**جاسوسی سایبری در سیاست کیفری ایران و افغانستان[[1]](#footnote-1)**

# **چکیده**

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. راهبرد کلی تحقیق، به لحاظ هدف کاربردی و از جهت شیوه اجرا تحلیلی- توصیفی و روش گردآوری آن به شیوه کتابخانه­ای است. 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. یافته­های تحقیق نشان می­دهد که 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 وکسی 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.

**واژه­گان کلیدی:** فضای سایبری، جاسوسی سایبری، سیاست کیفری

# **1: مقدمه و بیان مسأله**

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، 1396: ص 21). 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 ضروری تر 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 تامین امنیت، جاسوسی سایبری است که هرکشوری برای تامین 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.

# **2: ادبیات موضوع و پیشینه**

## **2-1: ادبیات نظری و مفهوم شناسی**

### **2-1-1: 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 پیچیده شان، مدعیان امنیت فضای سابیر 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، 1393: ص 23). 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 ارایه 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 مادۀ 851 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، 1396: ماده 851).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 می­گیرد 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 کاملا 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، 1395: ص 16).

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.

### **2-1-2: 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 توسعۀ 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 جامعۀ 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، 2001).* بر این تعریف نقد­های زیر وارد شده است: 1- با ذکر کردن از اسرار تجاری یا حرفه­ای در آن عملا 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. 2- راجع به قصد مجرم از ارتکاب این بزه که در تعریف صرفا منافع اقتصادی مدنظر قرارداده شده است که این هم صحیح نیست؛ چون که امکان دارد جاسوسی اهدافی برتر از منافع اقتصادی داشته باشد که مثلا امکان دارد فقط هدف­های ملی در نظر باشد. 3- در این تعریف، جاسوسی سایبری بیان نشده است، بلکه صرفا 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.

### **2-1-3: 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 می­پردازد: «در سال 1803 م اصطلاح سیاست کیفری یا سیاست جنایی، نخستین بار، توسط «فوئرباخ» (Feuerbach) 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،1395: 19) 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، 1395: 19).

سیاست کیفری از زیرشاخه­های سیاست جنایی است. (قیاسی،1385: ص41). 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.

## **2-2: پیشینه پژوهش**

فتارحی زفرقندی و همکاران (1399) در مقالۀ تحت عنوان «پیشگیری از جرم جاسوسی سایبری نیروهای مسلح و نقش آن در تأمین حق امنیت» معتقدند که به کارگیری از دو راهکار پیشگیری کیفری و غیرکیفری در پیشگیری از جاسوسی سایبری، ممکن است درست نتیجه بدهد.

زارع و قره­باغی (1394) در پژوهشی تحت عنوان «تعارض میان جاسوسی و آزادی اطلاعات در حقوق بین­المللی بشردوستانه» می­گویند که جاسوسی در جلوه حقوق بشر از اهمیت زیاد برخوردار است و این اهمیت وقتی روشن می­شود که اشخاص در زیر پرچم حقوق بشر دست به جاسوسی می­زند یا این­که دولت­ها به بهانه پیشگیری از جاسوسی حقوق بشر را اهمیت نمی­دهند. این مقاله تلاش دارد که برای تعارضات حاکم راهگشا باشد؛ به گونۀ که به حقوق اساسی اشخاص آسیب وارد نشود و از طرفی دیگر امنیت ملی دولت­ها نیز خدشه­دار نگردد.

امیری و نمامیان (1401) در مقالۀ با عنوان «مقابله با جاسوسی سایبری؛ رویکردی آینده پژوهانه در پیشگیری از جرایم تروریستی با نگاهی به اسناد حقوقق بشری» چنین نتیجه گرفته­اند؛ نتایج تحقق نشان می­دهد که دسترسی غیرقانونی به اطلاعات در محیط مجازی که فراهم کننده وقوع جرم­های تروریستی است، این جرایم به دلایل بشردوستانه و حقوق بشری، مورد واکنش دستگاه عدالت کیفری و سازمان­های بین­المللی قرار می­گیرد. از طرفی لازم است که دستگاه قضایی، انتظامی و سازمان­های بین­المللی درجهت مقابله با جاسوسی سایبری برای پیشگیری از بزه­های تروریستی به علاوه تدابیر فنی و حقوقی با به­استفاده و کارگیری مفهوم­های آینده­پژوهانه در پیشگیری از اتفاق جرم­های تروریستی اقدام کنند.

رضائی­ور (1398) درمقالۀ با عنوان «بررسی قوانین و مواد مرتبط با جرم جاسوسی رایانه­ای» به صورت گذرا مواد قانونی مربوط به جاسوسی سایبری را کنارهم قرار داده و تحلیل علمی از مسأله ارائه نکرده است. این تحقیق گزارشی از مواد قانونی مرتبط است.

 اشرافی مهابادی و فرنوش (1396) در مقالۀ تحت عنوان «پیشگیری وضعی از جرم جاسوسی سایبری» پرداخته است. در این پژوهش نویسندگان به راه­های پیشگیری وضعی و فنی می­پردازند و راه­کارهای مقابله و پیشگیری از این جرم را بیان کرده است. یافته­های این تحقیق بیانگر این است که پلیس با بهره­گیری از آموزه­های جرم­شناسی سایبری و انواع پیشگیری­های اجتماعی و وضعی از راه آموزش عمومی، افزایش خطرهای ارتکاب بزه، کاهش جاذبۀ آماج­ها، گشت­زنی در محیط سایبر و به استفاده از نرم­افزارهای تخصصی اعلام خطر و باقی تدابیر نظارتی به مبارزه و جلوگیری جاسوسی رایانه­ای اقدام کند.

قدسی (1392) با مقالۀ تحت عنوان « مبانی فقهی جاسوسی» به بررسی فقهی و حقوقی این جرم پرداخته است.

عطازاده و انصاری (1400) در فصل هفتم از کتاب «حقوق جزای اختصاصی جرایم رایانه­ای» به جرم جاسوسی سایبری اختصاص داده است. نویسندگان در این فصل به بررسی مواد قانونی در این مورد و به تبیین عناصر مادی، قانونی و معنوی این جرم اشاره کرده است. همچنین در این پژوهش از اهداف، رفتارشناسی، علل­گرایش و انگیزه­های جاسوسان سایبری بحث شده است.

همه این پژوهش­های متذکره در هدف و موضوع، متفاوت از تحقیق حاضر است؛ زیرا هیچ­کدام به سیاست کیفری جاسوسی سایبری و مقایسه و تطبیق جرم جاسوسی دو کشورایران و افغانستان نپرداخته است. به طور خلاصه، پیشینه این تحقیق شامل بررسی مفاهیم کلیدی مرتبط با فضای سایبری، جرایم سایبری، جاسوسی سایبری و سیاست کیفری، و همچنین مرور پژوهش های پیشین در این حوزه است. نوآوری این تحقیق در تمرکز بر مقایسه سیاست کیفری ایران و افغانستان در قبال جاسوسی سایبری و پرداختن به ابعاد جرم انگاری و کیفری این جرم نهفته است.

**وجه نوآوری پژوهش حاضر نسبت به مطالعات پیشین:** تحقیق حاضر کوششی است نو، در تبیین علمی سیاست کیفری ایران و افغانستان درباره جاسوسی سایبری. نتیجه این مقاله می­تواند راه­گشای حل بعضی از مسائل در تامین امنیت سایبری و داشتن سیاست کیفری کلان در حوزه جاسوسی سایبری باشد. این پژوهش به دلیل تطبیقی و مقایسوی بودن جدید است؛ زیرا هنوز کار پژوهشی تطبیقی در مورد جاسوسی دو کشور ایران و افغانستان انجام نشده است. از سوی دیگر، این تحقیق به بعد جرم­انگاری و کیفری این جرم در سیاست کیفری دو کشور پرداخته است و هنوز پژوهشی که به سیاست کیفری توجه داشته باشد در این راستا انجام نشده است.

اهم امتیازات و نورآوری تحقیق حاضر را می­توان به موارد ذیل خلاصه کرد:

مقایسه سیاست های کیفری: نوآوری اصلی این تحقیق، مقایسه سیاست­های کیفری ایران و افغانستان در حوزه جاسوسی سایبری است.

شناسایی خلاء های قانونی: این تحقیق با شناسایی خلاء های قانونی در سیاست­های کیفری هر دو کشور، زمینه را برای اصلاحات قانونی فراهم می کند. به طور مثال، عدم توجه به مسئولیت کیفری معاونین جرم و همچنین نبود تعاریف دقیق و روشن از اصطلاحات کلیدی، از جمله این موارد است.

توصیه های کاربردی برای افغانستان: پیشنهاد تدوین سیاست کیفری منطبق با شریعت اسلام برای افغانستان، با توجه به شرایط این کشور، بسیار حائز اهمیت است.

توجه به آیین دادرسی سایبری: تاکید بر ضرورت تحقیق در زمینه آیین دادرسی سایبری، نشان از توجه به یکی از جنبه های مهم و در حال تحول حقوق کیفری دارد.

رویکرد بین رشته­ای: پیشنهاد ارائه توضیحات فنی جرایم سایبری برای حقوقدانان، بر ضرورت همکاری بین متخصصان حقوق و فناوری تاکید می­کند.

## **3: 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.

## **4: یافته­های تحقیق**

## **4-1: سیاست کیفری ایران در قبال جاسوسی سایبری**

 هر رفتار اجتماعی اگر جرم شناخته شود و برای آن کیفر در نظر گرفته شود؛ مطابق با مادۀ 2 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 3 و 4 و 5 قانون جرایم رایانه­ای مصوب 1388 شمسی و مادۀ 64 و 75 قانون تجارت الکترونیک مصوب 1382 شمسی، پرداخته است که در ادامه به بررسی و تحلیل این مواد خواهیم پرداخت.

ماده­های 3 تا 5 قانون جرایم رایانه­ای ایران، عنصر قانونی جرم جاسوسی سایبری را تشکیل می­دهند. مطابق با ماده 3 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 داده های 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؛ مثلا رمز ورود را دراختیارش قرار می­دهد تا او برود به داده­های سری دسترسی پیدا کند.

مادۀ 4 این قانون در رابطه به نقض تدابیر امنیتی سامانه­های رایانه­ای به هدف دسترسی به داده­های سری پرداخته است. در ماده 5، 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 504 و قانون مجازات جرایم نیروهای مسلح ماده 27 به عنوان جرم علیه امنیت یاده شده است ولی در قانو جرایم یارانه­ای جرم جاسوسی یاد می­شود. مادۀ 131 قانون جرایم نیروهای مسلح به جرایم سایبری تمرکز دارد. قسمت دوم این ماده در رابطه به تسلیم دادن اطلاعات طبقه­بندی شدۀ 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 بزه جاسوسی بررسی می­شود. در رابطه با رفتارهای غیرعمدی و سهوی که به افشای اطلاعات به دشمن از طریق سایبر منتهی شود، طبق ماده 27 این قانون، خاطی کیفر خواهد شد.

عنصر مادی جرم جاسوسی سایبری تنها فعل مثبت نیست بلکه طبق ماده 27 و 28 قانون مجازات جرایم نیروهای مسلح، بی­احتیاطی، 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 ناخواستۀ مجرمانه است» (اردبیلی، 1399: ص 43). 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 4 قانون جرایم رایانه­ای به آن تذکر رفته است، مشروط است که مجرم باید قصد دسترسی به داده­های سری مطرح شده در ماده 3 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، 1399: ص 61).

در مادۀ 3 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 25 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 می­کرد.

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، 1398: 124). 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.

## **4-2: سیاست کیفری افغانستان در قبال جاسوسی سایبری**

ماده 864 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، 1396: ماده 864).*

 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 مادۀ 240 و 241 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 ماده241 کد جزا کسی که در زمان جنگ مرتکب جاسوسی شود به حبس دوام درجه1[[2]](#footnote-2) و در حالت عادی به حبس دوام درجه2[[3]](#footnote-3) 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.

# **5: بحث، نتیجه­گیری و پیشنهادها**

# **5-1: بحث**

### **5-1-1:** **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 نحوۀ 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، 1395: ص73). 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 کمترین نیروی انسانی و هزینه، اطلاعات لازم و حساسی را از یک کشور به دست آورند (صدیق، 1395: ص 87). 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 (https://parsi.euronews.com/). 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 می­توان 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.

### **5-1-2: جاسوسی سنتی و سایبری**

جاسوسی فضای سایبری یکی از مصطلات 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 امنیت شان 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،1398: ص 120):

1- کارمندان نه چندان وفادار؛

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

3- هکرها: دسترسی غیر مجاز بسیار ناب به سیستم­های پردازش، عمدتا به وسیلۀ هکرها صورت می­گیرد.

4- 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، 1395: ص79). 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، 1400: ص338):

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](https://fa.wikipedia.org/wiki/%D8%AA%D8%B1%D9%88%D8%A2_%28%D8%B1%D8%A7%DB%8C%D8%A7%D9%86%D9%87%29) ارتباط دارد که با معرفی خود به‌عنوان سودمند یا بی‌خطر، کاربر را وادار به نصب و اجرای آن‌ها می‌کنند. (<https://www.irna.ir/news/84432966>).

ب- یکی از روش­های دیگر جاسوسی در فضای سایبر، سرقت هویت[[4]](#footnote-4) است. سرقت هویت عبارت است از: «تصاحب یا ادعای داشتن هویت شخص دیگر» معمولا سرقت هویت به هدف کسب مال یا ارتکاب جرم صورت می­گیرد که شخص سارق بعدا 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.

## **5-2: 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 کاملا 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 تامین امنیت، جاسوسی سایبری است که هرکشوری برای تامین امنیت خود و برای مبارزه با جرم جاسوسی، سیاست کیفری مختص به خودش را دارد. یافته­های تحقیق نشان می­دهد که در مادۀ 3 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 ماده241 کد جزا کسی که در زمان جنگ مرتکب جاسوسی شود به حبس دوام درجه1[[5]](#footnote-5) و در حالت عادی به حبس دوام درجه2[[6]](#footnote-6) 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.

## **5-3: پیشنهادها**

1. 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 تامین 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.
2. 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 کیفری­ای را تدوین کنند که مطابق با روح حقوق اسلامی و مطابق با معیارهای حقوق و اسناد بین­المللی و جهانی باشد.
3. **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.
4. **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.

# **6: منابع**

1. قرآن کریم.
2. اردبیلی، محمدعلی (1399)، حقوق جزای عمومی، تهران: نشر میزان، چاپ دوم.
3. اله­وردی، فرهاد(1396ش)، حقوق کیفری سایبری، تهران: انتشارات جنگل-جاودانه.
4. السان، مصطفی(1398ش)، حقوق فضای مجازی، تهران: موسسه مطالعات و پژوهش­های حقوقی شهر دانش، چاپ سیزدهم.
5. اشرافی مهابادی، محمود و فرنوش، توبی (پاییز1396)، «پیشگیری وضعی از جرم جاسوسی سایبری»، نشریه مطالعات حقوق، شماره 14، از ص 103 تا 124.
6. امیری، نجات و نمامیان، پیمان (1401)، «مقابله با جاسوسی سایبری؛ رویکردی آینده پژوهانه در پیشگیری از جرایم تروریستی با نگاهی به اسناد حقوق بشری»، فصلنامه علمی مطالعات حقوق بشر اسلامی، دوره11، شماره4، شماره پیاپی (27)، زمستان، ص51-73.
7. جعفری دولت آبادی، عباس (1395 ش)، جایگاه امنیت در سیاست کیفری ایران، تهران: انتشارات فکر سازان.

حرعاملی، محمد بن­حسن (1368ش)، وسائل الشیعه، ج12، قم: رضی.

1. حسنوی، رضا و فرسایی، داریوش (1378ش)، فرهنگ تشریحی کمپیوتر، تهران: دانشیار، چاپ دوم.

حلی، حسن بن­یوسف (1413ق)، قواعد الاحکام، قم: جامعه مدرسین.

1. رضائی­ور، پیمان (1398)، «بررسی قوانین و مواد مرتبط با جرم جاسوسی رایانه­ای»، نشریه علم و وکالت. (1)، صص 107-128.
2. زارع، محسن و قره­باغی، ونوس (1394)، «تعارض میان جاسوسی و آزادی اطلاعات از منظر حقوق بین­المللی بشردوستانه»، مطالعات حقوق عمومی، شماره4، زمستان، 609-629.
3. زندی، محمدرضا (1393 ش)، تحقیقات مقدماتی در جرایم سایبری، تهران: انتشارات جنگل.

صدیق، میرابراهیم (بهار 1395)، «انقلاب سایبری و تحول در پدیدۀ جاسوسی»، فصلنامه مطالعات راهبردی، ، شماره 71.

طوسی، محمد بن­حسن (1393ق)، المبسوط، بی­جا: الکتبه المرتضویه لاحیاء آثار الجعفریه،.

1. عطازاده، سعید و انصاری، جلال (1400ش)، حقوق جزای اختصاصی جرایم رایانه­ای، تهران: بنیاد حقوقی میزان، چاپ دوم.
2. فتاحی زفرقندی، سجاد، اسماعیلی، مهدی و حاجی­تبار فیروزجایی، حسن (1399)، «پیشگیری از جرم جاسوسی سایبری نیروهای مسلح و نقش آن در تامین حق امنیت»، حقوق بشر اسلامی، شماره9، بهار، 255-276.
3. قیاسی، جلال الدین (1385 ش)، مبانی سیاست جنایی حکومت اسلامی، قم، پژوهشگاه علوم و فرهنگ اسلامی.
4. لازرژ، کریستین (1382ش)، درآمدی به سیاست جنایی، ترجمه علی حسین نجفی ابرندآبادی، تهران: نشرمیزان.
5. متقی هندی، علاءالدین علی بن­حسام (بی­تا)، کنز العمال، ج ۱۱، بی­جا: موسسه الرساله.
6. محمدنسل، غلام رضا (1395 ش)، حقوق جزای اختصاصی جرایم رایانه­ای در ایران، تهران، بنیاد حقوقی میزان، چاپ دوم.

مغربی، قاضی نعمان (1385ق)، دعائم الاسلام و ذکر الحلال و الحرام و القضایا و الاحکام، تحقیق آصف فیضی، قم: موسسه آل­البیت، چاپ دوم،.

<https://parsi.euronews.com23>...

<https://www.irna.ir/news/8443296624>.

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

**Abstract**

The current research, under the title "Cyber espionage in the criminal policy of Iran and Afghanistan" has been conducted with the aim of understanding, identifying the differences and similarities and adapting the criminal policy of the two countries, regarding cyber espionage.

The general strategy of the research is practical in terms of its purpose and analytical-descriptive in terms of its execution method and its collection method is library-style. The findings of the research have been analyzed based on the researchers' understanding of the sources and legal texts about the criminal policy of the two countries. By comparing the criminal policy of two countries regarding cyber espionage, one can understand the advantages and disadvantages of each one well and use the advantages of one to solve the disadvantages of the other. The findings of the research show that the superiority of Iran's criminal policy compared to Afghanistan's criminal policy is in the accuracy and differentiation of the criminal aspect of the crime of cyber espionage; Because between the one who got access to secret information and the one who gave this information to unqualified people and the one who gave this information to strangers and enemies; It has distinguished and considered the punishment of these people in proportion to the crime committed. This is while the criminal policy of Afghanistan has included the same punishment for these people without any difference. One of the advantages of Afghanistan's criminal policy is that it has distinguished espionage during wartime from espionage in normal conditions. Another violation in the criminal policy of the two countries is the lack of attention to the criminalization and punishment of accomplices and herald of cyber espionage.

**Keywords:** Cyber ​​espionage, Cyberspace, Penal policy

1. 1. 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» [↑](#footnote-ref-1)
2. . بیش از بیست تا سی سال. [↑](#footnote-ref-2)
3. . بیش از شانزده تا بیست سال. [↑](#footnote-ref-3)
4. . Identity theft [↑](#footnote-ref-4)
5. . بیش از بیست تا سی سال. [↑](#footnote-ref-5)
6. . بیش از شانزده تا بیست سال. [↑](#footnote-ref-6)