فصلنامهٔ علمی دیدگاه‌های حقوق قضائی
مقاله پژوهشی، دورهٔ۲۸، شمارهٔ ۱۰۳، پاییز ۱۴۰۳، صفحات ۱۷۳ تا ۲۰۰
تاریخ دریافت: ۱۴۰۱/۰۳/۲۴ – تاریخ پذیرش: ۱۴۰۲/۰۸/۰۷

# آسیب‌شناسی سیاست کیفری ایران در قبال تحصیل غیرمجاز داده‌های رایانه‌ای نظامی

**|هادی مرسی*|** دانشجوی دکتری حقوق جزا و جرم‌شناسی، دانشکدهٔ الهیات و معارف اسلامی، دانشگاه میبد، یزد، ایران
**|محمد زرنگ|** مربی حقوق، دانشکدهٔ مدیریت، دانشگاه افسری امام علی (ع)، تهران، ایران

**چکیده**
تحصیل غیرمجاز داده‌های رایانه‌ای نظامی موجب می‌شود تا تحصیل‌کنندگان با استفاده از آن‌ها برای حملهٔ سایبری به زیرساخت‌های نظامی استفاده کنند که در عمل ممکن است به تخریب سامانه‌های رایانه‌ای حیاتی نظامی ازقبیل سامانه‌های آفندی و پدافندی بینجامد. قانون‌گذار در بند (الف) مادهٔ ۷۳۱ قانون مجازات اسلامی صرفاً تحصیل داده‌های سری را به‌طور عام پیش‌بینی کرده است و در مادهٔ ۱۳۱ قانون مجازات جرائم نیروهای مسلح نسبت به عنوان مجرمانهٔ «تحصیل غیرمجاز داده‌های رایانه‌ای» صراحتی وجود ندارد. اهمیت و حساسیت داده‌های رایانه‌ای نظامی اقتضا دارد که تدابیر متناسب با آن‌ها چه در حوزهٔ جرم‌انگاری و چه کیفرگزینی مقرر شود. در این پژوهش به این امر که سیاست کیفری ایران در قبال تحصیل غیرمجاز داده‌های 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 ضمن بررسی مواد مربوطه در قانون مجازات جرائم نیروهای مسلح و قانون جرائم رایانه‌ای به روش توصیفی ـ تحلیلی و مبتنی بر منابع کتابخانه‌ای نتیجه‌گیری می‌کند که سیاست کیفری ایران در قبال تحصیل غیرمجاز داده‌های رایانه‌ای نظامی اعم از طبقه‌بندی‌شده و فاقد طبقه‌بندی از سوی اشخاص نظامی و غیرنظامی از اصل بازدارندگی و اصل تناسب جرم و مجازات برخوردار نیستند که در این

* نویسندهٔ مسئول
***Email:*** Stu.h.mersi@meybod.ac.ir

خصوص نیازمند اصلاح است و خلأهای تقنینی وجود دارد که مستلزم پیش‌بینی تدابیری متناسب با اهمیت داده‌های رایانه‌ای نظامی است که در این راستا پیشنهاداتی ارائه شده است.
**واژگان کلیدی:** سیاست کیفری، فضای سایبر، جرم نظامی، تحصیل غیرمجاز دادهٔ رایانه‌ای، جاسوسی رایانه‌ای.

**مقدمه**

از آغاز پیدایش نهادهای نظامی رعایت این اصل مهم یعنی حفظ محرمانگی اطلاعات با توجه به وظیفهٔ مهم آن‌ها یعنی حفظ امنیت و اراضی کشور در مقابل تجاوز بیگانگان و دشمنان با توجه به نیازها و تحولات زمانی و مکانی، همواره ضروری بود و در پرتو همین اصل است که حقوق کیفری نظامی در قانون مجازات جرائم نیروهای مسلح، رفتارهای مجرمانهٔ ناقض محرمانگی اطلاعات نظامی ازقبیل اسناد، نقشه‌ها و ... را جرم‌انگاری کرده است.

تحصیل غیرمجاز داده‌های رایانه‌ای نظامی از سوی اشخاص نظامی و غیرنظامی می‌تواند به عواقب جدی و امنیتی منجر شود. تحصیل غیرمجاز داده‌های رایانه‌ای نظامی می‌تواند عملیات نظامی را تحت تأثیر قرار دهد و طراحی عملیات نظامی مخفیانه را به خطر بیندازد. همچنین به ازبین رفتن امنیت ملی و تهدید امنیت داخلی و خارجی منجر شود. اطلاعات رایانه‌ای حساس نظامی شامل اطلاعات استراتژیک، نقشه‌های نظامی، اطلاعات کارکنان نیروهای مسلح، تجهیزات نظامی و سامانه‌های ارتباطی هستند که اگر در اختیار دشمنان، بیگانگان و افراد فاقد صلاحیت قرار گیرد، می‌تواند به تضعیف قدرت نظامی و تهدیدی علیه امنیت ملی منجر شود. در صورت تحقق تحصیل غیرمجاز اطلاعات رایانه‌ای نظامی، امکان رخ دادن اختلافات و تنش‌های بین‌المللی بین کشورها و سازمان‌های نظامی به‌وجود می‌آید که این امر ممکن است به ازبین رفتن وثاقت و همکاری با کشورهای دیگر منجر شود. تحصیل غیرمجاز اطلاعات رایانه‌ای نظامی می‌تواند به تضعیف نظام اطلاعاتی نهادهای نظامی منجر شود که باعث کاهش کارایی و قابلیت عملکرد سازمانی شود و در موارد بحرانی، امکان پاسخ‌گویی به تهدیدات و حملات سایبری را کاهش دهد و حتی ممکن است به کاهش اعتماد عمومی منجر شود. همچنین تحصیل غیرمجاز اطلاعات رایانه‌ای نظامی ممکن است باعث نقض حریم خصوصی اطلاعات نظامیان شود که می‌تواند به ردیابی، جاسوسی و دسترسی غیرمجاز به اطلاعات شخصی آن‌ها منجر شود.

ارتقا و به‌روزرسانی قوانین و مقررات مربوط به امنیت سایبری و مقابله با تحصیل غیرمجاز داده‌های نظامی می‌تواند در تأمین محافظت، و اتخاذ سیاست کیفری متناسب و بازدارنده در برابر

تهدیدات سایبری کمک کند. درواقع، تدوین قوانین جامع و مانع 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 سامانهٔ رایانه‌ای، حامل داده و دادهٔ رایانه‌ای در مادهٔ ۱۳۱ قانون مجازات جرائم نیروهای مسلح مصوب ۱۳۸۲/۱۰/۰۹ به جرم‌انگاری برخی رفتارهای مجرمانهٔ سایبری از سوی اشخاص نظامی[۱] اقدام کرده است. لیکن نسبت به عنوان مجرمانهٔ تحصیل غیرمجاز دادهٔ رایانه‌ای مسکوت مانده است.[۲] گفتنی است قانون‌گذار در بند (الف) مادهٔ ۷۳۱ از عبارت تحصیل داده‌های سری به‌طور عام استفاده کرده، اما مقصود خود را از عبارت (تحصیل غیرمجاز) بیان نکرده است. عدم تعریف عبارت «تحصیل غیرمجاز رایانه‌ای» از سوی مقنن چه در قانون مجازات جرائم نیروهای مسلح و چه در قانون جرائم رایانه‌ای، پرسش‌های بنیادین و اساسی را مطرح می‌سازد که منظور از تحصیل غیرمجاز دادهٔ رایانه‌ای در فضای سایبر چیست؟ چه رفتارهای مجرمانهٔ سایبری را می‌توان مصداق تحصیل غیرمجاز داده‌های رایانه‌ای تلقی کرد؟ آیا سیاست کیفری ایران در قبال تحصیل غیرمجاز 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

---

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 است. جرم نظامی در مفهوم موسع «به هر جرمی گفته می‌شود که فرد نظامی به مناسبت شغل یا وظیفهٔ خود مرتکب گردد، مانند سرقت و اختلاس (ر.ک. خالقی، علی (۱۳۹۵)، **آیین دادرسی کیفری**، جلد دوم، تهران، نشر مؤسسهٔ مطالعات و پژوهش‌های حقوقی شهر دانش، چاپ سی و دوم، ص ٦٢). در پژوهش حاضر جرم نظامی در مفهوم موسع آن مدنظر است. در واقع جرائمی که دارای ماهیت عمومی هستند، اگر در ارتباط با یک وظیفهٔ نظامی واقع شوند جرم خاص نظامی تلقی می‌شوند (ر.ک. رامشی، رضا (۱۳۸۸)، **تفکیک جرائم نظامی از جرائم عمومی در قلمرو جرائم علیه امنیت ملی کشور با تأکید بر صلاحیت محاکم**، پایان‌نامهٔ دورهٔ کارشناسی ارشد، دانشگاه پیام نور مرکز تهران، ص۱۲).

۲. مادهٔ ۱۳۱ مقرر می دارد: «هرگونه تغییر یا حذف اطلاعات، الحاق، تقدیم یا تأخیر تاریخ نسبت به تاریخ حقیقی و نظایر آن که به‌طور غیرمجاز توسط نظامیان در سیستم رایانه و نرم‌افزارهای مربوط صورت گیرد[ جعل رایانه ای] و همچنین اقداماتی ازقبیل تسلیم اطلاعات طبقه‌بندی‌شدهٔ رایانه ای به دشمن یا افرادی که صلاحیت دسترسی به آن اطلاعات را ندارند [جاسوسی رایانه‌ای]، افشای غیرمجاز اطلاعات، سرقت اشیای دارای ارزش اطلاعاتی مانند سی دی (CD) یا دیسک‌های حاوی اطلاعات یا معدوم کردن آن‌ها یا سوءاستفاده‌های مالی که نظامیان به‌وسیلهٔ رایانه مرتکب شوند جرم محسوب و حسب مورد مشمول مجازات‌های مندرج در مواد مربوط به این قانون می باشند».

استخراج خلأهای قانونی، پژوهش حاضر به اتخاذ یک سیاست کیفری افتراقی متناسب و بازدارنده اهتمام ورزیده است و در این راستا، در سه قسمت «مفهوم تحصیل غیرمجاز و جلوه‌های آن»، «تحصیل غیرمجاز داده‌های رایانه‌ای فاقد طبقه‌بندی نظامی» و «تحصیل غیرمجاز داده‌های رایانه‌ای طبقه‌بندی‌شدهٔ نظامی» تدوین یافته است.

## ۱. مفهوم تحصیل غیرمجاز و جلوه‌های آن

یافتن خلأهای قانونی و اتخاذ یک سیاست کیفری متناسب و بازدارنده نسبت به تحصیل غیرمجاز اطلاعات رایانه‌ای نظامی مستلزم این است که مفهوم تحصیل غیرمجاز مشخص شود. این الزام از آنجا که در قانون مجازات جرائم نیروهای مسلح، قانون جرائم رایانه‌ای و سند بین‌المللی شورای اروپا در زمینهٔ جرائم سایبر (کنوانسیون بوداپست) مفهوم تحصیل غیرمجاز تبیین نشده است، دوچندان می‌شود.

### ۱-۱. مفهوم تحصیل غیرمجاز رایانه‌ای

مقنن در بند (الف) مادهٔ ۷۳۱ ق.م.ا (تعزیرات) که مقرر می‌دارد: «دسترسی به داده‌های مذکور یا تحصیل آن‌ها یا شنود محتوای سری ...» از واژهٔ «تحصیل داده» استفاده کرده است، اما مقصود خود را از واژهٔ «تحصیل داده» بیان نکرده است. به‌نظر می‌رسد تحصیل غیرمجاز شامل هر رفتاری در فضای سایبر[1] است که موجب در اختیار قرار گرفتن داده‌های رایانه‌ای می‌شود. فضای سایبر، فضایی حقیقی و واقعی است و مجازی نیست[2] هر چند که به‌شکل مادی و ملموس احساس‌شدنی

---

1. cyber space

سایبر در زبان انگلیسی پیشوند و در زبان فارسی پسوندی است که به کلمات جدید و امروزی متصل می‌شود تا به آن‌ها معنا و مفهوم دهد. در ترجمهٔ فارسی این لغت معمولاً سه اصطلاح رایانه‌ای، سایبری و آنلاین به‌کار برده شده و جایگزین عناوین دیگری مانند فناوری اطلاعات و ارتباطات، انفورماتیک و ... شده است. این اصطلاح «سایبر» نخستین بار توسط «ویلیام گیبسون» نویسندهٔ داستان‌های علمی ـ تخیلی برای نشان دادن شبکه‌های رایانه‌ای دنیای آنلاین، به‌کار گرفته شده است (ر.ک. قاجارقیونلو، سیامک (۱۳۹۱)، **مقدمهٔ علم حقوق سایبر**، تهران: نشر میزان، ص ۱۰۸).

۲. برخی نویسندگان فضای سایبر را محیطی مجازی دانسته و آن را این‌گونه تعریف کرده‌اند:«محیطی مجازی و غیرملموس که در فضای شبکه‌های بین‌المللی (که از طریق اینترنت به هم متصل می‌شوند)» (ر.ک. باستانی، برومند (۱۳۸۳)، **جرائم کامپیوتری و اینترنتی جلوی نوین از بزهکاری**، تهران، نشر بهنامی، به نقل از: کیهانلو، فاطمه و ←

نیست (زندی، ۱۳۹۳: ۱۶۰؛ یکرنگی و همکاران، 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 همهٔ منابع اطلاعاتی قابل‌دسترس در شبکه‌های رایانه‌ای دانسته‌اند (www.library.arizona.edu/rio/glossary.html).

وزارت دفاع ایالات‌متحده فضای سایبر را این‌گونه تعریف کرده است: «دامنه‌ای جهانی در فضای اطلاعات که متشکل از شبکه‌ها و سامانه‌های مستقل فناوری اطلاعات ازقبیل اینترنت، شبکه‌های مخابراتی، سامانه‌های رایانه‌ای و پردازنده و کنترل‌هایی تعبیه شده است» (Joint Chiefs of Staff, 2011: 141). در تعریف فضای سایبر گفته شده است: فضایی است 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 تحصیل غیرمجاز داده‌های رایانه‌ای نظامی می‌پردازد. با تعریف ارائه‌شده از مفهوم تحصیل غیرمجاز و فضای سایبر می‌توان گفت رفتارهای مجرمانه‌ای سایبری ازقبیل سرقت رایانه‌ای و شنود غیرمجاز که به ترتیب در مواد ۷۳۰ و ۷۴۰ قانون مجازات اسلامی ـ تعزیرات پیش‌بینی شده‌اند، همگی از مصادیق و جلوه‌های تحصیل غیرمجاز داده‌ها و اطلاعات رایانه‌ای در فضای سایبر به‌شمار می‌روند.

### ۱-۲. جلوه‌های تحصیل غیرمجاز داده‌های رایانه‌ای نظامی

رفتار مجرمانهٔ شنود غیرمجاز[1] اطلاعات و داده‌های رایانه‌ای یکی از جلوه‌های تحصیل غیرمجاز داده‌های رایانه‌ای است که موضوع آن محتوای در حال انتقال است، چراکه منظور از شنود همان دریافت است و بدیهی است رفتار فیزیکی دریافت کردن نیز از مصادیق تحصیل داده‌ها و اطلاعات رایانه‌ای است که می‌تواند نسبت به محتواهای در حال انتقال تحقق یابد. از سوی دیگر، رفتار مجرمانهٔ سرقت اطلاعات و داده‌های رایانه‌ای نیز یکی دیگر از مصادیق تحصیل غیرمجاز داده‌های رایانه‌ای تلقی می‌شود که در حقوق کیفری ایران پیش‌بینی شده است. رفتار فیزیکی «ربایش» در سرقت رایانه‌ای عبارت است از رونوشت از داده‌ها و اطلاعات رایانه‌ای یا برش داده‌ها و اطلاعات

---

وحید رضادوست (۱۳۹۳)، «حملات سایبری به‌مثابهٔ توسل به زور در سیاق منشور ملل متحد»، **تحقیقات حقوقی**، شمارهٔ ٦٩، ص ٩٥).

1. illegal interception

رایانه‌ای و مرز تمایز این دو رفتار در این است که در رونوشت عین داده‌ها و اطلاعات رایانه‌ای باقی می‌ماند، ولی در برش عین داده و اطلاعات باقی نمی‌ماند. بدین‌سان، این دو رفتار ارتکابی از مصادیق تحصیل غیرمجاز داده نیز به‌شمار می‌روند. به عبارت دیگر، در سرقت رایانه‌ای، عنوان مجرمانهٔ تحصیل غیرمجاز داده‌های رایانه‌ای به‌واسطهٔ دو رفتار فیزیکی «برش» و «رونوشت» نسبت به داده‌ها و اطلاعات ذخیره‌شده رایانه‌ای تحقق می‌یابد و در شنود غیرمجاز عنوان مجرمانهٔ تحصیل غیرمجاز داده‌های رایانه‌ای به‌واسطهٔ رفتار ارتکابی شنود (دریافت) نسبت به محتوای رایانه‌ای در حال انتقال تحقق می‌یابد. با وجود این، ذکر این نکته خالی از لطف نیست، گاهی ممکن است شخص نظامی نسبت به داده‌ها و اطلاعات رایانه‌ای مرتکب رفتار فیزیکی «رونوشت»، «برش» یا «شنود» نشود، بلکه داده‌های حذف‌شده را از سامانهٔ رایانه‌ای یا حامل‌های داده بازیابی کند که در این فرض عنوان مجرمانهٔ تحصیل غیرمجاز به‌واسطهٔ رفتار فیزیکی «بازیابی اطلاعات» تحقق یافته است.

در قانون جرائم رایانه‌ای صرفاً دو عنوان مجرمانهٔ «شنود غیرمجاز» و «سرقت رایانه‌ای» پیش‌بینی شده است. لذا در این قسمت ابتدا به رفتار مجرمانهٔ شنود غیرمجاز (۱-۲-۱) و سپس به سرقت رایانه‌ای (۲-۲-۱) پرداخته می‌شود. با توجه به اینکه رفتار مجرمانهٔ بازیابی غیرمجاز داده‌ها و اطلاعات رایانه‌ای در قانون جرائم رایانه‌ای پیش‌بینی نشده، شایسته است مقنن با پیش‌بینی عنوان مجرمانهٔ تحصیل غیرمجاز داده‌ها و اطلاعات رایانه‌ای در قانون جرائم رایانه‌ای خلأ موجود را مرتفع سازد.

### ۱-۲-۱. شنود غیرمجاز محتوای در حال انتقال نظامی

#### ۱-۲-۱-۱. رکن قانونی جرم شنود غیرمجاز

قانون‌گذار ایران با الهام از مادهٔ ۳ کنوانسیون بوداپست[1] در مادهٔ یک قانون جرائم رایانه‌ای (مادهٔ ۷۳۰ قانون مجازات اسلامی ـ تعزیرات) مقرر می‌دارد: «هرکس به‌طور غیرمجاز محتوای در حال

---

۱. مادهٔ ۳ کنوانسیون بوداپست مقرر می‌دارد: «هریک از اعضا باید به گونه‌ای اقدام به وضع قوانین و سایر تدابیر کنند که در صورت لزوم براساس حقوق داخلی خود، شنود عمدی و حق داده‌های رایانه‌ای در حال انتقال غیرعمومی را که با ابزارهایی ایجاد شده‌اند و از سامانه‌های رایانه‌ای ارسال شده یا در میان آن‌ها جریان دارند، جرم‌انگاری کنند. همچنین انتشار امواج الکترومغناطیسی از یک سامانهٔ رایانه‌ای که این‌گونه داده‌های رایانه‌ای را انتقال می‌دهند، نیز دربر می‌گیرد. اعضا می‌توانند مقرر دارند این جرم در صورتی محقق می‌شود که قصد ناروایی وجود داشته یا سامانهٔ رایانه‌ای به سامانهٔ رایانه‌ای دیگری متصل باشد (ر.ک. جلالی فراهانی، امیرحسین (۱۳۹۵)، **کنوانسیون جرائم سایبر و پروتکل الحاقی آن**، تهران: نشر خرسندی، ص ۲۸).

انتقال ارتباطات غیرعمومی در سامانه‌های رایانه‌ای یا مخابراتی یا امواج الکترومغناطیسی یا نوری را شنود کند، 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».

**۱-۲-۱-۲. رکن مادی جرم شنود غیرمجاز**

درخصوص رکن مادی این جرم باید خاطر نشان کرد که مقنن در توصیف رفتار فیزیکی از واژهٔ «شنود» استفاده کرده است. شنود فعلی مستمر و ساده است که در همان معنای «دریافت اطلاعات» یا «محتوا» به‌کار می‌رود. هر چند نسبت به داده‌های شنیداری، شنود در همان معنای واقعی خود یعنی «شنیدن» به‌کار می‌رود، ولی نسبت به داده‌ها و اطلاعات رایانه‌ای، شنود همان دریافت کردن یا در اختیار گرفتن محتواست. درواقع، می‌توان گفت هر چند معنای شنود که همان شنیدن گفت و شنیده‌های تلفنی است، واقعی و ظاهری است، ولی شنود داده‌ها و اطلاعات و نیز امواج الکترومغناطیسی به معنای شنیدن با گوش نیست، بلکه به معنای دریافت کردن یا به اختیار گرفتن داده‌ها و اطلاعات است که در این میان واژگان «بویش»[1] و «ره‌گیری»[2] نیز به‌کار برده می‌شود (عالی‌پور، ۱۳۹۳: ۱۱۷). به عبارت دیگر، می‌توان گفت واژهٔ «شنود»، به‌طور دقیق و ظاهری عنوان مجرمانهٔ «شنود غیرمجاز» را بازگو نمی‌کند، بلکه مانند جرائم کلاهبرداری و پولشویی، معنای کنایه‌ای دارد، زیرا شنود داده‌ها و اطلاعات رایانه به معنای شنیدن با گوش نیست، بلکه منظور از آن، در اختیار گرفتن و دریافت کردن داده‌ها و اطلاعات رایانه‌ای است. واژهٔ «شنود» در بند «و» مادهٔ ۱ آیین‌نامهٔ جمع‌آوری و استنادپذیری ادله الکترونیکی مترادف با «دریافت» به این نحو تعریف شده است: «هرگونه دستیابی به محتوای در حال انتقال ارتباطات غیرعمومی در سامانه‌های رایانه‌ای یا مخابراتی یا امواج الکترومغناطیسی با استفاده از سامانه‌ها و تجهیزات سخت‌افزاری و نرم‌افزاری مربوط».

درخصوص شرایط تحقق جرم شنود غیرمجاز در پرتو مادهٔ ۷۳۰ قانون مجازات اسلامی ـ تعزیرات می‌توان این‌گونه شرح داد که موضوع جرم «شنود غیرمجاز»، «داده‌محتوا» است (بابایی، ۷۰:۱۳۹۸). داده‌محتوا یا اطلاعات، حاصل پردازش داده‌های رایانه‌ای است، درواقع به داده‌های رایانه‌ای پس از پردازش، داده‌محتوا گفته می‌شود. از این رو، مفهوم داده‌محتوا، خاص‌تر از داده

---

1. sniffing

2. interception

است و نسبت به داده‌های شنیداری، دیداری، نوشتاری و مانند آن گفته می‌شود که دربردارندۀ درون‌مایه یا پیام بامعنایی است. موضوع جرم در شنود غیرمجاز یعنی «داده‌محتوا» چون کانون توجه پژوهش حاضر داده‌های رایانه‌ای نظامی است باید علاوه بر وصف «در حال انتقال» موصوف به «نظامی بودن» باشد. داده‌محتوای در حال انتقال در برابر داده‌محتوای ذخیره‌شده یا ایستا، به داده‌هایی گفته می‌شود که میان آغازگاه (مبدأ) و پایانه (مقصد) قرار دارند (بابایی، ۱۳۹۸:۷۰). بنابراین، شنود غیرمجاز داده‌های ذخیره‌شده از شمول این ماده خارج است، زیرا موضوع جرم «شنود غیرمجاز» دارای وصف «در حال انتقال» است. برخی به استناد ذیل مادۀ ۶۸۳ قانون آیین دادرسی کیفری، دسترسی غیرمجاز به داده‌های ذخیره‌شده را نیز مشمول مجازات شنود غیرمجاز می‌دانند (محمدنسل، ۱۳۹۵: ۱۰۳). در حالی که تبصرۀ مذکور ناظر بر کنترل محتوای ذخیره‌شده است (زراعت، ۱۳۹۴:۳۷۴)، نه اینکه مجازات شنود نسبت به آن اعمال شود. همچنین برخی عقیده دارند واژۀ «کنترل»، متفاوت از واژۀ «شنود»، مرتبۀ بالاتری از کنترل است (زندی، ۱۳۹۳: ۱۷۵).

شرط دیگری که در جرم «شنود غیرمجاز» پیش‌بینی شده است آن است که بستر و فرایند محتوای در حال انتقال جنبۀ «غیرعمومی»داشته باشد، خواه محتوا عمومی یا خصوصی باشد (عزیزی، ۱۳۹۶: ۷۹). در مقابل برخی قید «غیرعمومی» را ناظر بر محتوا می‌دانند (الهی‌منش و سدره‌نشین، ۱۳۹۵:۲۵).

لازم است که رفتار شنود به‌طور غیرمجاز (غیرقانونی) انجام شود. بنابراین در صورتی که شخص نظامی به موجب قانون یا دستورات مقام قضائی یا اجازه از طرف افراد و مقامات مسئول و مجاز مافوق داده‌های در حال انتقال شنود کند، عمل وی فاقد وصف جزایی است. همان‌طور که بیان شد، جرم «شنود غیرمجاز»، جرمی علیه محرمانگی داده‌هاست، بنابراین باید مبدأ و مقصد آن اشخاص نظامی باشند که شایستگی فرستادن و دریافتن داده‌محتوا را داشته باشند؛ از این رو محتوا در حال انتقال باید در یک بستر خصوصی میان دو یا چند شخص نظامی انجام گیرد. بنابراین در فرضی که یک شخص نظامی که صلاحیت و اجازۀ ارسال داده‌محتوا را نداشته در نقطۀ مبدأ اقدام به ارسال داده‌محتوا کند و شخص نظامی دیگری که فاقد صلاحیت و اجازه است اقدام به دریافت داده‌محتواها در نقطۀ میانۀ مسیر کند و درنهایت شخص نظامی دیگری که فاقد صلاحیت و اجازه است، در نقطۀ مقصد اقدام به دریافت داده‌محتوا کند، هر سه شخص نظامی، مرتکب جرم «شنود غیرمجاز» شده‌اند.

نکتۀ دیگری که شایسته است در این قسمت بدان اشاره کرد این است که لازم نیست شنود نسبت به محتواهایی ارتکاب یابد که با تدابیر امنیتی حفاظت شده باشند. بنابراین امروزه که محتوا

به محض ارسال در نقطهٔ مبدأ به شیوه‌های نوینی رمزنگاری شده و در پایان مسیر در نقطهٔ مقصد رمزگشایی می‌شوند تا برای دریافت‌کننده قابل فهم باشند، حال چنانچه یک شخص نظامی در میانهٔ مسیر انتقال محتواهای رمزنگاری‌شده را دریافت کند، شخص نظامی مرتکب جرم «شنود غیرمجاز» شده است. خواه شخص نظامی توانایی رمزگشایی و پردازش آن‌ها را پس از دریافت داشته باشد خواه از چنین توانایی برخوردار نباشد.

عنوان مجرمانهٔ «شنود غیرمجاز» به‌عنوان یک جرم عمومی جرمی مطلق است و نیازی به تحقق نتیجه ندارد.

### ۱-۲-۱-۳. رکن معنوی جرم شنود غیرمجاز

دربارهٔ عنصر معنوی «شنود غیرمجاز» به‌عنوان یکی از مصادیق تحصیل غیرمجاز باید خاطر نشان کرد که ابتدا لازم است مرتکب بداند متعلق رفتار وی محتوای در حال انتقال نظامی است (علم به موضوع و اوصاف آن)، و نداشتن اجازه از سوی مقام ذی‌الصلاح (علم به شرایط) است. منظور از سوءنیت عام این است که شخص، قصد رفتار «شنود» به محتوای در حال انتقال نظامی را داشته باشد. بنابراین چنانچه شنود به محتوای در حال انتقال نظامی به قصد یا انگیزهٔ کنجکاوی، کسب مال، کسب شهرت، فرار از خدمت، ربودن یا تخریب داده، ارتکاب یابد حائز اهمیت نیست؛ آنچه اهمیت دارد حفظ محرمانگی محتوای در حال انتقال نظامی است.

### ۱-۲-۱-۴. مجازات جرم شنود غیرمجاز داده‌های رایانه‌ای نظامی

درخصوص مجازات شنود غیرمجاز باید اذعان داشت، مقنن به اعتبارهای متفاوت رویکردهای متفاوتی اتخاذ کرده است.

مقنن به اعتبار شخصیت مرتکب، سیاست کیفری افتراقی اتخاذ کرده است، بدین نحو که چنانچه مرتکب جرم شخص غیرنظامی باشد، مطابق مادهٔ ۷۳۰ قانون مجازات اسلامی به حبس از شش ماه تا دو سال یا جزای نقدی از ده میلیون ریال تا چهل میلیون ریال یا هر دو مجازات حبس و جزای نقدی محکوم خواهد شد. اما چنانچه مرتکب جرم شخص نظامی باشد مطابق بند (الف) مادهٔ ۷۵۴ ق.م.ا به بیش از دوسوم حداکثر یک یا دو مجازات پیش‌بینی‌شده در مادهٔ ۷۳۰ قانون مجازات اسلامی محکوم خواهد شد.

مقنن به اعتبار تعلق داده به دولت، نهادها و مراکز ارائه‌دهندهٔ خدمات عمومی نیز سیاست کیفری افتراقی اتخاذ کرده است. بدین نحو که چنانچه سامانه یا داده به دولت، نهادها و مراکز

ارائه‌دهندهٔ خدمات عمومی متعلق باشد، مطابق بند (ج) مادهٔ ۷۵۴ ق.م.ا مرتکب به بیش از دوسوم حداکثر یک یا دو مجازات پیش‌بینی‌شده در مادهٔ ۷۲۹ قانون مجازات اسلامی محکوم خواهد شد.

بند (ج) ناظر بر حمایت از داده‌ها و اطلاعات رایانه‌ای دولتی ازجمله داده و اطلاعات رایانه‌ای نظامی است. وجه تمایز بند (ج) و بند (الف) در این است که مرتکب جرم بند (ج) لزوماً شخص نظامی نیست، اما موضوع جرم می‌تواند داده‌ها و اطلاعات رایانه‌ای نظامی باشد.

### ۱ـ۲ـ۲. سرقت رایانه‌ای داده‌های رایانه‌ای نظامی

#### ۱ـ۲ـ۲ـ۱. رکن قانونی جرم سرقت رایانه‌ای

مادهٔ ۱۲ قانون جرائم رایانه‌ای (مادهٔ ۷۴۰ قانون مجازات اسلامی ـ تعزیرات) مقرر می‌دارد: «هر کس به‌طور غیرمجاز داده‌های متعلق به دیگری را برباید، چنانچه عین داده‌ها در اختیار صاحب آن باشد، به جزای نقدی از یک میلیون (۱.۰۰۰.۰۰۰) ریال تا بیست میلیون (۲۰.۰۰۰.۰۰۰) ریال و در غیر این صورت به حبس از ۹۱ 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».

#### ۱-۲-۲-۲. رکن مادی جرم سرقت رایانه‌ای

درخصوص رکن مادی این جرم باید خاطر نشان کرد که رفتار فیزیکی در جرم سایبری «سرقت رایانه‌ای»، همانند سرقت سنتی «ربودن» است. ربودن یا ربایش، واژه‌ای است که معنای خود را از عرف وام می‌گیرد وگرنه ظاهر این واژه‌ها تنها بر رفتاری صدق می‌کنند که مرتکب به‌طور غافلگیرانه مال دیگری را ببرد. ربایش در معنای عرفی از معنای بیرونی خود دور افتاده است و به هرگونه دست‌اندازی به مال دیگری گفته می‌شود که به محروم شدن دائم وی بینجامد (عالی‌پور، ۲۵۵:۱۳۹۳). دربارهٔ رفتار ارتکابی «ربایش داده» می‌توان گفت که «ربایش داده» به معنای دست‌اندازی به دادهٔ دیگری است که یا با رو گرفتن (کپی)[1] است یا با برش (کات)[2] تحقق می‌یابد. بنابراین درمورد سرقت رایانه‌ای نظامی می‌توان گفت منظور از ربودن در مادهٔ ۷۴۰ ق.م.ا تعزیرات دو رفتار است:

---

1. cut
2. copy

یک ـ «روگرفتن» که با تعبیر «... چنانچه عین داده‌ها در اختیار صاحب آن باشد...» همخوانی دارد. دوم ـ «برش» که ناظر بر فرضی است که داده از محلی که قرار دارد برداشته شده و به جای دیگری خواه سامانهٔ رایانهٔ نظامی یا غیرنظامی باشد و خواه رایانامهٔ نظامی یا غیرنظامی یا حامل دادهٔ نظامی یا غیرنظامی انتقال داده شود. در تفاوت میان روگرفت داده با برش داده می‌توان گفت که در روگرفت جابه‌جایی صورت گرفته و عین داده‌ها در سامانه یا حامل‌های دادهٔ نظامی باقی مانده، ولی در برش جابه‌جایی صورت گرفته است، ولی عین داده از سامانه یا حامل دادهٔ نظامی حذف می‌شود.

موضوع جرم ـ موضوع جرم سرقت رایانه‌ای «دادهٔ رایانه‌ای» است چون کانون توجه پژوهش حاضر داده‌های رایانه‌ای نظامی است باید به وصف «نظامی بودن» موصوف شده باشد. بنابراین سخت‌افزارهایی همچون سامانهٔ رایانه‌ای نظامی و ساختارهای سخت‌افزاری درون و برون آن ازقبیل، نمایشگر: صفحه کلید: صفحهٔ سخت اطلاعاتی (هارد دیسک) و ... چنانچه مورد ربایش قرار گیرند، از شمول عنوان سرقت رایانه‌ای خارج است.

سؤالی که در این قسمت قابل طرح است این است که آیا داده‌های رایانه‌ای نظامی موضوع سرقت رایانه‌ای همانند سرقت سنتی باید دارای ارزش مالی باشند؟ دربارهٔ سرقت رایانه‌ای چالش کم‌تری هست، زیرا در مادهٔ ۱۲ به مال یا ارزش مالی داده نپرداخته است و تعبیر «دادهٔ متعلق به دیگری» هرگونه از داده‌های رایانه‌ای نظامی را دربر می‌گیرد؛ خواه داده‌ها دارای ارزش مالی باشند خواه نباشند.

مکان ارتکاب جرم سرقت رایانه‌ای نظامی ـ رفتار ربایش (روگرفت یا کپی) باید در فضای سایبر انجام گیرد؛ به نحوی که شخص نظامی بدون اینکه دادهٔ نظامی را جعل یا تخریب کند، آن را بر روی افزارهای حامل‌های دادهٔ نظامی یا غیرنظامی ارسال کند یا به لوح‌های فشردهٔ نظامی و غیرنظامی انتقال دهد یا از رهگذر رایانامه به صندوق پست الکترونیکی خود یا یک شخص غیرنظامی بفرستد یا از طریق تروجان‌ها و فایل‌های مخرب که بر روی سامانهٔ رایانهٔ هدف، مستقر می‌شود، امکان دریافت اطلاعات از رایانهٔ هدف را فراهم می‌سازد (صبحی شیشوان، ۱۳۸۳: ۷۰).

سرقت رایانه‌ای، همانند سرقت سنتی جرمی است که نتیجهٔ آن ربوده شدن است که به محض ربودن تحقق می‌یابد، ولی برخی از حقوقدانان از محروم شدن دارنده (عزیزی، ۱۳۹۴: ۱۴۱؛ محمدنسل، ۱۳۹۵: ۱۰۳) و برخی از دراختیار گرفتن رباینده یاد می‌کنند (بابایی، ۱۳۹۸: ۱۳۱)، و در مقابل برخی عقیده دارند محروم شدن نتیجه نیست، بلکه اثر نتیجه است (عالی‌پور، ۱۳۹۳: ۲۵۴). به‌نظر می‌رسد نظر اخیر شایسته است، زیرا اگر نتیجهٔ «محروم شدن» یا «در اختیار قرار

گرفتن» رباینده شرط بود، با توجه به مادهٔ ۱۴۴ ق.م.ا که مقرر داشته است: «... در جرائمی که وقوع آن‌ها براساس قانون منوط به تحقق نتیجه است ...» لازم بود نتیجه را بیان می‌کرد و نمی‌توان گفت چون نتیجه بدیهی بود قانون‌گذار از ذکر آن امتناع کرده است. درواقع اگر نتیجه واضح بود برخی از حقوقدانان «محروم شدن» و برخی دیگر «دراختیار قرار گرفتن» به‌عنوان نتیجهٔ جرم عقیده نداشتند و اختلافی نمی‌بایست حادث می‌شد. از طرف دیگر، بر پایهٔ اصل قانونی بودن باید نتیجهٔ جرم به‌عنوان یکی از اجزای رکن مادی به آن اشاره می‌شد.

### ۱ـ۲ـ۲ـ۳. رکن معنوی جرم سرقت رایانه‌ای

دربارهٔ عنصر معنوی «شنود غیرمجاز» به‌عنوان یکی از مصادیق تحصیل غیرمجاز باید خاطر نشان کرد که ابتدا لازم است مرتکب بداند متعلق رفتار وی داده‌های متعلق به نهادهای نظامی (علم به موضوع و اوصاف آن)، و نداشتن اجازه از سوی مقام ذی‌صلاح (علم به شرایط) است. منظور از سوء نیت عام این است که برای مثال کاربر نظامی، قصد رفتار «ربایش» را نسبت به داده‌های رایانه‌ای نظامی داشته باشد. جرم «سرقت رایانه‌ای» جرمی مطلق است و نیاز به حصول نتیجه ندارد، بنابراین چنانچه ربایش نسبت به داده‌های نظامی به قصد یا انگیزهٔ کنجکاوی، کسب مال، کسب شهرت، فرار از خدمت، ربودن یا تخریب داده ارتکاب یابد، حائز اهمیت نیست، آنچه که اهمیت دارد حفظ محرمانگی داده‌های رایانه‌ای نظامی است.

### ۱-۲-۲-۴. مجازات جرم سرقت رایانه‌ای داده‌های رایانه‌ای نظامی

درخصوص مجازات سرقت رایانه‌ای باید اذعان داشت، مقنن به اعتبارهای متفاوت رویکردهای متفاوتی اتخاذ کرده است.

مقنن به اعتبار شخصیت مرتکب، سیاست کیفری افتراقی اتخاذ کرده است، بدین نحو که چنانچه مرتکب جرم شخص غیرنظامی باشد، مطابق مادهٔ ۷۴۰ قانون مجازات اسلامی به حبس از شش ماه تا دو سال یا جزای نقدی از ده میلیون ریال تا چهل میلیون ریال یا هر دو مجازات حبس و جزای نقدی محکوم خواهد شد. اما چنانچه مرتکب جرم شخص نظامی باشد مطابق بند (الف) مادهٔ ۷۵۴ ق.م.ا به بیش از دوسوم حداکثر یک یا دو مجازات پیش‌بینی‌شده در مادهٔ ۷۳۰ قانون مجازات اسلامی محکوم خواهد شد.

مقنن به اعتبار تعلق داده به دولت، نهادها و مراکز ارائه‌دهندهٔ خدمات عمومی نیز سیاست کیفری افتراقی اتخاذ کرده است. بدین نحو که چنانچه سامانه یا دادهٔ متعلق به دولت، نهادها و

مراکز ارائه‌دهندهٔ خدمات عمومی باشد، مطابق بند (ج) مادهٔ ۷۵۴ ق.م.ا مرتکب به بیش از دوسوم حداکثر یک یا دو مجازات پیش‌بینی‌شده در مادهٔ ۷۴۰ قانون مجازات اسلامی محکوم خواهد شد. بند (ج) ناظر بر حمایت از داده‌ها و اطلاعات رایانه‌ای دولتی ازجمله داده و اطلاعات رایانه‌ای نظامی است. همان‌طور که اشاره شد، وجه تمایز بند (ج) و بند (الف) در این است که مرتکب جرم بند (ج) لزوماً شخص نظامی نیست، اما موضوع جرم می‌تواند داده‌ها و اطلاعات رایانه‌ای نظامی باشد.

## ۲. سیاست کیفری ایران در قبال تحصیل غیرمجاز داده‌های رایانه‌ای فاقد طبقه‌بندی نظامی

تحصیل غیرمجاز داده‌های رایانه‌ای فاقد طبقه‌بندی نظامی می‌تواند از سوی اشخاص نظامی و غیرنظامی ارتکاب یابد. بدین منظور در این قسمت ابتدا به تحصیل غیرمجاز داده‌های رایانه‌ای فاقد طبقه‌بندی از سوی اشخاص نظامی (۱ـ۲) و سپس به تحصیل غیرمجاز داده‌های رایانه‌ای فاقد طبقه‌بندی از سوی اشخاص غیرنظامی (۲ـ۲) پرداخته شده است.

### ۲ـ۱. سیاست کیفری ایران در قبال تحصیل غیرمجاز داده‌های رایانه‌ای فاقد طبقه‌بندی از سوی اشخاص نظامی

به‌طور کلی 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: ۳۲-۳۴). در افتراقی‌سازی فرد بزهکار براساس گونهٔ بزهکاری مبنا و ملاک قرار داده می‌شود نه براساس نوع جرم یا شخصیت بزه‌دیده .به‌طور کلی 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 به مراتب 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 تحصیل غیرمجاز داده‌های رایانه‌ای به واسطهٔ رفتار ارتکابی شنود (دریافت) نسبت به داده‌ها و اطلاعات در حال انتقال از سوی اشخاص نظامی بدین نحو است که مرتکب مطابق بند (الف) مادهٔ ۷۵۴ ق.م.ا به بیش از دوسوم حداکثر

یک یا دو مجازات پیش‌بینی‌شده در مادهٔ ۷۳۰ قانون مجازات اسلامی محکوم خواهد شد و سیاست کیفری ایران در قبال عنوان مجرمانهٔ تحصیل غیرمجاز داده‌های رایانه‌ای به‌واسطهٔ رفتار ارتکابی رونوشت یا برش داده‌ها و اطلاعات از سوی اشخاص نظامی بدین نحو است که مرتکب مطابق بند (الف) مادهٔ ۷۵۴ ق.م.ا به بیش از دوسوم حداکثر یک یا دو مجازات پیش‌بینی‌شده در مادهٔ ۷۳۰ قانون مجازات اسلامی محکوم خواهد شد.

اولین ایراد و اشکال وارد بر سیاست کیفری ایران در قبال تحصیل غیرمجاز داده‌های رایانه‌ای فاقد طبقه‌بندی از سوی اشخاص نظامی این است که قانون‌گذار حداکثر مجازات را افزایش نداده، بلکه حداقل آن را افزایش داده است، این امر سبب می‌شود اگر یک شخص غیرنظامی داده‌های رایانه‌ای غیرنظامی را تحصیل کند و مقام قضائی وی را به اشد مجازات محکوم کند، مجازات وی با مجازات شخص نظامی که دادهٔ نظامی را تحصیل کند، از حیث حداکثر مجازات یکسان است که شایسته است میزان درجهٔ اهمیت داده‌ها و اطلاعات نظامی به موجب 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 کنونی این است که مطابق مادهٔ ۲ قانون مجازات جرائم نیروهای مسلح و تبصرهٔ آن، جرائمی که مجازات آن‌ها در قانون مذکور ذکرشده، 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 شنود غیرمجاز و سرقت رایانه‌ای 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. همچنین اگر تحصیل غیرمجاز نسبت به داده‌ها و اطلاعات طبقه‌بندی‌شده رایانه‌ای ارتکاب یابد، با تفسیری که خواهد آمد (۱-۳)، رفتار ارتکابی مشمول قانون مجازات جرائم نیروهای مسلح است، اما اگر تحصیل غیرمجاز نسبت به اطلاعات فاقد طبقه‌بندی رایانه‌ای ارتکاب یابد، رفتار ارتکابی مشمول قانون مجازات اسلامی است. بدیهی است چنین سیاست کیفری افتراقی از سوی مقنن قابل توجیه نیست.

ایراد سوم سیاست کیفری کنونی این است چنانچه شخص نظامی به‌واسطهٔ رفتار بازیابی اطلاعات، داده‌ها و اطلاعات رایانه‌ای نظامی فاقد طبقه‌بندی را تحصیل کند، رفتار وی منطبق با هیچ‌یک از مواد پیش‌بینی‌شده در قانون مجازات جرائم نیروهای مسلح و قانون جرائم رایانه‌ای

نیست و با توجه به اصل قانونی بودن جرائم و مجازات‌ها وی اساساً قابل مجازات نیست. شایسته است مقنن جهت برون‌رفت از این خلأ قانونی در قانون مجازات جرائم نیروهای مسلح چاره‌اندیشی کند.

### ۲ـ۲. سیاست کیفری ایران در قبال تحصیل غیرمجاز داده‌های رایانه‌ای فاقد طبقه‌بندی از سوی اشخاص غیرنظامی

مقنن به اعتبار تعلق داده‌های رایانه‌ای به دولت، نهادها و مراکز ارائه‌دهندهٔ خدمات عمومی نیز سیاست کیفری افتراقی اتخاذ کرده است. بدین نحو که چنانچه عنوان مجرمانهٔ تحصیل غیرمجاز داده‌های رایانه‌ای به‌واسطهٔ رفتار ارتکابی شنود (دریافت) نسبت به داده‌ها و اطلاعات در حال انتقال از سوی اشخاص غیرنظامی ارتکاب یابد مطابق بند (ج) مادهٔ ۷۵۴ ق.م.ا مرتکب به بیش از دوسوم حداکثر یک یا دو مجازات پیش‌بینی‌شده در مادهٔ ۷۳۰ قانون مجازات اسلامی محکوم خواهد شد. بند (ج) ناظر بر حمایت از داده‌ها و اطلاعات رایانه‌ای دولتی ازجمله داده و اطلاعات رایانه‌ای نظامی است. چنانچه عنوان مجرمانهٔ تحصیل غیرمجاز داده‌های رایانه‌ای نظامی به‌واسطهٔ رفتار ارتکابی رونوشت یا برش داده‌ها و اطلاعات از سوی اشخاص غیرنظامی تحقق یابد، مطابق بند (ج) مادهٔ ۷۵۴ ق.م.ا مرتکب به بیش از دوسوم حداکثر یک یا دو مجازات پیش‌بینی‌شده در مادهٔ ۷۴۰ قانون مجازات اسلامی محکوم خواهد شد.

ایراد و اشکال وارد بر سیاست کیفری ایران این است که چون قانون‌گذار حداکثر مجازات را افزایش نداده، بلکه حداقل آن را افزایش داده است، این امر سبب می‌شود اگر یک شخص غیرنظامی داده‌های رایانه‌ای غیرنظامی را تحصیل کند و مقام قضائی وی را به اشد مجازات محکوم کند، مجازات وی در وضعیتی که داده‌های رایانه‌ای نظامی را تحصیل کند، از حیث حداکثر مجازات یکسان است. شایسته است میزان درجهٔ اهمیت داده‌ها و اطلاعات نظامی به موجب دستورالعملی از سوی ستاد کل نیروهای مسلح تدوین شود تا مجازات مرتکب تابع درجهٔ اهمیت داده‌ها و اطلاعات رایانه‌ای نظامی از بازدارندگی برخوردار باشد.[۱]

---

۱. قانون مجازات اسلامی در مادهٔ 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 ارائهٔ خدمات ضروری عمومی به‌کار می‌روند، ازقبیل 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 مادهٔ ۷۳۹ در ←

ایراد دیگر سیاست کیفری کنونی این است چنانچه شخص غیرنظامی به‌واسطهٔ رفتار بازیابی اطلاعات، داده‌ها و اطلاعات رایانه‌ای نظامی فاقد طبقه‌بندی را تحصیل کند، رفتار وی منطبق با هیچ‌یک از مواد پیش‌بینی‌شده در قانون مجازات جرائم نیروهای مسلح و قانون جرائم رایانه‌ای نیست و با توجه به اصل قانونی بودن جرائم و مجازات‌ها وی اساساً قابل مجازات نیست. شایسته است مقنن جهت برون‌رفت از این خلأ قانونی در قانون مجازات اسلامی چاره‌اندیشی کند.

### ۳. سیاست کیفری ایران در قبال تحصیل غیرمجاز داده‌های طبقه‌بندی‌شدهٔ رایانه‌ای نظامی

تحصیل غیرمجاز داده‌های طبقه‌بندی‌شدهٔ نظامی همانند داده‌های فاقد طبقه‌بندی نظامی می‌تواند از سوی اشخاص نظامی و غیرنظامی ارتکاب یابد. بدین منظور در این قسمت ابتدا به تحصیل غیرمجاز داده‌های طبقه‌بندی‌شدهٔ رایانه‌ای از سوی اشخاص نظامی (۳ـ۱) و سپس به تحصیل غیرمجاز داده‌های رایانه‌ای طبقه‌بندی‌شدهٔ رایانه‌ای از سوی اشخاص غیرنظامی (۳ـ۲) پرداخته شده است.

### ۳ـ۱. سیاست کیفری ایران در قبال تحصیل غیرمجاز داده‌های طبقه‌بندی‌شدهٔ رایانه‌ای نظامی از سوی اشخاص نظامی

هدف این بند تحلیل و ارزیابی سیاست کیفری ایران در قبال رفتار مجرمانه تحصیل غیرمجاز داده‌های رایانه‌ای طبقه‌بندی‌شده[1] از سوی اشخاص نظامی در فضای سایبر است که مطابق صدر مادهٔ ۲۴ قانون مزبور و بند (ب) آن مرتکب آن جاسوس محسوب می‌شود.[2] جاسوسی در فضای سایبر دارای سه مرحله است: مرحلهٔ اول آن دسترسی به داده‌ها و سامانه‌های رایانه‌ای

---

مادهٔ مستقلی به حمایت از داده‌ها و سامانه‌های رایانه‌ای نظامی از سوی اشخاص غیرنظامی در برابر رفتارهای مجرمانه بپردازد و سیاست کیفری افتراقی اتخاذ کند.

۱. طبقه‌بندی اسناد براساس میزان ارزش حفاظتی اسناد و مدارک و اهمیت خطرات ناشی از افشای آن‌ها برای کشور صورت می‌گیرد. تعیین طبقه‌بندی عبارت است از قرار دادن سند در یکی از چهار نوع طبقه‌بندی (به کلی سری، سری، خیلی محرمانه و محرمانه). به‌منظور حفظ سند و تعیین محدودیت‌های لازم جهت دسترسی به آن و جلوگیری از افشا و دسترسی غیرمجاز. ر.ک. مهران‌فر، ابراهیم و علیرضا قلی‌پور شهرکی (۱۳۹۹)، **شرح جامع و کاربردی قانون مجازات جرائم نیروهای مسلح مصوب ۱۳۸۲/۱۰/۰۹**، تهران، نشر جنگل، ص ۱۴۵. و میرمحمدصادقی، حسین (۱۳۹۳)، **جرائم علیه امنیت و آسایش عمومی**، تهران، نشر میزان، ص ۱۱۰.

۲. جهت مطالعه بیشتر ر.ک. میرمحمدصادقی، حسین (۱۳۹۳)، **جرائم علیه امنیت و آسایش عمومی**، تهران، نشر میزان، صص ۸۵-۹۴.

طبقه‌بندی‌شده است، مرحلهٔ دوم آن تحصیل داده‌های طبقه‌بندی‌شده و درنهایت مرحلهٔ سوم در دسترس قرار دادن داده‌های مذکور است (عالی‌پور، ۱۳۹۳: ۱۹۳). با توجه به عنوان پژوهش حاضر، کانون توجه پژوهش حاضر بر مرحلهٔ دوم جاسوسی رایانه‌ای یعنی تحصیل غیرمجاز داده‌های رایانه‌ای طبقه‌بندی‌شده نظامی در فضای سایبر است.

مقنن در بند «ب» مادهٔ ۲۴ در فضای سنتی جرم «تحصیل اسناد یا اطلاعات» برای دشمن یا بیگانه را که ناظر بر مرحلهٔ دوم جاسوسی است، پیش‌بینی کرده است.[۱] از سوی دیگر، مقنن در مادهٔ ۱۳۱ قانون مجازات جرائم نیروهای مسلح مقرر داشته است[۲]: «... تسلیم اطلاعات طبقه‌بندی رایانه‌ای به دشمن و افرادی که صلاحیت دسترسی به آن ندارند ... جرم محسوب و حسب مورد مشمول مجازات‌های مندرج در مواد مربوط به این قانون می‌باشند» که ناظر بر مرحلهٔ سوم جرم جاسوسی یعنی تسلیم داده‌های رایانه‌ای طبقه‌بندی شده است.

حال این پرسش مطرح می‌شود که هرگاه شخص نظامی داده‌ها و اطلاعات طبقه‌بندی‌شده نظامی را تحصیل کند آیا می‌توان رفتار وی را مصداق بند (ب) مادهٔ ۲۴ قانون مجازات جرائم نیروهای مسلح دانست یا خیر؟ یک استدلال می‌تواند این باشد که بند ب مادهٔ ۲۴ ق.م.ج.ن.م اطلاق دارد و در حدود شرایط ماده، قسمتی از نقص قانونی را پوشش می‌دهد. نقدی که بر این استدلال می‌تواند وارد باشد این است که قانون‌گذار در بند (الف) مادهٔ ۲۴ از عبارت «... در اختیار دشمن یا بیگانه قرار دهد...» و در بند (ج) مادهٔ مزبور از عبارت «... تسلیم اسرار نظامی و یا آن‌ها را از مفاد آن آگاه سازد» و در مادهٔ 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، ولی با وجود این در

---

۱. بند «ب» مادهٔ ٢٤ قانون مجازات جرائم نیروهای مسلح مقرر می‌دارد: «هر نظامی که اسناد یا اطلاعات برای دشمن یا بیگانگان تحصیل کرده، به هر دلیلی موفق به تسلیم آن نشود به حبس از سه تا پانزده سال محکوم می‌گردد پیش‌بینی شده است».

۲. مادهٔ ۱۳۱ قانون مجازات جرائم نیروهای مسلح مقرر می‌دارد: «هرگونه تغییر یا حذف اطلاعات، الحاق، تقدیم یا تأخیر تاریخ نسبت به تاریخ حقیقی و نظایر آن که به‌طور غیرمجاز توسط نظامیان در سیستم رایانه و نرم‌افزارهای مربوط صورت گیرد و همچنین اقداماتی ازقبیل تسلیم اطلاعات طبقه‌بندی رایانه‌ای به دشمن یا افرادی که صلاحیت دسترسی به آن اطلاعات را ندارند، افشای غیرمجاز اطلاعات، سرقت اشیای دارای ارزش اطلاعاتی مانند سی دی (CD) یا دیسکت‌های حاوی اطلاعات یا معدوم کردن آن‌ها یا سوءاستفاده‌های مالی که نظامیان به وسیلهٔ رایانه مرتکب شوند جرم محسوب و حسب مورد مشمول مجازات‌های مندرج در مواد مربوط به این قانون می‌باشند».

مادهٔ ۱۳۱ قانون‌گذار به رفتار مجرمانهٔ تسلیم اطلاعات طبقه‌بندی‌شدهٔ رایانه‌ای اشاره کرده است. درواقع، می‌توان گفت قانون‌گذار در مادهٔ 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 به‌نظر 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 مادهٔ ۱۳۱ قانون مجازات جرائم نیروهای مسلح.

استدلال دوم این‌گونه می‌تواند مطرح شود که قانون‌گذار در مادهٔ ۱۳۱ از عبارت «اقداماتی ازقبیل ...» استفاده کرده است که نظر به تمثیلی بودن موارد مزبور در مادهٔ ۱۳۱ دارد و شامل تحصیل غیرمجاز داده‌های طبقه‌بندی‌شدهٔ رایانه‌ای نیز می‌شود و مرتکب به مجازات پیش‌بینی‌شده در بند (ب) مادهٔ ۲۴ قانون مجازات جرائم نیروهای مسلح محکوم می‌شود. این استدلال قابل پذیرش است و می‌توان رفتار شخص نظامی را مصداق بند (ب) مادهٔ ۲۴ قانون مجازات جرائم نیروهای مسلح دانست. اما باید درنظر داشت، ذکر عباراتی مانند امثالهم، نظایر آن و ازقبیل 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 و به تشت آراء قضائی نیز منجر شوند و درنهایت 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 است. با وجود این به‌نظر می‌رسد با توجه به لزوم تفسیر مضیق قوانین کیفری و رعایت حقوق متهم موضوع رفتارهای تمثیلی را باید محدود به داده‌ها و اطلاعات طبقه‌بندی‌شدهٔ رایانه‌ای دانست.

ایراد وارد بر سیاست کیفری کنونی این است که در بند «الف» مادهٔ ۷۳۱ قانون مجازات اسلامی شخصیت طرف مقابل به «دشمن» یا «بیگانه» مقید نشده است، در حالی‌که در بند «ب» مادهٔ ۲۴ قانون مجازات جرائم نیروهای مسلح شخصیت طرف مقابل به «دشمن» یا «بیگانه» مقید شده است. بنابراین اگر شخص نظامی داده‌ها یا اطلاعات رایانه‌ای طبقه‌بندی‌شده را برای دشمن یا بیگانه تحصیل نکند، رفتار وی از شمول بند «ب» مادهٔ ۲۴ قانون مجازات جرائم نیروهای مسلح خارج است و به شرط آن‌که موضوع رفتار وی داده‌های سری باشد، عمل وی مشمول بند (الف) مادهٔ 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 حسب مورد مصداق عنوان مجرمانهٔ شنود غیرمجاز یا سرقت رایانه‌ای قرار می‌گیرد. نتیجهٔ قهری این رویکرد این است که از آنجایی‌که کیفیات مخففه یا نهادهای ارفاقی ازقبیل تعویق صدور حکم، تعلیق اجرای مجازات و ... درخصوص جرائم علیه امنیت داخلی و خارجی ازجمله جاسوسی قابل اعمال نیستند.[۱] 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 باشد که از درجهٔ اهمیت بالاتری نسبت به داده‌های سری برخوردارند، مرتکب می‌تواند از کیفیات مخففه و نهادهای ارفاقی طبق قانون مجازات اسلامی بهره‌مند شود.

## ۳ـ۲. سیاست کیفری ایران در قبال تحصیل غیرمجاز داده‌های طبقه‌بندی‌شدهٔ رایانه‌ای نظامی از سوی اشخاص غیرنظامی

قانون‌گذار در بند (الف) مادهٔ ۳ قانون جرائم رایانه‌ای (۷۳۱ قانون مجازات اسلامی) صرفاً تحصیل یک قسم از طبقه‌بندی اطلاعات رایانه‌ای یعنی داده‌های سری را مصداق جاسوسی رایانه‌ای و جرمی علیه امنیت داخلی و خارجی تلقی کرده است و تحصیل سایر اقسام طبقه‌بندی اطلاعات ازقبیل به‌کلی سری، خیلی محرمانه و محرمانه، مصداق جاسوسی ندانسته است.

### ۳ـ۲ـ۱. عنصر قانونی تحصیل غیرمجاز داده‌های سری رایانه‌ای

در قانون جرائم رایانه‌ای مقنن در قسمت صدر و بند (الف) مادهٔ ۳ قانون جرائم رایانه‌ای (مادهٔ ۷۳۱ قانون مجازات اسلامی) به‌دلیل اهمیت داده‌ها و اطلاعات سری رایانه‌ای که امنیت کشور وابسته به آن‌هاست، تحصیل غیرمجاز این داده‌ها و اطلاعات را تحت عنوان مجرمانهٔ «جاسوسی رایانه‌ای» جرم‌انگاری کرده است.[۲]

---

۱. مادهٔ ۴۷ قانون مجازات اسلامی مقرر می‌دارد: «صدور حکم و اجرای مجازات درمورد جرائم زیر و شروع به آن‌ها قابل تعویق و تعلیق نیست: الف- جرائم علیه امنیت داخلی و خارجی کشور ...».

مادهٔ ۱۰۹ قانون مجازات اسلامی مقرر می‌دارد:«جرائم زیر مشمول مرور زمان تعقیب، صدور حکم و اجرای مجازات نمی¬شوند: الف- جرائم علیه امنیت داخلی و خارجی کشور...»

۲. مادهٔ ۳ قانون جرایم رایانه‌ای (مادهٔ ۷۳۱ قانون اسلامی) مقرر می‌دارد: «هرکس به‌طور غیر مجاز نسبت به داده‌های سری در حال انتقال یا ذخیره‌شده در سامانه‌های رایانه‌ای یا مخابراتی یا حامل‌های داده مرتکب اعمال زیر شود، به مجازات‌های مقرر محکوم خواهد شد:

←

### ۳ـ۲ـ۲. عنصر مادی تحصیل غیرمجاز داده‌های سری

درخصوص رفتار فیزیکی باید خاطرنشان کرد که در بند (الف) مادهٔ ۷۳۱ قانون مجازات اسلامی مقنن از واژه‌های «تحصیل» استفاده کرده، اما مقصود خود را از واژهٔ «تحصیل» بیان نکرده است. این امر در بند اول پژوهش حاضر (مفهوم تحصیل غیرمجاز و جلوه‌های آن) به تفصیل مورد بررسی و ارزیابی قرار گرفت و مشخص شد به‌کار بردن عنوان تحصیل غیرمجاز به مراتب دقیق‌تر و جامع‌تر از ذکر مصادیق آن یعنی شنود غیرمجاز و سرقت رایانه‌ای است. موضوع جرم بند «الف» مادهٔ ۷۳۱ قانون مجازات اسلامی «داده‌های سری» است. چون کانون توجه پژوهش حاضر داده‌های رایانه‌ای نظامی است باید علاوه بر اوصاف «سری» و «ذخیره‌شده» یا «در حال انتقال» به «نظامی بودن» موصوف شده باشد.

درخصوص شرایط و اوضاع و احوال لازم برای تحقق جرم مزبور لازم است که رفتار مجرمانهٔ تحصیل داده‌های سری به‌طور غیرمجاز (غیر قانونی) انجام شود. بنابراین در صورتی که شخص

---

الف) دسترسی به داده‌های مذکور یا تحصیل آن‌ها یا شنود محتوای سری در حال انتقال، به حبس از یک تا سه سال یا جزای نقدی از بیست میلیون (۲۰.۰۰۰.۰۰۰) ریال تا شصت میلیون (۶۰.۰۰۰.۰۰۰) یا هر دو مجازات.

ب) در دسترس قرار دادن داده‌های مذکور برای اشخاص فاقد صلاحیت، به حبس از دو تا ده سال.

ج) افشا یا در دسترس قرار دادن داده‌های مذکور برای دولت، سازمان، شرکت یا گروه‌های بیگانه یا عاملان آن‌ها، به حبس از پنج تا پانزده سال.

تبصرهٔ ۱- داده‌های سری داده‌هایی است که افشای آن‌ها به امنیت کشور یا منافع ملی لطمه می‌زند.

تبصرهٔ ۲- آیین‌نامهٔ نحوهٔ تعیین و تشخیص داده‌های سری و نحوهٔ طبقه‌بندی و حفاظت آن‌ها ظرف سه ماه از تاریخ تصویب این قانون توسط وزارت اطلاعات با همکاری وزارت‌خانه‌های دادگستری کشور، ارتباطات و فناوری اطلاعات و دفاع و پشتیبانی نیروهای مسلح تهیه و به تصویب هیئت دولت خواهد رسید.

مادهٔ ٤ قانون جرائم رایانه‌ای (مادهٔ ۷۳۲ قانون مجازات اسلامی) نیز مقرر می‌دارد: «هر کس به قصد دسترسی به داده‌های سری موضوع مادهٔ ۳ قانون جرائم رایانه‌ای یا مخابراتی را نقض کند، به حبس از شش ماه تا دو سال یا جزای نقدی از ده میلیون (۱۰.۰۰۰.۰۰۰) ریال تا چهل میلیون (٤۰.۰۰۰.۰۰۰) ریال یا هر دو مجازات محکوم خواهد شد».

مادهٔ ۵ قانون جرائم رایانه‌ای (مادهٔ ۷۳۳ قانون اسلامی) نیز مقرر می‌دارد: «چنانچه مأموران دولتی که مسئول حفظ داده‌های سری 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 بر اثر بی‌احتیاطی، بی‌مبالاتی یا عدم رعایت تدابیر امنیتی موجب دسترسی اشخاص فاقد صلاحیت به داده‌ها، حامل‌های داده یا سامانه‌های مذکور شوند، به حبس از نود و یک روز تا دو سال یا جزای نقدی از پنج تا چهل میلیون ریال یا هر دو مجازات و انفصال از خدمت از شش ماه تا دو سال محکوم خواهند شد».

غیرنظامی به موجب قانون یا دستورات مقام قضائی یا اجازه از طرف افراد و مقامات مسئول و مجاز مافوق به محتوای در حال انتقال را شنود می‌کند، عمل وی فاقد وصف جزایی است.

درخصوص نتیجهٔ مجرمانهٔ جرم تحصیل غیرمجاز داده‌های سری رایانه‌ای موضوع بند (الف) مادهٔ ۷۳۱ قانون مجازات اسلامی باید خاطرنشان کرد با صرف تحصیل غیرمجاز داده‌های مزبور عنوان مجرمانهٔ تحصیل غیرمجاز تحقق می‌یابد. بنابراین جرم مزبور مطلق بوده و حصول نتیجه در آن ضروری نیست.

### ۳ـ۲ـ۳. عنصر معنوی تحصیل غیرمجاز داده‌های سری

از مادهٔ ۷۳۰ (شنود غیرمجاز)، مادهٔ ۷۴۰ (سرقت رایانه‌ای) و بند (الف) مادهٔ ۷۳۱ قانون مجازات اسلامی و تبیین مفهوم تحصیل غیرمجاز، قابل استنباط است که شخص غیرنظامی باید بداند متعلق رفتار«دادهٔ رایانه‌ای» است که به وصف «سری» اعم از ذخیره‌شده و در حال انتقال و «نظامی بودن» موصوف شده است (علم به موضوع و اوصاف آن). منظور از سوء نیت عام این است که مرتکب، قصد رفتار «تحصیل» ازقبیل شنود، سرقت و ... داشته باشد. با توجه به اینکه در جرم مزبور، از جرائم مقید نیست، بنابراین، وجود سوء نیت خاص (قصد حصول نتیجهٔ مورد نظر قانونگذار) در مرتکب ضروری نیست و مرتکب به صرف «تحصیل» مشمول مجازات‌های مقرر خواهد شد.

ایراد اول وارد بر سیاست کیفری ایران در قبال تحصیل غیرمجاز اطلاعات رایانه‌ای طبقه‌بندی‌شدهٔ نظامی از سوی اشخاص غیرنظامی این است که قانون‌گذار در مادهٔ 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 داده‌ها و اطلاعات رایانه‌ای به‌کلی سری نظامی را برای مثال با رفتار مجرمانهٔ شنود غیرمجاز تحصیل کند، مطابق بند (ج) مادهٔ ۷۵۴ قانون مجازات اسلامی به بیش از دوسوم حداکثر یک یا دو مجازات مقرر در مادهٔ 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.

ممکن است گفته 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 از لحاظ اهمیت در چهار دسته قرار می‌گیرد و اگر مقصود مقنن از عبارت «داده‌های سری»، اطلاعات طبقه‌بندی‌شده باشد،

می‌بایست درخصوص تعیین مجازات نیز اهمیت اطلاعات طبقه‌بندی‌شده را لحاظ می‌کرد و برای اطلاعات به کلی سری، مجازات شدیدتری را نسبت به اطلاعات محرمانه درنظر می‌گرفت که در این ماده چنین امری صورت نگرفته است.

ایراد دوم وارد بر سیاست کیفری ایران در قبال تحصیل غیرمجاز اطلاعات طبقه‌بندی‌شدهٔ 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، داده‌ها و اطلاعات طبقه‌بندی‌شدهٔ رایانه‌ای نظامی تحصیل کنند و با آگاهی و اطلاعات کافی حملات سایبری خویش را علیه سامانه‌های حیاتی نظامی مرتکب شوند و امنیت کشور را به مخاطره اندازد. شایسته است مقنن در برابر حمایت از داده‌ها یا اطلاعات طبقه‌بندی‌شدهٔ رایانه‌ای که ممکن است از آن سوی مرزها توسط دشمنان و بیگانگان به واسطهٔ رفتارهایی ازقبیل شنود (دریافت)، برش، رونوشت و ... که محرمانگی آن‌ها را نقض می‌کند چاره‌اندیشی کند.

بدیهی است سیاست کیفری کنونی متناسب و بازدارنده نیست، چراکه نتیجهٔ قهری چنین سیاست کیفری این است که از نظر قانون‌گذار در فرضی که بیگانه‌ای به‌طور غیرمجاز محتوای سری در حال انتقال نظامی را دریافت کند، مطابق بند (الف) مادهٔ ۷۳۰ قانون مجازات اسلامی رفتار وی جاسوسی رایانه‌ای بوده و در فرض دیگر، اگر بیگانه‌ای به‌طور غیرمجاز محتوای رایانه‌ای نظامی به‌کلی سری در حال انتقال را شنود کند، رفتار وی مصداق جاسوسی نبوده و صرفاً با رعایت مادهٔ ۷۵۴ قانون مجازات اسلامی به مجازات پیش‌بینی‌شده در مادهٔ ۷۳۰ قانون مجازات اسلامی محکوم شود. شایسته است مقنن جهت برون‌رفت از چنین سیاست کیفری نامتناسب و ناکارآمد با پیش‌بینی جرم تحصیل غیرمجاز دادهٔ طبقه‌بندی‌شدهٔ رایانه‌ای در قانون مجازات جرائم نیروهای مسلح در پرتو بند (ه) مادهٔ ۲۴ قانون مزبور بیگانه‌ای را که از آن سوی مرزها مرتکب جرم تحصیل غیرمجاز داده‌های رایانه‌ای طبقه‌بندی نظامی می‌شود به حبس تعزیری درجه چهار محکوم کند.

در اهمیت این امر می‌توان به بدافزار «فلیم»[1] که علیه نیروگاه هسته‌ای نطنز رخ داد، اشاره کرد. پیرامون این بدافزار برخی از متخصصان فنی شرکت کاسپرسکی[2] (از برجسته‌ترین شرکت‌های تولید ضد بدافزار) بیان داشتند که بدافزار فلیم نه‌تنها اطلاعات را کپی و به سرور مقصد انتقال می‌داد، بلکه توانایی تغییر در دستورات و اطلاعات موجود در سامانه‌های رایانه‌ای موردنظر و

---

1. flame

2. kaspersky

همچنین توانایی فعال کردن میکروفن‌های سامانه‌های رایانه‌ای جهت ضبط کردن صداهای اطراف خود را داشت. دیگر توانایی‌هایی بدافزار فلیم که برای نخستین‌بار دیده شد، توانایی آن در استفاده از فناوری بلوتوث[1] جهت انتشار خود به دیگر سامانه‌های رایانه‌ای بود که در فاصلهٔ کمی از سامانهٔ رایانه‌ای آلوده قرار داشتند که به سرقت اطلاعات موجود در سامانه‌های رایانه‌ای اطراف نیز منجر می‌شد (مؤسسهٔ فرهنگی مطالعات و تحقیقات بین‌المللی ابرار معاصر، ۱۳۹۱: ۳۳۱).

همچنین می‌توان به بدافزار «دوکو»[2] علیه نیروگاه هسته‌ای جمهوری اسلامی ایران اشاره کرد که هدف آن جمع‌آوری و سرقت داده‌ها و اطلاعات طبقه‌بندی حساس نیروگاه هسته‌ای و دیگر سازمان‌ها بود. کارشناسان با بررسی‌های خود پیرامون بدافزار دوکو دریافتند که طراحان بدافزار دوکو برای نفوذ به سامانه‌های رایانه‌ای از یک اشکال ناشناخته‌ای که در مدیریت فونت[3]های موجود در هستهٔ ویندوز وجود داشت به سامانه‌های رایانه‌ای موردنظر خود نفوذ کردند. سپس بدافزار به اجزای مختلف سامانه‌های رایانه‌ای نفوذ می‌کرد و از طریق یک فایل متنی ورد[4] که از محصولات شرکت مایکروسافت[5] است، گسترش می‌یافت و سطح امنیت سامانه‌های رایانه‌ای را تحت تأثیر قرار می‌داد و به‌علت آنکه این بدافزار فایل‌هایی با پسوند دی کیو[6] می‌ساخت، متخصصان نام این بدافزار را «دوکو» نامیدند. همچنین آنان دریافتند که هنگامی بدافزار دوکو در سامانه‌های رایانه‌ای هدف قرار می‌گرفت عملکرد خود را در همان لحظه آغاز نمی‌کرد، بلکه هنگامی‌که سامانه‌های رایانه‌ای برای مدت تقریباً ده دقیقه مورداستفاده قرار نمی‌گرفتند بدافزار دوکو آغاز به فعالیت می‌کرد و به سرقت اطلاعات حساس صنعتی و دیگر سازمان‌ها منجر می‌شد. درواقع دوکو قادر بود اطلاعاتی را از طراحان و سازندگان سامانه‌های کنترلی تحصیل کند و مسیر را برای حملات بعدی هموارتر سازد و نکتهٔ جالب آنکه این بدافزار سامانه‌های رایانه‌ای خود را با دقت انتخاب می‌کند و برای حمله به هر یک از آن‌ها از روش منحصربه‌فرد و اختصاصی استفاده می‌کرد و تلاش فزایندهٔ دوکو برای پنهان‌کاری و حذف ردپای خود امری غیرقابل باور بود

---

1. bluetooth
2. Duqu
3. font
4. Word
6. Microsoft
7. DQ

(http://www.gerdab.ir/fa/news/8175). دور از ذهن است در آینده داده‌ها و اطلاعات رایانه‌ای نظامی مورد هجوم این قبیل از بدافزارهای رایانه‌ای قرار گیرند.

**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 ... ، رفته رفته در پیروزی‌های نهادهای نظامی بر هم‌آوردان 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.

در خصوص مفهوم تحصیل غیرمجاز و مصادیق آن این نتیجه حاصل شد که تحصیل غیرمجاز شامل هر رفتار مجرمانه‌ای در فضای سایبر است که موجب در اختیار قرار گرفتن داده‌های رایانه‌ای می‌شود. حال هرگاه موضوع تحصیل غیرمجاز داده‌های ذخیره شده باشد، عنوان مجرمانه مستقل سرقت رایانه‌ای تحقق می‌یابد و هرگاه موضوع آن محتوای در حال انتقال باشد، عنوان مجرمانه مستقل شنود غیرمجاز تحقق می‌یابد و در موردی که داده‌های حذف‌شده با روش‌های فنی بازیابی شوند رفتار ارتکابی مصداق تحصیل غیرمجاز است.

ایرادت وارد بر سیاست کیفری ایران در قبال تحصیل غیرمجاز داده‌های رایانه‌ای فاقد طبقه‌بندی نظامی از سوی اشخاص نظامی و غیرنظامی به شرح زیر است:

چنانچه مرتکب جرم شخص نظامی باشد، این ایراد متوجه قانون‌گذار است که چون حداکثر مجازات را افزایش نداده است، بلکه حداقل آن را افزایش داده، این امر سبب شده است که حداکثر مجازات تحصیل غیرمجاز داده‌های رایانه‌ای فاقد طبقه‌بندی نظامی از سوی اشخاص نظامی و غیرنظامی تفاوتی وجود نداشته باشد. در حالی باید درنظر داشت نظم و انضباط و حساسیت شغلی و مأموریت‌های نظامی ایجاب می‌کند بر شدت و حدت مجازات‌ها افزود، چراکه غفلت از مقررات و بی‌توجهی فرد نظامی، به ضوابط موجود، می‌تواند اثرات جبران‌ناپذیری بر امنیت داخلی و خارجی بر جای گذارد.

ایراد دوم این است چون عنوان مجرمانه شنود غیرمجاز و سرقت رایانه‌ای در قانون مجازات جرائم نیروهای مسلح پیش‌بینی‌نشده است، مجازات آن‌ها از حیث تخفیف و تبدیل تابع قانون مجازات اسلامی است. اما چون جرمی مانند جعل رایانه‌ای که از سنخ جرائم سایبری است و در قانون مجازات جرائم نیروهای مسلح پیش‌بینی شده است، مجازات آن‌ها از حیث تخفیف و تبدیل

تابع قانون مجازات جرائم نیروهای مسلح است. بدیهی است چنین سیاست کیفری افتراقی از سوی مقنن قابل توجیه نیست و شایسته است مقنن به نحو حصری و مستقل آن‌ها را در قانون مجازات جرائم نیروهای مسلح پیش‌بینی کند.

چنانچه مرتکب جرم شخص غیرنظامی باشد، این ایراد متوجه قانون‌گذار است که چون حداکثر مجازات را افزایش نداده، بلکه حداقل آن را افزایش داده است، اگر یک شخص غیرنظامی داده‌های رایانه‌ای غیرنظامی را تحصیل کند و مقام قضائی وی را به اشد مجازات محکوم کند، مجازات وی در وضعیتی که داده‌های رایانه‌ای نظامی را تحصیل کند، از حیث حداکثر مجازات یکسان است. شایسته است میزان درجهٔ اهمیت داده‌ها و اطلاعات رایانه‌ای نظامی به موجب دستورالعملی از سوی ستاد کل نیروهای مسلح تدوین شود تا مجازات مرتکب تابع درجهٔ اهمیت داده‌ها و اطلاعات رایانه‌ای نظامی از اصول بازدارندگی و تناسب جرم و مجازات برخوردار باشد.

ایراد دیگری که نسبت به سیاست کیفری کنونی وارد است این است چنانچه شخص نظامی یا غیرنظامی به‌واسطهٔ رفتار بازیابی اطلاعات، داده‌ها و اطلاعات رایانه‌ای نظامی فاقد طبقه‌بندی را تحصیل کند، رفتار وی منطبق با هیچ‌یک از مواد پیش‌بینی‌شده در قانون مجازات جرائم نیروهای مسلح و قانون جرائم رایانه‌ای نیست و با توجه به اصل قانونی بودن جرائم و مجازات‌ها وی اساساً قابل مجازات نیست. شایسته است مقنن جهت برون‌رفت از این خلأ قانونی در قانون مجازات جرائم نیروهای مسلح چاره‌اندیشی کند.

ایرادات وارد بر سیاست کیفری ایران در قبال تحصیل غیرمجاز داده‌های رایانه‌ای طبقه‌بندی‌شده نظامی از سوی اشخاص نظامی و غیرنظامی به شرح زیر است:

چنانچه مرتکب جرم شخص نظامی باشد، چون قانون‌گذار در مادهٔ ۱۳۱ از عبارت (اقداماتی ازقبیل ...) استفاده کرده است که نظر به تمثیلی بودن موارد مزبور در مادهٔ ۱۳۱ داشته، شامل تحصیل غیرمجاز داده‌های طبقه‌بندی‌شده رایانه‌ای نیز می‌شود، بنابراین مرتکب به مجازات پیش‌بینی‌شده در بند (ب) مادهٔ ۲۴ قانون مجازات جرائم نیروهای مسلح محکوم می‌شود، اما این نقد به قانون‌گذار وارد است که ذکر عباراتی مانند امثالهم، نظایر آن و ازقبیل 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 کند از اینکه به‌طور شفاف مقصود خودش را از مخاطبان بخواهد. همچنین 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 است.

ایراد دیگر بر سیاست کیفری ایران این است که چنانچه یکی از شروط تحقق جرم موضوع بند «ب» مادهٔ ۲۴ قانون مجازات جرائم نیروهای مسلح احراز نشود و موضوع رفتار وی داده‌های سری باشد، عمل وی با تحقق سایر شرایط مشمول بند (الف) مادهٔ 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 حسب مورد مصداق عنوان مجرمانه شنود غیرمجاز یا سرقت رایانه‌ای قرار می‌گیرد. نتیجهٔ قهری این رویکرد این است که در فرض اول کیفیات مخففه یا نهادهای ارفاقی ازقبیل تعویق صدور حکم، تعلیق اجرای مجازات نسبت به مرتکب قابل اعمال نیست، اما در فرض اخیر حتی اگر متعلق رفتار وی داده‌های به‌کلی سری که از درجهٔ اهمیت بالاتری نسبت به داده‌های سری برخوردارند، باشد حسب مورد به مجازات‌های پیش‌بینی در مادهٔ ۷۳۰ و ۷۴۰ قانون مجازات اسلامی با رعایت بند (الف) مادهٔ ۷۵۴ محکوم شده و کیفیات مخففه و نهادهای ارفاقی مطابق قانون مجازات اسلامی نسبت به وی قابل اعمال است.

چنانچه مرتکب جرم شخص غیرنظامی باشد، اشکال اول وارد بر سیاست کیفری ایران در قبال تحصیل غیرمجاز اطلاعات رایانه‌ای طبقه‌بندی‌شده این است قانون‌گذار در مادهٔ ۷۳۱ تنها داده‌های سری را مصداق جاسوسی رایانه‌ای دانسته و سایر اشکال طبقه‌بندی اطلاعات رایانه‌ای را مصداق جاسوسی ندانسته است. بنابراین اگر یک شخص غیرنظامی داده‌ها و اطلاعات رایانه‌ای به‌کلی سری، خیلی محرمانه یا محرمانه نظامی را با رفتار شنود غیرمجاز تحصیل کند، مطابق بند (ج) مادهٔ ۷۵۴ قانون مجازات اسلامی به بیش از دوسوم حداکثر یک یا دو مجازات مقرر در مادهٔ 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. اشکال دوم این است که امروزه فضای سایبر امکاناتی را فراهم آورده است تا دشمنان و بیگانگان بدون خطراتی که جاسوسی سنتی به همراه داشت داده‌ها و اطلاعات طبقه‌بندی‌شده رایانه‌ای نظامی تحصیل کنند و با آگاهی و اطلاعات کافی حملات سایبری علیه سامانه‌های حیاتی نظامی مرتکب شوند و امنیت کشور را به مخاطره اندازد. شایسته است مقنن در برابر حمایت از داده‌ها یا اطلاعات طبقه‌بندی‌شدهٔ رایانه‌ای نظامی که ممکن است از آن سوی مرزها توسط دشمنان و بیگانگان به‌واسطهٔ رفتارهایی ازقبیل شنود (دریافت)، برش، رونوشت و ... محرمانگی آن‌ها نقض شود در پرتو بند (ه) مادهٔ ۲۴ قانون مجازات جرائم نیروهای مسلح یا مادهٔ ۷۳۹ قانون مجازات اسلامی سیاست کیفری متناسب و بازدارنده‌ای را اتخاذ کند.

## فهرست منابع

### الف) منابع فارسی


- الهام، غلامحسین (۱۳۸۹)، **حقوق جزای نظامی**، تهران: دادگستر.
- الهام، غلامحسین و محسن برهانی (۱۳۹۴)، **درآمدی بر حقوق جزای عمومی (جرم و مجرم)**، جلد اول، تهران: میزان.
- الهی‌منش، محمدرضا و ابوالفضل سدره‌نشین (۱۳۹۵)، **محشای قانون جرائم رایانه‌ای**، تهران: مجد.
- بابایی، جواد (۱۳۹۸)، **جرائم رایانه‌ای و آیین دادرسی حاکم بر آن**، تهران: نشر مرکز مطبوعات و انتشارات قوهٔ قضائیه.
- باری، مجتبی (۱۳۹۸)، **حقوق جزای نظامی**، تهران: دادستان.
- پاک‌نیت، مصطفی (۱۳۹۶)، **افتراقی شدن دادرسی کیفری**، تهران: میزان.
- جلالی فراهانی، امیرحسین (۱۳۹۵)، **کنوانسیون جرائم سایبر و پروتکل الحاقی آن**، تهران: خرسندی.
- خالقی، علی (۱۳۹۵)، **آیین دادرسی کیفری**، جلد دوم، تهران: مؤسسهٔ 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**، پایان‌نامهٔ کارشناسی ارشد، تهران: دانشگاه پیام نور مرکز تهران.
- زراعت، عباس (۱۳۹۴)، **شرح مختصر قانون مجازات اسلامی**، جلد دوم، تهران: ققنوس.
- زندی، محمدرضا (۱۳۹۳)، **تحقیقات مقدماتی در جرائم سایبری**، تهران: انتشارات جنگل، جاودانه.
- سبزگلی، مجید و سیدعلی موسوی (۱۳۹۲)، **مفاهیم پایهٔ فناوری اطلاعات**، تهران: شرکت چاپ و نشر کتاب‌های درسی ایران.
- صبحی شیشوان، بهنام (۱۳۸۳)، «شیوه‌های گوناگون سرقت رایانه‌ای»، **ماهنامهٔ وکالت**، شمارهٔ ۲۱.
- عالی‌پور، حسن (۱۳۹۳)، **حقوق کیفری فناوری اطلاعات**، تهران: خرسندی.
- عزیزی، امیرمهدی (۱۳۹۴)، **حقوق کیفری جرائم رایانه‌ای**، تهران: مجد.
- عمید، حسن (۱۳۶۵)، **فرهنگ عمید**، تهران: امیرکبیر.
- قاجارقیونلو، سیامک (۱۳۹۱)، **مقدمهٔ علم حقوق سایبر**، تهران: میزان.
- کیهانلو، فاطمه و وحید رضادوست (۱۳۹۳)، «حملات سایبری به‌مثابهٔ توسل به‌زور در سیاق منشور ملل متحد»، **فصلنامهٔ تحقیقات حقوقی**، شمارهٔ ۶۹.
- گلدوزیان، ایرج (۱۳۹۶)، **بایسته‌های حقوق جزای عمومی**، تهران: میزان.
- محمدنسل، غلامرضا (۱۳۹۵)، **حقوق جزای اختصاصی جرائم رایانه‌ای در ایران**، تهران: میزان.
- مرسی، هادی (۱۳۹۷)، **مقابله با حملات سایبری در حقوق کیفری ایران و اسناد بین‌المللی (با تأکید بر حملات سایبری علیه ایران)**، پایان‌نامهٔ کارشناسی ارشد، تهران: دانشکدهٔ حقوق و علوم سیاسی دانشگاه تهران.
- مؤسسهٔ فرهنگی مطالعات و تحقیقات بین‌المللی ابرار معاصر (۱۳۹۱)، **امنیت و جنگ سایبری (۲) (ویژهٔ سلاح‌ها، جنگجویان و حملات سایبری)**، تهران: نشر مؤسسهٔ فرهنگی مطالعات و تحقیقات بین‌المللی ابرار معاصر.
- مهران‌فر، ابراهیم و علیرضا قلی‌پور شهرکی (۱۳۹۹)، **شرح جامع و کاربردی قانون مجازات جرائم نیروهای مسلح مصوب ۱۳۸۲/۱۰/۰۹**، تهران: جنگل.
- میرمحمدصادقی، حسین (۱۳۹۳)، **جرائم علیه امنیت و آسایش عمومی**، تهران: میزان.

- یزدانیان، محمدرضا (۱۳۹۰)، **قانون مجازات جرائم نیروهای مسلح در نظم حقوقی کنونی**، تهران: میزان.
- یکرنگی، محمد، هادی مرسی و مهسا علیزاده (۱۴۰۰)، «امکان‌سنجی استناد به دفاع مشروع به‌عنوان مانع مسئولیت کیفری در مقابل حملات سایبری»، **مجلۀ مطالعات حقوق کیفری و جرم‌شناسی**، شمارۀ ۲.
- یکرنگی، محمد و هادی مرسی (۱۳۹۹)، «تحلیل جرم‌انگاری تولید و پخش نرم‌افزار و ابزارهای الکترونیکی صرفاً مجرمانه در سیاست کیفری ایران در پرتو اسناد فرامرزی»، **مجلۀ دیدگاه‌های حقوق قضائی**، دورۀ ۲۵، شمارۀ ۹۲.


## ب) منابع انگلیسی


- Clarke, A., K. Richard, & R. Knanke (2010), *Cyber War:The Next Thread to National Security and What to Do about it*,Manhattan, New York, Ecco.
- www.library.arizona.edu/rio/glossary.html (visited: 2023-1-7)
- Joint Chiefs of Staff, Joint Publication 1-02, Dep't of Def. Dict. of Military and Assoc'd Terms, 2001, p.141 available at: http://www.dtic. mil/doctrine/ jel/newoubs/ jp102.pdf (visited 2023-1-4)
- http://www.gerdab.ir/fa/news/8175