ششمین همایش جرم شناسی و پیشگیری از ارتکاب جرم، خودکشی و انحرافات جوانان

نهاد برگزار کننده همایش: بنیاد علمی و حقوقی قانون یار

(با همکاری و حمایت معنوی دادگستری بروجرد، دانشگاه امام صادق، انجمن علمی معارف دانشگاه شهید بهشتی، دانشگاه لرستان، آموزش و پرورش، دانشگاه آزاد رفسنجان، سازمان ارشاد اسلامی، جامعه المصطفی العالمیه و....

سردبیر علمی و مسئول برگزاری همایش: دکتر بهنام اسدی (نمایه مقالات در ۸ پایگاه ملی و بین المللی)

تاریخ برگزاری همایش: ۲۹ آذرماه ۱۴۰۲ شماره مقاله: ۲۸/۲۷۵۷ رده بندی کنگره: ب ۵۶/۰۸۵۱

بررسی و مقایسه تطبیقی جاسوسی رایانه ای با دیگر جرائم مشابه

دکتر حسین یار احمدی[1]

عاطفه محمدی

چکیده

جاسوسی رایانه‌ای یکی از مهم‌ترین جرائم علیه محرمانگی داده‌ها و در عین حال از مصادیق نوپدید تهدیدکننده امنیت ملی و امنیت اقتصادی است. قانون‌گذار ایران با جرم‌انگاری «جاسوسی رایانه‌ای» در قانون جرایم رایانه‌ای، تلاش کرده میان دو قلمرو متفاوت یعنی حریم محرمانگی اطلاعات و حفاظت از منافع و امنیت کشور پیوندی کیفری برقرار کند. با این حال، این جرم به‌لحاظ مفهومی و عملی، مرزهای نزدیکی با جرائم مشابهی مانند دسترسی غیرمجاز، شنود غیرمجاز، تحصیل/سرقت داده، و نیز با «جاسوسی» در معنای سنتیِ جرائم علیه امنیت دارد. پژوهش حاضر با روش توصیفی—تحلیلی و رویکرد تطبیقی، نخست ارکان و عناصر جاسوسی رایانه‌ای در حقوق ایران را بر مبنای ماده ۳ قانون جرایم رایانه‌ای واکاوی می‌کند، سپس آن را با جرائم مشابه داخلی مقایسه کرده و در گام بعد، الگوهای تقنینی منتخب از جمله کنوانسیون بوداپست، دستورالعمل ۴۰/۲۰۱۳ اتحادیه اروپا، حقوق بریتانیا و ایالات متحده را بررسی می‌نماید. نتیجه نشان می‌دهد: (۱) در ایران، «سری بودن داده» و «جهت‌دهی به دولت/سازمان/گروه خارجی» نقش تعیین‌کننده در تمایزگذاری دارد، اما معیارهای تشخیص «سری» بودن و حدود «عدم مجاز بودن» نیازمند شفاف‌سازی است. (۲) بسیاری از نظام‌های حقوقی به جای ساختن

---

[1] نویسنده مسئول

عنوان مستقل «جاسوسی رایانه‌ای»، از ترکیب جرائم دسترسی/شنود غیرمجاز با قوانین اسرار رسمی یا اسرار تجاری استفاده می‌کنند. (۳) در سطح بین‌الملل، به‌ویژه طبق رویکردهای مطرح در ادبیات حقوق بین‌الملل سایبری، «جاسوسی سایبری» غالباً در منطقه خاکستریِ «غیرممنوع/کم‌هنجار» قرار می‌گیرد، هرچند ممکن است با قواعد حاکمیت، عدم مداخله یا حقوق بشر تداخل پیدا کند .

واژگان کلیدی: جاسوسی رایانه‌ای، محرمانگی داده، دسترسی غیرمجاز، شنود غیرمجاز، امنیت ملی، تطبیق حقوقی

مقدمه

تحول فناوری اطلاعات باعث شده «اطلاعات» از یک موضوع صرفاً اداری یا سازمانی به دارایی راهبردی تبدیل شود. دارایی‌ای که هم می‌تواند ارزش اقتصادی (اسرار تجاری، طرح‌های صنعتی، داده‌های مشتریان) داشته باشد و هم ارزش امنیتی (اسناد سیاست خارجی، نظامی، اطلاعات طبقه‌بندی‌شده). در چنین فضایی، جاسوسی نیز از شکل کلاسیکِ «نفوذ انسانی و انتقال اسناد» به شکل‌های ترکیبی و پیچیده‌تری ارتقا یافته است. از نفوذ به شبکه‌های رایانه‌ای، استراق سمع داده‌های در حال انتقال، تا استخراج خاموش داده‌ها و بهره‌برداری اطلاعاتی بلندمدت. همین دگرگونی سبب شده نظام‌های کیفری با دو پرسش کلیدی مواجه شوند:

۱. آیا باید «جاسوسی رایانه‌ای» را عنوان مستقل دانست یا آن را ذیل جرائم عمومی دسترسی و شنود غیرمجاز و افشای اسرار تحلیل کرد؟

۲. چگونه می‌توان مرز میان «کسب/افشای اطلاعات سری» و «صرف نقض محرمانگی یا حریم خصوصی» را دقیق، قابل اثبات و منطبق با اصل قانونی بودن جرم و مجازات ترسیم نمود؟

در ایران، قانون جرایم رایانه‌ای در فصل جرائم علیه محرمانگی داده‌ها، سه‌گانه‌ای را بنا می‌نهد : دسترسی غیرمجاز (ماده ۱)، شنود غیرمجاز (ماده ۲) و جاسوسی رایانه‌ای (ماده ۳) این چینش نشان می‌دهد قانون‌گذار جاسوسی رایانه‌ای را از لحاظ «حقِ مورد حمایت» نزدیک به محرمانگی داده‌ها می‌بیند، ولی هم‌زمان با افزودن وضعیت‌های تشدیدشده (به‌ویژه افشا برای دولت/سازمان/گروه خارجی)، آن را به قلمرو امنیت ملی پیوند می‌زند.

۱) مفهوم‌شناسی و قلمرو جاسوسی رایانه‌ای

۱-۱) تعریف و مؤلفه‌های اصلی

در ادبیات تخصصی، «جاسوسی سایبری/رایانه‌ای» معمولاً به تحصیل مخفیانه یا غیرمجاز اطلاعات حساس یا طبقه‌بندی‌شده از طریق ابزارها و بسترهای دیجیتال برای کسب برتری سیاسی، نظامی یا اقتصادی اشاره دارد .در نگاه تحلیلی، چهار مؤلفه غالب دیده می‌شود:

۱. موضوع اطلاعاتی (داده‌های سری/حساس/دارای ارزش امنیتی یا اقتصادی).

۲. رفتار مجرمانه (دسترسی، تحصیل، رهگیری، انتقال، افشا، در دسترس قرار دادن).

۳. غیرمجاز بودن (بدون حق/بدون رضایت/خلاف مجوز قانونی یا قراردادی).

۴. جهت‌گیری و غایت (به‌ویژه در برخی نظام‌ها: سود رساندن به دولت خارجی یا لطمه به امنیت)

در حقوق ایران، قانون‌گذار به‌طور صریح «داده‌های سری» را کانون جرم می‌گیرد و رفتارهای سه‌گانه‌ای را علیه آن جرم‌انگاری می‌کند (دسترسی/تحصیل/شنود. در دسترس قرار دادن برای فاقد صلاحیت. افشا یا در دسترس قرار دادن برای دولت/سازمان/گروه خارجی) .

۱-۲) تمایز با جاسوسی سنتی

جاسوسی سنتی در حقوق کیفری ایران غالباً ذیل جرائم علیه امنیت داخلی و خارجی تحلیل می‌شود. از جمله مقرراتی مانند ماده ۵۰۱ قانون مجازات اسلامی (تعزیرات) که بر «قرار دادن نقشه‌ها/اسرار/اسناد/تصمیمات مربوط به سیاست داخلی یا خارجی در اختیار افراد فاقد صلاحیت» با وصف «متضمن نوعی جاسوسی» تأکید دارد .تفاوت کلیدی جاسوسی رایانه‌ای با جاسوسی

سنتی در این است که ابزار و محیط ارتکاب (سامانه‌ها و حامل‌های داده) نقش محوری دارد و رفتارهایی مانند «شنود محتوای سری در حال انتقال» یا «تحصیل داده سری ذخیره‌شده» به صورت مستقل صورت‌بندی می‌شود . با این حال، در سطح سیاست جنایی، هر دو جرم یک نقطه مشترک دارند :حفاظت از اسرار و منافع راهبردی کشور .اختلاف اصلی در «مدل جرم‌انگاری» است: قانون جرایم رایانه‌ای، جرم را در دلِ جرائم محرمانگی داده‌ها قرار داده، اما با تشدید مجازات در حالت ارتباط با بازیگران خارجی، آن را به امنیت ملی نزدیک کرده است .

۲) مبانی جرم‌انگاری و سیاست جنایی

جرم‌انگاری جاسوسی رایانه‌ای را می‌توان بر سه مبنا توضیح داد:

۱. حفاظت از محرمانگی و طبقه‌بندی اطلاعات :اسرار دولتی یا سازمانی بدون حفاظت کیفری، در برابر تهدیدات سایبری شکننده‌اند.

۲. پیشگیری از تهدیدات امنیت ملی :بسیاری از عملیات نفوذ سایبری لزوماً تخریبی نیستند. هدف اصلی «جمع‌آوری اطلاعات» است و همین «جمع‌آوری» می‌تواند زمینه اقدامات بعدی (فشار سیاسی، تحریم هدفمند، خرابکاری، عملیات نفوذ شناختی) را فراهم کند.

۳. حفاظت از رقابت اقتصادی و فناوری :در جهان امروز «جاسوسی اقتصادی» سهم بزرگی از تهدیدات را تشکیل می‌دهد. برخی نظام‌ها مثل آمریکا با قانون خاص «جاسوسی اقتصادی» به اسرار تجاری پرداخته‌اند .

از منظر تطبیقی نیز مشاهده می‌شود بسیاری از اسناد بین‌المللی حوزه جرائم رایانه‌ای (مانند کنوانسیون بوداپست) به جای جرم‌انگاری مستقل «جاسوسی»، بر جرم‌انگاری پایه‌ایِ «دسترسی غیرمجاز»، «شنود غیرمجاز»، «مداخله در داده/سامانه» تکیه دارند .همین امر یک پرسش

سیاست‌گذارانه ایجاد می‌کند: آیا بهتر است جاسوسی رایانه‌ای به عنوان جرم مستقل باقی بماند یا با اصلاحات مفهومی و ارجاعی، در تعامل با قوانین اسرار رسمی/امنیتی و اسرار تجاری تنظیم شود؟

۳) ارکان و عناصر جرم جاسوسی رایانه‌ای در حقوق ایران

۳-۱) رکن قانونی

مبنای اصلی جرم، ماده ۳ قانون جرایم رایانه‌ای است که در ترجمه و بازنشر رسمی/بین‌المللی نیز انعکاس یافته است .مطابق این ماده، هر کس «به طور غیرمجاز» نسبت به «داده‌های سری» (در حال انتقال یا ذخیره‌شده) در سامانه‌های رایانه‌ای/مخابراتی یا حامل‌های داده، یکی از رفتارهای مقرر را انجام دهد، حسب بندهای الف، ب و ج با مجازات‌های متفاوت روبه‌رو می‌شود . دنکته مهم در سال‌های اخیر، به‌روزرسانی مبالغ جزای نقدی در متن‌های تجمیع‌شده قوانین (به‌عنوان نمونه گزارش‌های مبتنی بر اصلاحات جزای نقدی در سال ۱۴۰۳) است .بنابراین، در نگارش علمی باید روشن شود که «ساختار جرم» ثابت مانده ولی «مقادیر جزای نقدی» ممکن است طبق مصوبات اصلاحی تغییر کرده باشد.

۳-۲) رکن مادی (رفتار مجرمانه و موضوع)

الف) موضوع جرم: داده‌های سری

محور جرم «داده‌های سری» است. نه هر داده‌ای. این انتخاب تقنینی برای محدود کردن دایره جرم و جلوگیری از سرایت آن به همه نقض‌های محرمانگی بوده است. با این حال، چالش اصلی در عمل، تعریف و معیار تشخیص سری بودن است: آیا هر داده‌ای که سازمان آن را «محرمانه» بنامد، سری است؟ یا باید طبق نظام طبقه‌بندی رسمی و آثار امنیتی سنجش شود؟

ب) رفتارهای سه‌گانه ماده ۳

۱. دسترسی/تحصیل/شنود محتوای سری در حال انتقال :یعنی نفوذ و مشاهده یا به‌دست آوردن داده سری یا رهگیری محتوای سری در مسیر انتقال .

۲. در دسترس قرار دادن برای فاقد صلاحیت :این حالت، حتی اگر «دولت خارجی» در میان نباشد، جرم مستقل با مجازات سنگین‌تر از بند (الف) پیش‌بینی کرده است .

۳. افشا یا در دسترس قرار دادن برای دولت/سازمان/شرکت/گروه خارجی یا عامل آنها : شدیدترین حالت که پیوند روشن با امنیت ملی دارد .

در تحلیل تطبیقی، این سه‌گانه یادآور تفکیک «تحصیل» از «انتشار/افشا» در قوانین اسرار رسمی و نیز تفکیک «دسترسی غیرمجاز» از «استفاده و بهره‌برداری» در برخی نظام‌هاست.

۳-۳) رکن روانی

برای تحقق جرم، عمد در رفتار و علم به دو امر اهمیت دارد:

۱. علم به غیرمجاز بودن (بدون حق/فاقد مجوز).

۲. علم یا دست‌کم آگاهی قابل انتساب از سری بودن داده‌ها (یا اینکه داده‌ها موضوع حفاظت ویژه‌اند)

در بند (ج)، عنصر جهت‌گیری (افشا برای دولت/سازمان/گروه خارجی) معمولاً به تقویت عنصر روانی و تشدید واکنش کیفری منجر می‌شود.

۳-٤) چالش‌های اثبات و ادله دیجیتال

در جاسوسی رایانه‌ای، اثبات غالباً بر لاگ‌ها، ردپاهای شبکه‌ای، ادله فنی، زنجیره نگهداری ادله و نیز احراز «انتساب» استوار است. دشواری ویژه اینجاست که بسیاری از عملیات جاسوسی «کم‌صداتر» از حملات تخریبی است. یعنی ممکن است بدون ایجاد اختلال، صرفاً «برداشت داده» انجام شود. این ویژگی، هم ضرورت توان فنی ضابطان را افزایش می‌دهد و هم حساسیت دادگاه را نسبت به استانداردهای کارشناسی بیشتر می‌کند.

٤) مقایسه با جرائم مشابه در حقوق ایران

٤-١) جاسوسی رایانه‌ای و «دسترسی غیرمجاز»

دسترسی غیرمجاز طبق ماده ۱ قانون جرایم رایانه‌ای ناظر به «دسترسی بدون مجوز به داده‌ها یا سامانه‌های حفاظت‌شده با تدابیر امنیتی» است .

تمایز کلیدی با جاسوسی رایانه‌ای:

- در دسترسی غیرمجاز، «سری بودن داده» شرط نیست. هر داده یا سامانه حفاظت‌شده می‌تواند موضوع جرم باشد.
- در جاسوسی رایانه‌ای، موضوع جرم «داده سری» است و دامنه رفتارها علاوه بر دسترسی، «تحصیل و شنود و افشا» را نیز پوشش می‌دهد .

نتیجه: هر جاسوسی رایانه‌ای معمولاً مستلزم نوعی دسترسی غیرمجاز هست، اما هر دسترسی غیرمجاز لزوماً جاسوسی نیست.

٤-٢) جاسوسی رایانه‌ای و شنود غیرمجاز

شنود غیرمجاز در ماده ۲، شنود محتوای در حال انتقالِ «ارتباطات غیرعمومی» را جرم می‌داند . تمایز:

- شنود غیرمجاز ماده ۲، بر «غیرعمومی بودن ارتباط» تمرکز دارد. نه لزوماً «سری» بودن داده.
- جاسوسی رایانه‌ای بند (الف)، شنود «محتوای سری در حال انتقال» را در کنار دسترسی/تحصیل جرم‌انگاری می کند .

بنابراین، اگر داده در حال انتقال «صرفاً خصوصی/غیرعمومی» باشد، ماده ۲ فعال است. اما اگر «سری» باشد، ظرفیت ماده ۳ نیز مطرح می‌شود و ممکن است در مقام تعدد یا انتخاب عنوان صحیح، بحث‌های جدی ایجاد گردد.

٤-٣) جاسوسی رایانه‌ای و جرائم علیه تمامیت داده/سامانه (تخریب و اخلال)

کنوانسیون بوداپست و بسیاری از قوانین، میان «جمع‌آوری اطلاعات» و «تخریب/اخلال» تفکیک می‌کنند .در ایران نیز مواد مربوط به تخریب داده‌ها و اخلال در سامانه‌ها (مانند مقررات مشابه مواد ۸ و ۹) بیشتر ناظر به تمامیت و دسترس‌پذیری است نه محرمانگی . در مقام مقایسه، جاسوسی رایانه‌ای غالباً «بی‌سر و صدا»ست و هدفش تخریب نیست. اما ممکن است در عملیات واقعی، جاسوسی با خرابکاری ترکیب شود (مثلاً پس از سرقت داده، پاک‌سازی ردپا یا تخریب محدود).

٤-٤) جاسوسی رایانه‌ای و «جاسوسی/افشای اسرار» در قانون مجازات اسلامی

ماده ۵۰۱ قانون مجازات اسلامی (تعزیرات) افشای اسناد و اسرار مرتبط با سیاست داخلی/خارجی را در صورتی که «متضمن نوعی جاسوسی باشد» مستوجب حبس می‌داند . این ماده نسبت به جاسوسی رایانه‌ای چند تفاوت دارد:

- موضوع در ماده ۵۰۱ «نقشه‌ها، اسرار، اسناد و تصمیمات» سیاسی/امنیتی است. در ماده ۳ قانون جرایم رایانه‌ای «داده‌های سری» در بستر دیجیتال.
- رفتار در ماده ۵۰۱ بیشتر بر «در اختیار قرار دادن/مطلع کردن» تمرکز دارد. در ماده ۳ علاوه بر افشا، «تحصیل/شنود/دسترسی» نیز جرم است .
- ماده ۵۰۱ به‌صورت کلاسیک در قلمرو امنیت ملی می‌نشیند، در حالی که ماده ۳ از مسیر محرمانگی داده‌ها وارد می‌شود.

در عمل، اگر داده سریِ دیجیتال، همان اسرار موضوع ماده ۵۰۱ باشد، احتمال همپوشانی مطرح می‌شود و قاضی باید با تحلیل «خاص و عام»، «تعدد» و «اصل تفسیر مضیق قوانین کیفری» عنوان درست را برگزیند.

٤-٥) جرائم نیروهای مسلح و افشای اطلاعات طبقه‌بندی‌شده

در حوزه نیروهای مسلح، مقررات خاصی درباره افشای اطلاعات و اسناد طبقه‌بندی‌شده وجود دارد. از جمله مقرراتی که بی‌احتیاطی/بی‌مبالاتی منجر به افشای اسناد طبقه‌بندی‌شده را نیز قابل مجازات می‌داند .

این نقطه، از حیث «سیاست جنایی افتراقی» مهم است: جاسوسی رایانه‌ای در قانون جرایم رایانه‌ای عمدتاً یک جرم عمدی است، اما در قلمرو نظامی، حتی سهل‌انگاری هم ممکن است ضمانت اجرای کیفری داشته باشد. در نتیجه، قیاس تطبیقی درون‌ملی نشان می‌دهد که «موقعیت داده» و «نهاد دارنده داده» می‌تواند سطح واکنش کیفری را تغییر دهد.

۵) تطبیق با اسناد و نظام‌های حقوقی منتخب

۵-۱) کنوانسیون بوداپست (الگوی جرم‌انگاری پایه‌ای)

کنوانسیون بوداپست، برای هماهنگ‌سازی بین‌المللی، عمدتاً بر جرم‌انگاری‌های پایه مانند دسترسی غیرمجاز، شنود غیرمجاز، مداخله در داده و سامانه تکیه دارد و عنوان مستقل «جاسوسی» را به‌عنوان جرم خاصِ اطلاعات سری تعریف نمی‌کند .

پیام تطبیقی: بسیاری از کشورها «جاسوسی سایبری» را از ترکیب همین جرائم پایه با قوانین امنیتی/اسرار رسمی نتیجه می‌گیرند، نه اینکه در قانون جرائم رایانه‌ای عنوان مستقلی بسازند.

۵-۲) اتحادیه اروپا: دستورالعمل ۴۰/۲۰۱۳

دستورالعمل اتحادیه اروپا درباره حملات علیه سامانه‌های اطلاعاتی نیز بر جرم‌انگاری‌های مشترک مانند illegal access، illegal interception، data/system interference تأکید می‌کند .

این الگو نیز نشان می‌دهد که EU عموماً «نقض محرمانگی/تمامیت/دسترس‌پذیری» را محور می‌گیرد و «جاسوسی» را بیشتر در قلمرو حقوق امنیت ملی کشورهای عضو یا قواعد اسرار رسمی/دفاعی دنبال می‌کند.

۵-۳) بریتانیا Computer Misuse Act + Official Secrets Act :

در بریتانیا، قانون ۱۹۹۰ Computer Misuse Act جرم‌انگاری‌های محوری درباره دسترسی و سوءاستفاده رایانه‌ای را مقرر می‌کند و به‌روزرسانی‌های متعدد آن تا اوایل ۲۰۲۶ در متون رسمی ذکر شده است .همچنین راهنمای دادستانی (CPS) نشان می‌دهد که این قانون ابزار اصلی تعقیب جرائم دسترسی و سوءاستفاده رایانه‌ای است و در موارد خاص به قوانین دیگر (مانند داده‌ها) توجه می‌شود . اما اگر موضوع «اسرار دولتی» باشد، Official Secrets Act ۱۹۸۹ چارچوب تعقیب «افشا» را فراهم می‌کند .

پس مدل بریتانیا دوپایه است:

- نفوذ/دسترسی/اخلال CMA →
- افشا/انتشار اسرار رسمی OSA →

این مدل از حیث تطبیقی نشان می‌دهد که تفکیک «فعل فنی نفوذ» از «فعل حقوقی افشا» می‌تواند شفافیت بیشتری در عناصر جرم ایجاد کند، در حالی که ماده ۳ ایران هر دو را در یک ماده گرد آورده است .

۵-٤) ایالات متحده CFAA + Economic Espionage Act :

در آمریکا، Computer Fraud and Abuse Act (۱۸ U.S.C. § ۱۰۳۰) شالوده تعقیب کیفری بسیاری از اشکال دسترسی غیرمجاز و سوءاستفاده از سامانه‌هاست . اما برای «جاسوسی اقتصادی» و حفاظت از اسرار تجاری، Economic Espionage Act ۱۹۹۶ و به‌ویژه ۱۸ U.S.C. § ۱۸۳۱) به‌طور خاص بر سرقت/انتقال اسرار تجاری با قصد منفعت رساندن به دولت خارجی تمرکز دارد . این تفکیک ساختاری یک نکته تطبیقی مهم دارد:

- در ایران، جاسوسی رایانه‌ای حول «داده سری» (اغلب با رنگ امنیتی) جرم‌انگاری شده.
- در آمریکا، جاسوسی اقتصادی (trade secrets) مسیر خاص خود را دارد و جاسوسی دولتی/امنیتی نیز غالباً ذیل رژیم‌های جداگانه یا قواعد امنیت ملی تحلیل می‌شود.

۵-۵) جمع‌بندی تطبیقی

با کنار هم گذاشتن ایران، بریتانیا، آمریکا و اسناد اروپایی/بوداپست، می‌توان گفت:

۱. ایران :عنوان مستقل «جاسوسی رایانه‌ای» با محور «داده سری» و تشدید ویژه برای بازیگران خارجی .

۲. اروپا/بوداپست :تمرکز بر جرائم پایه (access/interception/interference)و واگذاری جاسوسی به قوانین امنیتی داخلی .

۳. بریتانیا :تفکیک روشن‌تر میان «نفوذ (CMA) «و «افشا .(OSA) «

۴. آمریکا :دو مسیر کلیدی CFAA—برای نفوذ/دسترسی و EEA برای اسرار تجاری و منفعت دولت خارجی .

٦) جاسوسی رایانه‌ای در حقوق بین‌الملل: منطقه خاکستری

یکی از بحث‌های پرچالش در حقوق بین‌الملل سایبری این است که آیا «جاسوسی سایبری» فی‌نفسه غیرقانونی است یا خیر. در برخی تحلیل‌های حقوقی مطرح شده که چون حقوق

بین‌الملل در مورد جاسوسی (به‌طور کلی) سکوت دارد، «جاسوسی سایبری به عنوان یک قاعده کلی» لزوماً ناقض حقوق بین‌الملل تلقی نمی‌شود، هرچند ممکن است در شرایطی با قواعد دیگر (حاکمیت، عدم مداخله، حقوق بشر، یا منع توسل به زور) تداخل پیدا کند . نتیجه برای حقوق داخلی این است که حتی اگر در سطح بین‌المللی «هنجار سخت» وجود نداشته باشد، کشورها در سطح ملی می‌توانند و معمولاً می‌خواهند با جرم‌انگاری، از دارایی اطلاعاتی خود محافظت کنند اما باید مراقب باشند که تعریف جرم آن‌قدر موسع نشود که با آزادی‌های مشروع، پژوهش امنیتی مجاز، یا حق دسترسی قانونی به اطلاعات تداخل پیدا کند.

۷) آسیب‌شناسی و پیشنهادهای اصلاحی (با تأکید بر ایران)

۷-۱) ابهام در مفهوم «داده سری

نقطه قوت قانون ایران این است که «سری بودن» را شرط کرده تا هر نقض محرمانگی، جاسوسی تلقی نشود .اما در عمل، فقدان معیار روشن می‌تواند به: اختلاف کارشناسی، تشتت آراء، و خطر توسعه‌گرایی در تفسیر کیفری منجر شود. پیشنهاد: تدوین یا ارجاع روشن‌تر به نظام طبقه‌بندی رسمی و معیارهای ماهوی (آسیب به امنیت/منافع ملی) در کنار معیارهای شکلی (برچسب محرمانه/سری).

۷-۲) مدیریت همپوشانی با ماده ۵۰۱ و سایر جرائم امنیتی

با توجه به شباهت‌های ماهوی با جرم جاسوسی در تعزیرات، نیاز است رویه یا مقررات تبیینی روشن کند که در چه شرایطی ماده ۳ قانون جرایم رایانه‌ای مقدم است و در چه شرایطی مواد امنیتی تعزیرات اعمال می‌شوند .

۷-۳) تفکیک میان جاسوسی امنیتی و جاسوسی اقتصادی

الگوی آمریکا نشان می‌دهد تفکیک «اسرار تجاری» از «اسرار امنیتی» می‌تواند به دقت تقنینی کمک کند .پیشنهاد: در حقوق ایران نیزدر کنار ماده ۳ می‌توان مسیرهای روشن‌تری برای اسرار تجاری و صنعتی (در چارچوب قوانین تجارت، رقابت، مالکیت فکری) طراحی کرد تا همه پرونده‌ها ناچاراً امنیتی نشوند.

۷-٤) نسبت با حق دسترسی به اطلاعات و شفافیت

قانون انتشار و دسترسی آزاد به اطلاعات، اصل «دسترسی» را تقویت می‌کند، هرچند استثنائات مربوط به اطلاعات شخصی و محرمانه را نیز پیش‌بینی کرده است .پیشنهاد: در تحلیل و اجرای جاسوسی رایانه‌ای، باید مرز میان «اطلاعات قابل دسترسی عمومی/قانونی» و «اطلاعات سری/طبقه‌بندی‌شده» کاملاً روشن باشد تا از تعارض‌های غیرضروری جلوگیری شود.

نتیجه‌گیری

جاسوسی رایانه‌ای در حقوق ایران، با محوریت «داده‌های سری» و رفتارهای سه‌گانه «تحصیل/شنود»، «در دسترس قرار دادن برای فاقد صلاحیت»، و «افشا برای بازیگران خارجی»، ساختاری نسبتاً روشن اما در جزئیات، نیازمند شفاف‌سازی است .مقایسه تطبیقی نشان داد بسیاری از نظام‌ها ترجیح می‌دهند به جای جرم‌انگاری مستقل جاسوسی در قانون جرائم رایانه‌ای، از جرائم پایه نفوذ و شنود در کنار قوانین اسرار رسمی یا اسرار تجاری بهره بگیرند .در سطح بین‌الملل نیز جاسوسی سایبری غالباً در منطقه خاکستری قرار دارد و همین امر اهمیت سیاست‌گذاری دقیق داخلی را دوچندان می‌کند .در نهایت، پیشنهادهای اصلی شامل: تعریف/معیارگذاری دقیق‌تر برای «داده سری»، مدیریت همپوشانی با جرائم امنیتی کلاسیک، تفکیک بهتر جاسوسی امنیتی و اقتصادی، و تنظیم رابطه آن با رژیم دسترسی به اطلاعات است.

منابع و مآخذ

رهامی، محسن، و پرویزی، سیروس .(۱۳۹۱) .جاسوسی رایانه‌ای در حقوق ایران و وضعیت بین‌المللی آن .مطالعات حقوق خصوصی

مجلس شورای اسلامی(۱۳۸۸) .قانون جرایم رایانه‌ای .(منتشرشده در مجموعه قوانین و مقررات)

مجلس شورای اسلامی .(۱۳۷۵) قانون مجازات اسلامی (کتاب پنجم: تعزیرات و مجازات‌های بازدارنده)، ماده ۵۰۱ .

مجمع تشخیص مصلحت نظام .(۱۳۸۸) قانون انتشار و دسترسی آزاد به اطلاعات .

پیری زمانه، مسلم. پیری زمانه، داریوش. قدمی، کاوه. بازگلی، حمیدرضا .(۱۳۹۵) جاسوسی رایانه‌ای ابزاری در حوزه جنگ نرم (گونه‌شناسی، موانع حاکم بر تحقیقات و قوانین مترتب بر جاسوسی رایانه‌ای) .مطالعات قدرت نرم، ۶(۱۵)، ۱۵۸–۱۳۶ .

Council of Europe. (۲۰۰۱). Convention on Cybercrime (ETS No. ۱۸۵).

European Parliament & Council. (۲۰۱۳). Directive ۲۰۱۳/٤۰/EU on attacks against information systems.

Lindsay, J. R. (۲۰۲۱). Cyber espionage. In P. Cornish (Ed.), The Oxford Handbook of Cyber Security (pp. ۲۲۳–۲۳۸). Oxford University Press. doi: ۱۰.۱۰۹۳/oxfordhb/۹۷۸۰۱۹۸۸۰۰٦۸۲.۰۱۳.۱۲

United Kingdom. (۱۹۸۹). Official Secrets Act ۱۹۸۹.

United Kingdom. (۱۹۹۰). Computer Misuse Act ۱۹۹۰.

United States. (n.d.). ۱۸ U.S.C. § ۱۰۳۰ (Computer Fraud and Abuse Act).

United States. (۱۹۹٦). Economic Espionage Act of ۱۹۹٦ (Pub. L. No. ۱۰٤-۲۹٤).

United States. (n.d.). ۱۸ U.S.C. § ۱۸۳۱ (Economic espionage).

NATO Cooperative Cyber Defence Centre of Excellence. (۲۰۱۷). Tallinn Manual ۲.۰: Cyber espionage generally not unlawful (commentary/news).

جهت همکاری با بنیاد علمی قانون یار در راستای برگزاری سمینار، کارگاه های آموزشی، کنگره و نشست های علمی با موسسه تماس بگیرید ۵۲۶ و ۰۲۱۶۶۹۷۹۵۱۹ مدیرپژوهش ۰۹۱۹۶۷۴۸۶۲۵