‌ها عنوان مناسب باشد. اگر مرتکب بدون مجوز وارد سامانه شرکت شود و داده‌های محرمانه را مشاهده یا استخراج کند، تحلیل کیفی غالباً در قالب دسترسی غیرمجاز و سپس سرقت داده مطرح می‌شود. اگر داده‌ها در مسیر انتقال رهگیری شود، بحث شنود و رهگیری داده‌ها مطرح خواهد بود. اگر فرد مجاز بوده اما داده را به صورت غیرمجاز کپی و منتقل کرده، عنوان سرقت داده یا دست کم تحصیل غیرمجاز قابل بررسی است، هرچند اختلاف نظر درباره حدود این عناوین وجود دارد.

در کنار جرایم رایانه‌ای، برخی عناوین عمومی نیز ممکن است مطرح شود. نقض تعهدات قراردادی به تنهایی جرم نیست، اما اگر افشاء اسرار همراه با خیانت در امانت یا تحصیل مال یا منفعت نامشروع باشد، امکان انطباق با برخی عناوین سنتی مطرح می‌شود. همچنین در برخی حوزه‌ها، افشای اسرار شغلی یا حرفه‌ای دارای عنوان کیفی خاص است، هرچند دامنه آن ممکن است همه اسرار تجاری شرکت‌های خصوصی را پوشش ندهد. این پراکندگی نشان می‌دهد که نظام موجود، از طریق مسیرهای متعدد تلاش می‌کند از محرمانگی حمایت کند، اما لزوماً یک مسیر اختصاصی و شفاف برای اسرار تجاری در مبادلات الکترونیکی ندارد.

عنصر نتیجه در بسیاری از عناوین، لزوماً تحقق ضرر مالی را شرط نمی‌داند و صرف انجام رفتار ممنوع کفایت می‌کند. این نکته در اسرار تجاری مهم است، زیرا در بسیاری موارد، صرف افشاء یا تحصیل، فارغ از اثبات خسارت قطعی، زیان بالقوه جدی ایجاد می‌کند. با این حال، در مرحله تعیین مجازات و نیز در دعوای ضرر و زیان، میزان خسارت و گستره افشاء اهمیت پیدا می‌کند.

عنصر روانی نیز در پرونده‌های اسرار تجاری چالش برانگیز است. باید نشان داد مرتکب آگاه بوده که اطلاعات محرمانه است و با قصد غیرمجاز دسترسی یا افشاء یا بهره‌برداری کرده است. در فضای الکترونیکی، دفاع رایج مرتکبان این است که فایل‌ها بدون برچسب محرمانه بوده، دسترسی از طریق حساب کاربری خودشان انجام شده، یا انتقال داده برای انجام وظیفه کاری بوده است. بنابراین سیاست‌های داخلی شرکت، قراردادهای عدم افشاء، پیام‌های هشدار سامانه، و طبقه‌بندی سطح دسترسی نقش تعیین‌کننده در اثبات سوءنیت دارد. اگر سازمان هیچ قاعده روشنی نداشته باشد، اثبات آگاهی مرتکب دشوارتر می‌شود و

پرونده ممکن است به اختلاف استخدامی یا قراردادی فروکاسته شود.

## بخش هفتم: ادله الکترونیکی و دشواری‌های اثبات در جرایم مربوط به اسرار تجاری

حتی اگر عنوان کیفری مناسب تشخیص داده شود، موفقیت پرونده وابسته به اثبات فنی و انتساب دقیق است. ادله دیجیتال در عین حال که قابلیت ثبت خودکار دارد، به شدت به نحوه جمع‌آوری و نگهداری وابسته است. یک فایل لاگ اگر بدون زنجیره حفاظتی و بدون تضمین تمامیت نگهداری شود، ممکن است در دادگاه با تردید مواجه شود. همچنین داده‌های ذخیره‌شده در سرویس‌های خارجی ممکن است دسترس‌پذیر نباشد یا دیر به دست آید و در این فاصله حذف شود.

در پرونده‌های نقض محرمانگی، چند دسته دلیل معمولاً اهمیت بیشتری دارد. دسته نخست، ادله مرتبط با هویت و دسترسی است، مانند سوابق احراز هویت، لاگ ورود، تغییرات رمز عبور، و ثبت دستگاه‌های متصل. دسته دوم، ادله مربوط به انتقال یا استخراج است، مانند تاریخچه دانلود، اتصال حافظه USB، ارسال ایمیل با پیوست، بارگذاری در فضای ابری، یا رخدادهای مربوط به اجرای کوثری‌های غیرعادی در پایگاه داده. دسته سوم، ادله مربوط به افشاء و انتشار است، مانند پیام‌ها، لینک‌های اشتراک‌گذاری و ردپای انتشار در مخازن عمومی. دسته چهارم، ادله بهره‌برداری است، مانند شباهت‌های فنی میان محصول رقیب و اطلاعات محرمانه، یا تطبیق زمان‌بندی خروج کارمند با ظهور محصول مشابه.

اما هر دسته با دشواری‌هایی همراه است. در انتساب، باید میان «حساب کاربری» و «شخص» تفکیک کرد. ورود با حساب یک کارمند لزوماً ثابت نمی‌کند که خود او پشت دستگاه بوده است، مگر اینکه قرائن تکمیلی مانند موقعیت مکانی، دوربین، دستگاه اختصاصی، یا الگوی رفتاری وجود داشته باشد. همچنین رمزنگاری و انتقال از طریق کانال‌های امن می‌تواند تشخیص محتوای انتقال‌یافته را دشوار کند و دادگاه ناچار شود به دلایل غیرمستقیم تکیه کند، مانند حجم انتقال، نام فایل‌ها، یا زمان‌بندی رخدادهای.

یک چالش مهم دیگر، تعادل میان کشف جرم و حریم خصوصی است. در برخی پرونده‌ها، شرکت‌ها برای یافتن عامل افشاء، صندوق ایمیل یا پیام‌رسان کارکنان را بررسی می‌کنند. اگر این بررسی بدون مبنای قانونی و بدون رعایت اصول دادرسی انجام شود، ممکن است

ارزش اثباتی ادله زیر سؤال رود و حتی خود شرکت با ادعاهای نقض حریم خصوصی مواجه شود. بنابراین به‌ویژه در پرونده‌های کیفری، توصیه می‌شود جمع‌آوری ادله تحت نظارت مرجع قضایی و با رعایت اصول زنجیره نگهداری انجام گیرد.

از منظر آیین دادرسی، تخصص ضابطان و کارشناسان نقش کلیدی دارد. نقض محرمانگی اسرار تجاری معمولاً نیازمند کارشناسی هم‌زمان در سه حوزه است: امنیت اطلاعات، ماهیت تجاری و اقتصادی راز، و تطبیق حقوقی با عنوان مجرمانه. نبود هماهنگی میان این سه حوزه، پرونده را آسیب‌پذیر می‌کند و احتمال صدور قرار منع تعقیب یا برائت را افزایش می‌دهد.

### بخش هشتم: سیاست جنایی و سنجش تناسب در جرم‌انگاری و مجازات

حمایت کیفری از اسرار تجاری، در نقطه تلاقی چند ارزش قرار دارد. از یک سو، حمایت از سرمایه‌گذاری، نوآوری و رقابت منصفانه مطرح است. از سوی دیگر، آزادی اشتغال، جابه‌جایی نیروی انسانی، و گردش اطلاعات نیز اهمیت دارد. اگر حمایت کیفری بیش از حد گسترده باشد، ممکن است هر انتقال تجربه یا دانش عمومی به عنوان «سرقت راز» تفسیر شود و فضای کسب‌وکار را ناامن کند. اگر حمایت کیفری بسیار محدود باشد، انگیزه سرمایه‌گذاری در تحقیق و توسعه کاهش می‌یابد و اقتصاد دانش‌بنیان آسیب می‌بیند. بنابراین سیاست جنایی مطلوب باید میان این دو قطب تعادل برقرار کند.

در مبادلات الکترونیکی، به دلیل شدت و سرعت آسیب، وسوسه تقویت کیفرها بیشتر است. اما تجربه تطبیقی نشان می‌دهد که شدت مجازات به‌تنهایی بازدارندگی ایجاد نمی‌کند، بلکه «احتمال کشف و محکومیت» نقش بیشتری دارد. بنابراین کارآمدترین سیاست جنایی آن است که در کنار جرم‌انگاری روشن و متناسب، سازوکارهای کشف و اثبات تقویت شود. برای مثال، مقررات دقیق درباره ادله الکترونیکی، امکان صدور دستور حفظ داده‌ها، همکاری پلتفرم‌ها با مقامات قانونی، و آموزش تخصصی ضابطان می‌تواند اثر بازدارنده بیشتری نسبت به افزایش صرف مجازات داشته باشد.

یکی دیگر از مؤلفه‌های تناسب، تفکیک میان مرتکبان است. رفتار کارمندی که به سبب اختلاف کاری بخشی از اطلاعات را برای اثبات ادعا در مرجع حل اختلاف ارائه می‌کند، با فردی که سازمان‌یافته و با قصد رقابت، پایگاه داده مشتریان را استخراج و به رقیب می‌فروشد، یکسان نیست. سیاست جنایی باید امکان تمایزگذاری را فراهم کند؛ هم در

تعریف جرم و هم در مرحله تعیین مجازات. همچنین باید میان «افشای عمومی» و «افشای محدود» تفاوت گذاشت، زیرا گستره انتشار، میزان زیان و خطر تکرار را تغییر می‌دهد. موضوع دیگری که در سیاست جنایی اسرار تجاری مطرح است، استثنای و توجیهات است. در بسیاری از نظام‌ها، افشاء برای گزارش فساد، حفاظت از منافع عمومی، یا دفاع از حق در مرجع قضایی، تحت شرایطی می‌تواند موجه باشد. نبود تبیین روشن از این موارد، موجب می‌شود یا گزارش‌دهندگان از ترس تعقیب کیفری سکوت کنند یا افراد متخلف با ادعای گزارشگری، افشاء را توجیه نمایند. بنابراین تنظیم دقیق استثنای، بخشی از طراحی سیاست جنایی متعادل است.

### بخش نهم: پیشنهاد های تقنینی و اجرایی برای ارتقای حمایت کیفری

برای بهبود وضعیت، مجموعه‌ای از راهکارها قابل ارائه است که بخشی به قانون‌گذاری و بخشی به اجرا مربوط می‌شود.

در سطح تقنین، نخستین پیشنهاد، ارائه تعریف قانونی روشن از اسرار تجاری در چارچوب معیارهای شناخته‌شده است، به گونه‌ای که هم ارزش اقتصادی و محرمانگی و اقدامات حفاظتی را پوشش دهد و هم از ادعاهای موسع جلوگیری کند. این تعریف باید به دادگاه کمک کند موضوع جرم را دقیق شناسایی کند.

پیشنهاد دوم، تفکیک رفتاری در جرم‌انگاری است. قانون‌گذار می‌تواند رفتارهای دسترسی غیرمجاز، تحصیل و استخراج، افشاء، و بهره‌برداری غیرمجاز را به صورت تفکیک‌شده و با درجات مختلف مسئولیت پیش‌بینی کند. این کار باعث می‌شود پرونده‌ها ناچار نباشند به عناوین پراکنده متوسل شوند و پیش‌بینی‌پذیری افزایش یابد.

پیشنهاد سوم، توجه به عنصر روانی و انگیزه‌های اقتصادی است. جرم‌انگاری باید بر رفتارهای عمدی و سودمحور تمرکز کند و برای موارد اشتباه یا سهل‌انگاری، از سازوکارهای مدنی و انتظامی بهره گیرد، مگر آنکه تقصیر سنگین و خطر گسترده وجود داشته باشد.

پیشنهاد چهارم، پیش‌بینی استثنای محدود و روشن است، مانند افشاء برای دفاع از حق در مرجع قضایی با رعایت محرمانگی، یا گزارشگری فساد تحت ضوابط مشخص. این استثنای از یک سو مانع سوءاستفاده از کیفری‌سازی می‌شود و از سوی دیگر، مرزهای رفتار ممنوع را شفاف می‌کند.

در سطح اجرایی، پیشنهاد مهم، تقویت سازوکارهای ادله الکترونیکی است. باید دستورهای

فوری برای حفظ داده‌ها، ثبت زنجیره نگهداری، و استانداردهای کارشناسی فنی توسعه یابد. آموزش تخصصی ضابطان و قضات در حوزه امنیت اطلاعات و تحلیل دیجیتال نیز ضروری است.

پیشنهاد دیگر، تشویق بنگاه‌ها به پیاده‌سازی برنامه‌های انطباق و امنیت اطلاعات است. هرچه سیاست‌های دسترسی، طبقه‌بندی و قراردادهای عدم افشاء دقیق‌تر باشد، هم احتمال وقوع نقض کمتر می‌شود و هم در صورت وقوع، اثبات عنصر روانی و محدوده راز آسان‌تر خواهد شد. در عمل، حمایت کیفری بدون انضباط سازمانی، به نتیجه مطلوب نمی‌رسد. همچنین ایجاد سازوکارهای میانجی‌گرانه یا تخصصی برای حل برخی تعارضات، می‌تواند از ورود غیرضروری پرونده‌های صرفاً قراردادی به نظام کیفری جلوگیری کند. این امر در نهایت به تمرکز نظام کیفری بر پرونده‌های جدی‌تر و سازمان‌یافته‌تر می‌انجامد.

### نتیجه‌گیری

نقض محرمانگی اسرار تجاری در مراودات و مبادلات الکترونیکی، یکی از جدی‌ترین تهدیدات علیه رقابت منصفانه و سرمایه‌گذاری در نوآوری است. ویژگی‌های فضای دیجیتال، از جمله سهولت کپی‌برداری، سرعت انتقال، امکان ناشناس‌سازی و فرامرز بودن داده‌ها، سبب می‌شود که هم وقوع جرم محتمل‌تر باشد و هم اثبات آن پیچیده‌تر گردد. در حقوق ایران، حمایت کیفری از این حوزه عمدتاً از مسیر عناوین پراکنده و با اتکا به قواعد جرایم رایانه‌ای و برخی عناوین عمومی صورت می‌گیرد. این وضعیت اگرچه امکان تعقیب را در بسیاری موارد فراهم می‌کند، اما به دلیل نبود تعریف جامع از راز تجاری و نیز نبود جرم‌انگاری اختصاصی برای تحصیل، افشاء و بهره‌برداری غیرمجاز در بستر مبادلات الکترونیکی، با ناهمسانی تحلیلی و کاهش پیش‌بینی‌پذیری مواجه است.

تحلیل مقاله نشان داد که برای پاسخ کیفری مؤثر، باید نخست «موضوع جرم» به‌طور دقیق شناسایی شود و معیارهای محرمانگی، ارزش اقتصادی و اقدامات حفاظتی مورد توجه قرار گیرد. سپس تفکیک رفتاری میان دسترسی، تحصیل، افشاء و بهره‌برداری، به طراحی واکنش متناسب کمک می‌کند. در نهایت، بدون تقویت سازوکارهای ادله الکترونیکی و همکاری‌های فرامرزی، حتی بهترین جرم‌انگاری نیز در عمل کارآمد نخواهد بود.

پیشنهاد‌های ارائه شده، بر ترکیب هوشمندانه تقنین و اجرا تأکید دارد: تعریف روشن، جرم‌انگاری تفکیکی و متناسب، استثنای محدود و دقیق، و تقویت ظرفیت‌های فنی در

کشف و اثبات. چنین رویکردی می‌تواند هم از تورم کیفی جلوگیری کند و هم امنیت حقوقی لازم برای رشد تجارت الکترونیکی و اقتصاد دانش‌بنیان را فراهم آورد.

## منابع و مأخذ

- ابراهیمی، محمد. حقوق تجارت الکترونیکی. تهران: سمت. چاپ سوم. ۱۳۹۶.
- اردبیلی، محمدعلی. حقوق جزای عمومی. جلد‌های یک و دو. تهران: میزان. چاپ‌های متعدد.
- آشوری، محمد. آیین دادرسی کیفری. جلد‌های مرتبط. تهران: سمت. چاپ‌های متعدد.
- جعفری لنگرودی، محمدجعفر. ترمینولوژی حقوق. تهران: گنج دانش. چاپ‌های متعدد.
- خالقی، علی. آیین دادرسی کیفری. تهران: شهر دانش. چاپ‌های متعدد.
- میرمحمدصادقی، حسین. جرایم علیه امنیت و آسایش عمومی و اخلاق و عفت عمومی و جرایم رایانه‌ای منتخب. تهران: میزان. چاپ‌های متعدد.
- قانون تجارت الکترونیکی مصوب ۱۳۸۲.
- قانون جرایم رایانه‌ای مصوب ۱۳۸۸.
- قانون مجازات اسلامی مصوب ۱۳۹۲.
- قانون آیین دادرسی کیفری مصوب ۱۳۹۲
- Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS). World Trade Organization. ۱۹۹۴.
- Aplin, Tanya. Trade Secrets: A Global Perspective. Cheltenham: Edward Elgar Publishing. ۲nd edition. ۲۰۲۲.
- Bently, Lionel, Sherman, Brad, Gangjee, Dev, and Johnson, Phillip. Intellectual Property Law. Oxford: Oxford University Press. ۶th edition. ۲۰۲۲.
- Booth, Stephen. Cybercrime: Investigations, Prosecution and Defense. Boca Raton: CRC Press. ۲nd edition. ۲۰۱۶.
- Hannah, Dominic. Trade Secrets and Confidential Information in Commercial Law. London: Sweet & Maxwell. ۲۰۱۸.
- Milgrim, Roger M. Milgrim on Trade Secrets. New York: LexisNexis. Updated treatise.
- Rowe, Elizabeth A., and Sandeen, Sharon K. Trade Secret Law.

St. Paul: West Academic Publishing. ۳rd edition. ۲۰۲۱.

- United States. Defend Trade Secrets Act of ۲۰۱۶. Public Law ۱۱۴-۱۵۳.
- European Union. Directive (EU) ۲۰۱۶/۹۴۳ on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure. ۲۰۱۶.
- Casey, Eoghan. Digital Evidence and Computer Crime. Amsterdam: Academic Press. ۳rd edition. ۲۰۱۱.