Interdisciplinary Legal Research
Jun 2025, 6(2): 43-54
Available online on: www. ilrjournal.ir
e-ISSN:2717-1795

ORIGINAL RESEARCH PAPER

Cyber Espionage in the Criminal Policy of Iran and Afghanistan

Qorban Fayyaz✱ [1], Mohammad Ali Hajidehabadi [2], Saeid Attarzadeh[3]

Received:
14 Feb 2025
Revised:
15 Mar 2025
Accepted:
18 Mar 2025
Available Online:
22 Jun 2025

Abstract

Background and Aim: The present study, entitled *"Cyber Espionage in the Criminal Policy of Iran and Afghanistan"*, has been conducted with the aim of understanding, identifying the distinguishing and common aspects, and comparing the criminal policies of the two countries regarding cyber espionage.

Materials and Methods: The overarching research strategy is applied in terms of purpose, and analytical–descriptive in method of execution; data collection has been conducted through library-based research.

Ethical Considerations: All ethical principles have been followed in writing this article.

Findings: The findings of the study have been analyzed based on the researchers' understanding of legal sources and texts relating to the criminal policies of the two countries. A comparative examination of the criminal policies of Iran and Afghanistan with respect to cyber espionage reveals the strengths and shortcomings of each, enabling the adoption of the strengths of one to remedy the weaknesses of the other.

Conclusion: The advantage of Iran's criminal policy, compared with that of Afghanistan, lies in its precision and differentiation concerning the criminal dimension of the cyber espionage offense. Specifically, it distinguishes between: an individual who merely gains access to classified information, an individual who delivers such information to unauthorized persons, and an individual who delivers such information to foreigners or enemies, and assigns punishments commensurate with the nature of the committed offense. In contrast, Afghanistan's criminal policy imposes a uniform punishment on all such individuals without differentiation. A strength of Afghanistan's criminal policy is that it distinguishes espionage committed during wartime from espionage committed under normal circumstances. A common deficiency in the criminal policies of both countries is the lack of attention to the criminalization and penal dimension concerning accomplices and accessories to the offense of cyber espionage.

Keywords:
Cyber Espionage, Cyberspace, Penal Policy.

1* Ph.D Student of Criminal Law and Criminology, Al-Mustafa International University, Qom, Iran. (Corresponding Author)
2 Faculty Member, University of Qom, Qom, Iran.
3 Assistant Professor, University and Police Research Institut.e, Tehran, Iran

Please Cite This Article As: Fayyaz, Q; Hajidehabadi, MA & Attarzadeh, S (2025). "Cyber Espionage in the Criminal Policy of Iran and Afghanistan". *Interdisciplinary Legal Research*, 6 (2): 43-54.

مقاله پژوهشی
(صفحات ۴۳-۵۴)

جاسوسی سایبری در سیاست کیفری ایران و افغانستان

قربان فیاض*[۱]، محمدعلی حاجی‌ده‌آبادی[۲]، سعید عطارزاده[۳]

۱. دانشجوی دکتری حقوق کیفری و جرم‌شناسی، جامعه المصطفی العالمیه، قم، ایران. (نویسنده مسؤول)
۲. عضو هیآت علمی دانشکده حقوق، دانشگاه قم، قم، ایران.
۳. استادیار، دانشگاه و پژوهشگاه انتظامی، تهران، ایران.

دریافت: ۱۴۰۳/۱۱/۲۵ ویرایش: ۱۴۰۳/۱۲/۲۵ پذیرش: ۱۴۰۳/۱۲/۲۸ انتشار: : ۱۴۰۴/۰۴/۰۱

چکیده

زمینه و هدف: تحقیق حاضر، تحت عنوان «جاسوسی سایبری در سیاست کیفری ایران و افغانستان» به هدفِ فهم، شناختِ وجه تمایز و تشابه و تطبیق سیاست کیفری دو کشور، در مورد جاسوسی سایبری انجام شده است.

مواد و روش‌ها: راهبرد کلی تحقیق، به لحاظ هدف کاربردی و از جهت شیوه اجرا تحلیلی- توصیفی و روش گردآوری آن به شیوه کتابخانه‌ای است.

ملاحظات اخلاقی: تمامی اصول اخلاقی در نگارش این مقاله رعایت شده است.

یافته‌ها: یافته‌های تحقیق، براساس فهم محققان از منابع و متون قانونی در مورد سیاست کیفری دو کشور، تجزیه و تحلیل شده است. با مقایسه سیاست کیفری دو کشور در مورد جاسوسی سایبری می‌توان امتیازات و کاستی‌های هر یک را به خوبی متوجه شده و از امتیازات یکی برای رفع کاستی‌های دیگری، الگوگیری کرد.

نتیجه‌گیری: امتیاز سیاست کیفری ایران نسبت به سیاست کیفری افغانستان، در دقت و تفاوت قائل شدن به بعدکیفری جرم جاسوسی سایبری است؛ زیرا بین کسی که به اطلاعات سری فقط دسترسی پیدا کرده است و کسی که این اطلاعات را به افراد فاقد صلاحیت تسلیم کرده است و کسی که این اطلاعات را به بیگانگان و دشمنان تسلیم داده است؛ تفاوت قائل شده و مجازات این افراد را متناسب به جرم ارتکابی در نظر گرفته است. این درحالی است که در سیاست کیفری افغانستان برای این افراد بدون تفاوت، مجازات یکسان لحاظ کرده است. از امتیاز سیاست کیفری افغانستان این است که جاسوسی در زمان جنگ با جاسوسی در حالت عادی را فرق گذاشته است. کاستی دیگری در سیاست کیفری دو کشور، عدم توجه به بعد جرم‌انگاری و بعد کیفری شریک و معاون جاسوسی سایبری است.

کلمات کلیدی: فضای سایبری، جاسوسی سایبری، سیاست کیفری.

مقدمه

امروزه فناوری مخابراتی، بشر را در یک دهکده جهانی گردهم جمع کرده است و در تمام عرصه‌های زندگی با کمک تکنولوژی ارتباطی می‌توانند به راحتی کار و تعامل کنند، بشرِ امروز می‌تواند با یک کلیک در فضای سایبر؛ به دنیایی از معلومات و اطلاعات دست یابد یا در گوشه‌ای از این کره‌خاکی پشت کامپیوتر نشسته دنیا را اداره کرده یا بهم‌بریزد. در کنار تمام سهولت‌ها و امکاناتی که فضای مجازی به ارمغان آورده است طوری که یک روز اگر این فضا از دسترس کاربران خارج شود تمام امورات زندگی دچار چالش می‌شود؛ خطرهای فضای مجازی نیز جدی و جامعه برانداز است. قانون‌گذاران و مدیران یک کشور؛ اگر به آسیب‌های این حوزه توجه نکنند؛ پدیده بزهکاری‌ای که در فضای مجازی اتفاق می‌افتد باتوجه به ویژگی‌های این فضا؛ مانند گسترده بودن، جهان شمول بودن، پوشیده بودن، گزینشی بودن اطلاعات، قابل کنترل نبودن (الهوردی، ۱۳۹۶: ۲۱). ممکن است مخرب‌تر از فضای حقیقی باشد. با آن‌که کار و پژوهش در هرزمینه از حقوق افغانستان را لازم می دانم چون همانند طبیعت افغانستان حوزه حقوقی این کشور نیز بکر و دست ناخورده است و هیچ شرح و بسط کافی راجع به قوانین و مقررات این کشور برای کمک به دادرسی عادلانه صورت نگرفته است اما پژوهش در مورد جاسوسی سایبری را به دلیل اهمیت امنیت ضروری‌تر می‌دانم؛ زیرا در این چند سال اخیر با توجه به افزایش چشمگیر کاربران افغانستانی؛ بزهکاری سایبری در افغانستان بر علیه امنیت به شدت افزایش یافته است وبررسی و تحقیق در سیاست کیفری افغانستان و ایران در قبال جاسوسی سایبری که ضربه شدیدی به امنیت وارد می‌کند خالی از لطف نیست؛ زیرا با تطبیق و مقایسه سیاست کیفری دو کشور در جاسوسی سایبری می‌توان امتیازات و کاستی‌های هر یک را به خوبی متوجه شده و از امتیازات یکی برای رفع کاستی‌های دیگر الگوگیری کرد.

باتوجه به اهمیت امنیت در کشورها، در عصرحاضر فناوری و فضای سایبری باعث شده است که اخلال‌گران امنیت این محیط را برای نا امن کردن جغرافیایی مورد نظرشان انتخاب کنند. انتخاب این راه به دلیل سرعت، گستردگی، کم هزینه و آسان بودن این فضا آگاهانه است. فضای سایبری، نسبت به گذشته جاسوسی را راحت و بدون خطر کرده است که بدون دخیل بودن نیروی انسانی و خطری گیرافتادن او، توسط ابزار و فناوری سایبری به راحتی می‌توان از هدف جاسوسی کرد و معلومات محرمانه را بدست آورد. بنابر این، یکی از مشکلات کشورها برای تأمین امنیت، جاسوسی سایبری است که هرکشوری برای تأمین امنیت خود و برای مبارزه با جرم جاسوسی، سیاست کیفری مختص به خودش را دارد. هدفم از این تحقیق کاربردی، بررسی سیاست کیفری افغانستان در قبال جرم جاسوسی سایبری در ایران و افغانستان است تا نشان دهم که میزان انطباق آن با سیاست کیفری عادلانه چگونه بوده و تا چه اندازه این سیاست کیفری در قبال جاسوسی سایبری، کارایی دارد.

۲- مفهوم شناسی

۲-۱-جرایم فضای سایبری

امنیت روزافزون فضای سایبری، مدیون نابغه‌های فناوری اطلاعات است که مسئولین امنیت را وادار به حفظ امنیت فضای سایبری و طراحی برنامه‌های پیچیده کرده است تا از نفوذ خرابکاران و نابغه‌های بیکار یا انتقامجو در امان باشد. گاهی این نابغه‌های فناوری با گستراندن دام‌های پیچیده‌شان، مدعیان امنیت فضای سایبر را به ستوه آورده‌اند. بزهکاران از فناوری اطلاعات استفاده کرده و باتوجه به ویژگی فضای سایبر به راحتی دست به ناهنجارهایی می‌زنند که امنیت و نظم جامعه را با چالش مواجه می‌سازند. پیچیدگی جرایم سایبری و مشخص نبودن ماهیت جرم سایبری، باعث شده است که تعریف دقیقی هنوز از این جرم ارائه نگردیده است. حتی کشورها در مورد تعریف و ماهیت جرایم سایبری از الگوی یکسانی تبعیت نکرده است. شورای اروپا، سوء استفاده از رایانه به عنوان هر رفتاری غیرقانونی- غیراخلاقی یا غیر مجاز مربوط به پردازش اتوماتیک و انتقال داده‌ها را جرم رایانه‌ای می‌داند (زندی، ۱۳۹۳: ۲۳). ایراد این تعریف در این است که براساس ابزار به جودآورنده «محیط سایبر» شکل گرفته است. دقت به مفهوم شناسی سخت افزاری با درنظر گرفتن تغییرات دوامدار در بخش فناوری اطلاعات، صحت و کامل بودن آن تعریف را خدشه دار کرده است. وزارت دادگستری ایالات متحده، تعریف موسعی از جرایم رایانه‌ای ارائه می‌دهد. از دیدگاه این نهاد، جرم

رایانه‌ای هرجرمی را شامل می‌شود که برای ارتکاب، تحقیق و بازرسی یا دادرسی نسبت به آن از فناوری رایانه استفاده شود (National Institute of justice, 1998:2).

کد جزای افغانستان در ماده ۸۵۱ جرم سایبری را به جرایمی تعریف کرده است که این جرایم توسط فناوری مدرن اطلاعات و ارتباطات الکترونیکی یا اینترنتی در محیط سایبر تحقق می‌یابد (کدجزای افغانستان، ۱۳۹۶: ماده ۸۵۱). آن‌چه که جرم سایبری را از غیرسایبری متمایز می‌کند؛ مسائل و چالش‌هایی است که بهره‌مندی از فضای سایبر برای ارتکاب جرم آن‌ها را به وجود می‌آورد. جرایم سایبری را می‌شود به سه بخش، دسته‌بندی و بررسی نمود: بخش نخست جرایمی‌اند که در آن‌ها کامپیوتر و ابزار جانبی و فرعی آن موضوع جرم قررا می گیرد مثل سرقت، تخریب. بخش دوم بزه‌های اند که در آن‌ها کامپیوتر به حیث ابزار و وسیله تحقق بزه استعمال می‌گردد. در آخر، بخش سوم جرایمی‌اند که می‌شود آن‌ها را بزه سایبری محض و خالص نامگذاری کرد. این گونه از جرایم کاملاً با بزه‌های سنتی تفاوت دارد که درجهان سایبری تحقق یافته اما در جهان حقیقی نمود پیدا می‌کند؛ مثل دستری غیر مجاز به سیستم‌های رایانه‌ای و جاسوسی (محمدنسل، ۱۳۹۵: ۱۶).

امروزه دنیای مجازی بسیار وسیع است و هیچ‌گونه تأکیدی بر وسایل وجود ندارد. ابزارهای متفاوتی درست شده است که هریک روش تازه و نو را در راه‌یافتن به این دنیا، بدون نیاز مستقیم به رایانه به ارمغان آورده است؛ از باب مثال گوشی‌های همراهِ هوشمند یکی از این ابزار است که بدودن نیاز به رایانه ما را به جهان سایبر وصل می‌کند.

۲-۲- جاسوسی سایبری

برای بزه جاسوسی رایانه‌ای تعریف واضح آورده نشده است، بایسته خواهد بود که کارشناسان فناوری و حقوق‌دانان به اتفاق، تعریف کامل انجام بدهند که بتواند مسیر سیاست کیفری کشورها را هموار سازد. همه کوشش کشورها در رابطه با این جرم در مورد جرم‌انگاری و برخورد قانونی باین جرم، هنوزهم دارای نقایص است که بسیاری از این نقض‌ها در قوانین مصوب شده موجود می‌باشد. همچنین نهادهای بین‌المللی مربوطه، تعریف شفاف از این بزه ندارند؛ به طور نمونه سازمان همکاری و توسعه اقتصادی، عنوان جاسوسی سایبری را به صورت روشن در جرم‌های یاد شده، نیاورده است و شورای اروپا در فهرست خود، نگاه ویژه به این عملکرد بزهکارانه حائز اهمیت، توجه نکرده است. همینطور سازمان ملل عملکرد شبیه به این در این مورد دارد. بنابراین، سزاوار است نهادهای بین‌المللی با بررسی دوباره و دقیق‌تری راجع به جرم‌های سایبری، جاسوسی سایبری را مورد توجه ویژه قرار داده و نگاه دیگر کشورها در بخش بین‌الملل را به این جرم جلب کنند تا عکس‌العمل آن‌ها، مانع قوی برای جلوگیری از گسترش روزافزون این جرم جدید در جامعه جهانی باشد.

جاسوسی، جرم عمدی است به این شکل که مجرم با نیت بد اطلاعات طبقه‌بندی شده را در اختیار بیگانگان و عوامل غیرمجاز می‌گذارد، ولی توجه به این‌که جرم جاسوسی اهمیت زیاد و خاص دارد؛ قانون‌گذار را مجبور به جرم‌انگاری برای این‌نوع سهل‌انگاری‌ها و بی‌مبالاتی‌ها کرده است.

شورای اروپا جاسوسی سایبری را این گونه بیان کرده است: **«کسب اسرار تجاری یا حرفه‌ای از راهای نادرست یا افشا، انتقال و یا استفاده از این اسرار بدون داشتن حق یا هرگونه توجیه قانونی با قصد وارد کردن زیان اقتصادی به فردی که محق در نگه داشتن اسرار است یا تحصیل یک امتیاز اقتصادی غیرقانونی برای خود یا یک شخص ثالث»** (کنوانسیون بوداپست، ۲۰۰۱). بر این تعریف نقدهای زیر وارد شده است: ۱- با ذکر کردن از اسرار تجاری یا حرفه‌ای در آن عملاً این تعریف را از شکل‌های دیگر اسرار از جمله اسرار امنیتی و اطلاعاتی و فرهنگی بیرون نموده است که دربردارنده جاسوسی سایبری نمی‌شود و با این عنوان به صورت کلی تناسب ندارد. ۲- راجع به قصد مجرم از ارتکاب این بزه که در تعریف صرفاً منافع اقتصادی مدنظر قرارداده شده است که این هم صحیح نیست؛ چون که امکان دارد جاسوسی اهدافی برتر از منافع اقتصادی داشته باشد که مثلاً امکان دارد فقط هدف‌های ملی در نظر باشد. ۳- در این تعریف، جاسوسی سایبری بیان نشده است، بلکه صرفاً مصادیق جاسوسی سایبری آن‌نیز نه به طور کامل ذکر گردیده است. چنانچه ذکر شد در قانون جزای افغانستان، تعریف روشن از جاسوسی سایبری ذکر نشده است، فقط به موارد و مصادیق

جاسوسی اشاره کرده است.

۲-۳- سیاست کیفری

ترکیب **«سیاست کیفری»** اصطلاح حقوقی است که از دو کلمه «سیاست» و «کیفر» ترکیب شده و برای استراتیژی‌جنایی کشورها؛ به منظور مجازات مجرمین و اصول کلی مربوط به قوانین جزایی کشورها می‌باشد. در کتاب «جایگاه امنیت در سیاست کیفری ایران» در تعریف سیاست کیفری چنین می پردازد: «در سال ۱۸۰۳ م اصطلاح سیاست کیفری یا سیاست جنایی، نخستین بار، توسط **فوئرباخ**[1] حقوق‌دان آلمانی به کار رفت. وی در تعریف سیاست جنایی گفته است: **«مجموعه روش‌های سرکوب‌گری است که دولت با استفاده از آن‌ها علیه جرم واکنش نشان می‌دهد»** (جعفری دولت‌آبادی،۱۳۹۵: ۱۹) در ادامه می‌گوید: **«سیاست کیفری یا سیاست جنایی در مفهوم مضیق، نقض هنجارهای صرفاً کیفری را مورد توجه قرار می‌دهد که نظام عدالت کیفری که توسط دولت اداره می‌شود، پاسخ‌گویی به آن را بر عهده دارد»** (جعفری دولت‌آبادی، ۱۳۹۵: ۱۹).

سیاست کیفری از زیرشاخه‌های سیاست جنایی است (قیاسی،۱۳۸۵: ۴۱). سیاست کیفری از سیاست‌های گرفته شده در برابر بزه است که فقط به برخورد کیفری از مسیر سیستم قضایی انحصار دارد. از شاخصه‌های این برخورد نخست دولتی بودن است، زیرا دستگاه قضایی نهاد دولتی است و دوم این‌که مقابله با انحراف شامل سیاست کیفری نمی‌گردد، چون سیستم کیفری تنها وظیفه رسیدگی به بزه‌ها را دارد.

۳- روش تحقیق

راهبرد کلی تحقیق، به لحاظ هدف کاربردی و از جهت شیوه اجرا تحلیلی- توصیفی و روش گردآوری آن به شیوه کتابخانه‌ای است و تجزیه و تحلیل یافته‌ها براساس درک و فهم محققان از منابع و متون قانونی و حقوقی در مورد سیاست کیفری دو کشور در رابطه به جرم جاسوسی بوده است. به دلیل تطبیقی بودن تحقیق، ضرورت داشت تا محققان، منابع و متون قانونی هر دو کشور را، مورد تجزیه و تحلیل قرار داده و وجه تمایز و تشابه احتمالی را به‌دست آورد.

بحث و نظر

۱- تحولات جاسوسی در محیط سایبر

به نظر نگارنده، آنچه مهم است در گام اول شناخت موضوع است که آیا تفاوت میان جاسوسی سنتی و جاسوسی سایبری از نوع درجه، مقدار و وسیله است یا این‌که تفاوت ماهوی و بنیادی است؟ به تعبیر دیگر، آیا می‌توان گفت که فقط وسیله و فضای ارتکاب جرم تغییر کرده است؟ جاسوسی همان جاسوسی است؛ فقط وسیله ارتکاب آن متفاوت شده است. ابزار و وسایل جاسوسی دگرگون شده است؟ یا این‌که ماهیت جاسوسی و نحوه ارتکاب آن در جهان سایبر متفاوت است؟

اگر تفاوت از نوع اول باشد، با اصول و مبانی سیاست کیفری فعلی هم می‌توان با جرم جاسوسی سایبری مقابله کرد. تفاوت فقط در نوع امکاناتی است که برای اجرای سیاست کیفری لازم است. ولی اگر تفاوت جرم جاسوسی سنتی و سایبری از نوع دوم باشد؛ نظام کیفری فعلی با قوانین ماهوی، شکلی و سازو کار موجود قادر به تحقق اهداف خود در راستای مبارزه با جرایم نوین نخواهد بود و نیازمند تبیین سیاست کیفری جدید خواهد بود (صدیق، ۱۳۹۵: ۷۳). به نظر می‌رسد فضای سایبر تاثیرات عمیق و بنیادین در ماهیت و محتوای جاسوسی گذاشته است، به نحوی که به کارگیری از کلمه جاسوسی سایبری خود بیانگر این تأثیر ژرف در این زمینه است.

در گذشته محدودیت زمانی و مکانی از مهم‌ترین موانع جاسوسی بود. ولی امروزه فضای سایبر زمینه جاسوسی فرازمانی و فرامکانی را فراهم کرده است و هرکس در هرنقطه باشد از دورترین مکان جغرافیایی و در هرساعتی از شبانه روزی می‌تواند دست به اقدام جاسوسی بزند. نکته مهم‌تر این‌که تقریباً تمام محیط‌های فردی، شخصی، اقتصادی، نظامی، سیاسی، اطلاعاتی و امنیتی به گونه‌ای به دنیای سایبر اتصال دارند و یا این‌که فضای سایبر، زمینه‌های نفوذ به آن‌ها را مهیا کرده است. فضای سایبر امکان دسترسی به اطلاعات حساس به تمام ابعاد و حوزه‌های مختلف کشورها را به صورت گسترده آن هم با کمترین هزینه و زمان فراهم کرده است. برای بازیگران مختلف از جمله دولت‌ها و یا کسانی که از طرف دولت‌ها هدایت می‌شوند؛ این فرصت در فضای سایبر مهیا شده است که با

[1] - Feuerbach

کمترین نیروی انسانی و هزینه، اطلاعات لازم و حساسی را از یک کشور به دست آورند (صدیق، ۱۳۹۵: ۸۷). در گذشته اگر با فرستادن نیروی انسانی از سیاست‌مداران جاسوسی می‌کردند اما امروز با رصد کردن مکالمات تلفنی و ارتباط‌های اینترنتی؛ به حساس‌ترین اطلاعات سیاسی دست خواهند یافت؛ چنانچه ما در سال‌های اخیر و عصر ارتباط، شاهد جاسوسی از سیاست‌مداران بزرگ جهان توسط امریکا بوده‌ایم که مکالمات تلفنی خانم مرکل صداعظم آلمان و رئیس جمهور فرانسه و نخست وزیر انگلیس توسط امریکا رصد اطلاعاتی شده است. یکی از عمده‌ترین بخش و هدف در جاسوسی، حوزه نظامی است که در جاسوسی سنتی توسط نیروی انسانی انجام می‌شد و طبعاً مشکلات و محذورات زیاد مکانی و زمانی داشت. اما در عصر ارتباط این موانع برداشته شده است و از طریق سایبر می توان به حساس‌ترین اطلاعات نظامی و امنیتی از قبیل: ساحه‌های نظامی- امنیتی، آمار نظامیان، امکانات تسلیحاتی، قدرت نظامی دشمن، ضعف نظامی دشمن، برنامه جنگی دشمن، برنامه‌های آموزشی، جنگی و ... دست یافت. وقتی فضای سایبر راه را برای جاسوسی سیاسی و نظامی که از ضریب امنیتی بیشتری برخوردار است؛ هموار کرده است، جاسوسی از منابع صنعتی، اقتصادی، علمی، فرهنگی و اجتماعی به راحتی امکان پذیر است. امروزه غول‌های فضای سایبری تمام برنامه‌های استثماری و اهداف‌شان را با رصد کردن اطلاعاتی از فضایی سایبری؛ پیگیری می‌کنند. به نظر می‌رسد با فراهم شدن محیط سایبر و دهکده پیچیده جهانی سایبر، تحولات عمیق در زمینه جاسوسی ایجاد شده است و تمام نهادهای امنیتی و اطلاعاتی را در برابر غول‌های جاسوسی و سایبری بسیار شکننده و نفوذپذیر کرده است.

۲- جاسوسی سنتی و سایبری

جاسوسی فضای سایبری یکی از مصطلحات جدید در بخش امنیت است که نگرانی و دغدغه جدی جهانی در این رابطه شکل گرفته است. همه کشورها، شرکت‌های بزرگ چندملیتی، سازمان‌ها و اشخاص از جاسوسی سایبری به عنوان چالش کلان برضد منفعت و امنیتشان می‌دانند. این اصطلاح دارای پیچیدگی‌های گسترده و وسیع معنایی و محتوایی است که بخشی از این ابهام به جهت پیچیدگی‌هایی ذاتی فضای مجازی برمی‌گردد.

کم خرج بودن، شناخته نبودن، معلوم نبودن محدوده سرزمینی تهدیدکننده، اثر عمیق و شفاف نبودن عمومی در محیط مجازی، باعث شده بازیگران قدرت‌مند اعم از کشورها، دسته‌های سازمان یافته و تروریستی و حتی اشخاص به این محیط داخل شده و جاسوسی سایبری را مرتکب می‌شوند. جاسوسی سایبری مرتبه جدید در حیطه جاسوسی است که در بیشتر بخش‌ها قابل مقایسه با جاسوسی کلاسیک نیست. فضای مجازی چنین ظرفیتی برای جاسوسی تهیه کرده است که هر بازیگری در هر بخشی که بخواهد، در فرض دارابودن قدرت و دانش لازم، می‌توانند هدف خود را به مرحله اجرا بگذارند. با توجه به این خصوصیت جاسوسان سایبری در بخش‌های زیر شامل‌اند (رضائی‌ور،۱۳۹۸: ۱۲۰)

۱- کارمندان نه چندان وفادار؛

۲- کپی برداران برنامه‌های رایج یعنی کاربران کامپیوتر و دلالان نرم افزار؛

۳- هکرها: دسترسی غیر مجاز بسیار ناب به سیستم‌های پردازش، عمدتاً به وسیله هکرها صورت می‌گیرد.

۴- دولت‌ها: به عنوان یکی از استفاده کنندگان عمده جاسوسی رایانه‌ای به شمار می‌آیند. امریکایی‌ها پیش از حمله به عراق از طریق اینترنت به درون شخصیت مردم عراق پی‌برده و توانستند شمار بیشتری از آن‌ها را جذب کنند. در مدت بیست سال حضور در افغانستان از طریق شبکه‌های اجتماعی و اینترنت جوانان زیادی را جذب انجوهایی کردند که در راستایی اهداف امریکایی‌ها و ضد فرهنگ اسلامی و سنتی افغانستان کار می‌کردند (صدیق، ۱۳۹۵: ۷۹). در جاسوسی سنتی با نیروی انسانی رصد اطلاعاتی انجام می‌شد و برای به‌دست آوردن هدف جاسوسی نیروی انسانی زمان زیاد و خطر زیادی را تحمل می‌کرد تا به اطلاعات حساس دست یابند. نفوذ پذیری در جاسوسی سنتی خیلی مشکل بود و چه بسا جاسوس در ماموریت‌ها به راحتی شناسایی می‌شد. البته ممکن است جاسوسی از طریق ارسال پیام‌های الکترونیکی (اسپم) ارتکاب یابد. شخصی که این پیام (اسپم) را باز می‌کند به صورت ناخواسته زمینه ورود جاسوس را فراهم کرده است زیرا ممکن

است این پیام حامل نرم افزارهای جاسوسی باشد که با بازکردن این پیام، طرف مقابل به اطلاعات داخل سیستم رایانه دست یابد.

روش ساده‌تری دیگر که شبیه با روش جاسوسی سنتی است؛ فریب یا تحریک فرد متصدی حفاظت از اطلاعات رایانه‌ای طبقه‌بندی شده با بهره‌گیری از مسائل شخصی یا عاطفی است که با این‌کار آن فرد اطلاعات حساس را در اختیار جاسوس قرار می‌دهند. با توجه با امکانات فراهم شده توسط فضای سایبر برای جاسوسی، روش‌های متنوعی برای جاسوسی به کار گرفته می‌شود که به عنوان نمونه به چند روش جاسوسی سایبری اشاره می‌شود (عطازاده و انصاری، ۱۴۰۰: ۳۳۸):

الف- روش عملیاتی است که ممکن است توسط سازمان‌های تروریستی به‌کار رود و در یک شرکت‌امنیتی آزموده شده است. این روش به «اسب تروجان» معروف است.» اسب تروجان به اصطلاحی برای توضیح هر ترفندی که باعث شود دشمن را به استحکامات یا محلی حفاظت‌شده دعوت کند؛ گفته می‌شود. امروزه اغلب با برنامه‌های رایانه‌ای بدافزار ارتباط دارد که با معرفی خود به‌عنوان سودمند یا بی‌خطر، کاربر را وادار به نصب و اجرای آن‌ها می‌کنند.

ب- یکی از روش‌های دیگر جاسوسی در فضای سایبر، سرقت هویت[1] است. سرقت هویت عبارت است از: «تصاحب یا ادعای داشتن هویت شخص دیگر» معمولاً سرقت هویت به هدف کسب مال یا ارتکاب جرم صورت می‌گیرد که شخص سارق بعداً به آسانی با هویت دیگری می‌تواند دست به ارتکاب جرم زند. در این روش با هویت دیگری وارد سیستم رایانه شده و اطلاعات حساس و طبقه‌بندی شده را دستبرد می‌زند. امروزه سرقت هویت افراد توسط پست‌های الکترونیکی امر رایج است که با ارسال پیام‌های الکترونیکی از هویت افراد مورد هدف سرقت می‌کند. گرچه در نخست به نظر می‌رسد که این پیام‌ها ازطرف شرکت معروف باشد، اما با بازکردن ایمیل، زمینه سرقت هویت و اطلاعات افراد فراهم می‌شود.

۳- سیاست کیفری ایران در قبال جاسوسی سایبری

هر رفتار اجتماعی اگر جرم شناخته شود و برای آن کیفر در نظر گرفته شود؛ مطابق با ماده ۲ قانون مجازات اسلامی ایران لازم است که در قانون جرم‌انگاری شده و برای آن مجازات مشخص شده باشد. بنابراین، مطابق با اصل قانونی بودن جرم و مجازات، هر پدیده ضد اجتماعی، جرم نیست. در مورد جرم جاسوسی رایانه‌ای نیز چنین است و قانون گذار برای جرم دانستن آن به قانونگذاری و سیاست کیفری خاص رو آورده است و مجازات این جرم را مشخص نموده است. راجع به سیاست کیفری جاسوسی سایبری در حقوق ایران، مواد ۳ و ۴ و ۵ قانون جرایم رایانه‌ای مصوب ۱۳۸۸ شمسی و ماده ۶۴ و ۷۵ قانون تجارت الکترونیک مصوب ۱۳۸۲ شمسی، پرداخته است که در ادامه به بررسی و تحلیل این مواد خواهیم پرداخت.

ماده‌های ۳ تا ۵ قانون جرایم رایانه‌ای ایران، عنصر قانونی جرم جاسوسی سایبری را تشکیل می‌دهند. مطابق با ماده ۳ این قانون، هرنوع دسترسی و شنود غیرمجازه داده‌های سرّی یا افشاء و در دسترس قراردادنِ آن‌ها در خدمت افراد و اشخاص غیرمجاز یا بیگانگان، جرم حساب می‌شود. در این ماده صحبت از دسترسی، شنود و افشاء یا در دسترس قرار دادن داده‌های سری است. تفاوت افشا با در دسترس قرار دادن این است که در افشاء خود شخص فرد غیرصالح را مطلع می‌سازد اما در دسترسی، زمینه مطلع ساختن؛ مثلاً رمز ورود را دراختیارش قرار می‌دهد تا او برود به داده‌های سری دسترسی پیدا کند.

ماده ۴ این قانون در رابطه به نقض تدابیر امنیتی سامانه‌های رایانه‌ای به هدف دسترسی به داده‌های سری پرداخته است. در ماده ۵، بی‌مبالاتی در نگهداری اطلاعات طبقه بندی، به عنوان جرم شناخته شده و ترک فعل و بی‌مبالاتی در آن را جرم دانسته است. این عمل در قانون مجازات اسلامی ماده ۵۰۴ و قانون مجازات جرایم نیروهای مسلح ماده ۲۷ به عنوان جرم علیه امنیت یاده شده است ولی در قانو جرایم یارانه‌ای جرم جاسوسی یاد می‌شود. ماده ۱۳۱ قانون جرایم نیروهای مسلح به جرایم سایبری تمرکز دارد. قسمت دوم این ماده در رابطه به تسلیم دادن اطلاعات طبقه‌بندی شده سایبری به دشمن یا افراد فاقد صلاحت و ناظر به جرم‌های علیه امنیت داخلی و خارجی است. بنابراین، باید ذکر کرد که هرگونه عملکرد عمدی که به افشای اسرار و اطلاعات نظامی از طریق سایبر منجر شود، در چارچوب

[1]. Identity Theft

بزه جاسوسی بررسی می‌شود. در رابطه با رفتارهای غیرعمدی و سهوی که به افشای اطلاعات به دشمن از طریق سایبر منتهی شود، طبق ماده ۲۷ این قانون، خاطی کیفر خواهد شد.

عنصر مادی جرم جاسوسی سایبری تنها فعل مثبت نیست بلکه طبق ماده ۲۷ و ۲۸ قانون مجازات جرایم نیروهای مسلح، بی احتیاطی، بی‌مبالاتی یا مراعات نکردن تدابیر امنیتی که به شکل ترک فعل است؛ نیز از مصادیق رکن مادی جرم جاسوسی سایبری شناخته می‌گردد. **«بی‌مبالاتی همان بی‌احتیاطی به صورت ترک فعل است. مقصود از بی‌مبالاتی ترک تکلیفی است که مقتضای پیشگیری از نتایج ناخواسته مجرمانه است»** (اردبیلی، ۱۳۹۹: ۴۳). بنابراین، اگر فردی در نیروی نظامی وظیفه‌ای خودش را انجام ندهد و ترک فعل کند که در اثر ترک فعل آن دشمن بتواند به اطلاعات سری دسترسی پیدا کند؛ درحقیقت عنصر مادی جرم که بی‌مبالاتی و بی‌احتیاطی به شکل ترک فعل است تحقق یافته است و این شخص مجازات خواهد شد.

جرم جاسوسی سایبری تنها یک جرم مادی صرف نیست، بلکه اثبات عنصر روانی این جرم نیز الزامی است. رکن روانی بزه جاسوسی، سوء نیت عام است و در رفتار جاسوسی، نیاز به قصد خاص ندارد؛ اما در نقض تدابیر امنیتی سامانه‌های سایبری یا مخابراتی که در ماده ۴ قانون جرایم رایانه‌ای به آن تذکر رفته است، مشروط است که مجرم باید قصد دسترسی به داده‌های سری مطرح شده در ماده ۳ این قانون را داشته باشد که این رفتار مشمول عمد در عملکرد و اراده کردن و آگاه بودن او از محرمانه و سری بودن داده‌هاست؛ یعنی این فرد مرتکب به قصد و هدف لطمه زدن به امنیت ملی و نقض تدابیر امنیتی کشور، این اطلاعات سری را در اختیار دشمنان و بیگانگان قرار دهد. از طرف دیگر، جرم جاسوسی از جمله جرایم مقید است که فردی، اول، مطالب و داده‌ها را به‌دست می‌آورد و بعد در اختیار اشخاص فاقد صلاحیت قرار می‌دهد و با انتشار و در دسترس قراردان، این جرم شکل می‌گیرد (اردبیلی، ۱۳۹۹: ۶۱).

در ماده ۳ قانون جرایم رایانه‌ای اصطلاحاتی مانند «تدابیر حفاظتی»، «بیگانه»، «افشاء اطلاعات» وجود دارد که تعریف روشنی از آن توسط قانون‌گذار ارائه نشده است این مفاهیم ابهام دارد. شایسته بود در قانون، اصطلاحاتی که به‌کار برده می‌شود دارای مفهوم و تعریف روشن باشد. یکی از مواردی که در سیاست کیفری جاسوسی سایبری ایران به آن توجه نشده است جرم‌انگاری شریک و معاون جرم جاسوسی سایبری است. در قانون جرایم رایانه‌ای در مورد کیفر شریک جرم جاسوسی ساکت بوده و فقط مجازات معاون جرم را در ماده ۲۵ به‌طور ضمنی اشاره کرده است که این مقدار کافی نیست و می‌بایست قانون‌گذار برای شریک و معان جاسوسی سایبری به صورت صریح اقدام کرده و رفتار مجرمانه آن دو را جرم‌انگاری می کرد.

در سیاست کیفری ایران به دادگاه صالح رسیدگی به جرم جاسوسی سایبری اشاره نشده است. شایسته بود که به دادگاه صالح این جرم وچگونگی رسیدگی به آن به صورت شفاف پرداخته می‌شد (رضائی‌ور، ۱۳۹۸: ۱۲۴). امیتاز سیاست کیفری ایران نسبت به سیاست کیفری افغانستان، در دقت و تفاوت قائل شدن به بعدکیفری جرم جاسوسی سایبری است؛ زیرا بین کسی که به اطلاعات سری فقط دسترسی پیدا کرده است و کسی که این اطلاعات را به افراد فاقد صلاحیت تسلیم کرده است و بین کسی که این اطلاعات را به بیگانگان و دشمنان تسلیم داده است؛ تفاوت قائل شده و مجازات این فرد را متناسب به جرم ارتکابی در نظر گرفته است.

۴- سیاست کیفری افغانستان در قبال جاسوسی سایبری

ماده ۸۶۴ قانون جزای افغانستان در مورد جرم جاسوسی سایبری مصادیقی را به عنوان جرم جاسوسی سایبری معرفی کرده است و گفته است که اگر کسی غیر مجاز در رابطه به سامانه، برنامه یا اطلاعات رایانه‌ای حاوی اطلاعات سری، دست به ارتکاب یکی از اعمال زیر زند، به مجازات بزه خیانت ملی یا جاسوسی ذکر شده در این قانون، محکوم می‌شود:

– دسترسی غیرمجاز به اطلاعات سری؛

– در دسترس قراردادن اطلاعات سری برای دیگران؛

– افشاء یا در دسترس قرار دادن اطلاعات سری برای دولت، سازمان، شرکت یا گروه خارجی یا عاملان آن‌ها (کدجزای افغانستان، ۱۳۹۶: ماده ۸۶۴).

قانونگذار افغانستان در این ماده قانونی، تعریف روشن از جاسوسی رایانه‌ای ارائه نکرده است بلکه مصادیقی را به عنوان

جرم جاسوسی رایانه‌ای ذکر کرده است. مورد اول از مصادیق سه گانه بالا که صرف دسترسی غیر مجاز به اطلاعات سری باشد؛ نیز به عنوان جاسوسی قلمداد شده است. این مورد را اگر جاسوسی بدانیم دور از ذهن به نظر می‌رسد. چون صرف دسترسی به اطلاعات سری بدون آگاه کردن بیگانگان؛ شامل عنوان متعارف جاسوسی نیست. اما به نظر می‌رسد قانونگذار همین مقدار تجسس را که فرد یا گروهی به اطلاعات سری دستری پیدا کنند؛ جاسوسی دانسته‌اند. چون با دسترسی به آن اطلاعات، دیگر سری نیست. یکی از کاستی‌های سیاست‌گذاری کیفری افغانستان در این مورد این است که مجازات این جرم را در همینجا به صورت شفاف ذکر نکرده است بلکه در فصل جاسوسی و خیانت ملی سنتی حواله داده است. شایسته بود در همینجا کیفر جرم را بعد از جرم‌انگاری آن ذکر می‌کرد. در ماده ۲۴۰ و ۲۴۱ کدجزای افغانستان به مجازات جرم جاسوسی پرداخته شده است. نقصی که در این سیاست کیفری وجود دارد عدم تفاوت قائل شدن در بعد کیفری است؛ بین کسی که اطلاعات سری را جمع آوری کرده است اما تسلیم دشمن نداده است با کسی که علاوه بر جمع‌آوری به دشمن نیز تحویل داده است. از نظر منطق حقوقی، مجازات این دو جرم نباید مساوی باشد چنانچه در قانون ایران این تفاوت را دیدیم. البته از امتیاز سیاست کیفری افغانستان این است که جاسوسی در زمان جنگ با جاسوسی در حالت عادی را فرق گذاشته است؛ طبق ماده ۲۴۱ کد جزا کسی که در زمان جنگ مرتکب جاسوسی شود به حبس دوام درجه ۱ و در حالت عادی به حبس دوام درجه ۲ مجازات می‌گردد. کاستی دیگری که در سیاست کیفری دو کشور وجود دارد؛ عدم توجه به بعد جرم‌انگاری و بعد کیفر شریک و معاون جاسوسی سایبری است که هردو کشور از شریک و معاون این جرم سخنی به‌میان نیاورده است.

نتیجه‌گیری

هنوز تعریف روشن از جاسوسی سایبری ارائه نشده است و پیشینه موضوع هم نشان می‌دهد که در مورد جاسوسی سایبری پژوهش و تحقیق صورت گرفته است اما موضوع این تحقیق که سیاست کیفری ایران و افغانستان باشد، موضوعی کاملاً تازه و جدید است که کار تطبیقی در این مورد انجام نشده است. باتوجه به اهمیت امنیت در کشورها، در عصرحاضر فناوری و فضای سایبری باعث شده است که اخلال‌گران امنیت این محیط را برای نا امن کردن جغرافیایی مورد نظرشان انتخاب کنند. انتخاب این راه به دلیل سرعت، گستردگی، کم هزینه و آسان بودن این فضا آگاهانه است. فضای سایبری، نسبت به گذشته جاسوسی را راحت و بدون خطر کرده است که بدون دخیل بودن نیروی انسانی و خطری گیرافتادن او، توسط ابزار و فناوری سایبری به راحتی می‌توان از هدف، جاسوسی کرد و معلومات محرمانه را به‌دست آورد. بنابر این، یکی از مشکلات کشورها برای تأمین امنیت، جاسوسی سایبری است که هرکشوری برای تأمین امنیت خود و برای مبارزه با جرم جاسوسی، سیاست کیفری مختص به خودش را دارد. یافته‌های تحقیق نشان می‌دهد که در ماده ۳ قانون جرایم رایانه‌ای اصطلاحاتی مانند «تدابیر حفاظتی»، «بیگانه»، «افشاء اطلاعات» وجود دارد اما تعریف روشنی از آن توسط قانون‌گذار ارائه نشده است و این مفاهیم ابهام دارد. لازم است در قانون اصطلاحاتی که به‌کار برده می‌شود دارای مفهوم و تعریف روشن باشد. یکاستی دیگر این‌که در سیاست کیفری ایران به دادگاه صالح رسیدگی به جرم جاسوسی سایبری اشاره نشده است، شایسته بود که به دادگاه صالح این جرم وچگونگی رسیدگی به آن به صورت شفاف پرداخته می‌شد. امیتاز سیاست کیفری ایران نسبت به سیاست کیفری افغانستان، در دقت و تفاوت قائل شدن به بعدکیفری جرم جاسوسی سایبری است؛ زیرا بین کسی‌که به اطلاعات سری فقط دسترسی پیدا کرده است و کسی‌که این اطلاعات را به افراد فاقد صلاحیت تسلیم کرده است و کسی‌که این اطلاعات را به بیگانگان و دشمنان تسلیم داده است؛ تفاوت قائل شده و مجازات این فرد را متناسب به جرم ارتکابی در نظر گرفته است. این درحالی است که در سیاست کیفری افغانستان برای این افراد بدون تفاوت، مجازات یکسان لحاظ کرده است. از نظر منطق حقوقی، مجازات این جرم‌ها نباید مساوی باشد. البته از امتیاز سیاست کیفری افغانستان این است که جاسوسی در زمان جنگ با جاسوسی در حالت عادی را فرق گذاشته است؛ طبق ماده ۲۴۱ کد جزا کسی که در زمان جنگ مرتکب جاسوسی شود به حبس دوام درجه ۱ (۲۰ الی ۳۰ سال) و در حالت عادی به حبس دوام

درجه ۲ (۱۶ الی ۲ سال) مجازات می‌گردد. کاستی دیگری که در سیاست کیفری دو کشور وجود دارد؛ عدم توجه به بعد جرم‌انگاری و بعد کیفری، شریک و معاون جاسوسی سایبری است که هردو کشور از شریک و معاون این جرم، سخنی به‌میان نیاورده است.

در گذشته محدودیت زمانی و مکانی از مهم‌ترین موانع جاسوسی بود. ولی امروزه فضای سایبر زمینه جاسوسی فرازمانی و فرامکانی را فراهم کرده است و هرکس در هرنقطه باشد از دورترین مکان جغرافیایی و در هرساعتی از شبانه روزی می‌تواند دست به اقدام جاسوسی بزند. در نتیجه برای مبارزه با این پدیده، داشتن سیاست کیفری به‌روز و کاراست تا گام به‌گام با رشد فناری به سیاست‌گذاری در این مورد اقدام صورت بگیرد.

پیشنهادها

۱- جامعه نیاز به قانون دارد و این قانون چه عرفی باشد و چه مستخرج از فقه و شریعت. اگر قانونی که مسخترج از فقه و شریعت باشد، طبعاً برای تأمین سعادت دنیا و آخرت در یک جامعه اسلامی به صواب نزدیک‌تر است. امروز جامعه اسلامی افغانستان در حاکمیت دولت امارت اسلامی از خلأ قانونی رنج می‌برد و این نگرانی وجود دارد که در نبود یک قانون مدون اگر کسی متهم می‌شود یا جرم را مرتکب می‌شود؛ نسبت به او قاضی رفتار سلیقه‌ای کرده و عدالت اسلامی در حق او به نحو شایسته اجرا نگردد. بنابراین، اولین پیشنهادی که برای زمامداران کشور و دستگاه قضایی می‌شود این است که جامعه را از خلأ قانونی نجات داده با تدوین قانون و سیاست کیفری متخذ از فقه، شریعت اسلامی، دکترین حقوقی و عرف حقوقی جامعه ملل، به عدل و انصاف قضاوت صورت بگیرد تا خدای ناخواسته در اثر عدم آگاهی یا سلیقه‌ای رفتار کردن قاضی در حق مظلومی ظلم نشود.

۲- برای حاکمان فعلی افغانستان توصیه می‌شود که با توجه به هرج و مرج در فضای سایبری و پراکندگی سیاست کیفری جرایم سایبری در قانون گذشته، شایسته است سیاست کیفری ای را تدوین کنند که مطابق با روح حقوق اسلامی و مطابق با معیارهای حقوق و اسناد بین‌المللی و جهانی باشد.

۳- آیین‌دادرسی سایبری مورد پژوهش و تحقیق بیشتر قرار بگیرد: آیین‌دادرسی سایبری، مهم‌ترین بخش در محاکمه عادلانه است و بیشترین تغییر در این قسمت از حقوق سایبری به وجود آمده است. اگر پژوهشگری علاقه‌مند تحقیق در رابطه با جرایم سایبری است یکی از مباحث نیازمند تحقیق، آیین دادرسی جرایم سایبری است که با رویکرد سیاست کیفری مورد مداقه و توجه قراربگیرد. چون در این زمینه کار نشده و نیازمند تحقیق و پژوهش همه جانبه است.

۴- پژوهش فنی جرایم سایبری: یکی از چالش‌های که در مراحل پژوهش با آن روبه‌رو شدم عدم درک درست از چگونگی تحقق جرایم سایبری است؛ زیرا جرایم سایبری، ماهیت فنی دارد که فقط متخصص تکنالوژی و فنی (IT) می‌تواند درک درست از ماهیت و حقیقت این جرم داشته باشد. بنابراین، یکی از پژوهش‌های که نیاز است انجام شود؛ بیان ماهیت و حقیقت جرایم سایبری با زبان فنی و علمی توسط متخصصان مربوطه است تا حقوق‌دانان و قانونگذران بتواند درک فنی از این جرایم داشته باشد.

ملاحظات اخلاقی: در تمام مراحل نگارش پژوهش حاضر، صداقت و امانتداری رعایت شده است.

تعارض منافع: مقاله مستخرج از رساله دکتری تخصصی جامعه المصطفی العالمیه، تحت عنوان: «سیاست کیفری اسلام، افغانستان و اسناد بین‌الملل در قبال بزهکاری سایبری (مطالعه موردی جرایم علیه امنیت و اخلاق عمومی») است.

سهم نویسندگان: نگارش مقاله مشترکاً توسط نویسندگان صورت گرفته است.

تشکر و قدردانی: از کلیه کسانی که در معرفی منابع و تهیه این مقاله ما را یاری رساندند، تشکر و قدردانی می‌نماییم.

تأمین اعتبار پژوهش: این پژوهش فاقد تأمین کننده مالی بوده است.

منابع و مآخذ

الف. منابع فارسی و عربی

– اردبیلی، محمدعلی (۱۳۹۹). *حقوق جزای عمومی*. تهران: نشر میزان، چاپ دوم.

– اشرافی مهابادی، محمود و فرنوش، توبی (پاییز ۱۳۹۶). «پیشگیری وضعی از جرم جاسوسی سایبری». *نشریه مطالعات حقوق*، ۱۴: ۱۰۳–۱۲۴.

– السان، مصطفی (۱۳۹۸). *حقوق فضای مجازی*. چاپ سیزدهم، تهران: مؤسسه مطالعات و پژوهش‌های حقوقی شهر دانش.

– الهوردی، فرهاد (۱۳۹۶). *حقوق کیفری سایبری*. تهران: انتشارات جنگل–جاودانه.

– امیری، نجات و نامیان، پیمان (۱۴۰۱). «مقابله با جاسوسی سایبری؛ رویکردی آینده‌پژوهانه در پیشگیری از جرایم تروریستی با نگاهی به اسناد حقوق بشری». *فصلنامه علمی مطالعات حقوق بشر اسلامی*، ۱۱ (۴): ۵۱–۷۳.

– جعفری دولت‌آبادی، عباس (۱۳۹۵). *جایگاه امنیت در سیاست کیفری ایران*. تهران: انتشارات فکر سازان.

– حرعاملی، محمد بن‌حسن (۱۳۶۸). *وسائل الشیعه*. جلد دوازدهم، قم: رضی.

– حسنوی، رضا و فرسایی، داریوش (۱۳۷۸). *فرهنگ تشریحی کمپیوتر*. چاپ دوم، تهران: دانشیار.

– حلی، حسن بن‌یوسف (۱۴۱۳). *قواعد الاحکام*. قم: جامعه مدرسین.

– رضائی‌ور، پیمان (۱۳۹۸). «بررسی قوانین و مواد مرتبط با جرم جاسوسی رایانه‌ای». *نشریه علم و وکالت*، ۱: ۱۰۷–۱۲۸.

– زارع، محسن و قره‌باغی، ونوس (۱۳۹۴). «تعارض میان جاسوسی و آزادی اطلاعات از منظر حقوق بین‌المللی بشردوستانه». *مطالعات حقوق عمومی*، ۴: ۶۰۹–۶۲۹.

– زندی، محمدرضا (۱۳۹۳). *تحقیقات مقدماتی در جرایم سایبری*. تهران: انتشارات جنگل.

– صدیق، میرابراهیم (۱۳۹۵). «انقلاب سایبری و تحول در پدیده جاسوسی». *فصلنامه مطالعات راهبردی*، شماره ۷۱.

– طوسی، محمد بن‌حسن (۱۳۹۳). *المبسوط*. بی‌جا: الکتبه المرتضویه لاحیاء آثار الجعفریه.

– عطازاده، سعید و انصاری، جلال (۱۴۰۰). *حقوق جزای اختصاصی جرایم رایانه‌ای*. چاپ دوم، تهران: بنیاد حقوقی میزان.

– فتاحی زفرقندی، سجاد، اسماعیلی، مهدی و حاجی‌تبار فیروزجایی، حسن (۱۳۹۹). «پیشگیری از جرم جاسوسی سایبری نیروهای مسلح و نقش آن در تأمین حق امنیت». *حقوق بشر اسلامی*، ۹: ۲۵۵–۲۷۶.

– قیاسی، جلال‌الدین (۱۳۸۵). *مبانی سیاست جنایی حکومت اسلامی*. قم: پژوهشگاه علوم و فرهنگ اسلامی.

– لازرژ، کریستین (۱۳۸۲). *درآمدی به سیاست جنایی*. ترجمه علی حسین نجفی ابرندآبادی. تهران: نشر میزان.

– متقی هندی، علاءالدین علی بن‌حسام (بی‌تا). *کنز العمال*. جلد یازدهم، بی‌جا: مؤسسه الرساله.

– محمدنسل، غلامرضا (۱۳۹۵). *حقوق جزای اختصاصی جرایم رایانه‌ای در ایران*. چاپ دوم، تهران: بنیاد حقوقی میزان.

– مغربی، قاضی نعمان (۱۳۸۵). *دعائم الاسلام و ذکر الحلال و الحرام و القضایا و الاحکام*. تحقیق آصف فیضی، چاپ دوم، قم: مؤسسه آل‌البیت.

ب. منابع انگلیسی

- National Institute of justice, DOJ (1998). Computer Crime: Criminal Justice Resource Manual, Vol. 2.