فصلنامه دیدگاه‌های حقوق قضایی (علمی)

دوره ۳۰، شماره ۱۱۱، پاییز ۱۴۰۴
نوع مقاله: پژوهشی
دریافت: ۱۴۰۱/۱۲/۱۲ - پذیرش: ۱۴۰۳/۰۴/۰۲

آسیب‌شناسی سیاست کیفری ایران در دسترسی غیرمجاز به داده‌ها و سامانه‌های رایانه‌ای نظامی

✍ **هادی مرسی** ✉ Stu.h.mersi@meybod.ac.ir
دانشجوی دکتری حقوق جزا و جرم‌شناسی، دانشکدهٔ الهیات و معارف اسلامی، دانشگاه میبد، یزد، ایران
محمد زرنگ
مربی گروه حقوق، دانشکدهٔ مدیریت، دانشگاه افسری امام علی (ع)، تهران، ایران

چکیده: دسترسی غیرمجاز به داده‌های رایانه‌ای نظامی موجب می‌شود تا سایر جرایم و تهدیدات سایبری از قبیل تحصیل داده‌های رایانه‌ای نظامی، جاسوسی رایانه‌ای، حملهٔ سایبری به زیرساخت‌های نظامی، تخریب سامانه‌های رایانه‌ای حیاتی نظامی تحقق یابند. قانون‌گذار در بند (الف) ماده ۷۳۱ قانون مجازات اسلامی صرفاً دسترسی غیرمجاز داده‌های سری را به‌طور عام پیش‌بینی کرده است و در ماده ۱۳۱ قانون مجازات جرایم نیروهای مسلح نسبت به‌عنوان مجرمانهٔ دسترسی غیرمجاز به داده‌ها و اطلاعات فاقد طبقه‌بندی و طبقه‌بندی‌شده رایانه‌ای نظامی صراحتی وجود ندارد. اهمیت و حساسیت داده‌ها و سامانه‌های رایانه‌ای نظامی اقتضا دارد که تدابیر متناسب با آن‌ها چه در حوزهٔ جرم‌انگاری و چه کیفرگزینی مقرر گردد. در این پژوهش به این امر که سیاست کیفری ایران در قبال دسترسی غیرمجاز به داده‌ها و سامانه‌های رایانه‌ای نظامی به چه نحو است و اینکه آیا در این راستا خلأ و نارسایی قابل‌توجهی وجود دارد یا با وجود قوانین دیگر، چنین نقص یا خلأیی منتفی خواهد شد، پرداخته می‌شود. پژوهش حاضر به روش توصیفی ـ تحلیلی و مبتنی بر منابع کتابخانه‌ای نتیجه‌گیری می‌نماید که سیاست کیفری ایران در قبال دسترسی به داده‌ها وسامانه‌های رایانه‌ای نظامی طبقه‌بندی‌شده و فاقد طبقه‌بندی از سوی اشخاص نظامی و غیرنظامی از اصل بازدارندگی و اصل تناسب جرم و مجازات برخوردار نبوده که در این خصوص نیاز به اصلاحات خلأهای قانونی است که مستلزم پیش‌بینی تدابیری متناسب با اهمیت داده‌های رایانه‌ای نظامی است که در این راستا پیشنهادهایی ارائه شده است.

واژگان کلیدی: سیاست کیفری، دسترسی غیرمجاز، جرم رایانه‌ای، جرم نظامی، جاسوسی رایانه‌ای

استناد: مرسی، هادی و زرنگ، محمد. (۱۴۰۴). آسیب‌شناسی سیاست کیفری ایران در دسترسی غیرمجاز به داده‌ها و سامانه‌های رایانه‌ای نظامی. دیدگاه‌های حقوق قضایی، ۳۰ (۱۱۱)، ۲۱۹-۲۴۷.
https://doi.org/10.22034/jlvi.2025.732316
ناشر: دانشگاه علوم قضایی و خدمات اداری.

مقدمه

فضای سایبر ، فضایی حقیقی و واقعی است و مجازی نیست هرچند که به شکل مادی و ملموس احساس شدنی نیست (زندی، ۱۳۹۳: ۱۶۰؛ یکرنگی و دیگران، ۱۴۰۰: ۵۶۴). برخی از نویسندگان فضای سایبر را شامل تمام شبکه‌های رایانه‌ای موجود در دنیا و هر آنچه به این شبکه‌ها متصل است یا آنان را کنترل می‌کند، دانسته‌اند (Clarke, 2010: 6). برخی دیگر فضای سایبر را فقط ناظر به همه منابع اطلاعاتی قابل‌دسترس در شبکه‌های رایانه‌ای دانسته‌اند.[1] وزارت دفاع ایالات‌متحده فضای سایبر را این‌گونه تعریف نموده است: «دامنه‌ای جهانی در فضای اطلاعات که متشکل از شبکه‌ها و سامانه‌های مستقل فناوری اطلاعات از قبیل اینترنت، شبکه‌های مخابراتی، سامانه‌های رایانه‌ای و پردازنده و کنترل‌هایی تعبیه‌شده است»(Joint Chiefs of Staff, 2011: 141). در تعریف فضای سایبر گفته‌شده است: «فضایی که داده‌های رایانه‌ای در آن به‌صورت صفر و یک ایجاد، ذخیره، جابه‌جا، دستخوش تغییرات و حذف می‌شوند» (مرسی، ۱۳۹۷: ۲۳). پژوهش حاضر با اتخاذ تعریف اخیر به آسیب‌شناسی سیاست کیفری ایران در قبال دسترسی غیرمجاز به داده‌ها و سامانه‌های رایانه‌ای نظامی می‌پردازد.

یکی از رفتارهای مجرمانه‌ای که در فضای سایبر ممکن است محرمانگی داده‌ها، حامل‌های داده[2] و سامانه‌های رایانه‌ای نظامی را تحت‌الشعاع قرار دهد، «دسترسی غیرمجاز» است. جرم «دسترسی غیرمجاز» ازجمله جرائمی است که با پیدایش داده و سامانهٔ رایانه‌ای پدید آمده و نقش اساسی در ارتکاب سایر جرائم رایانه‌ای ایفا می‌کند، که این نقش اساسی سبب شده برخی این جرم را تحت عنوان «جرم مانع» یا «بازدارنده» قلمداد کنند (یکرنگی و مرسی، ۱۳۹۹: ۳۱۳) و برخی دیگر این جرم را تحت عنوان «جرم مادر» یا «زاینده» در نظر گرفته‌اند (تحیری، ۱۳۸۳: ۸۰)؛ زیرا در اغلب موارد سایر رفتارهای مجرمانه سایبری از قبیل رفتارهای مجرمانه ناقض محرمانگی، تمامیت و دسترس‌پذیری سامانه‌ها و داده‌های رایانه‌ای از رهگذر آن می‌گذرند.

دسترسی غیرمجاز به داده‌ها یا سامانه‌های رایانه‌ای نظامی از سوی اشخاص نظامی و غیرنظامی در فضای سایبر می‌تواند منجر به عواقب خطیر و امنیتی شود. هرکس که به‌طور غیرمجاز به داده‌ها و سامانه‌های رایانه‌ای نظامی دسترسی یابد، ممکن است از این اطلاعات سوءاستفاده استفاده کنند. این سوءاستفاده شامل کلاهبرداری، جاسوسی صنعتی، سرقت اموال فکری، اختلاس و تلاش برای

---

1 .www.library.arizona.edu/rio/glossary.html

۲. منظور از حامل‌های داده، ابزارهایی از نوع حافظه جانبی یا کمکی هستند که از آن‌ها برای ذخیره یا انتقال داده‌ها استفاده می‌شود (ر.ک سبزگلی و موسوی، ۱۳۹۲: ۳۱).

انحراف از اهداف نظامی است. سوءاستفاده از این اطلاعات باعث تضرر جدی برای سازمان‌ها، افراد و جوامع نظامی می‌شود. همچنین مرتکب ممکن است از رهگذر دسترسی غیرمجاز تلاش کند تا داده‌های نظامی را تخریب یا باعث اخلال در عملکرد سامانه‌های رایانه‌ای نظامی شود و یا کنترل آن‌ها را در دست بگیرد. این امر می‌تواند به توقف عملکرد سامانه‌های رایانه‌ای، اختلال در خدمات عمومی و خسارت به بنیان‌های نظامی و اقتصادی منجر شود. اشخاص نظامی یا غیرنظامی که به‌طور غیرمجاز به داده‌ها و سامانه‌های نظامی دسترسی می‌یابند، ممکن است اطلاعات حساس را به دشمنان یا سازمان‌های خارجی فاش کنند که این باعث کاهش آمادگی نظامی، تضعیف امکانات دفاعی و آسیب به امنیت ملی می‌شود.

ارتقا و به‌روزرسانی قوانین و مقررات مرتبط با امنیت سایبری و مقابله با دسترسی غیرمجاز به داده‌ها و سامانه‌های رایانه‌ای نظامی می‌تواند در تأمین محافظت و اتخاذ سیاست کیفری متناسب و بازدارنده در برابر تهدیدات سایبری کمک کند. درواقع، تدوین قوانین جامع‌ومانع و اتخاذ یک سیاست کیفری مؤثر و کارآمد می‌تواند ارتقای امنیت سایبری را در کنار اتخاذ تدابیر فنی تضمین کند.

حقوق کیفری نظامی در راستای تسری کیفر جرائم سنتی نسبت به جرائم مرتبط با سامانه رایانه‌ای، حامل داده و داده رایانه‌ای در ماده ۱۳۱ قانون مجازات جرائم نیروهای مسلح مصوب ۱۳۸۲/۱۰/۰۹ اقدام به جرم‌انگاری برخی رفتارهای مجرمانهٔ سایبری از سوی اشخاص نظامی[1] کرده است. لیکن نسبت به‌عنوان مجرمانه دسترسی غیرمجاز به داده‌ها و سامانه‌های رایانه‌ای مسکوت مانده است.[2] شایان‌ذکر است قانون‌گذار در بند (الف) ماده ۷۳۱ از عبارت دسترسی به داده‌های

---

۱. جرم نظامی و انتظامی در دو مفهوم مضیق و موسع قابل طرح است. اولین مورد آن جرم نظامی در مفهوم مضیق است. جرم نظامی را در معنای مضیق یا خاص آن، می‌توان جرمی دانست که ماهیت آن نظامی است و فقط توسط یک فرد نظامی قابل تحقق می‌باشد. جرم نظامی در مفهوم موسع «به هر جرمی گفته می‌شود که فرد نظامی به مناسبت شغل یا وظیفه خود مرتکب گردد، مانند سرقت و اختلاس (ر.ک به: خالقی، ۱۳۹۵: ۶۲). در پژوهش حاضر جرم نظامی در مفهوم موسع آن مدنظر است. در واقع جرایمی که دارای ماهیت عمومی هستند، اگر در ارتباط با یک وظیفه نظامی واقع شوند جرم خاص نظامی تلقی می‌شوند (ر.ک: رامشی، ۱۳۸۸: ۱۲).

۲. ماده ۱۳۱ مقرر می دارد:«هرگونه تغییر یا حذف اطلاعات، الحاق، تقدیم یا تأخیر تاریخ نسبت به تاریخ حقیقی و نظایر آن که به طور غیرمجاز توسط نظامیان در سیستم رایانه و نرم افزارهای مربوط صورت گیرد [جعل رایانه ای] و همچنین اقداماتی از قبیل تسلیم اطلاعات طبقه بندی شده رایانه ای به دشمن یا افرادی که صلاحیت دسترسی به آن اطلاعات را ندارند[جاسوسی رایانه ای]، افشا غیرمجاز اطلاعات، سرقت اشیاء دارای ارزش اطلاعاتی مانند سی دی (CD) یا دیسکت های حاوی اطلاعات یا معدوم کردن آن ها یا سوءاستفاده های مالی که نظامیان به وسیله رایانه مرتکب شوند جرم محسوب و حسب مورد مشمول مجازات های مندرج در مواد مربوط به این قانون می باشند.»

سری به‌طور عام استفاده کرده است. پرسش‌های بنیادین و اساسی مطرح می‌شود که منظور از دسترسی غیرمجاز در فضای سایبر چیست؟ شرایط تحقق جرم دسترسی غیرمجاز زمانی که موضوع آن داده‌ها و سامانه‌های رایانه‌ای نظامی چیست؟ چنانچه شخص نظامی مرتکب جرم دسترسی غیرمجاز در فضای سایبر شود، رفتار وی مصداق کدام ماده یا مواد پیش‌بینی‌شده در قانون مجازات جرائم نیروهای مسلح قرار می‌گیرد؟ آیا سیاست کیفری ایران در قبال دسترسی غیرمجاز به داده‌های طبقه‌بندی‌شده و فاقد طبقه‌بندی رایانه‌ای نظامی از سوی اشخاص نظامی و غیرنظامی که می‌تواند امنیت کشور را به مخاطره اندازد، متناسب و بازدارنده است؟ با بررسی قوانین مربوطه و استخراج خلأهای قانونی پژوهش حاضر به اتخاذ یک سیاست کیفری افتراقی متناسب و بازدارنده اهتمام ورزیده است. شایان ذکر است برای آنکه بتوان خلأ قانونی را استخراج کرد و به یک سیاست کیفری مطلوب در حوزهٔ حمایت از داده‌ها و سامانه‌های رایانه‌ای نظامی در برابر رفتار مجرمانه دسترسی غیرمجاز دست یافت، لازم می‌آید با تمسک به «حقوق تطبیقی» یا به تعبیر برخی حقوق‌دانان «مطالعهٔ تطبیقی»، رویکرد اسناد بین‌المللی و سایر کشورهای پیشرو و پیشگام (آمریکا و انگلستان) در حوزهٔ امنیت سایبری را پیرامون دسترسی غیرمجاز با استفاده از روش‌های علمی مورد مقایسه، تطبیق و تقابل قرار داد تا برای اتخاذ یک سیاست کیفری مطلوب، بهترین و کارآمدترین راه‌حل را انتخاب نمود. در این راستا، در سه قسمت «مفهوم دسترسی غیرمجاز و عناصر سه‌گانه آن»، «سیاست کیفری ایران در قبال دسترسی غیرمجاز به داده‌ها و سامانه‌های رایانه‌ای فاقد طبقه‌بندی نظامی» و «سیاست کیفری ایران در قبال دسترسی غیرمجاز به داده‌ها و سامانه‌های رایانه‌ای طبقه‌بندی شده نظامی» تدوین یافته است.

۱. مفاهیم

یافتن خلأهای قانونی و اتخاذ یک سیاست کیفری افتراقی متناسب و بازدارنده نسبت به رفتارهای مجرمانهٔ دسترسی غیرمجاز به داده‌ها و سامانه‌های رایانه‌ای نظامی مستلزم این است که مفهوم دسترسی غیرمجاز و عناصر سه‌گانه آن مورد تجزیه‌وتحلیل قرار گیرند. این الزام از آنجا که تعریف واحد و مشترکی از مفاهیم یادشده میان حقوق‌دانان و اندیشمندان وجود ندارد، دوچندان می‌شود. لذا در این قسمت به تبیین مفاهیم پرداخته شده است.

۱-۱. مفهوم دسترسی غیرمجاز

در تعریف و بیان مفهوم دسترسی غیرمجاز[1] از سوی حقوق‌دانان مطالب متفاوتی بیان شده است. برخی آن را به معنای رخنه غیرقانونی به سامانهٔ رایانه‌ای حفاظت‌شده می‌دانند (عالی‌پور، ۱۳۹۳:

1. Illegal Access

۱۵۹). برخی دیگر معنای کسب بدون مجوز داده‌ها، برنامه‌ها و اطلاعات دانسته (کلیمانی و اکبری، ۱۳۹۴: ۹۰)، و عده‌ای هم به معنای دستیابی بدون مجوز به محتوای ذخیره‌شده یا در حال پردازش در یک یا چند سامانه رایانه‌ای دانسته‌اند (الهی‌منش و سدره نشین، ۱۳۹۵: ۱۳). بر هر یک از تعاریف اشاره شده نقدهایی وارد است (بابایی، ۱۳۹۸: ۵۷-۵۶). بااین‌وجود می‌توان آن را این‌گونه شرح داد: «دسترسی غیرمجاز به سامانه، حامل داده یا داده رایانه‌ای اعم از آنکه دارای تدابیر امنیتی حفاظت‌شده باشد خواه نباشد.» پژوهش حاضر با اتخاذ این تعریف به تحلیل عناصر مادی و معنوی جرم دسترسی غیرمجاز می‌پردازد.

۱-۲. تحلیل و ارزیابی عناصر سه‌گانهٔ جرم دسترسی غیرمجاز

به نظر می‌رسد کاربردی‌ترین تقسیم‌بندی با توجه به قوانین کشورها، تقسیم‌بندی به اعتبار تمهیدات حفاظتی و محیط ارتکاب جرم باشد که در این صورت انواع دسترسی غیرمجاز به چهار دسته قابل تقسیم‌بندی است: دستهٔ اول) دسترسی در فضای سایبر و با نقض تدابیر امنیتی سامانه‌های رایانه‌ای و مخابراتی؛ دستهٔ دوم) دسترسی در فضای سایبر و بدون نقض تدابیر امنیتی سامانه‌های رایانه‌ای و مخابراتی؛ دستهٔ سوم) دسترسی در فضای واقعی و با نقض تدابیر امنیتی سامانه‌های رایانه‌ای و مخابراتی؛ دستهٔ چهارم) دسترسی در فضای واقعی و بدون نقض تدابیر امنیتی سامانه‌های رایانه‌ای و مخابراتی (بای و پورقهرمانی، ۱۳۸۸: ۱۸۸).

قوانینی که در مورد جرم دست‌یابی غیرمجاز در کشورهای مختلف وضع شده، بسیار متنوع است و تنوع زیادی در ارکان تشکیل‌دهندهٔ جرم به چشم می‌خورد. در قوانین برخی کشورها، صرف دست‌یابی جرم شناخته شده است (مانند دانمارک، سوئد و فرانسه)، اما در برخی کشورهای دیگر، صرف دستیابی به اطلاعات (داده‌ها) و سامانه‌های رایانه‌ای جرم تلقی نشده است، بلکه کسب اطلاعات و مانند تحقق جرم اعلام شده است (محمدنسل و دیگران، ۱۳۹۹: ۸۶).

از حیث عنصر روانی جرم، در برخی از کشورها شرط جرم بودن دست‌یابی، عمدی بودن آن و در برخی دیگر متقلبانه بودن عمل مرتکب است. از حیث شرایط و اوضاع‌واحوال ملازم با جرم، در قوانین برخی کشورها نقض تدابیر امنیتی شرط جرم‌انگاری است و طبیعتاً دست یافتن به سامانهٔ رایانه‌ای یا داده‌های بدون قفل و بست امنیتی جرم تلقی نمی‌شود، لیکن در قوانین برخی دیگر از کشورها دست یافتن عامدانه به سامانه‌ها یا داده‌های آن، جرم تلقی می‌شود، خواه تدابیر امنیتی نقض شده باشد یا خیر (بای و پورقهرمانی، ۱۳۸۸: ۱۸۸).

۱-۲-۱. رکن قانونی جرم دسترسی غیرمجاز

قانون‌گذار ایران با الهام از ماده ۲ کنوانسیون بوداپست[۱] در ماده یک قانون جرائم رایانه‌ای (ماده ۷۲۹ قانون مجازات اسلامی بخش تعزیرات) نسبت به جرم‌انگاری دسترسی غیرمجاز اقدام کرده است. ماده ۷۲۹ قانون مجازات اسلامی بخش تعزیرات مقرر می‌دارد: «هرکس به‌طور غیرمجاز به داده‌ها و سامانه‌های رایانه‌ای یا مخابراتی که به‌وسیله تدابیر امنیتی حفاظت شده است دسترسی یابد، به حبس از نود و یک روز تا یک سال یا جزای نقدی از پنج میلیون (۵/۰۰۰/۰۰۰) ریال تا بیست میلیون (۲۰/۰۰۰/۰۰۰) ریال یا هر دو مجازات محکوم خواهد شد».

۱-۲-۲. رکن مادی جرم دسترسی غیرمجاز

در خصوص رکن مادی این جرم باید خاطرنشان کرد که مقنن در توصیف رفتار فیزیکی از واژهٔ «دسترسی» استفاده کرده است. منظور از «دسترسی»، در اختیار گرفتن و تسلط بر داده، حامل داده یا سامانهٔ رایانه‌ای است به‌گونه‌ای که مرتکب امکان تصرف در کارکرد سامانه یا ملاحظه و نظارت بر داده را، داشته باشد (بابایی، ۱۳۹۸: ۵۹). به نظر می‌رسد مفهوم «دسترسی» یا «داشتن توانایی بهره‌گیری از سامانه یا داده رایانه‌ای»، نسبت به مفهوم هک مفهومی کلی‌تر و عام‌تر باشد. درواقع می‌توان گفت دسترسی، شامل هرگونه بهره‌مندی از سامانه رایانه‌ای یا داده رایانه‌ای می‌شود، خواه آن سامانه یا داده دارای تدابیر امنیتی باشد، خواه نباشد. اما مفهوم هک ناظر بر فرضی است که داده یا سامانه رایانه‌ای با تدابیر امنیتی برای عموم غیرقابل‌دسترس باشد و شخص تنها بتواند با انجام برخی روش‌ها و فنون فنی از این گذرگاه عبور کند و به درون سامانه رایانه‌ای راه یابد. بنابر این با توجه به وصف موضوع جرم که وصف «حفاظت‌شدگی داده و سامانه رایانه‌ای به‌وسیله تدابیر امنیتی» است. می‌توان گفت مفهوم دسترسی در ماده ۷۲۹ قانون مجازات اسلامی در معنای خاص بوده و همان هک است.[۲]

---

۱. ماده ۲ کنوانسیون بوداپست مقرر می‌دارد:«هر یک از اعضاء باید به گونه‌ای اقدام به وضع قوانین و سایر تدابیر کنند که در صورت لزوم بر اساس حقوق داخلی خود، دسترسی غیر عمدی بدون حق را به تمام یا بخشی از یک سامانه رایانه‌ای جرم‌انگاری کنند. اعضاء می‌توانند مقرر دارند این جرم با نقض تدابیر امنیتی و به قصد تحصیل داده‌های رایانه‌ای یا سایر مقاصد ناروا یا نسبت به سامانه رایانه‌ای که با سامانه رایانه‌ای دیگری ارتباط دارد، محقق می‌شود.» (ر.ک: امیرمهدی، ۱۳۹۴: ۶۳؛ جلالی فراهانی، ۱۳۹۵: ۲۶؛ محمدنسل، ۱۳۹۵: ۲۷-۲۶).

۲. در این زمینه می‌توان به رأی شعبه ۱۰۸۳ دادگاه عمومی جزایی تهران ویژه کارکنان دولت اشاره کرد: « در خصوص اتهام آقای ش ... دایر بر هک ایمیل شاکی، با عنایت به اوراق و محتویات پرونده و ... بزهکاری نامبرده محرز و مسلم بوده و با استناد به ماده یک از قانون جرائم رایانه‌ای و با رعایت ماده ۲۲ قانون مجازات اسلامی به پرداخت پنجاه میلیون ←

با توجه به اهمیت داده‌ها و سامانه‌های نظامی، لازم است اشخاص نظامی موظف به اتخاذ تدابیر امنیتی جهت حفظ محرمانگی داده‌ها و سامانه‌های نظامی شوند. در این راستا می‌توان به ماده ۴۸ آیین‌نامه انضباطی نیروهای مسلح اشاره کرد: «هر یک از پرسنل نیروهای مسلح بایستی همواره با هوشیاری و رعایت اصول و مقررات حفاظتی در حفظ اسراری که در اختیار اوست کوشا باشد و حتی در شرایط بحرانی با نهایت فداکاری از افشای آن جلوگیری نماید و در برخورد یا موارد مشکوک از قبیل (براندازی، جاسوسی، خرابکاری، موارد ایجاد نارضایتی) مراتب را بلافاصله به مقام مافوق مسئول گزارش نماید». حال چنانچه یک شخص نظامی این امر قانونی را انجام ندهد، رفتار وی می‌باید در قالب ترک فعل دارای وصف مجرمانه باشد. در صورت پیش‌بینی رفتار مجرمانه «دسترسی غیرمجاز» در قانون مجازات جرائم نیروهای مسلح شایسته است تحت یک تبصره «هر نظامی که بر اثر بی‌احتیاطی یا بی‌مبالاتی یا سهل‌انگاری یا عدم رعایت نظامات دولتی اقدام به اتخاذ تدابیر امنیتی نسبت به داده و سامانه رایانه‌ی در اختیار خویش نکند، رفتار وی دارای ضمانت اجرای کیفری باشد».

گاهی ممکن است با تغییر جایگاه‌های شغلی داده‌ها و سامانه‌های رایانه‌ای نظامی از یک شخص نظامی به شخص نظامی دیگری سپرده شود، در این صورت شایسته است شخص نظامی جدید تدابیر امنیتی جدیدی را برای داده یا سامانه نظامی اتخاذ کند و ترک فعل وی را دارای وصف مجرمانه دانست. در فرضی که شخص نظامی با ترک فعل خویش تدابیر امنیتی جدیدی را اتخاذ نکرده باشد، آنگاه اگر دسترسی از سوی یک شخص نظامی انجام گیرد که پیش از آن به سامانه یا داده دسترسی داشته ولیکن اکنون به دلایل گوناگونی همچون تغییر سمت ممنوع از ورود به داده یا سامانه رایانه‌ای پیشین خود باشد، رفتار وی غیرمجاز بوده و دارای وصف مجرمانه «دسترسی غیرمجاز» است.[1]

ریال جزای نقدی بدل از حبس در حق صندوق دولت محکوم می‌گردد...» رأی مزبور عیناً در شعبه ۳۸ دادگاه تجدیدنظر استان تهران تأیید شد. همچنین می‌توان به رأی شعبه ۱۰۵۷ دادگاه عمومی تهران اشاره کرد: «در خصوص اتهام آقای ... دایر بر دسترسی غیر مجاز به داده‌ها و سامانه‌های رایانه‌ای و سرقت اموال، بدین توضیح که متهم با سرقت اموال شاکیه که شامل لپ تاپ وکیف پول به میزان دو میلیون ریال و کیف کارت‌های شخصی شامل کارت شناسایی، کارت بانکی و رمز دسترسی لپ‌تاپ شاکیه قرار داشته است به لپ‌تاپ مشارالیه که با تدابیر امنیتی حفاظت شده بود دسترسی پیدا کرده و مورد استفاده قرار داده است ... دادگاه اتهام نامبرده را محرز و مسلم تشخیص داده و به استناد ماده ۷۲۹ و ۶۵۶ قانون مجازات اسلامی به تحمل یک سال حبس تعزیری و به سه سال حبس تعزیری و ۷۴ ضربه شلاق تعزیری با رعایت ماده ۱۳۴ قانون مذکور محکوم می‌نماید. ...».

۱. در تأیید این نظر می‌توان به رأی شعبه ۱۰۵۷ دادگاه عمومی تهران اشاره کرد: «... در خصوص کیفرخواست شماره ۱۴-۰۰۰۶-۹۵۰۰۰۰۶-۱۳۹۰/۱/۹۰۱۰۴۳۲۱۷، دادگاه با عنایت به جمیع اوراق و محتویات پرونده.... که دلالت به حضور ←

سؤالی که ممکن است در این قسمت مطرح گردد این است که رفتار فیزیکی دسترسی باید به تمام داده یا سامانه‌ی رایانه‌ای ارتکاب یابد یا صرف اینکه به بخشی از آن داده یا سامانه نظامی دسترسی یافت این جرم تحقق یافته است؟ در پاسخ باید گفت با توجه به هدف پیش‌بینی چنین جرمی که بیان شد و اهمیت حفظ محرمانگی داده‌ها و سامانه‌های رایانه‌ای نظامی دسترسی به بخشی از داده و سامانهٔ نظامی نیز برای تحقق جرم اکتفا می‌کند. از حیث تطبیقی می‌توان به بند ۴۶ گزارش توجیهی کنوانسیون بوداپست اشاره کرد. در بند ۴۶ در تبیین اصطلاح «دسترسی» مقرر شده است: «دسترسی شامل ورود به تمام یا بخشی از سیستم رایانه‌ای می‌شود (سخت‌افزار، اجزای آن، داده‌های ذخیره در سیستم نصب‌شده، شاخه‌ها، داده‌های ترافیک و داده‌های مرتبط با محتوا). بااین‌حال، صرف ارسال یک رایانامه و یا فایل به آن سیستم را در برنمی‌گیرد. «دسترسی» شامل ورود به سیستم رایانه‌ای دیگری به‌وسیله شبکه‌های مخابراتی عمومی یا ورود به سیستم رایانه‌ای همان شبکه می‌شود. نظیر شبکه محلی یا اینترنت داخلی یک سازمان، نحوه برقراری ارتباط اهمیتی ندارد (مثلاً از راه دور، شامل خطوط بی‌سیم یا در طیف بسته)».

نکته‌ای که لازم است بدان اشاره کرد این است که با رشد و تحول و دگرگونی در افزارهای مجرمانه، مجرمان از روش‌ها و فنون جدید و فراوانی برای دسترسی به داده‌ها و سامانه‌های رایانه‌ای بهره می‌جویند. ممکن است در بادی امر به نظر رسد آنچه بسیار مهم و حائز اهمیت است، این است که حتماً رفتار دستیابی به تدابیر امنیتی داده یا سامانه رایانه‌ای در بستر فضای سایبر و به‌طور فنی و نرم‌افزاری باید باشد و هرگاه مرتکب از طریق گفتاری و یا فریب دادن دیگری و متعاقب آن گذرواژه سامانه وی را به دست آورد، رفتار ارتکابی وی از شمول ماده ۷۲۹ قانون مجازات اسلامی خارج است. به‌عبارت‌دیگر، پرسش این است آیا لزوماً رفتار ارتکابی «دسترسی» باید از رهگذر

آقای محسن ... در ساعت ۲۰:۲۰ مورخ ۱۳۸۹/۷/۱۶ (جمعه شب) در آتلیه متعلق به شاکی و اقدام به قرار دادن رم متعلق به خود در کامپیوتر و کپی نمودن از یک آلبوم دیجیتال می‌نماید، اقرار و اذعان متهم به حضور در محل کار سابق خود با وصف این‌که با وی قطع همکاری شده بوده و ادعای وی به این‌که فایل شخصی خود را کپی گرفته، عدم اثبات آن و این‌که پس از قطع همکاری وی با شاکی نامبرده بدون اجازه وی حق ورود به محل و همچنین کار با کامپیوتر را نداشته، تحقیقات انجام شده توسط بازپرس محترم، قرار مجرمیت و کیفرخواست اصداری و دفاع بلاوجه متهم و غیر مؤثر وکیل دادگاه بزهکاری مشارالیه را محرز دانسته مستنداً با استناد به ماده ۱ قانون جرائم رایانه‌ای و با رعایت بند ۵ ماده ۲۲ قانون مجازات اسلامی حکم به محکومیت وی به پرداخت مبلغ دو میلیون ریال جزای نقدی در حق صندوق دولت صادر و اعلام می‌دارد. رای صادره حضوری و ظرف مهلت بیست روز پس از ابلاغ قابل تجدیدنظرخواهی در محاکم محترم تجدیدنظر استان تهران می‌باشد».

اعمالی بر روی داده‌ها یا سامانه‌های رایانه‌ای تحقق یابد یا از رهگذر اعمالی بر روی شخص نظامی مسئول داده‌ها یا سامانه نظامی نیز قابل تحقق است؟ چنانچه رفتار ارتکابی تنها از رهگذر اعمالی بر روی داده یا سامانه نظامی قابل تحقق باشد، آنگاه اگر مرتکب از شیوه‌های غیر فنی مانند مهندسی اجتماعی که نوعی فریب گفتاری است شخص نظامی را بفریبد و با فریب آن به سامانه رایانه‌ای وارد شود. چنین رفتاری را نمی‌توان مصداق جرم «دسترسی غیرمجاز» دانست. زیرا شرط نقض تدابیر امنیتی به‌صورت فنی رخ نداده است.

چنانچه معیار یا کانون توجه خویش را در جرم «دسترسی غیرمجاز» متمرکز بر رفتار مرتکب یعنی دسترسی از طریق نقض تدابیر امنیتی باشد، نمی‌توان گفت مرتکب که رمز سامانه را یافته و سپس وارد آن شده، مرتکب جرم «دسترسی غیرمجاز» شده است. ولی اگر معیار و کانون توجه در جرم «دسترسی غیرمجاز» متمرکز بر حفظ محرمانگی از موضوع جرم یعنی حمایت از محرمانگی داده‌ها یا سامانه نظامی باشد؛ در اینجا معیار اول کارایی نداشته و رفتارهایی از قبیل مهندسی اجتماعی نمونه‌ای از شیوه‌های دسترسی به داده یا سامانه رایانه‌ای نظامی تلقی می‌شود.

به نظر می‌رسد با توجه به اهمیت داده‌ها و سامانه‌های نظامی معیار دوم که کانون توجه آن روی حمایت از موضوع جرم «دسترسی غیرمجاز» یعنی حفظ محرمانگی داده‌ها یا سامانه‌های رایانه‌ای نظامی قابل‌قبول است، ازاین‌رو، نحوهٔ دستیابی به تدابیر امنیتی موضوعیت ندارد آنچه موضوعیت دارد این است که نقض تدابیر امنیتی صرفاً در بستر فضای سایبر خواه به‌صورت فنی و خواه به‌صورت غیر فنی ارتکاب یابد.[۱]

از حیث تطبیقی می‌توان به بند ۴۴ گزارش توجیهی کنوانسیون بوداپست اشاره کرد. بند ۴۴ هدف از جرم‌انگاری دسترسی غیرمجاز را ایجاد مانعی برای سایر رفتارهای مجرمانه دیگر از قبیل تخریب داده، اخلال در سامانه رایانه‌ای و غیره دانسته است، به نظر می‌رسد نوع ابزار مورداستفاده در جرم دسترسی غیرمجاز موضوعیت نداشته بلکه آنچه دارای اهمیت است صرف دسترسی غیرمجاز به داده‌ها یا سامانه‌های رایانه می‌باشد. در این راستا بند ۴۸ گزارش توجیهی مقرر می‌دارد: «به‌کارگیری

---

۱. نظریه مشورتی شماره ۷/۹۳/۶۵۶ مورخ ۱۳۹۳/۳/۲۴ نیز مؤید این نظر است. متن نظریه بدین شرح است: سؤال در ماده یک قانون جرائم رایانه‌ای اشاره دارد به دسترسی غیر مجاز به داده‌ها. حال منظور از دسترسی غیر مجاز نیست؟ و این دسترسی از رهگذر سامانه‌های رایانه‌ای می‌باشد یا می‌تواند از طریق فیزیکی و اسنادی نیز صورت پذیرد.... پاسخ: با توجه به اطلاق ماده یک قانون جرائم رایانه‌ای، صرف دسترسی غیر مجاز به داده‌ها یا سامانه‌های رایانه‌ای یا مخابراتی که به وسیله تدابیر امنیتی حفاظت شده باشد مشمول مقررات ماده مذکور می‌باشد و طریق دسترسی اعم از مستقیم(فیزیکی) یا به واسطه (از طریق شبکه) تأثیری در قضیه ندارد...».

ابزارهای فنی خاص می‌تواند منجر به دسترسی موضوع ماده (۲) شود، مانند دسترسی مستقیم یا به‌وسیلهٔ پیوندهای فرامتن[1] به صفحهٔ وب که شامل پیوندهای عمیق[2] می‌شود یا استفاده از «کوکی‌ها»[3] یا «بات‌ها»[4] جهت مکان‌یابی و بازیابی اطلاعات به‌جای ارتباطات، به‌کارگیری چنین ابزارهایی به‌خودی‌خود «بدون حق» نیستند. داشتن یک وب‌سایت عمومی، رضایت ضمنی دارنده را مبنی بر دسترسی هر کاربر وب نشان می‌دهد. به‌کارگیری ابزارهای استاندارد تهیه‌شده بر پایهٔ پروتکل‌ها و برنامه‌های ارتباط مشترک، به‌خودی‌خود «بدون حق» نیست، به‌ویژه درجایی که فرض می‌شود صاحب حق سیستم دسترسی یافته، این‌گونه بهره‌برداری را پذیرفته و برای مثال نصب مقدماتی کوکی‌ها را رد و آن‌ها را پاک نکرده است.» به نظر می‌رسد وجود قید «می‌تواند» در بند ۴۸ گزارش توجیهی می‌تواند قرینه‌ای بر این امر باشد که به‌کارگیری ابزارهای فنی خاص در تحقق عنوان مجرمانه دسترسی غیرمجاز شرط نیست. با پذیرش این امر می‌توان گفت مواردی هم چون مهندسی اجتماعی[5] که طی آن افراد می‌توانند دیگران را به انجام کارهای مطلوب خود سوق دهند و با دریافت

---

1. Links Hypertext

هایپرتکست نوعی از یادداشت های مورد تأکید در صفحات وب می‌باشد که به کاربر اجازه می‌دهد با انتخاب آن به صفحه هات دیگر وب متصل گردد.

2. Deep Links

به هایپر تکست‌هایی اطلاق می‌گردد که از نظر ساختاری در رأس قرار داشته و از تعدادی هایپر تکست تشکیل شده است. قابل دسترس در:

https://searchmicroservices.techtarget.com/definition/deep-link

3. Cookies

کوکی ها، تکه‌هایی کوچکی از اطلاعات هستند که وب‌سایت‌ها آن‌ها را را روی سامانه رایانه‌ای کاربر ذخیره می کنند. قابل دسترس در:

http://www.farhangnews.ir/content/43597

4. Bots

بات، یک نرم افزار کاربردی می‌باشد که که یک عمل را به‌طور خودکار انجام می‌دهد. قابل دسترس در:

https://www.cnet.com/how-to/what-is-a-bot

۵. این اصطلاح اغلب به‌منظور توصیف فنون و روش‌هایی به کار می‌رود که افراد برای به دست آوردن اطلاعات حساسی که به آن دسترسی قانونی ندارند به کار می‌برند. از این افراد، اغلب به‌عنوان مهندسان اجتماعی یاد می‌شود و معمولاً آن‌ها کسانی را که دسترسی مشروع به اطلاعات دارند، به افشای این قبیل داده‌ها وادار می‌کنند. همچنین در حوزه امنیت رایانه، مهندسی اجتماعی جهت توصیف مقاصد خرابکارانهٔ افرادی که خواهان دسترسی به داده‌ها و اطلاعات حساس به شیوه غیرقانونی‌اند به کار می‌رود. برای کسب اطلاعات از طریق فنون مهندسی اجتماعی، داشتن ←

گذرواژه از آنان به سامانه‌های رایانه‌ای و داده‌های آنان دسترسی یابند مصداق عنوان مجرمانه دسترسی غیرمجاز قرار گیرند.

در نهایت باید در نظر داشت دسترسی، رفتاری آنی است که در یک‌لحظه به وقوع می‌پیوندد و حائز اهمیت نیست که دسترسی به بخشی از داده‌ها یا سامانه نظامی انجام گیرد یا به همهٔ آن‌ها انجام گیرد.

در خصوص شرایط تحقق جرم دسترسی غیرمجاز در پرتوی ماده ۷۲۹ قانون مجازات اسلامی تعزیرات می‌توان این‌گونه شرح داد که موضوع جرم «دسترسی غیرمجاز» دادهٔ رایانه‌ای و مخابراتی یا سامانه‌های رایانه‌ای است.[۱] موضوعِ جرم «دسترسی غیرمجاز» دارای ویژگی یا وصف حفاظت شده است. بنابراین چنانچه رفتار مجرمانه دسترسی غیرمجاز نسبت به داده‌ها و سامانه‌های رایانه‌ای ارتکاب یابد که فاقد تدابیر امنیتی است، مشمول ماده مذکور نخواهد بود. منظور از «تدابیر امنیتی»، تدابیر فنی و رایانه‌ای است که ممکن است به روش‌ها و شیوه‌های گوناگونی همچون مانند نصب دیوار آتشین، نصب گذرواژه، رمزنگاری و حتی پنهان گذاری انجام گیرد. در بندهای (1)(a)، (2)(a)، (3)(a) و (4)(a) قانون سوءاستفاده و تقلب رایانه‌ای مصوب ۱۹۸۶ آمریکا [۲]و مواد (۱)، (۲) و (۳) قانون جرائم رایانه‌ای مصوب ۱۹۹۰ انگلستان[۳] وجود چنین شرطی لازم و ضروری نیست.

مهارت فنی ضرورت ندارد، اما مهارت‌های اجتماعی لازمهٔ این کار می‌باشد (ر.ک: باگاویتی،جانسوزکی و آندرو ام. کلاریک، ۱۳۹۱: ۱۱۷).

۱. برخی معتقدند که منظور از داده‌ها یا سامانه‌های حفاظت شده، داده‌ها یا سامانه‌های دارای طبقه بندی و حیطه بندی شده بر اساس آیین نامه حفاظت اسناد است (ر.ک: ترکی، ۱۳۸۸: ۱۵). چنین عقیده‌ای مورد اتفاق نظر حقوقدانان نیست.

۲. قانون سوءاستفاده و تقلب رایانه‌ای مصوب ۱۹۸۶ به بیان انواع و ارکان جرم دسترسی غیرمجاز پرداخته است ر.ک به:

Computer Froud and Abuse Act of 1986 (CFAA). Available at:
https://www.congress.gov/bill/99th-congress/house-bill/4718

۳. قانون جرائم رایانه‌ای مصوب ۱۹۹۰، به بیان انواع و ارکان جرم دسترسی غیر مجاز اختصاص یافته است، ر.ک به:

Computer Misuse Act 1990. Available at:
https://www.legislation.gov.uk/ukpga/1990/18/contents

ماده یک قانون جرائم رایانه‌ای مصوب۱۹۹۰، به بیان انواع و ارکان جرم دسترسی غیر مجاز اختصاص یافته است، اما دسترسی غیرمجاز رایانه‌ای به دو نوع دسترسی غیر مجاز ساده و دسترسی غیر مجاز به قصد ارتکاب یا تسهیل ارتکاب جرائم دیگر تقسیم شده است.

رکن قانونی دسترسی غیر مجاز ساده، بند (۱) ماده ۱ قانون جرائم رایانه‌ای انگلستان (مصوب۱۹۹۰) است که مقرر می‌دارد: هر فردی در صورت ارتکاب اعمال زیر مجرم است: (الف) باعث شود که رایانه، عملکردی را با هدف به دست آوردن دسترسی به هر برنامه یا اطلاعاتی که در هر رایانه نگهداری می‌شود، اجرا کند یا دستیابی به چنین دسترسی ←

باید در نظر داشت ماده ۷۲۹ در مقام جرم‌انگاری «دسترسی غیرمجاز» به‌عنوان یک جرم عمومی بوده است، حال‌آنکه هدف نوشتار حاضر حمایت از داده‌ها و سامانه‌های رایانه‌ای نظامی است. ازاین‌رو، شایسته است در مواردی که موضوع جرم داده‌ها و سامانه‌های رایانه‌ای است از وصف «حفاظت‌شدگی داده و سامانه رایانه‌ای به‌وسیله تدابیر امنیتی» صرف‌نظر نموده و برخلاف مادهٔ یادشده واژهٔ «دسترسی» در معنای عام خود و نه خاص خود مدنظر قرار گیرد.

غیرمجاز بودن دسترسی: لازم است که رفتار دسترسی به‌طور غیرمجاز (غیرقانونی) انجام شود. بنابراین در صورتی‌که شخص به‌موجب قانون یا دستورات مقام قضایی یا اجازه از طرف افراد و مقامات مسئول و مجاز مافوق به داده‌ها یا سامانه‌های نظامی دسترسی یابد، عمل وی فاقد وصف جزایی است.

دسترسی غیرمجاز با توجه به صلاحیت شخص نظامی یا میزان دسترسی وی به دو حالت متصور است: حالت اول مربوط به نظامیانی است که صلاحیت دسترسی به حدود معینی از داده‌ها یا بخش‌های مشخصی از سامانه را دارند. حالت دوم مربوط به نظامیانی است که اساساً فاقد مجوز ورود و دسترسی باشد و بااین‌وجود به داده، سامانه‌ها یا حامل‌های داده نفوذ کند، بدون تردید رفتار وی مصداق عنوان مجرمانه «دسترسی غیرمجاز» است. درصورتی‌که شخص نظامی دارای صلاحیت ابتدایی دسترسی به سامانه خاصی را داشته باشد یا حدود صلاحیت وی محدود به فایل‌ها و داده‌های خاص یا بخش مشخصی از سامانه باشد اما پا را فراتر نهاده و به بقیهٔ سامانه یا داده‌ها دسترسی پیدا کند، رفتار وی نیز مصداق عنوان مجرمانهٔ «دسترسی غیرمجاز» قرار خواهد گرفت. این امر در بندهای (1)(a)، (2)(a) و (3)(a) در قانون سوءاستفاده و تقلب رایانه‌ای مصوب ۱۹۸۶ آمریکا نیز مورد توجه قرار گرفته شده است.[1]

را فراهم کند، (ب) دسترسی که او قصد دارد به آن دسترسی دست یابد یا دست‌یابی به آن را فراهم کند، (ب) دسترسی که او قصد دارد به آن دست یابد یا دستیابی به آن را فراهم کند، غیر مجاز باشد و (پ) در زمانی که منجر می‌شود رایانه آن عملکرد را اجرا کند، بداند که دسترسی غیر مجاز است.

در بند (۲) ماده ۱ هم مقرر شده است که نیازی نیست قصد شخص از ارتکاب این جرم ناظر بر برنامه یا اطلاعات به‌خصوص یا از نوع خاص یا در رایانه‌ای خاص باشد. اما رکن قانونی جرم دسترسی غیر مجاز برای ارتکاب جرائم دیگر، ماده ۲ قانون جرائم رایانه‌ای انگلستان(مصوب ۱۹۹۰) است و بند (۱) آن مقرر کرده که هرکس با مقاصد زیر مرتکب دسترسی غیر مجاز شود، مجرم است: (الف) به قصد ارتکاب یکی از جرائم مقرر در مبحث دوم و (ب) به قصد تسهیل ارتکاب جرائم بند الف چه توسط خود او یا هر فرد دیگر.

۱. (1)(a):«هرکس که به طور آگاهانه به یک سامانه رایانه‌ای بدون اجازه یا فراتر از دسترسی که اجازه داده شده است، ←

وسیله و شیوهٔ ارتکاب جرم: ازآنجایی‌که بستر ارتکاب جرائم سایبری فضای سایبر است، بنابر این وسیلهٔ ارتکاب آن افزارهایی هستند که قابلیت آن را دارند در بستر فضای سایبر تدابیر امنیتی داده‌ها و سامانه‌های را نقض کنند. نکته‌ای که در این قسمت می‌توان اشاره نمود این است که نقض تدابیر امنیتی گاهی ممکن است عنوان مجرمانه «دسترسی غیرمجاز» به‌واسطهٔ افزارها به‌صورت حضوری به سامانه نظامی تحقق یابد و گاهی ممکن است به‌صورت غیرحضوری و از طریق اتصال به یک شبکه رایانه‌ای تحقق یابد. این تفکیک در بند ۵۰ گزارش توجیهی کنوانسیون بوداپست مورد توجه قرار گرفته شده است، بند ۵۰ بیان می‌دارد: «اعضاء می‌توانند رویکرد گسترده‌ای اتخاذ کنند و مطابق جمله نخست ماده (۲) صرف هکینگ را جرم‌انگاری کنند. از سوی دیگر، می‌توانند تمام یا بخشی از عناصر کیفی را که در جمله دوم آمده اضافه کنند که عبارت‌اند از: نقض تدابیر امنیتی، داشتن سوءنیت خاص جهت دستیابی به داده‌های رایانه‌ای یا سایر مقاصد ناروایی که اعمال مسؤولیت کیفری را توجیه می‌کند با این شرط که این جرم نسبت به سیستم رایانه‌ای از راه دور متصل به سیستم رایانه‌ای دیگری ارتکاب یابد.» این بند به اعضا اجازه داده است تا وضعیتی را که در آن شخص به‌صورت فیزیکی و بدون به‌کارگیری سامانهٔ رایانه دیگری به یک رایانه مستقل دسترسی یابد، از شمول ماده (۲) استثنا کنند. بنابر این بر اساس قسمتی از بند ۵۰ گزارش توجیهی که مقرر می‌دارد

دسترسی یابد و از طریق این رفتار، اطلاعاتی را که از سوی دولت ایالات متحده بر اساس قانون یا فرمان اجرایی به منظور محافظت در برابر افشای غیر مجاز به دلایل دفاع ملی یا روابط خارجه تعیین شده‌اند یا هر داده محدوده شده مانند آنچه که در بند (y) بخش ۱۱ قانون انرژی اتمی مصوب ۱۹۵۴ بیان شده است را به دست بیاورد، با این قصد یا دلیل که می‌داند چنین اطلاعاتی که این‌گونه به دست آمده‌اند، به منظور آسیب رساندن به ایالات متحده یا به نفع هر دولت خارجه مورد استفاده قرار می‌گیرند، تحصیل کند، مرتکب به جزای نقدی یا حبس حداکثر ده سال یا هر دو مجازات محکوم می‌شود».

(2)(a): «هر کس عامدانه بدون اجازه یا فراتر از دسترسی که اجازه داده شده است به یک سامانه رایانه‌ای دسترسی یابد و در نتیجه آن اطلاعاتی را که شامل سوابق مالی یک مؤسسه مالی، یا سوابق مالی صادر کننده کارت است را به دست آورد، مرتکب به جزای نقدی یا حبس حداکثر ده سال یا هر دو مجازات محکوم می‌شود».

(3)(a): «هرکس عامدانه، بدون اجازه به هر سامانه رایانه‌ای متعلق به وزرات خانه یا نهاد ایالت متحده دسترسی یابد، یا به سامانه‌های رایانه‌ای متعلق به وزارت خانه یا نهادهایی که منحصراً برای استفاده از دولت ایالات متحده است، دسترسی یابد، یا در صورت اینکه سامانه رایانه‌ای انحصاراً برای چنین امری استفاده نشود. ولی سامانه رایانه‌ای از سوی دولت یا برای دولت ایالت متحده مورد استفاده قرار می‌گیرد و چنین رفتاری بر استفاده از عملکرد دولتی چنین سامانه‌هایی تأثیر می‌گذارد، مرتکب به جزای نقدی یا حبس حداکثر ده سال یا هر دو مجازات محکوم می‌شود».

«...با این شرط که این جرم نسبت به سیستم‌های رایانه‌ای از راه دور متصل به سیستم رایانه‌ای دیگری ارتکاب یابد... .» به نظر می‌رسد کنوانسیون درصدد تفکیک فضای سایبر به دو زیرفضای سایبری میان کاربر با سامانه رایانه‌ای و زیرفضای سایبری میان سامانه‌های رایانه‌ای با یکدیگر برآمده است و بر اساس این تفکیک به اعضا اجازه داده است که ارتکاب جرم دسترسی غیرمجاز در زیرفضای سایبری میان کاربر با سامانه رایانه‌ای از شمول ماده (۲) استثنا کنند و تنها ارتکاب جرم دسترسی غیرمجاز در زیر فضای سایبری میان سامانه‌های رایانه‌ای با یکدیگر مشمول ماده (۲) قرار دهند. با توجه به اینکه کانون توجه پژوهش حاضر حمایت کیفری از داده‌ها و سامانه‌های رایانه‌ای نظامی است، شایسته است تحقق دسترسی غیرمجاز در هر دو زیرفضا نسبت به داده‌ها و سامانه‌های رایانه‌ای نظامی جرم‌انگاری شود.

برای مثال ممکن است مرتکب در محل استقرار داده یا سامانهٔ نظامی حضور یافته و مرتکب جرم «دسترسی غیرمجاز» شود، گاهی ممکن است در اتاقش از طریق شبکه رایانه‌ای به داده یا سامانه نظامی متصل و به شبکهٔ رایانه‌ای نفوذ یافته و مرتکب جرم «دسترسی غیرمجاز» شود. همان‌طور که اشاره شد آنچه از جرم‌انگاری عنوان مجرمانهٔ «دسترسی غیرمجاز» مدنظر است حفظ محرمانگی داده‌ها، حامل‌های داده و سامانه‌های نظامی است، بنابراین مطلق دسترسی به هر نحو را باید جرم‌انگاری شود و وسیله یا شیوهٔ ارتکاب در این جرم موضوعیت ندارد.

نتیجه مجرمانه: در جرم دسترسی غیرمجاز قانون‌گذار حصول نتیجه‌ای را در آن شرط ندانسته، همین‌که فرد به داده و سامانه دسترسی یافت، کفایت می‌کند.[۱] اما می‌توان در شرایطی که منجر به نتیجه‌ی خاصی می‌شود همانند بندهای (1)(a)، (2)(a)،(3)(a) و (4)(a) قانون سوءاستفاده و تقلب رایانه‌ای مصوب ۱۹۸۶ آمریکا و یا همانند ماده ۲ قانون سوءاستفاده رایانه‌ای مصوب ۱۹۹۰ انگلستان[۲] چنانچه دسترسی با قصد خاصی انجام می‌شود به‌عنوان کیفیات مشدده، در نظر گرفته

---

۱. برخی معتقدند «دسترسی غیر مجاز» از جرائم مقید است که نتیجه آن دست یافتن و احاطه و تسلط بر سامانه دیگری است (ر.ک: بای و پورقهرمانی، ۱۳۸۸: ۱۹۶). چنین عقیده ای مورد اتفاق حقوق‌دانان نیست.

از حیث رویه قضایی می‌توان به رأی صادر شده از شعبه ۱۰۳۳ دادگاه عمومی جزائی تهران اشاره کرد: «در خصوص اتهام آقای علی ... دایر بر دسترسی غیرمجاز به داده‌ها برابر کیفرخواست صادره از دادسرای عمومی و انقلاب تهران با بررسی جامع اوراق و محتویات پرونده و ... با احراز بزهکاری متهم و با استناد به ماده ۷۲۹ قانون مجازات اسلامی با اعمال ماده ۲۲ قانون مذکور به لحاظ گذشت شاکی و اعلام پشیمانی به پرداخت سه میلیون ریال جزای نقدی محکوم می‌نماید،... ».

2. Computer Misuse Act 1990. Available at:

شوند. برای مثال در فرضی که مرتکب علاوه بر «دسترسی غیرمجاز» به داده‌های نظامی آن‌ها را پردازش می‌کند یا موجب شود سامانهٔ نظامی فعالیتی انجام دهد، به مجازت شدیدتری محکوم شود، نسبت به فرضی که مرتکب صرفاً به داده‌ها، حامل‌های داده یا سامانه‌های رایانه‌ای دسترسی یافته است. همچنین است، هرگاه شخص نظامی به‌قصد تخریب داده‌های رایانه‌ای مرتکب جرم دسترسی غیرمجاز به سامانه رایانه‌ای شود.

۱-۲-۳. رکن معنوی جرم دسترسی غیرمجاز در حقوق کیفری ایران

پیرامون رکن معنوی باید گفت در هر جرم عمدی، سوءنیت عام الزامی است. در جرم «دسترسی غیرمجاز» ابتدا لازم است مرتکب بداند متعلق رفتار وی داده، حامل داده یا سامانهٔ رایانه‌ای نظامی است (علم به موضوع و اوصاف آن) و نداشتن اجازه از سوی مقام ذی‌صلاح (علم به شرایط) است. منظور از سوءنیت عام این است که شخص نظامی، قصد رفتار «دسترسی غیرمجاز» به داده‌ها، حامل‌های داده یا سامانه‌های رایانه‌ای نظامی داشته باشد. جرم «دسترسی غیرمجاز» یک جرم مطلق است و نیاز به حصول نتیجه ندارد، بنابر این چنانچه دسترسی به داده و سامانه‌ها به‌قصد کنجکاوی، کسب مال، کسب شهرت، فرار از خدمت، ربودن یا تخریب داده ارتکاب یابد، حائز اهمیت نیست،

---

https://www.legislation.gov.uk/ukpga/1990/18/contents.

ماده (۱) شخصی مرتکب جرمی شده است اگر -

(الف) او باعث شود یک سامانه رایانه‌ای تا هر عملکردی را با هدف دسترسی ایمن به هر برنامه یا داده ای که در هر سامانه رایانه‌ای نگهداری می‌شود، انجام دهد؛

(ب) دسترسی او به سامانه رایانه‌ای غیرمجاز باشد؛ و

(ج) در زمانی که کامپیوتر را وادار به انجام عملکردی می‌کند، علم به رفتار مجرمانه خویش دارد.

ماده (۲) قصدی که یک شخص برای ارتکاب جرمی طبق این بخش باید داشته باشد، نیاز نیست که مستقیم باشد-

(الف) هر برنامه یا داده خاصی؛

(ب) یک برنامه یا داده از هر نوع خاص؛ یا

(ج)) برنامه یا داده‌ای که در هر رایانه خاصی نگهداری می شود.

(۳) شخصی که به موجب این بخش مرتکب جرم شده است، به حبس برای مدت حداکثر تا شش ماه یا به جزای نقدی درجه ۵ ا یا به هر دو محکوم خواهد شد.

۱-۲- اگر شخصی مرتکب جرمی طبق بند ۱ فوق شود (غیر مجازجرم دسترسی) با قصد دسترسی-

(الف) برای ارتکاب جرمی که این بخش در مورد آن اعمال می شود؛ یا

(ب) برای تسهیل ارتکاب چنین جرمی (چه توسط خودش یا توسط هر شخص دیگری)؛ و جرمی که او قصد ارتکاب یا تسهیل آن را دارد تحت عناوین مجرمانه این بخش باشد.

آنچه اهمیت دارد حفظ محرمانگی داده، حامل داده و سامانه‌ی رایانه‌ای نظامی است.[۱]

۲. سیاست کیفری ایران در قبال دسترسی غیرمجاز به داده‌ها و سامانه‌های رایانه‌ای فاقد طبقه‌بندی نظامی

دسترسی غیرمجاز به داده‌ها و سامانه‌های رایانه‌ای فاقد طبقه‌بندی نظامی می‌تواند از سوی اشخاص نظامی و غیرنظامی ارتکاب یابد. بدین منظور در این قسمت ابتدا به سیاست کیفری ایران در قبال دسترسی غیرمجاز به داده‌ها و سامانه‌های رایانه‌ای فاقد طبقه‌بندی از سوی اشخاص نظامی (۲-۱) و سپس به سیاست کیفری ایران در قبال دسترسی غیرمجاز به داده‌ها و سامانه‌های رایانه‌ای فاقد طبقه‌بندی از سوی اشخاص غیرنظامی (۲-۲) پرداخته شده است.

۲-۱. سیاست کیفری ایران در قبال دسترسی غیرمجاز به داده‌ها و سامانه‌های رایانه‌ای فاقد طبقه‌بندی از سوی اشخاص نظامی

به‌طورکلی در سیر تاریخی نسبتاً طولانی، عواملی موجب ایجاد بسترهایی در راستای افتراقی شدن دادرسی شده‌اند. افتراقی‌سازی تقنینی سیاست جنایی غالباً در چارچوب سه معیار، گونه‌شناسی جرائم، گونه‌شناسی بزهکاران و گونه‌شناسی بزه‌دیدگان صورت گرفته است (پاک‌نیت، ۱۳۹۶: ۳۴-۳۲). در افتراقی‌سازی بر اساس گونهٔ بزهکاری، فرد بزهکار مبنا و ملاک قرار داده می‌شود نه بر اساس نوع جرم یا شخصیت بزه‌دیده. به‌طورکلی دو رویکرد افتراقی کردن بر مبنای شخصیت بزهکار قابل اتخاذ است که عبارت‌اند از رویکرد حمایتی و رویکرد سخت‌گیرانه. در رویکرد اخیر از برخی حقوق اولیه و اساسی متهم عدول می‌شود. مثال بارز آن در حوزهٔ نظامی است که یکی از ارکان حیاتی و حساس حکومت محسوب می‌شود، انتظار این است که کوچک‌ترین تخطی، تخلف و جرم می‌تواند تبعات و آثاری به‌مراتب سنگین‌تر و وسیع‌تر نسبت به حوزه‌های دیگر خواهد داشت اما مقنن به این رویکرد در اغلب موارد توجهی نداشته است.

سیاست کیفری ایران در قبال تحقق عنوان مجرمانهٔ دسترسی غیرمجاز به داده‌های فاقد طبقه‌بندی نظامی بدین نحو است که مرتکب مطابق بند (الف) ماده ۷۵۴ ق.م.ا به بیش از دوسوم حداکثر یک یا دو مجازات پیش‌بینی‌شده در ماده ۷۲۹ قانون مجازات اسلامی محکوم خواهد شد.

---

۱. شایان ذکر است، در حقوق انگلستان دسترسی غیرمجاز به دو نوع دسترسی غیرمجاز ساده و دسترسی غیرمجاز به قصد ارتکاب یا تسهیل ارتکاب جرائم دیگر تقسیم شده است. در بند (۱) ماده ۲ قانون جرائم رایانه‌ای انگلستان (مصوب ۱۹۹۰) مقرر شده است که هرکس با مقاصد زیر مرتکب دسترسی غیر مجاز شود، مجرم است: (الف) به قصد ارتکاب یکی از جرائم مقرر در مبحث دوم و (ب) به قصد تسهیل ارتکاب جرائم بند الف چه توسط خود او یا هر فرد دیگر. در حالی‌که در حقوق ایران دسترسی غیرمجاز به قصد ارتکاب یا تسهیل جرائم دیگر پیش‌بینی نشده است.

اولین ایراد و اشکال وارد بر سیاست کیفری ایران در قبال دسترسی غیرمجاز به داده‌های رایانه‌ای فاقد طبقه‌بندی از سوی اشخاص نظامی این است که چون قانون‌گذار حداکثر مجازات را افزایش نداده است بلکه حداقل آن را افزایش داده است، این امر سبب می‌شود اگر یک شخص غیرنظامی به داده‌ها و سامانه‌های رایانه‌ای غیرنظامی را دسترسی یابد و مقام قضایی وی را به اشد مجازات محکوم کند، مجازات وی با مجازات شخص نظامی که به داده‌ها و سامانه‌های نظامی دسترسی یابد، از حیث حداکثر مجازات یکسان است که شایسته است میزان درجهٔ اهمیت داده‌ها و اطلاعات نظامی به‌موجب دستورالعملی از سوی ستاد کل نیروهای مسلح تدوین شود تا مجازات مرتکب تابع درجهٔ اهمیت داده‌ها و اطلاعات رایانه‌ای نظامی باشد.

ایراد دوم به سیاست کیفری فعلی این است که مطابق ماده ۲ قانون مجازات جرائم نیروهای مسلح و تبصرهٔ آن، جرائمی که مجازات آن‌ها در قانون مذکور ذکر شده، در تخفیف و تبدیل نیز تابع ترتیبات همین قانون است و در غیر این موارد، تخفیف و تبدیل تابع همان قانونی است که تعیین کیفر مطابق آن صورت گرفته است. چون عنوان مجرمانهٔ دسترسی غیرمجاز در قانون مجازات جرائم نیروهای مسلح پیش‌بینی نشده است، از حیث تخفیف و تبدیل تابع قانون مجازات اسلامی است. ولی چون جرمی مانند جعل رایانه‌ای که از سنخ جرائم رایانه‌ای است و در قانون مجازات جرائم نیروهای مسلح پیش‌بینی شده است، از حیث تخفیف و تبدیل تابع قانون مجازات جرائم نیروهای مسلح است. بدیهی است اتخاذ چنین سیاست کیفری افتراقی از سوی مقنن قابل توجیه نمی‌باشد. همچنین باید در نظر داشت قوانین خاص هر یک با هدف و فلسفهٔ خاصی وضع می‌شوند؛ ق.م.ج.ن.م به‌عنوان یک قانون خاص نیز دارای چنین ویژگی است؛ هدف این قانون آن است که برای جرائم نظامیان با توجه به حساسیت وظایف آنان، نظام کیفری خاصی تعیین و مجازات‌های قانونی را تشدید کند. با تسری قواعد قانون جرائم رایانه‌ای بر جرائم نظامیان، هدف و فلسفهٔ وضع ق.م.ج.ن.م نادیده گرفته می‌شود.

۲-۲. سیاست کیفری ایران در قبال دسترسی غیرمجاز به داده‌ها و سامانه‌های رایانه‌ای فاقد طبقه‌بندی از سوی اشخاص غیرنظامی

مقنن به اعتبار تعلق داده‌های رایانه‌ای به دولت، نهادها و مراکز ارائه‌دهنده خدمات عمومی نیز سیاست کیفری افتراقی اتخاذ کرده است. بدین نحو که چنانچه دسترسی غیرمجاز به داده‌های فاقد طبقه‌بندی نظامی تحقق یابد. مطابق بند (ج) ماده ۷۵۴ قانون مجازات اسلامی مرتکب به بیش از دوسوم حداکثر یک یا دو مجازات پیش‌بینی‌شده در ماده ۷۲۹ قانون مجازات اسلامی محکوم خواهد شد.

ایراد و اشکال وارد بر سیاست کیفری ایران این است که چون قانون‌گذار حداکثر مجازات را

افزایش نداده است بلکه حداقل آن را افزایش داده است، این امر سبب می‌شود اگر یک شخص غیرنظامی به داده‌های رایانه‌ای غیرنظامی دسترسی یابد و مقام قضایی وی را به حداکثر مجازات محکوم کند، مجازات وی در وضعیتی که به داده‌های رایانه‌ای نظامی دسترسی یابد، از حیث حداکثر مجازات یکسان است. شایسته است میزان درجهٔ اهمیت داده‌ها و اطلاعات نظامی به‌موجب دستورالعملی از سوی ستاد کل نیروهای مسلح تدوین شود تا مجازات مرتکب تابع درجه اهمیت داده‌ها و اطلاعات رایانه‌ای نظامی از بازدارندگی برخوردار باشد.[۱]

۳. سیاست کیفری ایران در قبال دسترسی غیرمجاز به داده‌ها و سامانه‌های طبقه‌بندی‌شده رایانه‌ای نظامی

دسترسی غیرمجاز به داده‌ها و سامانه‌های رایانه‌ای طبقه‌بندی‌شده نظامی می‌تواند از سوی اشخاص نظامی و غیرنظامی ارتکاب یابد. بدین منظور در این قسمت ابتدا به سیاست کیفری ایران در قبال دسترسی غیرمجاز به داده‌ها و سامانه‌های رایانه‌ای طبقه‌بندی‌شده رایانه‌ای نظامی از سوی اشخاص نظامی (۱-۳) و سپس به سیاست کیفری ایران در قبال دسترسی غیرمجاز به داده‌ها و سامانه‌های رایانه‌ای طبقه‌بندی‌شده رایانه‌ای نظامی از سوی اشخاص غیرنظامی (۲-۳) پرداخته شده است.

۳-۱. سیاست کیفری ایران در قبال دسترسی غیرمجاز به داده‌ها و سامانه‌های طبقه‌بندی‌شده رایانه‌ای نظامی از سوی اشخاص نظامی

حقوق کیفری نظامی در راستای حمایت از داده‌ها و اطلاعات طبقه‌بندی‌شده[۲] رایانه‌ای در برابر جاسوسی رایانه‌ای در ماده ۱۳۱ قانون مجازات جرائم نیروهای مسلح رفتار مجرمانه «تسلیم اطلاعات طبقه‌بندی‌شده رایانه‌ای» به‌عنوان یک جرم نظامی از سوی اشخاص نظامی را پیش‌بینی کرده است که بر اساس مراحل سه‌گانهٔ جاسوسی می‌توان گفت که صرفاً ناظر بر مرحلهٔ نهایی جاسوسی رایانه‌ای (ارائهٔ

---

۱. قانون مجازات اسلامی در ماده ۷۳۹ مقرر می‌دارد: «هرکس به قصد به خطر انداختن امنیت، آسایش و امنیت عمومی اعمال مذکور در مواد (۸)، (۹) و (۱۰) این قانون را علیه سامانه‌های رایانه‌ای و مخابراتی که برای ارائه خدمات ضروری عمومی به کار می‌روند، از قبیل خدمات درمانی، آب، برق، گاز، مخابرات، حمل و نقل و بانکداری مرتکب شود، به حبس از سه تا ده سال محکوم خواهد شد». شایسته است مقنن در قانون مزبور همانند ماده ۷۳۹ در ماده مستقلی به حمایت از داده‌ها و سامانه‌های رایانه‌ای نظامی از سوی اشخاص غیرنظامی در برابر رفتارهای مجرمانه بپردازد و سیاست کیفری افتراقی اتخاذ کند.

۲. طبقه بندی اسناد بر اساس میزان ارزش حفاظتی اسناد و مدارک و اهمیت خطرات ناشی از افشای آن‌ها برای کشور صورت می‌گیرد. تعیین طبقه بندی عبارت است از قرار دادن سند در یکی از چهار نوع طبقه بندی (به کلی سری، سری، خیلی محرمانه و محرمانه) به منظور حفظ سند و تعیین محدودیت‌های لازم جهت دسترسی به آن و جلوگیری از افشا و دسترسی غیر مجاز. (ر.ک: مهرانفر و قلی‌پورشهرکی، ۱۳۹۹: ۱۴۵ و میرمحمدصادقی، ۱۳۹۳: ۱۱۰).

اطلاعات جمع‌آوری‌شده یا تجزیه تحلیل آن‌ها) است و شامل مرحلهٔ اول جاسوسی یعنی دسترسی غیرمجاز به اطلاعات طبقه‌بندی‌شده رایانه‌ای نمی‌شود.[۱] این رویکرد قانون‌گذار با چالش‌ها و ابهاماتی مواجه است از قبیل اینکه چنانچه شخص نظامی مرتکب جرم دسترسی غیرمجاز به اطلاعات طبقه‌بندی‌شده رایانه‌ای شود، آیا می‌توان رفتار وی را مصداق جرم جاسوسی رایانه‌ای محسوب کرد؟ پاسخ به این پرسش ازاین‌جهت حائز اهمیت است که اگر رفتار وی مصداق جاسوسی رایانه‌ای قرار گیرد، کیفیات مخففه یا نهادهای ارفاقی از قبیل تعویق صدور حکم، تعلیق اجرای مجازات و... نسبت به وی قابل اعمال نیست؛ در غیر این‌صورت مرتکب می‌تواند از آن‌ها بهره‌مند شود. پرسش دیگر این است آیا سیاست کیفری ایران در برابر رفتار مجرمانهٔ دسترسی غیرمجاز به اطلاعات طبقه‌بندی‌شده رایانه‌ای از سوی اشخاص نظامی متناسب و بازدارنده است؟

برای پاسخ به پرسش‌های بنیادین مطروحه ابتدا باید بیان کرد بر اساس مفهوم ارائه‌شده از دسترسی غیرمجاز، دسترسی غیرمجاز شیوه سایبری ورود به محل نگهداری اسناد و اطلاعات موضوع بند (د) ماده ۲۴ قانون مجازات جرائم نیروهای مسلح است. بدین‌سان برخی قضات محاکم نظامی معتقد بودند که بند (د) ماده ۲۴ ق.م.ج.ن.م اطلاق دارد و در حدود شرایط ماده قسمتی از نقص قانونی را پوشش می‌دهد. نقدی که بر این نظر می‌تواند وارد باشد این است که قانون‌گذار در بند (الف) ماده ۲۴ از عبارت (... در اختیار دشمن یا بیگانه قرار دهد...) و در بند (ج) ماده مزبور از عبارت (... تسلیم اسرار نظامی و یا آن‌ها را از مفاد آن آگاه سازد) و در ماده ۲۶ قانون مزبور از عبارت (در اختیار قرار دادن اسناد، مذاکرات، تصمیمات یا اطلاعات طبقه‌بندی‌شده به افرادی که صلاحیت اطلاع نسبت به آن‌ها را ندارند یا به هر نحو آنان را از مفاد آن مطلع سازد) به‌طور مطلق استفاده کرده است ولی بااین‌وجود در ماده ۱۳۱ قانون‌گذار به رفتار مجرمانه تسلیم اطلاعات طبقه‌بندی‌شده رایانه‌ای اشاره کرده است. درواقع، می‌توان گفت قانون‌گذار در ماده ۱۳۱ در مقام تسری کیفر جرائم سنتی به برخی از جرائم جدید مرتبط با رایانه یعنی خود رایانه و داده و حامل‌های داده بوده است. بنابراین به نظر می‌رسد در پرتو اصل قانونی جرائم و مجازات‌ها و لزوم تفسیر مضیق

---

۱. شایان ذکر است قانون‌گذار در بندهای (الف)، (ب) و (ج) ماده ۳ قانون جرائم رایانه‌ای (ماده ۷۳۱ قانون مجازات اسلامی) مراحل سه‌گانه دسترسی غیرمجاز ، تحصیل غیر مجاز یا در دسترس قرار دادن داده‌های سری را تحت عنوان مجرمانه «جاسوسی رایانه‌ای» پیش‌بینی کرده است. همچنین قانون‌گذار در بندهای «الف»، «ب»، «ج» و «د» ماده ۲۴ قانون مجازات جرائم نیروهای مسلح مراحل سه گانه ورود غیر مجاز به محل نگهداری اسناد و اطلاعات طبقه‌بندی شده، تحصیل و تسلیم آن‌ها را در فضای سنتی (جاسوسی سنتی) پیش‌بینی کرده است. (در خصوص تحصیل غیرمجاز داده‌های رایانه‌ای نظامی ر.ک: مرسی و زرنگ، ۱۴۰۲).

قوانین کیفری نمی‌توان به اطلاق جرائم سنتی برای مجازات مرتکب جرائم رایانه‌ای تمسک جست مگر در موارد مصرح در ماده ۱۳۱ قانون مجازات جرائم نیروهای مسلح.

برخی از قضات محاکم نظامی معتقد بودند که قانون‌گذار در ماده ۱۳۱ از عبارت (اقداماتی از قبیل ...) استفاده کرده است که نظر به تمثیلی بودن موارد مزبور در ماده ۱۳۱ داشته و شامل دسترسی غیرمجاز به داده‌های طبقه‌بندی‌شده رایانه‌ای نیز می‌شود و مرتکب به مجازات پیش‌بینی‌شده در بند (د) ماده ۲۴ قانون مجازات جرائم نیروهای مسلح محکوم می‌شود. این عقیده قابل‌پذیرش است و می‌توان رفتار شخص نظامی را مصداق بند (د) ماده ۲۴ قانون مجازات جرائم نیروهای مسلح دانست. اما باید در نظر داشت، ذکر عباراتی مانند امثالهم، نظایر آن و از قبیل آن به‌ویژه در حقوق کیفری با اصل شفافیت قانون و حقوق متهم تنافی دارد؛ چراکه افراد باید بدانند تکلیفشان در برابر رفتارهایی که انجام می‌دهند چیست. قانون‌گذار نمی‌تواند خودش را رها بکند از اینکه به‌طور شفاف مقصود خودش را از مخاطبانش بخواهد. همچنین این عبارت‌ها می‌توانند توسط نهادهای رسیدگی به‌طور موسع تفسیر شوند و منجر به تشت آرای قضایی نیز بشوند و در نهایت استفاده از این قبیل عبارات با اصل قانونی بودن جرائم و مجازات‌ها مغایرت دارد و اتخاذ چنین رویه‌ای در قانون‌گذاری شایسته نیست. به‌ویژه در جرائمی که دارای مجازات‌های حبس‌های طولانی‌مدت یا سلب حیات هستند. بااین‌وجود به نظر می‌رسد با توجه به لزوم تفسیر مضیق قوانین کیفری و رعایت حقوق متهم موضوع رفتارهای تمثیلی را باید محدود به داده‌ها و سامانه‌های رایانه‌ای طبقه‌بندی‌شده رایانه‌ای دانست.[۱]

ایراد وارد بر سیاست کیفری فعلی ایران این است که در بند «الف» ماده ۷۳۱ قانون مجازات اسلامی شخصیت طرف مقابل به «دشمن» یا «بیگانه» مقید نشده است، درحالی‌که در بند «د» ماده ۲۴ قانون مجازات جرائم نیروهای مسلح شخصیت طرف مقابل به نفع «دشمن» یا «بیگانه» مقید شده است. بنابر این اگر شخص نظامی به نفع دشمن یا بیگانه نسبت به داده‌ها یا اطلاعات رایانه‌ای طبقه‌بندی‌شده مرتکب جرم دسترسی غیرمجاز نشود، رفتار وی از شمول بند «د» ماده ۲۴ قانون مجازات جرائم نیروهای مسلح خارج است و به‌شرط آن‌که موضوع رفتار وی داده‌های سری باشد، عمل وی مشمول بند (الف) ماده ۷۳۱ قانون مجازات اسلامی و مصداق جاسوسی رایانه‌ای است. اما اگر در فرض اخیر موضوع رفتار وی داده‌های به‌کلی سری، خیلی محرمانه و محرمانه نظامی

---

۱. دسترسی و مطالعه آرا قضایی نظامی و درج آن‌ها در پژوهش حاضر با توجه به ماهیت موضوع و محرمانه بودن پرونده‌ها از نظر سازمان قضایی نیروهای مسلح، با محدودیت هایی مواجه گردید. در این میان به منظور شناخت رویکرد قضات محاکم نظامی نسبت به جرم دسترسی غیرمجاز از سوی اشخاص نظامی تلاش شد با پرسش شفاهی به صورت مصاحبه نظر آن‌ها اخذ شود.

باشد، در این فرض اساساً رفتار وی جاسوسی نبوده بلکه مصداق جرم دسترسی غیرمجاز قرار می‌گیرد. نتیجهٔ قهری این رویکرد این است، ازآنجایی‌که کیفیات مخففه یا نهادهای ارفاقی از قبیل تعویق صدور حکم، تعلیق اجرای مجازات و ... در خصوص جرائم علیه امنیت داخلی و خارجی ازجمله جاسوسی قابل اعمال نیستند. در فرض اول که متعلق رفتار وی داده‌های سری رایانه‌ای است، اعمال کیفیات مخففه و نهادهای ارفاقی قابل اعمال نیستند اما در فرض اخیر حتی اگر متعلق رفتار وی داده‌های به‌کلی سری که از درجه اهمیت بالاتری نسبت به داده‌های سری برخوردارند باشد، مرتکب می‌تواند از کیفیات مخففه و نهادهای ارفاقی طبق قانون مجازات اسلامی بهره‌مند شود.

۳-۲. سیاست کیفری ایران در قبال دسترسی غیرمجاز به داده‌ها و سامانه‌های طبقه‌بندی‌شده رایانه‌ای نظامی از سوی اشخاص غیرنظامی

در قانون جرائم رایانه‌ای مقنن در قسمت صدر و بند (الف) ماده ۳ قانون جرائم رایانه‌ای (ماده ۷۳۱ قانون مجازات اسلامی) به دلیل اهمیت داده‌ها و اطلاعات سری رایانه‌ای که امنیت کشور وابسته به آن‌ها است، دسترسی غیرمجاز به این داده‌ها و اطلاعات را تحت عنوان مجرمانه «جاسوسی رایانه‌ای» جرم انگاری کرده است. قانون‌گذار در بند (الف) ماده ۷۳۱ قانون مجازات اسلامی، صرفاً دسترسی یک قسم از طبقه‌بندی اطلاعات رایانه‌ای یعنی داده‌های سری را مصداق جاسوسی رایانه‌ای و جرمی علیه امنیت داخلی و خارجی تلقی کرده است و دسترسی غیرمجاز به سایر اقسام طبقه‌بندی اطلاعات از قبیل به‌کلی سری، خیلی محرمانه و محرمانه، مصداق جاسوسی ندانسته است.

ایراد اول وارد بر سیاست کیفری ایران در قبال دسترسی غیرمجاز به اطلاعات رایانه‌ای طبقه‌بندی‌شده نظامی از سوی اشخاص غیرنظامی این است که قانون‌گذار در ماده ۷۳۱ تنها داده‌های سری را مصداق جاسوسی رایانه‌ای دانسته است و سایر اشکال طبقه‌بندی اطلاعات رایانه‌ای را مصداق جاسوسی ندانسته است. بنابر این اگر یک شخص غیرنظامی به داده‌ها و اطلاعات رایانه‌ای به‌کلی سری نظامی دسترسی یابد، مطابق بند (ج) ماده ۷۵۴ قانون مجازات اسلامی به بیش از دوسوم حداکثر یک یا دو مجازات مقرر در ماده ۷۲۹ قانون مجازات اسلامی محکوم می‌شود و چون رفتار وی مصداق جاسوسی نیست می‌تواند از کیفیات مخففه و نهادهای ارفاقی مطابق قانون مجازات اسلامی بهره‌مند شود.

ممکن است استدلالی بدین نحو مطرح شود که مقصود از عبارت «داده‌های سری»، اطلاعات طبقه‌بندی شده است و این عبارت در مقابل عبارت «داده‌های فاقد طبقه‌بندی» قرار می‌گیرد که در این صورت در راستای رد این استدلال می‌توان گفت که اطلاعات طبقه‌بندی‌شده ازلحاظ اهمیت در چهار دسته قرار می‌گیرند و اگر مقصود مقنن از عبارت «داده‌های سری»، اطلاعات طبقه‌بندی‌شده

باشد، می‌بایست در خصوص تعیین مجازات نیز اهمیت اطلاعات طبقه‌بندی‌شده را لحاظ می‌نمود و برای اطلاعات به‌کلی سری، مجازات شدیدتری را نسبت به اطلاعات محرمانه در نظر می‌گرفت که در این ماده چنین امری صورت نگرفته است.

ایراد دوم وارد بر سیاست کیفری ایران در قبال دسترسی غیرمجاز به اطلاعات طبقه‌بندی‌شده رایانه‌ای نظامی از سوی اشخاص غیرنظامی این است که امروزه فضای سایبر امکاناتی را فراهم آورده است تا دشمنان و بیگانگان بدون خطراتی که جاسوسی سنتی به همراه داشت به داده‌ها و اطلاعات طبقه‌بندی‌شده رایانه‌ای نظامی دسترسی یابند و امنیت کشور را به مخاطره می‌اندازد. شایسته است مقنن همانند بند (هـ) ماده ۲۴ قانون مجازات جرائم نیروهای مسلح در برابر داده‌ها و اطلاعات طبقه‌بندی‌شده رایانه‌ای نظامی که ممکن است از آن‌سوی مرزها توسط دشمنان و بیگانگان به‌واسطه دسترسی غیرمجاز به آن‌ها محرمانگی آن‌ها نقض شوند، چاره‌اندیشی کند.[۱] در اهمیت این امر می‌توان به بدافزار استاکس‌نت[۲] در سال ۱۳۸۹، دوکو[۳] در سال ۱۳۹۰و فلیم[۴] در سال۱۳۹۱ علیه نیروگاه‌های هسته‌ای ایران و حملات سایبری علیه سازمان بنادر و کشتیرانی سال ۱۳۹۹، زندان اوین ۱۴۰۰، شرکت هواپیمایی ماهان۱۴۰۰، صدا و سیما ۱۴۰۰ و سازمان فرهنگ و ارتباطات اسلامی ۱۴۰۱ اشاره کرد،[۵] که به داده‌ها و اطلاعات طبقه‌بندی‌شده رایانه‌ای دسترسی یافته بودند.

یک استدلال می‌تواند این‌گونه مطرح شود که می‌توان به اطلاق بند (هـ) ماده ۲۴ تمسک جست. در نقد این عقیده می‌توان گفت قانون‌گذار در ماده ۱۳۱ در مقام تسری کیفر جرائم سنتی به برخی از جرائم جدید مرتبط با رایانه یعنی خود سامانه رایانه‌ای، داده و حامل‌های داده بوده است. بنابر این به نظر می‌رسد در پرتو اصل قانونی جرائم و مجازات‌ها و لزوم تفسیر مضیق قوانین کیفری نمی‌توان به اطلاق جرائم سنتی برای مجازات مرتکب جرائم رایانه‌ای تمسک جست مگر در موارد مصرح در ماده ۱۳۱ قانون مجازات جرائم نیروهای مسلح.

استدلال دیگری که می‌تواند مطرح شود این است که قانون‌گذار در ماده ۱۳۱ از عبارت (اقداماتی از قبیل ...) استفاده کرده است که نظر به تمثیلی بودن موارد مزبور در ماده ۱۳۱ داشته و شامل دسترسی غیرمجاز داده‌های طبقه‌بندی‌شده رایانه‌ای نیز می‌شود و مرتکب به مجازات پیش‌بینی‌شده در بند (هـ) ماده ۲۴ قانون مجازات جرائم نیروهای مسلح محکوم می‌شود. در نقد این عقیده می‌توان

---

۱. در خصوص ضرورت‌سنجی جرم‌انگاری حملات سایبری در حقوق کیفری ایران ر.ک به: بهره‌مند و مرسی، ۱۴۰۱.

2. Stuxnet
3. Duqu
4. Flame
5. https://www.tasnimnews.com/fa/news/1401/06/20/2772788

گفت که در ماده ۱۳۱ به‌صراحت شخصیت مرتکب به شخص نظامی مقید شده است و در پرتو اصل قانونی بودن جرائم و مجازات‌ها و لزوم تفسیر مضیق قوانین کیفری نمی‌توان آن را به اشخاص غیرنظامی تسری داد.

بدیهی است سیاست کیفری فعلی ایران در قبال حمایت از داده‌ها و سامانه‌های رایانه‌ای نظامی در برابر رفتار مجرمانه دسترسی غیرمجاز متناسب و بازدارنده نمی‌باشد؛ چراکه نتیجهٔ قهری چنین سیاست کیفری این است که از نظر قانون‌گذار در فرضی که بیگانه‌ای به‌طور غیرمجاز به داده‌های رایانه‌ای سری نظامی دسترسی می‌یابد، مطابق بند (الف) ماده ۷۳۱ قانون مجازات اسلامی رفتار وی جاسوسی رایانه‌ای بوده و در فرض دیگر، اگر بیگانه‌ای به‌طور غیرمجاز به داده‌های رایانه‌ای نظامی به‌کلی سری دسترسی یابد، رفتار وی مصداق جاسوسی نبوده و صرفاً با رعایت ماده ۷۵۴ قانون مجازات اسلامی به مجازات‌های پیش‌بینی‌شده در ماده ۷۳۰ قانون مجازات اسلامی محکوم می‌شود. شایسته است مقنن جهت برون‌رفت از چنین سیاست کیفری نامتناسب و ناکارآمدی با پیش‌بینی جرم دسترسی غیرمجاز به داده طبقه‌بندی‌شده رایانه‌ای در قانون مجازات جرائم نیروهای مسلح در پرتوی بند (هـ) ماده ۲۴ قانون مزبور بیگانه‌ای که از آن‌سوی مرزها مرتکب جرم دسترسی غیرمجاز به داده‌های رایانه‌ای طبقه‌بندی نظامی می‌شود را به حبس تعزیری درجهٔ چهار محکوم کند.

نتیجه

ویژگی قدرت‌آوری یا حداقل ایجاد حس قدرت، یکی از جهت‌های بنیادین برای نهادهای نظامی شد تا همواره بخشی از کارها و برنامه‌های خویش را از دید بیگانگان و دشمنان خود پنهان نگه دارند. پنهان‌کاری و رعایت حفظ محرمانگی اسناد، نقشه‌ها و ... ، رفته‌رفته در پیروزی‌های نهادهای نظامی بر هماوردان خویش به چشم آمد. این شد که نهادهای نظامی کوشیدند تا اطلاعات حساس خویش را پنهان نگه دارند تا در جای مناسب از آن بهره ببرند.

با تحلیل و ارزیابی سیاست کیفری ایران در قبال حمایت از داده‌ها و سامانه‌های رایانه‌ای فاقد طبقه‌بندی نظامی در قبال از رفتار مجرمانه دسترسی غیرمجاز به داده‌ها و سامانه‌های رایانه‌ای نظامی در فضای سایبر از سوی اشخاص غیرنظامی و نظامی پژوهش حاضر به این نتیجه دست یافت که چنانچه مرتکب شخص غیرنظامی باشد، مطابق بند (ج) ماده ۷۵۴ قانون مجازات اسلامی به ترتیب به بیش از دوسوم حداکثر یک یا دو مجازات پیش‌بینی‌شده در ماده ۷۲۹ قانون مجازات اسلامی با اعمال بند (ج) ماده ۷۵۴ قانون مذکور محکوم خواهد شد.

ایراد وارد بر سیاست کیفری فعلی ایران این است که چون قانون‌گذار حداکثر مجازات را افزایش نداده است بلکه حداقل آن را افزایش داده است، این امر سبب می‌شود اگر یک شخص غیرنظامی به

داده‌ها یا سامانه‌های رایانه‌ای غیرنظامی دسترسی یابد و مقام قضایی وی را به اشد مجازات محکوم کند، مجازات وی در وضعیتی که به داده‌ها یا سامانه‌های رایانه‌ای نظامی دسترسی می‌یابد، از حیث حداکثر مجازات یکسان است. شایسته است میزان درجهٔ اهمیت داده‌ها و اطلاعات نظامی به‌موجب دستورالعملی از سوی ستاد کل نیروهای مسلح تدوین شود تا مجازات مرتکب تابع درجهٔ اهمیت داده‌ها و اطلاعات رایانه‌ای نظامی از بازدارندگی برخوردار باشد.

چنانچه مرتکب جرم شخص نظامی باشد، مرتکب مطابق بند (الف) ماده ۷۵۴ قانون مجازات اسلامی به بیش از دوسوم حداکثر یک یا دو مجازات پیش‌بینی‌شده در ماده ۷۲۹ قانون مجازات اسلامی با اعمال بند (ج) ماده ۷۵۴ قانون مذکور محکوم خواهد شد.

به نظر شایسته است، عنوان مجرمانهٔ دسترسی غیرمجاز به‌طور خاص در قانون مجازات جرائم نیروهای مسلح پیش‌بینی شود؛ زیرا از یک‌سو، مطابق ماده ۲ جرائمی که مجازات آن‌ها در قانون مذکور ذکرشده، در تخفیف و تبدیل نیز تابع ترتیبات همین قانون است و در غیر این‌موارد، تخفیف و تبدیل تابع همان قانونی است که تعیین کیفر مطابق آن صورت گرفته است. حال چون عنوان مجرمانهٔ دسترسی غیرمجاز در قانون مجازات جرائم نیروهای مسلح پیش‌بینی نشده است، از حیث تخفیف و تبدیل تابع قانون مجازات اسلامی است و از سوی دیگر، باید در نظر داشت قوانین خاص هر یک با هدف و فلسفهٔ خاصی وضع می‌شوند؛ ق.م.ج.ن.م به‌عنوان یک قانون خاص نیز دارای چنین ویژگی است؛ هدف این قانون آن است که برای جرائم نظامیان با توجه به حساسیت وظایف آنان، نظام کیفری خاصی تعیین و مجازات‌های قانونی را تشدید کند. با تسری قواعد قانون جرائم رایانه‌ای بر جرائم نظامیان، هدف و فلسفهٔ وضع ق.م.ج.ن.م نادیده گرفته می‌شود.

در راستای رفع خلأهای قانونی و اتخاذ یک سیاست کیفری افتراقی سخت‌گیرانه و بازدارنده در قبال حمایت از داده‌ها و سامانه‌های رایانه‌ای نظامی پژوهش حاضر با الهام از کنوانسیون بوداپست و حقوق کشورهای آمریکا و انگلستان به نتایج زیر دست یافت:

۱) با توجه به این‌که دسترسی غیرمجاز، مقدمهٔ ارتکاب جرائم مختلف دیگر رایانه‌ای محسوب می‌شود، لذا پیشنهاد می‌شود که قانون‌گذار ایران همانند قانون‌گذار انگلستان، بین دسترسی غیرمجاز ساده و دسترسی غیرمجاز برای ارتکاب جرائم بیش‌تر نسبت به داده‌ها و سامانه‌های رایانه‌ای نظامی، قائل به تفکیک شده و برای عنوان مجرمانه اخیر، مجازات شدیدتری در نظر بگیرد.

۲) قانون‌گذار ایران محافظت‌شده بودن داده‌ها و سامانه‌های رایانه‌ای مورد نفوذ با تدابیر امنیتی را شرط تحقق جرم تعیین کرده است. اما در حقوق آمریکا و انگلستان وجود چنین شرطی لازم و ضروری نیست. ازاین‌رو، شایسته است موضوع جرم از وصف «حفاظت‌شدگی داده و سامانه رایانه‌ای

به‌وسیله تدابیر امنیتی» برخوردار نبوده و برخلاف ماده ۷۲۹ واژهٔ «دسترسی» در معنای عام خود و نه خاص خود مدنظر قرار گیرد.

۳) در صورت پیش‌بینی رفتار مجرمانه «دسترسی غیرمجاز» در قانون مجازات جرائم نیروهای مسلح شایسته است تحت یک تبصره «هر نظامی که بر اثر بی‌احتیاطی یا بی‌مبالاتی یا سهل‌انگاری یا عدم رعایت نظامات دولتی اقدام به اتخاذ تدابیر امنیتی نسبت به داده و سامانه رایانه‌ی در اختیار خویش نمی‌کند، رفتار وی جرم شناخته شود». همچنین شایسته است در قالب تبصره‌ای ذکر شود: «چنانچه شخص نظامی که مسئولیت حفاظت و امنیت داده‌های رایانه‌ای، حامل‌های داده و سامانه‌های رایانه‌ای داشته در اعمال تدابیر حفاظتی و امنیتی بی‌احتیاطی یا بی‌مبالاتی کند» رفتار وی دارای وصف کیفری قلمداد شود.

فرامرزی بودن جرائم رایانه‌ای موجب می‌شود که بیگانگان یا دشمنان از آن‌سوی مرزها داده‌ها و سامانه‌های نظامی را تحت‌الشعاع قرار دهند، در این صورت شایسته است سیاست کیفری سخت‌گیرانه‌ای اتخاذ گردد.

با تحلیل و ارزیابی سیاست کیفری ایران در قبال حمایت از داده‌ها و سامانه‌های رایانه‌ای طبقه‌بندی‌شده نظامی در قبال از رفتارهای مجرمانه دسترسی غیرمجاز به داده‌ها و سامانه‌های رایانه‌ای نظامی، در فضای سایبر از سوی اشخاص غیرنظامی و نظامی پژوهش حاضر به این نتیجه دست یافت که چنانچه مرتکب شخص غیرنظامی باشد، مطابق بند (ج) ماده ۷۵۴ و بند (الف) ماده ۷۳۱ قانون مجازات اسلامی مرتکب به بیش از دوسوم حداکثر یک یا دو مجازت حبس از نود و یک روز تا یک سال یا جزای نقدی از پنج میلیون ریال تا بیست میلیون ریال محکوم خواهد شد.

ایراد اول وارد بر سیاست کیفری ایران در قبال دسترسی غیرمجاز به اطلاعات یا سامانه‌های رایانه‌ای طبقه‌بندی‌شده نظامی از سوی اشخاص غیرنظامی این است که قانون‌گذار در ماده ۷۳۱ تنها داده‌های سری را مصداق جاسوسی رایانه‌ای دانسته است و سایر اشکال طبقه‌بندی اطلاعات رایانه‌ای را مصداق جاسوسی ندانسته است. بنابراین اگر یک شخص غیرنظامی به داده‌ها و اطلاعات رایانه‌ای به‌کلی سری نظامی دسترسی یابد، مطابق بند (ج) ماده ۷۵۴ قانون مجازات اسلامی به بیش از دوسوم حداکثر یک یا دو مجازات مقرر در ماده ۷۲۹ قانون مجازات اسلامی محکوم می‌شود و چون رفتار وی مصداق جاسوسی نیست می‌تواند از کیفیات مخففه و نهادهای ارفاقی مطابق قانون مجازات اسلامی بهره‌مند شود.

ایراد دوم وارد بر سیاست کیفری ایران در قبال دسترسی غیرمجاز به اطلاعات طبقه‌بندی‌شده رایانه‌ای نظامی از سوی اشخاص غیرنظامی این است که امروزه فضای سایبر امکاناتی را فراهم آورده

است تا دشمنان و بیگانگان بدون خطراتی که جاسوسی سنتی به همراه داشت به داده‌ها و اطلاعات طبقه‌بندی‌شده رایانه‌ای نظامی دسترسی یابند و امنیت کشور را به مخاطره می‌اندازد. شایسته است مقنن همانند بند (هـ) ماده ۲۴ قانون مجازات جرائم نیروهای مسلح تدبیری اتخاذ کند تا از محرمانگی داده‌ها و اطلاعات طبقه‌بندی‌شده رایانه‌ای نظامی در برابر رفتار مجرمانه دسترسی غیرمجاز در فضای سایبر حمایت کند.

چنانچه مرتکب جرم شخص نظامی باشد، چون قانون‌گذار در ماده ۱۳۱ از عبارت (اقداماتی از قبیل ...) استفاده کرده است که نظر به تمثیلی بودن موارد مزبور در ماده ۱۳۱ داشته و شامل دسترسی غیرمجاز به داده‌ها و سامانه‌های رایانه‌ای طبقه‌بندی‌شده رایانه‌ای نظامی نیز می‌شود و مرتکب به مجازات پیش‌بینی‌شده در بند (د) ماده ۲۴ قانون مجازات جرائم نیروهای مسلح محکوم می‌شود.

در راستای رفع خلأهای قانونی و اتخاذ یک سیاست کیفری سخت‌گیرانه و بازدارنده در قبال حمایت از داده‌ها و سامانه‌های طبقه‌بندی‌شده رایانه‌ای نظامی نسبت به رفتارهای مجرمانه‌های دسترسی غیرمجاز پژوهش حاضر با الهام از کنوانسیون بوداپست و حقوق کشورهای آمریکا و انگلستان به نتایج زیر دست‌یافت:

۱) ایراد اول وارد بر سیاست کیفری ایران در قبال دسترسی غیرمجاز به داده‌های رایانه‌ای طبقه‌بندی‌شده نظامی از سوی اشخاص نظامی این است که باید در نظر داشت، ذکر عباراتی مانند امثالهم، نظایر آن و از قبیل آن به‌ویژه در حقوق کیفری با اصل شفافیت قانون و حقوق متهم تنافی دارد؛ چراکه افراد باید بدانند تکلیفشان در برابر رفتارهایی که انجام می‌دهند چیست. بااین‌وجود به نظر می‌رسد با توجه به لزوم تفسیر مضیق قوانین کیفری و رعایت حقوق متهم موضوع رفتارهای تمثیلی را باید محدود به داده‌ها و اطلاعات طبقه‌بندی‌شده رایانه‌ای دانست.

۲) ایراد دوم وارد بر سیاست کیفری فعلی ایران این است که در بند (الف) ماده ۷۳۱ قانون مجازات اسلامی شخصیت طرف مقابل به «دشمن» یا «بیگانه» مقید نشده است، درحالی‌که در بند (د) و (ب) ماده ۲۴ قانون مجازات جرائم نیروهای مسلح شخصیت طرف مقابل به نفع «دشمن» یا «بیگانه» مقید شده است. بنابراین اگر شخص نظامی نسبت به داده‌ها یا اطلاعات رایانه‌ای طبقه‌بندی‌شده نظامی به نفع دشمن یا بیگانه مرتکب جرم دسترسی غیرمجاز نشود، رفتار وی از شمول بند (د) ماده ۲۴ قانون مجازات جرائم نیروهای مسلح خارج است و به‌شرط آنکه موضوع رفتار وی داده‌های سری باشد، عمل وی مشمول بند (الف) ماده ۷۳۱ قانون مجازات اسلامی و مصداق جاسوسی رایانه‌ای است. اما اگر در فرض اخیر، موضوع رفتار وی داده‌های به‌کلی سری، خیلی محرمانه و محرمانه باشد، در این فرض اساساً رفتار وی جاسوسی نبوده بلکه مصداق جرم

دسترسی غیرمجاز موضوع ماده ۷۲۹ قانون مجازات اسلامی قرار می‌گیرد. نتیجهٔ قهری این رویکرد این است، ازآنجایی‌که کیفیات مخففه یا نهادهای ارفاقی از قبیل تعویق صدور حکم، تعلیق اجرای مجازات و ... در خصوص جرائم علیه امنیت داخلی و خارجی ازجمله جاسوسی قابل‌اعمال نیستند. در فرض اول که متعلق رفتار وی داده‌های سری رایانه‌ای است، اعمال کیفیات مخففه و نهادهای ارفاقی قابل‌اعمال نیستند اما در فرض اخیر حتی اگر متعلق رفتار وی داده‌های به‌کلی سری که از درجهٔ اهمیت بالاتری نسبت به داده‌های سری برخوردارند باشد، مرتکب می‌تواند از کیفیات مخففه و نهادهای ارفاقی طبق قانون مجازات اسلامی بهره‌مند شود.

۳) ایراد سوم وارد بر سیاست کیفری فعلی ایران این است که چنانچه مرتکب جرم شخص غیرنظامی باشد، قانون‌گذار در ماده ۷۳۱ تنها دسترسی به داده‌های سری را مصداق جاسوسی رایانه‌ای دانسته است و سایر اشکال طبقه‌بندی اطلاعات رایانه‌ای را مصداق جاسوسی ندانسته است. بنابراین اگر یک شخص غیرنظامی به داده‌ها و اطلاعات رایانه‌ای به‌کلی سری نظامی دسترسی یابد، مطابق بند (ج) ماده ۷۵۴ قانون مجازات اسلامی به بیش از دوسوم حداکثر یک یا دو مجازات مقرر در ماده ۷۳۰ قانون مجازات اسلامی محکوم می‌شود و چون رفتار وی مصداق جاسوسی نیست می‌تواند از کیفیات مخففه و نهادهای ارفاقی مطابق قانون مجازات اسلامی بهره‌مند شود. شایسته است مقنن جهت برون‌رفت از چنین سیاست کیفری نامتناسب و ناکارآمدی با پیش‌بینی عنوان مجرمانهٔ دسترسی غیرمجاز به داده‌های طبقه‌بندی‌شده رایانه‌ای در قانون مجازات جرائم نیروهای مسلح در پرتوی بند (هـ) ماده ۲۴ قانون مزبور بیگانه‌ای که از آن سوی مرزها مرتکب جرم دسترسی غیرمجاز به داده‌های رایانه‌ای طبقه‌بندی‌شده نظامی می‌شود را به حبس تعزیری درجهٔ چهار محکوم کند.

منابع

فارسی

- بابایی، جواد. (۱۳۹۸). جرائم رایانه‌ای و آیین دادرسی حاکم بر آن، چاپ چهارم، تهران: نشر مرکز مطبوعات و انتشارات قوه قضاییه.
- باستانی، برومند. (۱۳۸۳). جرائم کامپیوتری و اینترنتی جلوی نوین از بزهکاری، چاپ اول، تهران: نشر بهنامی.
- باری، مجتبی. (۱۳۹۸). حقوق جزای نظامی، چاپ اول، تهران: نشر دادستان.
- بای، حسینعلی و پورقهرمانی، بابک. (۱۳۸۸). بررسی فقهی - حقوقی جرائم رایانه‌ای، قم، چاپ اول، تهران: پژوهشگاه علوم و فرهنگ اسلامی.
- باگاویتی،جانسوزکی و کلاریک، آندرو ام. (۱۳۹۱)، مهندسی اجتماعی در جنگ سایبری. ترجمه موسسه فرهنگی و مطالعات و تحقیقات بین‌المللی ابرار معاصر، چاپ نخست، تهران: نشر موسسه فرهنگی مطالعات و تحقیقات بین‌المللی ابرار معاصر(امنیت و جنگ سایبری۲).
- بهره‌مند، حمید و مرسی، هادی. (۱۴۰۱). راهبرد جرم‌انگاری مستقل حملات سایبری در حقوق کیفری ایران، مجله مجلس و راهبرد. سال بیست و نهم، شماره ۱۱۱.
- پاک‌نیت، مصطفی. (۱۳۹۶). افتراقی شدن دادرسی کیفری. تهران: چاپ اول. نشر میزان.
- ترکی، غلامرضا. (۱۳۸۸). نگرش علمی و کاربردی به قانون جرائم رایانه‌ای. ماهنامه دادرسی، شماره ۷۸، سال سیزدهم.
- تحیری، فرزاد. (۱۳۸۳). دسترسی غیرمجاز جلوه‌ای از جرائم رایانه‌ای نوین، مجموعه مقالات همایش بررسی ابعاد حقوقی فناوری اطلاعات، معاونت حقوقی و توسعه قضایی قوه قضاییه.
- جلالی فراهانی، امیرحسین. (۱۳۹۵). کنوانسیون جرائم سایبر و پروتکل الحاقی آن. چاپ دوم، تهران: نشر خرسندی
- خالقی، علی. (۱۳۹۵). آیین دادرسی کیفری. جلد دوم، چاپ سی و دوم، تهران: نشر مؤسسه مطالعات و پژوهش‌های حقوقی شهر دانش.
- رامشی، رضا .(۱۳۸۸). تفکیک جرائم نظامی از جرائم عمومی در قلمرو جرائم علیه امنیت ملی کشور با تأکید بر صلاحیت محاکم. پایان‌نامه دوره کارشناسی ارشد، دانشگاه پیام نور مرکز تهران.
- زندی، محمدرضا. (۱۳۹۳). تحقیقات مقدماتی در جرائم سایبری، تهران: انتشارات جنگل، جاودانه.
- سبزگلی، مجید و موسوی، سیدعلی. (۱۳۹۲). مفاهیم پایه فناوری اطلاعات، تهران: شرکت چاپ و نشر کتاب‌های درسی ایران.
- صبحی شیشوان، بهنام. (۱۳۸۳). شیوه‌های گوناگون سرقت رایانه‌ای. ماهنامه وکالت، شماره ۲۱،
- عالی‌پور، حسن. (۱۳۹۳). حقوق کیفری فناوری اطلاعات. چاپ سوم، تهران: نشر خرسندی.
- عباسی کلیمانی، عاطفه و اکبری، عاطفه. (۱۳۹۴). جرائم سایبری، چاپ اول، تهران: انتشارات مجد.
- عزیزی، امیرمهدی. (۱۳۹۴). حقوق کیفری جرائم رایانه‌ای. چاپ دوم، تهران: نشر مجد.
- قاجارقیونلو، سیامک. (۱۳۹۱). مقدمه علم حقوق سایبر، چاپ اول، تهران: نشر میزان.
- کیهانلو، فاطمه و رضادوست، وحید. (۱۳۹۳). حملات سایبری به‌مثابه توسل به‌زور در سیاق منشور ملل متحد.

فصلنامه تحقیقات حقوقی، شماره ۶۹.

- لازرژ، کریستین. (۱۳۹۰). درآمدی بر سیاست جنایی. ترجمه علی حسین نجفی ابرندآبادی، چاپ دوم، تهران: نشر میزان.
- مرسی، هادی. (۱۳۹۷). مقابله با حملات سایبری در حقوق کیفری ایران و اسناد بین‌المللی (با تأکید بر حملات سایبری علیه ایران). پایان‌نامه برای دریافت درجه کارشناسی ارشد، تهران: دانشکده حقوق و علوم سیاسی دانشگاه تهران.
- مرسی، هادی و زرنگ، محمد. (۱۴۰۲). آسیب‌شناسی سیاست کیفری ایران در قبال تحصیل غیرمجاز داده‌های رایانه‌ای نظامی. فصلنامه دیدگاه‌های حقوق قضایی، دوره ۲۸، شماره ۱۰۳.
- مهران‌فر، ابراهیم و قلی‌پورشهرکی، علیرضا. (۱۳۹۹). شرح جامع و کاربردی قانون مجازات جرائم نیروهای مسلح مصوب ۱۳۸۲/۱۰/۰۹. چاپ اول، تهران: نشر جنگل.
- محمدنسل، زهرا؛ محمدنسل، غلامرضا و گلدوزیان، ایرج. (۱۳۹۹). مطالعه تطبیقی دسترسی غیرمجاز به داده‌ها و سامانه‌های رایانه‌ای در قوانین کیفری ایران و انگلستان و فرانسه. فصلنامه پژوهش‌های اطلاعاتی و جنایی، سال پانزدهم، شماره سوم.
- موسسه فرهنگی مطالعات و تحقیقات بین‌المللی ابرار معاصر. (۱۳۹۱). امنیت و جنگ سایبری (۲)(ویژه سلاح‌ها، جنگجویان و حملات سایبری). چاپ اول، تهران: نشر موسسه فرهنگی مطالعات و تحقیقات بین‌المللی ابرار معاصر.
- میر محمدصادقی، حسین(۱۳۹۳). جرائم علیه امنیت و آسایش عمومی. چاپ بیست و پنجم، تهران: نشر میزان.
- الهی‌منش، محمدرضا و سدره نشین، ابوالفضل. (۱۳۹۵). محشای قانون جرائم رایانه‌ای، چاپ پنجم، تهران: نشر مجد.
- یکرنگی، محمد؛ مرسی، هادی و علیزاده، مهسا. (۱۴۰۰). امکان‌سنجی استناد به دفاع مشروع به‌عنوان مانع مسئولیت کیفری در مقابل حملات سایبری. مجله مطالعات حقوق کیفری و جرم‌شناسی، دوره ۵۱، شماره ۲، ۵۶۱-۵۸۳.
- یکرنگی، محمد و مرسی، هادی. (۱۳۹۹). تحلیل جرم انگاری تولید و پخش نرم‌افزار و ابزارهای الکترونیکی صرفاً مجرمانه در سیاست کیفری ایران در پرتو اسناد فرامرزی. مجله دیدگاه‌های حقوق قضایی، شماره ۹۲.

انگلیسی

- Clarke, Richard, K. Knanke, Robert (2010), *Cyber War: The Next Thread to National Security and What to Do about it*, Manhattan, New York, Ecco.
- Joint Chiefs of Staff, Joint Publication 1-02, Dep't of Def. Dict. of Military and Assoc'd Terms, 2001, available at: http://www.dtic.mil/doctrine/jel/newoubs/jp102.pdf
- Computer Froud and Abuse Act of 1986 (CFAA). Available at: https://www.congress.gov/bill/99th-congress/house-bill/4718
- Computer Misuse Act 1990. Available at: https://www.legislation.gov.uk/ukpga/1990/18/contents.