Scientific-research Quarterly Journal Law Knowledge Of
Khatam Al-Nabieen University
Volume 2, Issue 4, smmer 2024

Cyber espionage crime in Afghanistan and Iranian law

Wahidullah Hamidi

PhD student in criminal law and criminology.
wahid.19hamidi@gmail.com

Abstract

Cyberspace is an electronic environment through which digital information is produced, sent, received, stored, processed, and deleted. Cyberspace has made committing crimes very easy and accessible to everyone by providing the absence of spatial and temporal limitations. With the advancement of technology and the storage or transfer of secret information by governments or large companies, the use of cyberspace and the storage and transfer of this information in it has made committing this crime more possible. Therefore, anyone who wants to obtain information can access the secret information of a country with a computer and does not need to spend exorbitant costs to send someone as a spy or military and equipment support. Rather, it is very easy, and through cyberspace, this possibility has been provided to collect secret information. Therefore, questions arise as to who can access this information and who can commit this crime. What reaction has been taken against those who illegally access this secret information? These questions are answered by the descriptive–analytical method and using library sources. This crime may be committed by ordinary people or by someone who has access to authority. If the perpetrator is a citizen of a domestic or foreign country, he will be dealt with differently in Afghan law. But in Iranian law, this distinction does not exist. People who have the authority to access and protect secret information must, by law, keep secret information in such a way that it does not fall into the hands of unauthorized persons; otherwise, they must be punished. This issue has not been predicted in Afghan law. Also, violating the security measures of the systems in Iranian law has been considered a crime, while Afghan law has not addressed this issue.

Keywords: Espionage, cyber espionage, computer espionage, secret information, Afghan law, Iranian law

[Downloaded from srqjl.knu.edu.af on 2025-12-28]

[DOI: 10.62134/srqjl/v2.i4.202409.6]

فصلنامه علمی-تحقیقی دانش حقوقی
دانشگاه خاتم‌النبیین(ص)
سال دم، شماره چهارم، تابستان ۱۴۰۳
صفحه ۱۷۲-۱۵۰

جرم جاسوسی سایبری در حقوق افغانستان و ایران

وحیدالله حمیدی*

چکیده

فضای سایبری عبارت است از محیطی الکترونیکی که اطلاعات دیجیتالی ازطریق آن تولید، ارسال، دریافت، ذخیره، پردازش و حذف می‌شوند. فضای سایبری با از بین بردن محدودیت‌های مکانی و زمانی، ارتکاب جرم را بسیار ساده کرده و در دسترس همگان قرار داده است. با پیشرفت فناوری و ذخیره یا انتقال اطلاعات سرّی توسط دولت‌ها یا شرکت‌های بزرگ، استفاده از فضای سایبری و ذخیره و انتقال اطلاعات در آن، ارتکاب این جرم را بیشتر ممکن ساخته است؛ بنابراین، هرکس با داشتن کمپیوتر می‌تواند به اطلاعات سرّی کشوری دسترسی پیدا کند و نیازی به صرف هزینه‌های گزافی برای فرستادن جاسوس، حمایت‌های نظامی و تجهیزاتی ندارد و می‌توان به‌صورت بسیار ساده ازطریق فضای سایبری اطلاعات سرّی را جمع‌آوری کند. با توجه به آنچه بیان شد، چه افرادی می‌توانند به این اطلاعات دسترسی داشته باشند و چه کسی ممکن است مرتکب این جرم شود؟ چه واکنشی در مواجهه با افرادی که به‌صورت غیرقانونی به این اطلاعات سرّی دسترسی پیدا می‌کنند در نظر گرفته شده است؟ در این مطالعه، با روش توصیفی- تحلیلی و استفاده از منابع کتابخانه‌ای به این سؤالات پاسخ داده می‌شود. ممکن است این جرم توسط اشخاص عادی یا توسط شخصی که صلاحیت دسترسی دارد، ارتکاب یابد. چنانچه مرتکب، تبعهٔ کشور داخلی یا خارجی باشد، در حقوق افغانستان با عناوین مختلفی با وی برخورد می‌شود؛ اما در حقوق ایران چنین تفکیکی وجود ندارد. اشخاصی که صلاحیت دسترسی و محافظت از اطلاعات سرّی دارند،

*دانشجوی دکتری حقوق جزا و جرم‌شناسی wahid.19hamidi@gmail.com

[Downloaded from srqjl.knu.edu.af on 2025-12-28]

[DOI: 10.62134/srqjl/v2.i4.202409.6]

به‌موجب قانون باید طوری از این اطلاعات نگهداری کنند که اشخاص بدون صلاحیت امکان دسترسی به آن را نداشته باشند؛ وگرنه باید مجازات شوند. این موضوع در حقوق افغانستان پیش‌بینی نشده است؛ همچنین، نقض تدابیر امنیتی سامانه‌ها در حقوق ایران جرم‌انگاری شده است، درحالی‌که حقوق افغانستان به این موضوع نپرداخته است.

واژگان کلیدی: جاسوسی، جاسوسی سایبری، جاسوسی رایانه‌ای، اطلاعات سرّی، حقوق افغانستان، حقوق ایران.

[Downloaded from srqjl.knu.edu.af on 2025-12-28]

[DOI: 10.62134/srqjl/v2.i4.202409.6]

مقدمه

جاسوسی سایبری از جرایم جدید حوزۀ امنیت و منافع کشورها محسوب می‌شود که نگرانی جدی نسبت به آن وجود دارد و کشورهای افغانستان و ایران به‌صورت جدی آن را جرم‌انگاری کرده‌اند. این جرم، به‌دلیل خطرناک بودن و تهدید بزرگی علیه منافع و امنیت کشورها، اهمیت به‌سزایی دارد و کشورها در قبال پیشگیری از آن هزینه‌های سنگینی را متقبل می‌شوند. با گسترش فناوری‌های کمپیوتری (رایانه‌ای) و مخابراتی و صنعتی شدن جوامع، جاسوسی از شکل سنتی فاصله گرفته است. امروزه، پدیدۀ جاسوسی سایبری، شیوۀ جدیدی از خبرگیری‌رواج‌یافته است که ازنظر مکانی و زمانی محدودیتی ندارد. پیدایش کمپیوتر، فراگیری سریع آن و رشد چشمگیر فناوری‌های جدید ارتباطی و اطلاعاتی، زمینه‌های به وجود آمدن بزهکار سایبری را ساده کرده‌اند؛ بنابراین، دیگر نیازی به برنامه‌نویسی و خلاقیت ویژه‌ای نیست. فضای مجازی مکان مناسبی برای انتقال بزهکاری و فعالیت‌های بزهکارانه فراهم می‌کند. هدف از نگارش این تحقیق بررسی تطبیقی جرم مذکور، به‌صورت توصیفی، برای فهم بیشتر این جرم و معرفی آن به پژوهشگران است.

به‌دلیل تجهیز مراکز دولتی و امنیتی به کمپیوتر و ذخیرۀ اطلاعات یا داده‌های سرّی و محرمانه در سامانه‌های رایانه‌ای یا کمپیوتری و اتصال این مراکز به شبکۀ انترنت، امکان نفوذ و دستیابی غیرمجاز به سامانه‌ها و دسترسی به داده‌ها یا اطلاعات و شکار اطلاعات سرّی برای بزهکاران امنیتی ایجاد می‌شود؛ بدین‌گونه، فضای مجازی به گسترش پدیدۀ جاسوسی سایبری کمک کرده است. این کمک‌رسانی به حدی است که امروزه هر کاربری می‌تواند با استفاده از نرم‌افزارهای جاسوسی به اطلاعات حیاتی و سرّی کشورها دسترسی پیدا کند، آن‌ها را افشا کند یا در دسترس دیگران قرار دهد (آقایی‌نیا و رستمی، ۱۴۰۰: ۱۰۵).

جرم‌انگاری جاسوسی سایبری، از جرایم مهم در حوزۀ امنیت اطلاعات و فضای مجازی، تاریخچه‌ای پیچیده دارد. در ابتدا، جاسوسی، جرمی سنتی و بیشتر در زمینه‌های نظامی و سیاسی شناخته می‌شد؛ اما با پیشرفت فناوری و گسترش انترنت، جاسوسی سایبری نیز به‌عنوان جرمی جدید و مهم مطرح شد. با گسترش شبکه‌های بین‌المللی و ارتباطات ماهواره‌ای، در دهۀ ۹۰ میلادی، نسل جدیدی از جرایم رایانه‌ای تحت‌عنوان جرایم سایبری شکل گرفتند. این جرایم شامل دسترسی غیرمجاز به اطلاعات، شنود غیرمجاز و جاسوسی

[Downloaded from srqjl.knu.edu.af on 2025-12-28]
[DOI: 10.62134/srqjl/v2.i4.202409.6]

در فضای مجازی می‌شوند. حقوق ایران به حد کافی به جرم جاسوسی سایبری پرداخته است؛ اما در حقوق افغانستان این مسئله را به‌صورت بسیار اندک تحقیق و بررسی کرده است که همین امر محقق را وادار به تحقیق دراین‌باره کرده است.

یکی از عوامل خطرساز برای این جرم، گسترش بیش از حد استفاده از انترنت و قیمت پایین کمپیوترها است. آنچه اهمیت دارد، تأثیر عمیق فناوری‌ها بر زندگی انسان‌ها و وابستگی کاربران به این فناوری‌ها است. مردم، مسئول موفقیت و خطای فناوری اطلاعات هستند؛ بنابراین، کارمند دولت یا شخص عادی- در قوانین افغانستان و ایران- می‌تواند مجرم جاسوسی سایبری شناخته شود. در این مقاله، به‌صورت تطبیقی، به بررسی تفاوت‌های ارکان تشکیل‌دهندهٔ این جرم در نظام حقوقی افغانستان و ایران پرداخته می‌شود و شباهت‌ها و تفاوت‌های موجود بین این دو نظام بررسی می‌شود.

الف. مفاهیم و مبانی جرم جاسوسی سایبری

در قدم نخست نیازمند بیان مفاهیمی هستم که در طول تحقیق به کارگرفته می شود تا معنای مدنظر نویسنده مشخص باشد و از مفاهیم دیگر تفکیک گردد.

۱. مفاهیم

برای اینکه بتوان تعریف خوبی از جرم جاسوسی رایانه‌ای ارائه داد ابتدا خوب است به تعریف جاسوسی و جرایم رایانه‌ای پرداخته شود.

۱-۱. تعریف جاسوسی

جاسوس در لغت به معنای خبرکش، جستجوکنندهٔ خبر، کسی که اخبار و اسرار شخصی، اداره یا مملکتی را به دست آورد و به دیگری اطلاع دهد است (عمید، ۱۳۶۷: ۳۶۴).

در قوانین کشور افغانستان جرم جاسوسی، به‌صورت دقیق و واضح، تعریف نشده است؛ به‌دلیل اینکه قانون‌گذار بتواند در هر حالت آن را به نفع کشور تعریف کند. ازنظر بین‌الملل، جاسوسی در مادهٔ ۱۹ قطعنامهٔ بروکسل- مصوب ۱۸۷۴ میلادی- چنین تعریف شده است: «جاسوس کسی است که مخفیانه و با وسایل و بهانه‌های مجعول، اطلاعات را جمع‌آوری می‌کند یا برای تحصیل اطلاعات در نقاط اشغال‌شده به‌وسیلهٔ نیروی دشمن با قصد اینکه آن‌ها را به طرف مقابل تسلیم کند، تجسس می‌کند.» مادهٔ ۲۹ آیین‌نامهٔ ضمیمهٔ قرارداد لاهه،

[Downloaded from srqjl.knu.edu.af on 2025-12-28]
[DOI: 10.62134/srqjl/v2.i4.202409.6]

مورخ ۱۸ اکتبر ۱۹۰۷ میلادی، چنین تعریف کرده است: «کسی را نمی‌توان جاسوس دانست؛ مگر اینکه مخفیانه و با بهانه‌های مجعول به نفع یکی از متخاصمین درصدد تحصیل اطلاعات یا جمع‌آوری اشیائی برآید» (رنه‌گارو، ۱۳۴۳: ۷۲۰). از تطبیق دو تعریف بالا می‌توان چنین تعریفی را ازنظر حقوق بین‌الملل به دست آورد که «جاسوس، کسی است که به‌صورت غیرقانونی با عناوین مجعول و غیرواقعی، اطلاعات و اخباری را از تشکیلات سیاسی یا نظامی کشوری به‌منظور تسلیم آن به دشمن جمع‌آوری می‌کند.» در اصطلاح حقوق نیز به کسی جاسوس گفته می‌شود که عملی را برای تحصیل اطلاعات یا جمع‌آوری اشیائی به‌طور مخفیانه یا تحت‌عناوین نادرست و غلط به نفع دشمن انجام دهد (جعفری لنگرودی، ۱۳۹۶).

۱-۲. تعریف جرایم رایانه‌ای

هر فعل یا ترک فعل غیرقانونی که با رایانه، اخلال در سیستم‌های رایانه‌ای یا نفوذ در سیستم‌های رایانه‌ای- که به‌موجب قانون برای آن مجازات تعیین شده باشد- جرایم رایانه‌ای هستند؛ به عبارت دیگر، هر جرمی که قانون‌گذار، رایانه را وسیلهٔ جرم و جزء رکن مادی آن اعلام کرده باشد، جرایم رایانه‌ای است (کامرانی، ۱۳۹۷: ۱۵). در تعریف جرایم رایانه‌ای، وسیلهٔ جرم- که رایانه است- اهمیت بالایی دارد؛ به همین دلیل، رایانه نیز جرایم ساده را به جرایم رایانه‌ای تبدیل می‌کند؛ مثلاً اگر در جرم جاسوسی ساده از وسیلهٔ رایانه‌ای استفاده شود، به آن جرم جاسوسی رایانه‌ای اطلاق شده و طبق مواد مربوط به آن رسیدگی می‌شود.

۱-۳. تعریف جرم جاسوسی رایانه‌ای

در تعریف جاسوسی رایانه‌ای می‌توان همان تعریف جاسوسی را بیان کرد و تنها رایانه یا کمپیوتر را وسیلهٔ آن بیان کرد که جاسوسی سنتی را با جاسوسی رایانه‌ای تفکیک می‌کند. در قوانین افغانستان و ایران تعریف دقیقی از جاسوسی رایانه‌ای یا سایبری وجود ندارد و قانون‌گذار در مادهٔ ۸۶۴ کود جزای افغانستان و مادهٔ ۳ قانون جرایم رایانه‌ای ایران به بیان مصادیق این جرم بسنده کرده است.

کمیتهٔ برگزیدهٔ کارشناسان جرایم رایانه‌ای شورای اروپا از سال ۱۹۸۵ تا ۱۹۸۹ ملادی به بحث دربارهٔ مسائل حقوقی جرایم رایانه‌ای پرداختند. این کمیته فهرستی تحت‌عناوین

[Downloaded from srqjl.knu.edu.af on 2025-12-28]
[DOI: 10.62134/srqjl/v2.i4.202409.6]

«فهرست حداقل» و «فهرست اختیاری» را به شورای اروپا پیشنهاد کرد که به تصویب رسید؛ در بند «ب» از فهرست اختیاری، جاسوسی رایانه‌ای این‌گونه تعریف شده است: «جاسوسی رایانه‌ای عبارت است از کسب اسرار حرفه‌ای یا تجاری از راه‌های نادرست یا افشا، انتقال یا استفاده از این اسرار بدون داشتن حق یا هرگونه توجیه قانونی، با قصد وارد کردن زیان اقتصادی به فردی که محق در نگه داشتن اسرار است یا تحصیل امتیاز اقتصادی غیرقانونی برای خود یا شخص ثالثی» (قدسی، ۱۳۹۲: ۷۲).

۱-۴. تعریف جرم جاسوسی سایبری

سایبر یا انترنت از دو فناوری رایانه و مخابرات متولد شده است. انترنت درمجموع از شبکه‌های به‌هم‌پیوسته تشکیل شده است که خود نیز از بسیاری از رایانه‌های متصل به یکدیگر تشکیل شده‌اند و فضایی با ویژگی‌های کاملاً متفاوت از دنیای فیزیکی به وجود آورده است که عده‌ای آن را فضای سایبری نامیده‌اند (جلالی فراهانی، ۱۳۸۴: ۱۳۵).

۲. مبانی جرم‌انگاری

برای مشخص کردن مبنای جرم ازنظر قانون‌گذار و اینکه چه‌چیزی برای مبنای جرم‌انگاری جرم جاسوسی سایبری مورد استفاده قرار گرفته است، باید به بررسی مبانی پرداخته شود. جرم در حقوق جزا براساس چند اصل جرم‌انگاری می‌شود که ازآن‌جمله می‌توان به اصل ضرورت اشاره کرد که از مهم‌ترین مبانی جرم‌انگاری است. منظور از اصل ضرورت این است که در جایی که ضرورت باشد، بعضی رفتارها مجرمانه تلقی می‌شوند و در قانون، رفتار مجرمانه تعریف می‌شوند (عبدالفتاح، ۱۳۸۱: ۱۵۷). اصل ضرورت در جرم‌انگاری به این معنای استفاده از حقوق کیفری برای رفتاری است که قابلیت کنترول داشته باشد؛ ضروری است که بر آن رفتار نظارت و کنترول وجود داشته باشد و از راه‌های دیگری پیشگیری این امکان وجود نداشته باشد که در این صورت، جرم‌انگاری تنها راه‌حل برخورد با آن رفتار است(فلاحی، ۱۳۹۴: ۲۲۰-۲۱۹)؛ بنابراین، برای جرم جاسوسی سایبری ضرورت ایجاب می‌کند تا جرم‌انگاری واقع شود، زیرا راه‌حلی برای پیشگیری به‌جز آن وجود نداشته است.

یکی از اصول دیگر جرم‌انگاری، که می‌توان برای مبانی این جرم تعریف کرد، اصل ضرر است؛ برخی جرایم به‌دلیل زیان و ضرر رساندن به جامعه، مردم یا امنیت باید جرم‌انگاری

[Downloaded from srqjl.knu.edu.af on 2025-12-28]

[DOI: 10.62134/srqjl/v2.i4.202409.6]

شوند. می‌توان گفت تنها هدفی که اِعمال صحیح قدرت علیه آزادی اعضای جامعهٔ متمدن را توجیه می‌کند، ممانعت از ایراد ضرر و زیان به دیگری است (عبدالفتاح، ۱۳۸۱: ۱۵۷). می‌توان گفت اصل ضرورت و اصل ضرر از اساسی‌ترین اصول جرم‌انگاری جرم جاسوسی سایبری در قوانین افغانستان و ایران هستند. در این دو کشور به‌دلیل اهمیت و ضرورت حفظ امنیت و اطلاعات مهم، اساسی و سرّی کشور و سازمان‌ها این رفتارها را جرم‌انگاری می‌کنند.

همان‌طور که مبانی حقوقی جرم‌انگاری بیان شد، در عین حال به مبنای فقهی یا اسلامی جرم‌انگاری نیز پرداخته می‌شود. به‌طور کلی جاسوسی در اسلام به دو قسم مشروع و نامشروع قابل تقسیم است؛ گاهی این عمل ستوده شده و گاهی نیز از منظر دیگر نکوهش شده است.

نخست، جاسوسی مشروع در جایی است که به‌منظور کسب اطلاعات و مراقبت از کارگزاران، مأموران و آنچه عقل و شرع به آن حکم می کند، صورت گیرد که پیامبر اسلام (ص) و ائمهٔ معصومین (ع) برای تحقق آن، افرادی را تعیین می‌کردند. دوم، جاسوسی علیه دشمنان و مخالفان حکومت، مشروع است که در آیات قرآنی و سیرهٔ معصومین (ع) دیده می‌شود که این امر از دیدگاه اسلام تأکید شده و یکی از ابزارها و وسایل دفاع از کیان اسلام و شکست دشمن به شمار می‌آید. تجسس در امور دشمنان و کسب اطلاعات از مواضع آن‌ها تنها اختصاص به زمان جنگ ندارد؛ هرچند که این امر در زمان جنگ اهمیت به‌سزایی دارد (موسوی بجنوردی، ۱۳۸۵: ۲۲۸). این دو نوع جاسوسی در اسلام مشروع هستند؛ اما ازنظر حقوقی نمی‌توان به اینها جاسوسی گفت و بهتر است عنوان کسب اطلاعات به نفع حکومت اسلامی برای آن‌ها گفته شود، چراکه ممکن است ازطرف حکومت اسلامی مشروع و قابل ستایش باشد، اما ازنظر دشمن یا طرف مقابل، همان جاسوسی نامشروع به حساب می‌آید؛ درنتیجه، کسب اطلاعات به نفع حکومت اسلامی، ستوده شده و خدمت‌گذاری به دین است.

جاسوسی نامشروع در اسلام در چند جا قابل تصور است که در قرآن کریم نیز به آن‌ها تصریح شده است؛ نخست، تجسس در اسرار خصوصی مردم در اسلام ممنوع است که برای تأمین امنیت مردم در زندگی خصوصی‌شان حائز اهمیت است و برای تأمین این امر مهم با تجسس در امور شخصی و مسائل پنهانی زندگی افراد مخالفت می‌کند و معتقد است آبروی مردم با افشای اسرار آن‌ها در خطر بوده و امنیتی در جامعه باقی نمی‌ماند. قرآن کریم، با صراحت، تجسس در زندگی

[Downloaded from srqjl.knu.edu.af on 2025-12-28]
[DOI: 10.62134/srqjl/v2.i4.202409.6]

خصوصی مردم را منع می‌کند و می‌فرماید: «ای کسانی که ایمان آورده‌اید، از بسیاری از گمان‌ها بپرهیزید؛ چراکه بعضی از گمان‌ها گناه است و هرگز (در کار دیگران) تجسس نکنید و هیچ‌یک از شما غیبت نکند.»[1] آیهٔ فوق به‌روشنی حرمت تجسس در امور شخصی دیگران را بیان کرده است تا مردم در زندگی خصوصی‌شان از هر نگاه در امنیت باشند.

دوم، جاسوسی به نفع اجانب و دشمنان و رساندن اطلاعات و اخبار به دشمنان اسلام و کشورهای اسلامی- به‌ضرورت عقل و دلالت برخی از آیات قرآن کریم و روایات معصومین (ع)- حرام و خیانت به خدا، پیامبر (ص) و مؤمنین است و این عمل براساس مفاد برخی از آیات قرآن کریم، خیانت به امانت بزرگ الهی شمرده شده و به‌طور قطع از گناهان بزرگ است. خداوند متعال در قرآن کریم چنین می‌فرماید: «ای رسول خدا، آنان که با زبان می‌گویند ایمان آوردیم و قلب آن‌ها ایمان نیاورده و در مسیر کفر بر یکدیگر سبقت می‌جویند، تو را اندوهگین نکنند و همچنین از یهودیان، آن‌ها زیاد به سخنان تو گوش می‌دهند تا دست‌آویزی برای تکذیب تو بیابند و آن‌ها جاسوسان جمعیت دیگری هستند که خود آن‌ها نزد تو نیامدند.»[2] مفسرین شیعه و اهل سنت در تفاسیر خود «سَمَّاعُونَ لِقَوْمٍ آخَرِينَ» را به جاسوسان دشمن و جاسوسان بنی قریظه معنا کردند و علاوه‌بر این دربارهٔ شأن نزول آیهٔ فوق دو احتمال را ذکر کرده‌اند که هر دو احتمال از مصادیق جاسوسی به نفع دشمن اسلام است (قدسی، ۱۳۹۲: ۷۸-۷۹).

در قرآن کریم گاهی از جاسوسی به معنای جستجوکننده نیز استفاده شده است؛ مانند این آیه که می‌فرماید: «بَعَثْنَا عَلَيْكُمْ عِبَادًا لَنَا أُولِي بَأْسٍ شَدِيدٍ فَجَاسُوا خِلَالَ الدِّيَارِ وَ كَانَ وَعْدًا مَفْعُولًا؛ گروهی از بندگان خویش را بر شما فرستادم تا در میان شما به جستجو بپردازند» (اسرا/۵). برخی با استناد به آیات قرآن کریم، بین جاسوسی و خیانت به کشور رابطهٔ عموم و خصوص مِن وجه را برقرار می‌دانند؛ زیرا در برخی از مصادیق جاسوسی، خیانت هم صدق می‌کند (پورسعید رضا، ۱۳۸۵: ۲۶) که برای تأیید این مطلب به آیهٔ ۲۷ سورهٔ انفال[3] تمسک

---

[1] «يَا أَيُّهَا الَّذِينَ آمَنُوا اجْتَنِبُوا كَثِيرًا مِنَ الظَّنِّ إِنَّ بَعْضَ الظَّنِّ إِثْمٌ وَلَا تَجَسَّسُوا وَلَا يَغْتَبْ بَعْضُكُمْ بَعْضًا أَيُحِبُّ أَحَدُكُمْ أَنْ يَأْكُلَ لَحْمَ أَخِيهِ مَيْتًا فَكَرِهْتُمُوهُ وَاتَّقُوا اللَّهَ إِنَّ اللَّهَ تَوَّابٌ رَحِيمٌ» (حجرات/۱۲)

[2] «يَا أَيُّهَا الرَّسُولُ لَا يَحْزُنْكَ الَّذِينَ يُسَارِعُونَ فِي الْكُفْرِ مِنَ الَّذِينَ قَالُوا آمَنَّا بِأَفْوَاهِهِمْ وَلَمْ تُؤْمِنْ قُلُوبُهُمْ وَمِنَ الَّذِينَ هَادُوا سَمَّاعُونَ لِلْكَذِبِ سَمَّاعُونَ لِقَوْمٍ آخَرِينَ» (مائده/۴۱).

[3] «يَا أَيُّهَا الَّذِينَ آمَنُوا لَا تَخُونُوا اللَّهَ وَالرَّسُولَ وَتَخُونُوا أَمَانَاتِكُمْ وَأَنْتُمْ تَعْلَمُونَ» (انفال/ ۲۷)

[Downloaded from srqjl.knu.edu.af on 2025-12-28]

[DOI: 10.62134/srqjl/v2.i4.202409.6]

شده است؛ زیرا شأن نزول آیهٔ متذکره را جاسوسی می‌دانند که خداوند آن را با لفظ خیانت بیان کرده است. سبب نزول آیهٔ مذکور در تفسیر منهاج الصادقین چنین آمده است: «جبرئیل، نزد پیامبر گرامی آمد و گفت: یا رسول‌الله، ابوسفیان در فلان جای فرود آمده است با جمعی از مشرکان، به تهیهٔ جنگ ایشان مشغول شوید. این خبر را پوشیده دارید تا ناگهان بر سر ایشان تازید. یکی از منافقان بر صورت حال اطلاع یافت و نامه‌ای نوشت و ابوسفیان را از آمدن مسلمانان خبر داد» (کاشانی، [بی‌تا]: ۱۸۲-۱۸۳).

به نظر ایشان، برخی از مصادیق جرم جاسوسی که ازطرف ذمی و کافر مستأمن ارتکاب یابند نیز از مصادیق تعدد معنوی بوده و خیانت هم بر آن‌ها صدق می‌کند؛ زیرا این‌گونه افراد، با عقد قرارداد ذمه یا عقد امان، متعهد می‌شوند که برخلاف مصالح کشوری که در آن ساکن هستند، عمل نکنند و درصورت انجام جاسوسی، خیانت‌کار نیز محسوب شوند. جاسوسی و خیانت ملی در کود جزای افغانستان تفکیک و جداگانه جرم‌انگاری شده‌اند؛ درحالی‌که در حقوق ایران این تفکیک انجام نشده و هرکس این جرم را انجام دهد، جاسوسی تلقی می‌شود.

ب. ارکان تشکیل‌دهندهٔ جرم جاسوسی سایبری

جرم جاسوسی سایبری ارکان مشخص دارد که باید قبل وارد شدن در مباحث دیگر مشخص گردد. بدان معنا که رکن قانونی، مادی و معنوی آن مشخص باشد.

۱. رکن قانونی

رکن قانونی جرم جاسوسی سایبری در حقوق افغانستان به‌صورت رکن قانونی مرکب جرم‌انگاری شده است که مصادیق رفتاری جرم مذکور را در مادهٔ ۸۶۴ کود جزا، مصوب ۱۳۹۶، چنین بیان می‌دارد: «(۱) شخصی که به‌صورت غیرقانونی نسبت به سیستم، برنامه یا اطلاعات کمپیوتری حاوی اطلاعات سرّی، مرتکب یکی از اعمال ذیل شود، به جزای جرم خیانت ملی یا جاسوسی مندرج این قانون محکوم می‌شود:

۱. دسترسی به اطلاعات سرّی درحال انتقال یا ذخیره‌شده در سیستم کمپیوتری یا مخابراتی یا حامل‌های اطلاعات؛

[Downloaded from srqjl.knu.edu.af on 2025-12-28]
[DOI: 10.62134/srqjl/v2.i4.202409.6]

۲. در دسترس قرار دادن اطلاعات سرّی درحال انتقال یا ذخیره‌شده در سیستم کمپیوتری یا مخابراتی یا حامل‌های اطلاعات؛

۳. افشا یا در دسترس قرار دادن اطلاعات سرّی درحال انتقال یا ذخیره‌شده در سیستم کمپیوتری یا مخابراتی یا حامل‌های اطلاعات برای دولت، سازمان، شرکت یا گروه خارجی یا عاملان آن‌ها ... .»

در مواد ۲۳۹ و ۲۴۰ پس از اینکه شخصیت مرتکب مشخص شد- که آیا تبعهٔ کشور افغانستان است یا تبعهٔ کشورهای خارجی- به مجازات این جرم پرداخته می‌شود. حقوق ایران در مواد ۳، ۴ و ۵ قانون جرایم رایانه‌ای، مصوب ۱۳۸۸، به جرم‌انگاری این جرم با عنوان جاسوسی رایانه‌ای پرداخته است. مادهٔ ۳ قانون حقوق ایران چنین مقرر داشته است: «هرکس به‌طور غیرمجاز نسبت به داده‌های سرّی درحال انتقال یا ذخیره‌شده در سامانه‌های رایانه‌ای یا مخابراتی یا حامل‌های داده مرتکب اعمال زیر شود، به مجازات‌های مقرر محکوم خواهد شد.»

مادهٔ ۵ نیز چنین مقرر می‌دارد: «چنانچه مأموران دولتی که مسئول حفظ داده‌های سرّی مقرر در مادهٔ ۳ این قانون یا سامانه‌های مربوط هستند و به آن‌ها آموزش لازم داده شده است یا داده‌ها یا سامانه‌های مذکور در اختیار آن‌ها قرار گرفته است، براثر بی‌احتیاطی، بی‌مبالاتی یا عدم رعایت تدابیر امنیتی موجب دسترسی اشخاص فاقد صلاحیت به داده‌ها، حامل‌های داده یا سامانه‌های مذکور شوند» به مجازات‌های مقرر محکوم می‌شوند. در ادامهٔ تحقیق به بررسی ارکان مادی و معنوی این جرم پرداخته می‌شود.

۲. رکن مادی

جرم رفتار متفکرانه‌ای است که خلاف قانون بوده و رکن مادی آن را تجلی عینی اندیشه و فکر مجرمانه را تشکیل می‌دهد. تا زمانی که رفتار مجرمانه در خارج ارتکاب نیفتاده و قصد مجرمانه همراه با رکن خارجی، ظهور عینی پیدا نکند، ماهیت جرم تحقق پیدا نکرده؛ پس مسئولیت کیفری و درنتیجه مجازات، محلی از اعراب ندارد (حبیب‌زاده، ۱۴۰۲: ۵۰۱)؛ به عبارت دیگر، هرقدر نیت و اندیشهٔ فرد شریرانه و زشت باشد، حقوق جزا تا زمانی که آن نیت سوء جلوهٔ خارجی را پیدا نکرده باشد، برای تنبیه فرد دخالت نمی‌کند (میرمحمد صادقی،

[Downloaded from srqjl.knu.edu.af on 2025-12-28]

[DOI: 10.62134/srqjl/v2.i4.202409.6]

۱۴۰۰: ۹۵-۹۴)؛ همچنین، رکن مادی جرم در واقع آثار مادی‌ای است که قابل لمس باشد و زمانی می‌توان برای رفتار مجرمانه‌ای مجازات در نظر گرفت که فعل مجرمانه تحقق پیدا کرده باشد (رسولی، ۱۳۹۶: ۲۳۷). در رکن مادی، که یکی از ارکان اساسی جرایم را تشکیل می‌دهد، لازم است رفتار مجرمانه، موضوع جرم، شرایط و اوضاع و احوال جرم، نتیجهٔ مجرمانه، رابطه سببیت- به‌دلیل خاص بودن جرم جاسوسی رایانه‌ای که با وسیلهٔ خاصی ارتکاب پیدا می‌کند- باید بررسی شوند. در ادامه به بررسی عناصر مهم رکن مادی این جرم می‌پردازیم و به‌صورت تطبیقی میان حقوق افغانستان و ایران مقایسه صورت می‌گیرد.

۲-۱. رفتار مجرمانه

منظور از واژهٔ رفتار این است که نه‌تنها فعل بلکه موارد دیگر، مثل ترک فعل، را نیز شامل می‌شود (میرمحمد صادقی، ۱۴۰۰: ۹۶). گاهی رفتار مجرمانه را به فعل مثبت (اقدام) یا فعل منفی (ترک فعل) نیز یاد می‌کنند (حبیب‌زاده، ۱۴۰۲: ۵۰۴-۵۰۵). فعل مثبت عبارت است از نقض یا زیرپا کردن دستور قانون‌گذار و اقدام علیه آن (همان: ۵۰۴)؛ درحالی‌که فعل منفی عبارت است از نقض امر و دستور قانون‌گذار و خودداری از انجام آن فعل (همان: ۵۰۵). در قانون افغانستان سه رفتار مجرمانه به‌صورت فعل مثبت مادی جرم جاسوسی سایبری واقع می‌شوند (حسینی و هاشمی، ۱۳۹۸: ۱۸۷)؛ اما در حقوق ایران چهار رفتار به‌صورت فعل مثبت مادی هستند و یک رفتار به‌صورت ترک فعل نیز ممکن است اتفاق بیفتد که در مادهٔ ۵ قانون جرایم رایانه‌ای به آن تصریح شده است. رفتار مجرمانهٔ این جرم در کود جزا عبارت است از دسترسی، در دسترس قرار دادن یا افشا کردن که در ادامه به آن‌ها اشاره می‌شود.

شکل اول رفتار مجرمانه در کود جزا و قانون جرایم رایانه‌ای به‌صورت «دسترسی»[1] واقع می‌شود. در این جرم، دسترسی به موضوع، جرم است و این نوع رفتار توسط شخصی که صلاحیت دسترسی به اطلاعات سرّی ندارد، قابل تصور است و تفاوتی نمی‌کند که شخص، کارمند دولت باشد یا نباشد.

[1] جزء ۱ فقرهٔ۱ مادهٔ ۸۶۴ کود جزا و جزء الف مادهٔ ۳ قانون جرایم رایانه‌ای.

[Downloaded from srqjl.knu.edu.af on 2025-12-28]

[DOI: 10.62134/srqjl/v2.i4.202409.6]

شکل دوم رفتار مجرمانه در کود جزا «در دسترس قرار دادن»[1] است که می‌تواند توسط فردی که صلاحیت دسترسی به اطلاعات ندارد یا توسط موظفی که قانوناً صلاحیت دسترسی به اطلاعات دارد، ارتکاب پیدا کند. قانون‌گذار کود جزا هیچ قیدی برای این رفتار در اینکه در دسترس چه کسی قرار دهد، بیان نکرده است؛ اما در قانون جرایم رایانه‌ای، «در دسترس قرار دادن»[2] به اشخاص فاقد صلاحیت قید شده است و درصورتی‌که این در دسترس قرار دادن به اشخاص فاقد صلاحیت اتفاق نیفتد، جرم محقق نمی‌شود.

شکل سوم رفتار مجرمانهٔ این جرم در کود جزا و قانون جرایم رایانه‌ای به‌صورت «افشا یا در دسترس قرار دادن»[3] است که شامل در دسترس قرار دادن اطلاعات سرّی به اشخاص، دولت‌ها، سازمان، گروه خارجی یا عاملان آن است. در این شکل از رفتار مجرمانه، قیدی نیز ذکر شده و زمانی محقق می‌شود که به دسترس «اشخاص، دولت ...خارجی یا عاملان آن‌ها» قرار داده شود. در این شکل از رفتار مجرمانه نیز فرقی نمی‌کند که شخص، کارمند دولت و موظف بوده و صلاحیت دسترسی داشته باشد یا شخصی عادی باشد که این اطلاعات را غیرقانونی به دست آورده است.

برای شکل چهارم در کود جزای افغانستان سه رفتار مجرمانه وجود دارد؛ اما در حقوق ایران و قانون جرایم رایانه‌ای، پنج رفتار مجرمانه بیان شده است که نوع چهارم آن عبارت است از «نقض تدابیر امنیتی سامانه‌های رایانه‌ای و مخابراتی»[4] که به‌صورت نقض تدابیر امنیتی اتفاق می‌افتد. این رفتار نیز ممکن است توسط کارمند دولت و شخص باصلاحیت یا شخص عادی ارتکاب پیدا کند.

طبق قانون جرایم رایانه‌ای، شکل پنجمِ رفتار مجرمانه عبارت است از «در دسترس قرار دادن غیرعمدی داده‌های سرّی برای اشخاص فاقد صلاحیت»[5]. این رفتار مجرمانه به‌صورت

---

[1] جزء ۲ فقرهٔ ۱ مادهٔ ۸۶۴ کود جزا.

[2] جزء ب مادهٔ ۳ قانون جرایم رایانه‌ای.

[3] جزء ۳ فقرهٔ ۱ مادهٔ ۸۶۴ کود جزا و جزء ج مادهٔ ۳ قانون جرایم رایانه‌ای.

[4] مادهٔ ۴ قانون جرایم رایانه‌ای.

[5] مادهٔ ۵ همان.

[Downloaded from srqjl.knu.edu.af on 2025-12-28]

[DOI: 10.62134/srqjl/v2.i4.202409.6]

غیرعمدی است و فقط توسط کارمند و شخص دارای صلاحیت دسترسی قابل تصور است که به‌صورت اشتباهی در دسترس غیر قرار داده می‌شود.

لازم به یادآوری است که هریک از رفتارهای مجرمانهٔ این جرم به‌صورت جرم مستقل از یکدیگر بوده و درصورتی‌که فردی مرتکب رفتارهای مجرمانهٔ دو جزء این ماده شود، مرتکب تعدد جرایم شده است (گروهی از نویسندگان، ۱۳۹۸: ۴۸۱؛ فتاحی، ۱۳۹۷: ۱۰۲).

۲-۲. موضوع جرم

موضوع جرم جاسوسی سایبری در کود جزای افغانستان، «اطلاعات سرّی دولت»[1] است (حسینی و هاشمی، ۱۳۹۸: ۱۸۷). اطلاعات سرّی در فقرهٔ ۲ مادهٔ ۸۶۴ کود جزا چنین تعریف شده است: «به‌مقصد فقرهٔ ۱ این ماده، اطلاعات سرّی، عبارت از اسرار مربوط به حاکمیت ملی، تمامیت اراضی یا امنیت ملی کشور است که در فصل مربوط به جرایم جاسوسی و خیانت ملی، من‌حیث اسرار دولتی شناخته شده باشد.» این اطلاعات در مادهٔ ۲۳۷ کود جزا نیز شرح داده شده‌اند. در قانون جرایم رایانه‌ای نیز موضوع این جرم، «داده‌های سرّی»[2] در نظر گرفته شده است و در تبصرهٔ ۱ مادهٔ ۳ این قانون چنین تعریف به عمل آورده است: «داده‌های سرّی، داده‌هایی هستند که افشای آن‌ها به امنیت کشور یا منافع ملی لطمه می‌زند.»

۲-۳. شرایط اوضاع و احوال

برای اینکه جرمی تحقق پیدا کند، باید شرایطی که برای ارتکاب آن در نظر گرفته شده‌اند، در نظر گرفته شوند؛ درصورتی‌که شرایط ارتکاب در رفتار مرتکب موجود باشند، شخص مظنون، مجرم است و طبق قانون به مجازات مقرر محکوم می‌شود. درصورت نبودن شرایط موجود در هر جرم- به‌ویژه جرم جاسوسی رایانه‌ای که در آن شرایط مرتکب، غیرمجاز بودن دسترسی یا وسیلهٔ ارتکاب جرم باید محرز شوند تا طبق مواد مقرر در قوانین مربوط بتوان مرتکب را مجرم جاسوسی رایانه‌ای دانست- امکان مجرم دانستن مظنون فراهم نیست. در ادامهٔ تحقیق به این شرایط پرداخته می‌پردازیم و قوانین مربوط در افغانستان و ایران بررسی می‌شوند.

---

[1] فقرهٔ ۱ مادهٔ ۸۶۴ کود جزا.

[2] مواد ۳، ۴ و ۵ قانون جرایم رایانه‌ای.

[Downloaded from srqjl.knu.edu.af on 2025-12-28]

[DOI: 10.62134/srqjl/v2.i4.202409.6]

۲-۳-۱. مرتکب

برخلاف جاسوسی سنتی، که خصوصیتی مثل خارجی بودن یا بی‌تابعیت بودن برای مرتکب آن شرط است، مرتکب در جاسوسی سایبری هیچ خصوصیتی ندارد و ممکن است هر شخصی- ازجمله خارجی، بدون تابعیت یا افغان- باشد (حسینی و هاشمی، ۱۳۹۸: ۱۸۶). مرتکب جرم جاسوسی سایبری در حقوق افغانستان و ایران متفاوت است؛ زیرا اگرچه قانون‌گذار حقوق افغانستان، مرتکب جرم را بدون خصوصیت در نظر گرفته، اما در قسمت مجازات دیده می‌شود که تفکیکی در مجازات تبعهٔ خارجی و بدون تابعیت با مرتکب تبعهٔ افغانستان صورت گرفته است.[۱] در حقوق ایران چنین تفکیکی دیده نشده و به‌صورت عام بیان شده که می‌تواند همه را شامل شود؛ تبعهٔ کشور ایران یا تبعهٔ کشورهای دیگر، همه به‌عنوان جاسوس یاد می‌شوند که این مسئله نیاز به اصلاحات دارد. به‌هرحال مرتکب جرم مذکور در مادهٔ ۸۶۴ کود جزا عبارت است از «شخص» که در این ماده خیانت ملی و جاسوسی را از یکدیگر تفکیک کرده و به مواد مربوط به آن‌ها ارجاع داده شده است. مطابق مادهٔ ۲۳۸ کود جزا خیانت ملی توسط شخصی محقق می‌شود که «تبعهٔ دولت جمهوری اسلامی افغانستان» باشد. مطابق مادهٔ ۲۴۰ قانون مذکور، جاسوسی توسط شخصی محقق می‌شود که «تبعهٔ دولت خارجی یا شخص بدون تابعیت» باشد؛ بنابراین، چنانچه شخص مرتکب، تبعهٔ کشور خارجی یا بدون تابعیت باشد و مرتکب جرم جاسوسی سایبری شود، جاسوس است و اگر تبعهٔ داخلی باشد، خائن است و به این عنوان مجازات می‌شود.

در حقوق ایران، ضابطهٔ دقیقی در رابطه با تفکیک جاسوسی و خیانت وجود ندارد؛ بر همین اساس، در برخی موارد مشخص نیست که جرم خاصی مصداق جاسوسی است یا خیانت به کشور. ضابطه‌ای که برای تشخیص این دو جرم پیشنهاد می‌شود، مانند حقوق افغانستان، تابعیت و ملیت است. هرگاه تبعهٔ کشور خارجی، اقدامی علیه امنیت خارجی کشوری که در آن است، انجام دهد، جاسوس بوده و اگر این رفتار ازطرف تبعهٔ داخلی کشوری انجام شود، آن شخص مرتکب خیانت شده است. این ضابطه در قوانین ایران تأیید نشده است. ضابطهٔ دیگری که پیشنهاد می‌شود این است که اگر مرتکب، اقدامی علیه امنیت

---

[۱] فقرهٔ ۱ مادهٔ ۸۶۴ کود جزای افغانستان.

[Downloaded from srqjl.knu.edu.af on 2025-12-28]

[DOI: 10.62134/srqjl/v2.i4.202409.6]

خارجی در اجرای مأموریتی خاص و درازای گرفتن اجرت مرتکب شود، رفتار وی جاسوسی تلقی شود وگرنه مرتکب خیانت شده است. ضابطهٔ دیگری نیز وجود دارد که اگر مرتکب، اطلاعاتی را تسلیم بیگانه کند که امانت در پیش خود داشته، خیانت کرده؛ اما اگر این اطلاعات را با تجسس به دست آورده باشد، جاسوسی به حساب می‌آید. این ضابطه را نیز قانون‌گذار ایران تأیید نکرده است (فتاحی، ۱۳۹۹: ۲۶۲).

بنابراین، مواد ۳ و ۴ قانون جرایم رایانه‌ای از واژهٔ «هرکس» استفاده کرده. هرکس، عام است و همه را شامل می‌شود؛ فرقی نمی‌کند تبعهٔ داخلی، خارجی یا بدون تابعیت باشد. بهتر بود قانون‌گذار ایران، مانند حقوق افغانستان، مرتکبان داخلی و خارجی را از یکدیگر تفکیک می‌کرد تا عدالت بهتر تأمین شده و عنوان مجرمانهٔ دقیق‌تری برای آن‌ها تعیین می‌گردید. مرتکب مادهٔ ۵ قانون مذکور عبارت از «مأموران دولتی» است که مسئول حفظ داده‌های سرّی یا سامانه‌های مربوط هستند. مأمور دولتی مسئول حفاظت از داده‌های سرّی است و باید از حق دسترسی به داده‌های سرّی به‌نحو درست استفاده کند و نباید علیه دولت خود رفتار مجرمانهٔ ضد امنیت داخلی و خارجی مرتکب شود؛ در همین راستا، به‌دلیل مسئولیتی که بر دوش داشته، باید از داده‌های سرّی حفاظت می‌کرد و آن‌ها را به شخص دیگری تحویل نمی‌داد. قانون‌گذار ایران، مرتکبی که مأمور دولتی را که مرتکب جرم جاسوسی رایانه‌ای شده، به مجازات شدیدتری نسبت به اشخاص عادی محکوم کرده است.

۲-۳-۲. غیرمجاز بودن دسترسی

یکی از شرایطی که برای تحقق این جرم باید وجود داشته باشد، غیرمجاز بودن یا غیرقانونی بودن دسترسی، در دسترس قرار دادن و افشای اطلاعات سرّی است. جزا شرط اساسی تحقق جرم جاسوسی سایبری طبق مادهٔ ۸۶۴ کود «به‌صورت غیرقانونی» است. در قانون جرایم رایانه‌ای نیز دسترسی، در دسترس قرار دادن و افشای اطلاعات سرّی باید «به‌طور غیرمجاز» باشد تا جرم مذکور محقق شود؛ بنابراین، چنانچه رفتارهای (دسترسی، در دسترس قرار دادن یا افشا) قانونی باشد، جرمی محقق نمی‌شود.

[Downloaded from srqjl.knu.edu.af on 2025-12-28]
[DOI: 10.62134/srqjl/v2.i4.202409.6]

۲-۴. وسیلهٔ مجرمانه

وسیلهٔ مجرمانه در جاسوسی سایبری از عناصر اصلی این جرم است که بدون آن امکان ارتکاب جرم وجود ندارد. زمانی که مرتکب با استفاده از «سیستم کمپیوتری، مخابراتی یا حامل‌های اطلاعات»[1] یا «رایانه»[2] دست به جاسوسی بزند، این جرم اتفاق می‌افتد. درصورتی‌که شخصی بدون استفاده از کمپیوتر یا رایانه مرتکب جاسوسی شود، جرم وی جاسوسی ساده است و به همان عنوان مورد پیگرد قرار می‌گیرد.

۲-۵. نتیجهٔ مجرمانه

جرایم ازحیث نتیجه به جرایم مطلقی که نیاز به نتیجهٔ خاصی ندارند و جرایم مقیدی که تحقق آن منوط به منتهی شدن رفتار مجرمانه به نتیجهٔ خاصی است- که در قانون مورد اشاره قرار گرفته باشد- تقسیم می‌شوند (میرمحمد صادقی، ۱۴۰۰: ۱۱۲)؛ بنابراین، این جرم از جرایمی است که رفتارهای مجرمانهٔ آن به‌صورت مطلق و مقید واقع می‌شود. مطابق جزء ۱ و ۲ فقرهٔ ۱ مادهٔ ۸۶۴ کود جزا رفتارهای دسترسی و در دسترس قرار دادن اطلاعات سرّی نیازی به نتیجهٔ خاصی ندارند و به‌صورت مطلق پیش‌بینی شده‌اند؛ درحالی‌که جزء ۳ مادهٔ مذکور، رفتار مجرمانهٔ این جرم را به‌صورت مقید به نتیجه پیش‌بینی کرده است. محکومیت تحت حکم این جزء مقید به تسلیم اطلاعات سرّی به دولت، سازمان، شرکت یا گروه خارجی یا عاملان آن‌ها است؛ یعنی رفتار مرتکب باید منجر به این نتیجه شود تا چنین رفتار مجرمانه‌ای محقق شود (گروهی از نویسندگان، ۱۳۹۸: ۴۸۱). برخی بر این نظر هستند که همهٔ مصادیق جاسوسی سایبری به‌صورت مطلق قابل تحقق است؛ یعنی بدون اینکه نیاز به تحقق نتیجه خاصی باشد با صِرف دسترسی غیرقانونی به اطلاعات سرّی دولت، در دسترس اشخاص فاقد صلاحیت قرار دادن آن یا افشا و در دسترس دولت، سازمان، گروه و دیگر عاملان خارجی قرار دادن آن، جرم جاسوسی سایبری تحقق یافته است (حسینی و هاشمی، ۱۳۹۸: ۱۸۸). نظر آخر به واقعیت نزدیک‌تر است؛ زیرا به نظر می‌رسد قانون‌گذار به‌دلیل اهمیت و خطرناک بودن جرم جاسوسی سایبری این جرم را به‌صورت مطلق پیش‌بینی کرده باشد.

---

[1] مادهٔ ۸۶۴ کود جزا.

[2] مادهٔ ۳ قانون جرایم رایانه‌ای.

[Downloaded from srqjl.knu.edu.af on 2025-12-28]

[DOI: 10.62134/srqjl/v2.i4.202409.6]

در قانون جرایم رایانه‌ای پنج رفتار مجرمانه داریم که به جز رفتار الف مادهٔ ۳ این قانون، که مطلق است، بقیهٔ رفتارها به‌صورت مقیدبه‌نتیجه پیش‌بینی شده‌اند و بدون رسیدن به نتیجهٔ مجرمانه محقق نمی‌شوند؛ بنابراین، نتیجهٔ مجرمانهٔ جزء ب مادهٔ ۳ عبارت است از تسلیم یا در دسترس قرار دادن داده‌های سرّی به شخص فاقد صلاحیت. نتیجهٔ مجرمانهٔ جزء ج مادهٔ ۳ قانون مذکور، افشا یا در دسترس قرار دادن داده‌های سرّی به دولت، سازمان، شرکت، گروه بیگانه یا عاملان آن‌ها است. مادهٔ ۴ این قانون، نقض تدابیر امنیتی را نتیجهٔ مجرمانه قرار داده است؛ اما نتیجهٔ مجرمانه در مادهٔ ۵ قانون یادشده، دسترسی اشخاص فاقد صلاحیت به داده‌های سرّی است و چنانچه دسترسی شخص بدون صلاحیت واقع نشود، جرم مذکور اتفاق نمی‌افتد.

۲-۶. رابطهٔ سببیت

احراز رابطهٔ سببیت میان رفتار مجرمانه و نتیجهٔ مترتب بر آن، در همهٔ جرایم مقید لازم و ضروری است و در تمام نظام‌های حقوقی بر آن تأکید شده است. وجود رابطهٔ سببیت بین رفتار مرتکب و نتیجهٔ مجرمانه در این جرم، که آن رفتارها به شکل مقید واقع شده باشند، به این معنا است که در دسترس قرار دادن اطلاعات سرّی به شخص فاقد صلاحیت یا دولت، سازمان، گروه یا عاملان آن‌ها مستند به رفتار مرتکب باشد وگرنه جرم، کامل نشده است. نقض تدابیر امنیتی و در دسترس قرار گرفتن اطلاعات سرّی نیز باید مستند به رفتار مرتکب باشد؛ در غیر این صورت، این جرم، کامل اتفاق نیفتاده است.

۳. رکن معنوی

ازلحاظ رکن معنوی، وجود علم و قصد برای تحقق جرم، ضروری است و مرتکب باید- افزون بر آگاهی به سرّی بودن اطلاعات و عدم صلاحیت فرد یا عامل بیگانه بودن گیرنده (در اجزای ۳ مادهٔ ۶۸۴ کود جزا و بندهای ۲ و ۳ قانون جرایم رایانه‌ای)- در ارتکاب اَعمال مقرر در قانون، قاصد باشد. چنانچه مجرم، موجبات دسترسی اشخاص فاقد صلاحیت به اطلاعات سرّی، حامل‌های این اطلاعات یا سامانه‌های مربوط به این نوع اطلاعات را بر اثر بی‌احتیاطی، بی‌مبالاتی یا عدم رعایت تدابیر امنیتی فراهم کند، به استناد دو قانون فوق، قابل مجازات نیست؛ مگر در جایی که- طبق مادهٔ ۵ قانون جرایم رایانه‌ای- مجرم از مأموران دولتی

[Downloaded from srqjl.knu.edu.af on 2025-12-28]
[DOI: 10.62134/srqjl/v2.i4.202409.6]

باشد که مسئول حفظ اطلاعات سرّی مقرر در قانون یا سامانه‌ها بوده و به او آموزش لازم داده شده است یا اطلاعات یا سامانه‌ها طبق قانون در اختیار وی قرار داده شده باشد. این حکم در کود جزا وجود نداشته است که یکی از خلل‌های این قانون به حساب می‌آید.

مادۀ ۴ قانون جرایم رایانه‌ای نیز که نقض تدابیر امنیتی سامانه‌ها را- به‌قصد دسترسی به اطلاعات سرّی- جرم‌انگاری کرده است، در کود جزا وجود ندارد. ممکن است نقض تدابیر امنیتی سامانه ازطریق به‌کارگیری روش‌های نرم‌افزاری، سخت‌افزاری یا ترکیبی از هردو باشد. رفتار ارتکابی در این جرم، نقض تدابیر امنیتی است و لازم نیست همراه با دسترسی به داده‌های سرّی باشد، بلکه باید احراز شود؛ درواقع، وجود قصد دسترسی، شرط تحقق جرم در ساختار رکن معنوی است. چنانچه نقض تدابیر، غیرعمدی و ناشی از بی‌احتیاطی، بی‌مبالاتی یا بدون قصد مذکور و تنها از سر کنجکاوی یا بلندپروازی انجام گرفته باشد، رفتار مرتکب قابل مجازات نیست (آقایی‌نیا و رستمی، ۱۴۰۰: ۱۰۷-۱۰۸).

بنابراین، در این جرم وقتی شخصی را مرتکب جرم جاسوسی سایبری می‌دانند که از سرّی بودن اطلاعات یا داده‌ها و غیرصالح بودن خود، مبنی‌بر دسترسی به اطلاعات سرّی یا وسایلی که در آن اطلاعات سرّی ذخیره شده، آگاه باشد؛ یعنی بتواند اطلاعات سرّی و غیرسرّی را از یکدیگر تفکیک کند. مرتکب جرم باید نسبت به در دسترس قرار دادن اطلاعات سرّی عمد داشته باشد؛ همچنین، باید آگاه باشد به غیرصالح بودن مخاطب‌هایی که اطلاعات سرّی را در اختیار آنان قرار می‌دهد. درنتیجه، سوءنیت عام این جرم به‌صورت قصد کسب اطلاعات سرّی، دسترسی یا در دسترس قرار دادن آگاهانه به آن بوده و سوءنیت خاص آن عبارت است از قصد تسلیم اطلاعات به دشمن که عمدی و غیرعمدی بودن آن را مشخص می‌کند.

ج. مجازات جرم جاسوسی رایانه‌ای

مطابق کود جزای افغانستان، مجازات مرتکب این جرم در مادۀ ۸۶۴ بیان نشده است؛ بلکه به مجازات جرم خیانت ملی یا جاسوسی کلاسیک یا ساده ارجاع داده شده است؛ در آنجا نیز درصورتی‌که مرتکب، تبعۀ کشور افغانستان باشد، خائن شناخته شده و مطابق مقررات مادۀ ۲۳۹ این قانون و احراز رفتار وی در مادۀ ۲۳۸ مجازات می‌شود. چنانچه رفتار وی مشمول اجزای ۱ تا ۹ مادۀ ۲۳۸ قرار گیرد، به حبس دوام درجۀ ۲ می‌شود که حبس بیش از ۱۶ تا ۲۰

[Downloaded from srqjl.knu.edu.af on 2025-12-28]

[DOI: 10.62134/srqjl/v2.i4.202409.6]

سال است؛ چنانچه مشمول اجزای ۱۰ تا ۱۲ مادۀ مذکور شود به حبس طویل محکوم می‌شود که حبس بیش از ۵ تا ۱۶ سال است. درصورتی‌که مرتکب این جرم، تبعۀ کشور خارجی یا شخص بدون تابعیت باشد، مطابق مادۀ ۲۴۰ قانون مذکور مجازات و به حبس دوام درجۀ ۲ محکوم می‌شود. هرگاه جاسوسی سایبری در زمان جنگ یا منازعۀ مسلحانه با دولت خارجی یا گروه مسلح مخالف دولت افغانستان ارتکاب یابد یا منجر به مرگ شود، مرتکب آن مطابق مادۀ ۲۴۱ به حبس درجۀ ۱، که حبس بیش از ۲۰ تا ۳۰ سال است، محکوم می‌شود.

مجازات این جرم در قانون جرایم رایانه‌ای ایران در همان مادۀ مزبور حکم شده است. مطابق مادۀ ۳ این قانون، مرتکب این جرم چنین مجازات می‌شود: «... الف: دسترسی به داده‌های ... به حبس از یک تا سه سال یا جزای نقدی از بیست میلیون (۲۰/۰۰۰/۰۰۰) ریال تا شصت میلیون (۶۰/۰۰۰/۰۰۰) ریال یا هر دو مجازات؛ ب: در دسترس قرار دادن ... به حبس از دو تا ده سال؛ ج: افشا یا در دسترس قرار دادن ... به حبس از پنج تا پانزده سال.»

مادۀ ۴ چنین مقرر می‌دارد: «هرکس به قصد دسترسی به داده‌های سری ... به حبس از شش ماه تا دو سال یا جزای نقدی از ده میلیون (۱۰/۰۰۰/۰۰۰) ریال تا چهل میلیون (۴۰/۰۰۰/۰۰۰) ریال یا هر دو مجازات محکوم خواهد شد.»

مادۀ ۵ نیز چنین مقرر می‌دارد: «چنانچه مأموران دولتی که ... به حبس از نودویک روز تا دو سال یا جزای نقدی از پنج میلیون (۵/۰۰۰/۰۰۰) ریال تا چهل میلیون (۴۰/۰۰۰/۰۰۰) ریال یا هر دو مجازات و انفصال از خدمت از شش ماه تا دو سال محکوم خواهند شد.»

درواقع، می‌توان درخصوص مجازات به این نتیجه رسید که در کود جزا مجازات جرم جاسوسی سایبری را به جاسوسی ساده و خیانت ملی ارجاع داده شده و برای همۀ رفتارها یک نوع مجازات تعیین شده است؛ درحالی‌که قانون جرایم رایانه‌ای برای هر رفتار، جداگانه مجازات تعیین کرده، از مزایای جزای نقدی نیز در این جرم استفاده شده است و در مصادیق مختلف این جرم به قاضی اختیار داده شده تا از یک مجازات یا هر دو مجازات استفاده کند.

نتیجه‌گیری

فضای سایبری عبارت است از محیطی الکترونیکی که اطلاعات دیجیتالی ازطریق آن تولید، ارسال، دریافت، ذخیره، پردازش و حذف می‌شوند. فضای سایبری با از بین بردن

[Downloaded from srqjl.knu.edu.af on 2025-12-28]
[DOI: 10.62134/srqjl/v2.i4.202409.6]

محدودیت‌های مکانی و زمانی، ارتکاب جرم را بسیار ساده کرده و در دسترس همگان قرار داده است. با پیشرفت فناوری و ذخیره یا انتقال اطلاعات سرّی توسط دولت‌ها یا شرکت‌های بزرگ، استفاده از فضای سایبری و ذخیره و انتقال اطلاعات در آن، ارتکاب این جرم را بیشتر ممکن ساخته است؛ بنابراین، هرکس با داشتن کمپیوتر می‌تواند به اطلاعات سرّی کشوری دسترسی پیدا کند و نیازی به صرف هزینه‌های گزافی برای فرستادن جاسوس، حمایت‌های نظامی و تجهیزاتی ندارد و می‌توان به‌صورت بسیار ساده ازطریق فضای سایبری اطلاعات سرّی را جمع‌آوری کند. جرم جاسوسی سایبری یکی از جرایم جدید و مورد توجه قانون‌گذاران است که در کود جزای افغانستان، در سال ۱۳۹۶، و در قانون جرایم رایانه‌ای ایران، در سال ۱۳۸۸، جرم‌انگاری شده است. پیش از این، این جرم در قوانین گذشته جرم‌انگاری نشده بود؛ بنابراین، از جرایمی است که با کمپیوتر یا رایانه ارتکاب می‌یابد و موضوع آن اطلاعات یا داده‌های سرّی است که در هر دو قانون به یک صورت عمل شده است. تفاوت‌های دو قانون نسبت به این جرم این است که کود جزای افغانستان عنوان آن را جرم جاسوسی سایبری قرار داده است درحالی‌که قانون جرایم رایانه‌ای در ایران به این جرم اشاره دارد. جاسوسی سایبری، عنوان بهتر و گسترده‌تری به نظر می‌رسد که شامل جاسوسی‌های انترنتی و کمپیوتری می‌شود؛ اما جاسوسی رایانه‌ای عنوان محدودتری به نظر می‌رسد که بیشتر شامل جاسوسی‌هایی می‌شود که توسط رایانه یا کمپیوتر اتفاق می‌افتند؛ البته از متن این قانون می‌توان جاسوسی سایبری را استخراج کرد.

تفاوت دیگر دو قانون این است که مصادیق رفتارهای مجرمانه این جرم در کود جزا سه نوع (دسترسی، در دسترس قرار دادن و افشا یا در دسترس قرار دادن آن به دولت ...) پیش‌بینی شده است؛ اما قانون جرایم رایانه‌ای ایران پنج رفتار جداگانه را پیش‌بینی کرده است که علاوه‌بر سه رفتار بالا، رفتارهای نقض تدابیر امنیتی و در دسترس قرار دادن غیرعمدی، که توسط کارمند موظف اتفاق می‌افتد، نیز جرم‌انگاری شده‌اند که جرم‌انگاری خوب قانون‌گذار را نشان می‌دهند و یکی از خلأهای کود جزا هستند.

[Downloaded from srqjl.knu.edu.af on 2025-12-28]

[DOI: 10.62134/srqjl/v2.i4.202409.6]

منابع

۱. قرآن کریم.

۲. آقایی‌نیا، حسین و هادی رستمی. (۱۴۰۰). حقوق کیفری اختصاصی (۲) جرایم علیه مصالح عمومی کشور. ایران، میزان.

۳. جعفری لنگرودی، محمدجعفر. (۱۳۹۶). ترمینولوزی حقوق. چ ۳۰. ایران: گنج دانش.

۴. حبیب‌زاده، محمدجعفر. (۱۴۰۲). حقوق کیفری عمومی: کلیات و ارکان تشکیل‌دهندهٔ جرم. ایران: میزان.

۵. حسینی، سید محمد و غازی هاشمی. (۱۳۹۸). حقوق جزای اختصاصی ۳. کابل: بنیاد آسیای افغانستان.

۶. رسولی، محمداشرف. (۱۳۹۶). دورهٔ کامل حقوق جزای عمومی. کابل: واژه.

۷. رنه گارو، ژرژ. (۱۳۴۳). مطالعهٔ نظری و عملی در حقوق جزا. ترجمهٔ ضیاءالدین نقابت. ج ۳. [بی‌جا]: ابن سینا.

۸. عمید، حسن. (۱۳۶۷). فرهنگ عمید. چ ۱۲. ایران: امیرکبیر.

۹. فتاحی، مختار. (۱۳۹۷). «عناصر تشکیل‌دهندهٔ مادی و معنوی مصادیق جرایم رایانه‌ای». فصلنامهٔ علمی-حقوقی قانون‌یار. دورهٔ دوم.

۱۰. کاشانی، فتح الله. ([بی‌تا]). تفسیر منهاج الصادقین. ج ۴. ایران: مؤسسهٔ تحقیقاتی و نشر معارف اهل‌بیت (ع).

۱۱. میرمحمد صادقی، حسین. (۱۴۰۰). حقوق جزای عمومی ۱. چ ۳. ایران: دادگستر.

۱۲. جلالی فراهانی، امیرحسین. «پیشگیری وضعی از جرایم سایبر در پرتو موازین حقوق بشر». فصلنامهٔ فقه و حقوق. ۲ (۶)، ۱۳۸۴.

۱۳. عبدالفتاح، عزت. «جرم چیست و معیارهای جرم‌انگاری کدامند». ترجمهٔ اسماعیل رحیمی‌نژاد. مجلهٔ قضایی و حقوق دادگستری. (۴۱)، ۱۳۸۱.

۱۴. فتاحی، سجاد و دیگران. «پیشگیری از جرم جاسوسی سایبری نیروهای مسلح و نقش آن در تأمین حق امنیت». دوفصلنامهٔ علمی مطالعات حقوق بشر اسلامی. ۹ (۱۸)، ۱۳۹۹.

[Downloaded from srqjl.knu.edu.af on 2025-12-28]

[DOI: 10.62134/srqjl/v2.i4.202409.6]

۱۵. فلاحی، احمد. «اصل ضرورت در جرم‌انگاری و محدودیت‌های وارد بر دخالت کیفری در مصرف مواد مخدر». پژوهشنامهٔ حقوق کیفری. (۱)، ۱۳۹۴.
۱۶. قدسی، زهرا. «مبانی فقهی جاسوسی». مبانی فقهی حقوق اسلامی. ۶ (۱۱)، ۱۳۹۲.
۱۷. موسوی بجنوردی، سید محمد. «مجموعه‌مقالات فقهی و حقوقی، فلسفی، اجتماعی». جرم سیاسی در حقوق کیفری اسلام. پژوهشکدهٔ امام خمینی و انقلاب اسلامی. چ ۱. ۱۳۸۵.
۱۸. پورسیدرضا، سید مجتبی. «بررسی فقهی تجسس در اسلام». پایان‌نامهٔ کارشناسی ارشد. دانشگاه آزاد اسلامی واحد کرج. ۱۳۸۵.
۱۹. کامرانی، مصطفی. «بررسی جرم جاسوسی و خرابکاری در قوانین جزایی ایران با نگاهی به قانون جرایم رایانه‌ای». پایان‌نامهٔ کارشناسی ارشد. دانشگاه آزاد اسلامی واحد شهر قدس. ۱۳۹۷.
۲۰. قانون جرایم رایانه‌ای، مصوب ۱۳۸۸.
۲۱. کود جزای افغانستان، مصوب ۱۳۹۶.

[Downloaded from srqjl.knu.edu.af on 2025-12-28]
[DOI: 10.62134/srqjl/v2.i4.202409.6]