مطالعات علوم سیاسی، حقوق و فقه
دوره ۱۱، شماره ۱، بهار ۱۴۰۴
صفحات ۹۳۶-۹۱۸

Online ISSN: ۲۴۷۶-۴۴۶۹
Print ISSN: ۲۵۳۸-۲۰۳۹
www.irijournals.com

تبیین جرایم سایبری و جرایم مرتبط با فضای مجازی و مسئولیت کیفری اشخاص در این زمینه

محسن رستمی

دانش آموخته ی کارشناسی ارشد رشته حقوق جزا و جرم شناسی دانشگاه آزاد اسلامی واحد نورآباد ممسنی. ایران.

چکیده

جرایم سایبری به فعالیت‌های غیرقانونی گفته می‌شود که از طریق رایانه، اینترنت و فضای مجازی انجام می‌گیرند و شامل سرقت اطلاعات، هک، جاسوسی سایبری، فیشینگ، انتشار محتوای غیرقانونی و خرابکاری در سیستم‌های رایانه‌ای است. با گسترش فناوری‌های نوین و افزایش استفاده از فضای مجازی، این جرایم به تهدیدی جدی برای امنیت و حقوق افراد تبدیل شده‌اند. قانون‌گذار ایران با تصویب قانون جرایم رایانه‌ای، به جرم‌انگاری این رفتارها و تعیین مسئولیت کیفری اشخاص حقیقی و حقوقی در این زمینه پرداخته است هدف از تبیین جرایم سایبری و جرایم مرتبط با فضای مجازی، شناخت دقیق این جرایم، تعیین حدود و مسئولیت کیفری مرتکبین و ایجاد چارچوب قانونی مناسب برای مقابله با آن‌ها است. همچنین، هدف شناسایی گستره مسئولیت کیفری افراد و اشخاص حقوقی در فضای مجازی و تأمین امنیت حقوقی و اجتماعی در این حوزه است. مطالعه و تحلیل قوانین و مقررات موجود در ایران، به ویژه قانون جرایم رایانه‌ای، بررسی انواع جرایم سایبری و مسئولیت کیفری مرتبط با آن‌ها و مرور ادبیات حقوقی و جرم‌شناسی درباره جرایم فضای مجازی و مسئولیت کیفری اشخاص در این فضا. جرایم سایبری شامل انواع مختلفی مانند سرقت اطلاعات شخصی و مالی، هک سیستم‌ها، جاسوسی سایبری، فیشینگ، انتشار محتوای غیرقانونی و خرابکاری در سیستم‌های رایانه‌ای است مجازات این جرایم بسته به نوع و شدت جرم از حبس (از ۹۱ روز تا چند سال) تا جزای نقدی و حتی در موارد خاص اعدام متغیر است قانون جرایم رایانه‌ای ایران برای نخستین بار مسئولیت کیفری اشخاص حقوقی را نیز در فضای مجازی به رسمیت شناخته و فصل ششم این قانون به موضوع مسئولیت کیفری اختصاص یافته است. مسئولیت کیفری در فضای سایبر شامل اشخاص حقیقی و حقوقی است و قانون‌گذار تأکید بر ایجاد چارچوب‌های حقوقی برای مقابله با این جرایم دارد. جرایم سایبری و جرایم مرتبط با فضای مجازی به دلیل پیچیدگی‌های خاص خود نیازمند جرم‌انگاری دقیق و تعیین مسئولیت کیفری مشخص برای اشخاص حقیقی و حقوقی هستند. قانون جرایم رایانه‌ای ایران گام مهمی در این زمینه برداشته و با تعیین مجازات‌ها و مسئولیت‌ها، زمینه مقابله مؤثر با این جرایم را فراهم کرده است. شناخت و تبیین مسئولیت کیفری در فضای سایبر برای حفظ امنیت حقوقی و اجتماعی ضروری است.

واژگان کلیدی: جرایم سایبری، فضای مجازی، مسئولیت کیفری، قانون جرایم رایانه‌ای، جاسوسی سایبری، فیشینگ

۱-مقدمه

با گسترش فناوری‌های اطلاعات و ارتباطات و افزایش استفاده از فضای مجازی، جرایم سایبری به یکی از چالش‌های مهم امنیتی، اجتماعی و حقوقی در جهان و به ویژه در ایران تبدیل شده‌اند. این جرایم که شامل دسترسی غیرمجاز، هک، سرقت اطلاعات، نشر محتوای غیرقانونی و سایر رفتارهای مجرمانه در فضای سایبر است، به دلیل ماهیت فرامرزی و پیچیدگی‌های فنی، مقابله با آن‌ها نیازمند قوانین دقیق و هماهنگ با استانداردهای بین‌المللی است. (گرکی، مارکو، ۱۴۰۱) با پیشرفت روزافزون فناوری‌های اطلاعات و ارتباطات و گسترش استفاده از اینترنت و فضای مجازی، جوامع امروزی با چالش‌های نوینی در حوزه امنیت و حقوق مواجه شده‌اند که مهم‌ترین آن‌ها جرایم سایبری است. جرایم سایبری به مجموعه‌ای از فعالیت‌های مجرمانه گفته می‌شود که با استفاده از رایانه، شبکه‌های ارتباطی و فضای مجازی انجام می‌گیرند و می‌توانند امنیت اطلاعات، حریم خصوصی افراد، اقتصاد و حتی امنیت ملی کشورها را به خطر اندازند. این جرایم به دلیل ماهیت غیرمادی و فرامرزی خود، مقابله با آن‌ها را پیچیده‌تر کرده و نیازمند چارچوب‌های قانونی دقیق و به‌روز است. (گیدنز، ۱۳۹۷)

در ایران، قانون جرایم رایانه‌ای مصوب سال ۱۳۸۸ به عنوان نخستین قانون جامع در این حوزه تصویب شده است که انواع جرایم سایبری را تعریف و برای آن‌ها مجازات تعیین کرده است. با این حال، این قانون به لحاظ جامعیت و پوشش کامل همه ابعاد جرایم سایبری و همچنین تطبیق با تحولات سریع فناوری و استانداردهای بین‌المللی، دارای کاستی‌هایی است. از جمله مشکلات این قانون می‌توان به عدم تعریف دقیق برخی جرایم جدید، نبود هماهنگی کامل با قوانین بین‌المللی و چالش‌های مربوط به تعیین مسئولیت کیفری اشخاص حقوقی و حقیقی اشاره کرد. (فرجی‌ها و دیگران ۱۴۰۰) همچنین، برخی جرایم خاص مانند جرایم علیه مذاهب یا جرایم پیچیده مالی سایبری به طور کامل در قانون پوشش داده نشده‌اند. با وجود تصویب قانون جرایم رایانه‌ای در ایران، هنوز خلأها و نواقصی در تعریف دقیق برخی جرایم سایبری و تعیین مسئولیت کیفری اشخاص وجود دارد که باعث می‌شود مقابله مؤثر با این جرایم دشوار باشد. همچنین، تطبیق قوانین داخلی با کنوانسیون‌ها و پیمان‌های بین‌المللی مانند پیمان بوداپست و سایر اسناد جهانی، نیازمند بازنگری و اصلاحات قانونی است. (عبقری، ۱۳۹۷)

جرایم سایبری به دلیل تأثیرات گسترده بر امنیت اطلاعات، حریم خصوصی، اقتصاد و نظم اجتماعی، اهمیت فراوانی دارند. در جامعه‌ای که فناوری‌های نوین به سرعت در حال نفوذ است، شناخت دقیق این جرایم و مسئولیت کیفری مرتبط با آن‌ها برای حفظ امنیت حقوقی و اجتماعی ضروری است. این پژوهش می‌تواند به بهبود سیاست‌های جنایی، ارتقای قوانین کیفری و افزایش آگاهی حقوقی در جامعه کمک کند. (عاملی، ۱۳۹۶)

با توجه به افزایش روزافزون استفاده از فضای مجازی در زندگی روزمره افراد و سازمان‌ها و همچنین افزایش حملات سایبری به زیرساخت‌های حیاتی کشور، ضرورت دارد که قوانین و مقررات مرتبط با جرایم سایبری به صورت مستمر بازنگری و به‌روزرسانی شوند تا بتوانند پاسخگوی نیازهای حقوقی و امنیتی جامعه باشند. (شیرزاد، ۱۳۹۹) این پژوهش با هدف شناسایی نقاط ضعف و قوت قانون فعلی، تطبیق آن با استانداردهای بین‌المللی و ارائه راهکارهای بهبود، می‌تواند به ارتقای امنیت حقوقی و اجتماعی در فضای مجازی کمک کند. همچنین، افزایش آگاهی عمومی و تخصصی درباره انواع جرایم سایبری و مسئولیت کیفری مرتبط با آن‌ها باعث کاهش آسیب‌های ناشی از این جرایم خواهد شد (عاملی، ۱۳۹۶)

مطالعات تطبیقی نشان می‌دهد که قانون جرایم رایانه‌ای ایران نسبت به برخی کشورها و کنوانسیون‌های بین‌المللی مانند کنوانسیون بوداپست، پیشرفت‌هایی داشته اما هنوز فاصله قابل توجهی با قوانین کشورهای پیشرفته دارد. برای مثال، در کشورهای پیشرفته‌تر، قوانین به طور جامع‌تر به موضوعاتی چون حفاظت از داده‌های شخصی، مسئولیت اشخاص حقوقی، و جرایم مالی سایبری پرداخته‌اند. همچنین، هماهنگی بین‌المللی و همکاری‌های فراملی در مقابله با جرایم سایبری در این

کشورها بیشتر توسعه یافته است. در ایران نیز با توجه به تهدیدهای سایبری متعدد، از جمله حملات پیشرفته به تأسیسات حیاتی، نیاز به هماهنگی بیشتر قوانین داخلی با استانداردهای جهانی احساس می‌شود. مطالعات تطبیقی نشان می‌دهد که قوانین ایران در حوزه جرایم سایبری نسبت به برخی کشورها و اسناد بین‌المللی پیشرفت‌هایی داشته اما همچنان نیازمند اصلاحات و به‌روزرسانی است تا هماهنگی بیشتری با استانداردهای جهانی و نیازهای روز داشته باشد (حسینی، ۱۳۹۵). به عنوان مثال، قانون جرایم رایانه‌ای ایران پس از سال‌ها تلاش تصویب شده اما در برخی موارد مانند حمایت از داده‌های شخصی و تعیین دقیق مسئولیت کیفری، با قوانین کشورهای پیشرفته مانند آلمان تفاوت‌هایی دارد. سوال اصلی که در اینجا مطرح می شود این است که آیا قوانین موجود در ایران به ویژه قانون جرایم رایانه‌ای، توانسته‌اند به طور کامل و جامع جرایم سایبری را تعریف و مسئولیت کیفری اشخاص را تعیین کنند؟ و چگونه می‌توان این قوانین را با استانداردهای بین‌المللی تطبیق داد تا مقابله مؤثرتری با جرایم سایبری صورت گیرد؟

۲-مفاهیم و مبانی نظری

۲-۱- مفهوم فضای سایبری

فضای سایبری به محیطی گفته می‌شود که از طریق شبکه‌های رایانه‌ای، اینترنت و فناوری‌های ارتباطی ایجاد شده است و امکان تبادل اطلاعات، انجام فعالیت‌های اجتماعی، اقتصادی و سیاسی را فراهم می‌کند. این فضا برخلاف فضای فیزیکی، ماهیتی غیرمادی، گسترده و فرامرزی دارد که کنترل و نظارت بر آن را دشوار می‌سازد. فضای سایبری شامل مولفه‌هایی مانند تصدیق هویت، پروتکل‌های امنیتی، تضمین کیفیت نرم‌افزار، رمزنگاری، مهندسی اجتماعی و ابزارهای کشف و نظارت است که همه در حفظ امنیت و سلامت این فضا نقش حیاتی دارند. (جوانشیر، پورقهرمانی، ۱۳۹۸)

۲-۲- مفهوم جرم و جرم سایبری

جرم به معنای هر رفتاری است که قانون آن را ممنوع و برای مرتکب آن مجازات تعیین کرده است. جرم سایبری، شاخه‌ای از جرایم است که در فضای سایبری و با استفاده از فناوری‌های اطلاعاتی انجام می‌شود. این جرایم می‌توانند شامل هک، سرقت اطلاعات، فیشینگ، نشر محتوای غیرقانونی، خرابکاری در سیستم‌های رایانه‌ای و جرایم مالی دیجیتال باشند جرم سایبری به دلیل ماهیت خاص خود، مانند غیرمادی بودن، سرعت انتقال و گستردگی جغرافیایی، از پیچیدگی‌های ویژه‌ای برخوردار است که در جرم‌های سنتی کمتر دیده می‌شود. (حیدری، شهبازی، شیرانی، ۱۳۹۷).

۳- مبانی نظری جرم‌انگاری جرایم سایبری

جرم‌انگاری در فضای سایبری بر اساس مبانی حقوقی و فلسفی خاصی انجام می‌شود که مهم‌ترین آن‌ها عبارتند از:

۳-۱- اصل صدمه: [1]

این اصل بیان می‌کند که تنها رفتارهایی باید جرم‌انگاری شوند که به دیگران صدمه وارد کنند. در فضای سایبری، این صدمه می‌تواند شامل خسارت مالی، نقض حریم خصوصی، اختلال در سیستم‌های حیاتی و آسیب‌های روانی باشد. اصل صدمه مرز

[1] -Harm Principle

مهمی برای تعیین دخالت کیفری دولت در آزادی‌های فردی است و در جرایم سایبری نیز باید با دقت به آن توجه شود تا حقوق فردی حفظ شود. (ریک، ۱۳۹۶)

۳-۲-اصل استقلال فردی:

این اصل تأکید می‌کند که هر فرد باید تا جایی که به دیگران آسیب نرساند، آزاد باشد و مداخله کیفری باید محدود به مواردی باشد که آزادی دیگران به خطر افتاده است. در فضای سایبری، این اصل چالش‌برانگیز است زیرا رفتارهای مجرمانه اغلب در مرزهای آزادی بیان، حریم خصوصی و امنیت قرار دارند.

۳-۳-اصل قانونی بودن جرم و مجازات:

بر اساس این اصل، هیچ رفتاری بدون پیش‌بینی قانونی نمی‌تواند جرم تلقی شود و هیچ مجازاتی بدون حکم قانون اعمال نشود. در فضای سایبری به دلیل نوظهور بودن بسیاری از جرایم، این اصل اهمیت ویژه‌ای دارد تا از سوءاستفاده‌های احتمالی جلوگیری شود.

۳-۴-اصل ملزومات عمومی:

این اصل به ضرورت جرم‌انگاری رفتارهایی اشاره دارد که به منافع عمومی و امنیت جامعه آسیب می‌زنند، مانند حملات سایبری به زیرساخت‌های حیاتی، که نیازمند مداخله کیفری هستند. (حیدری، شهبازی، شیرانی، ۱۳۹۷).

۳-۵- چارچوب نظری و مدل‌های مفهومی فضای سایبری

فضای سایبری به عنوان یک حوزه پیچیده، نیازمند مدل‌های مفهومی و چارچوب‌های نظری برای درک بهتر تهدیدات و آسیب‌ها است. این مدل‌ها شامل مولفه‌های زیر می‌شوند:

۳-۶-هویت سایبری:

نحوه شناسایی و تصدیق هویت کاربران در فضای مجازی که نقش کلیدی در امنیت دارد. هویت سایبری می‌تواند هدف حملات هکری و جعل هویت باشد.

۳-۷-امنیت فضای سایبری:

مجموعه اقدامات فنی، حقوقی و مدیریتی برای حفاظت از اطلاعات، سیستم‌ها و کاربران در برابر تهدیدات سایبری. این امنیت شامل رمزنگاری، مدیریت رخداد، نظارت و کشف حملات است (ریک، ۱۳۹۶)

۳-۸-نبرد سایبری:

استفاده از فناوری‌های سایبری به عنوان ابزار یا سلاح برای انجام عملیات تروریستی، خرابکاری یا جنگ اطلاعاتی علیه کشورها و سازمان‌ها که اهمیت امنیت ملی را برجسته می‌کند. (جلالی‌فراهانی، ۱۳۹۳)

جرم‌انگاری جرایم سایبری باید بر اساس تعادل میان حفظ آزادی‌های فردی و حمایت از منافع عمومی باشد. اصل صدمه به عنوان مبنای محدودکننده جرم‌انگاری، به ما می‌گوید که تنها رفتارهایی که به دیگران آسیب واقعی و قابل اثبات وارد کنند، باید جرم تلقی شوند. این امر در فضای سایبری که مرزهای آسیب و آزادی مبهم است، نیازمند تعریف دقیق‌تر و معیارهای

روشن است. از سوی دیگر، اصل استقلال فردی تأکید دارد که نباید مداخلات کیفری به گونه‌ای باشد که آزادی‌های مشروع کاربران محدود شود. (جلالی‌فراهانی، ۱۳۹۳)

همچنین، با توجه به ماهیت فرامرزی فضای سایبری، هماهنگی قوانین داخلی با استانداردهای بین‌المللی و ایجاد چارچوب‌های همکاری بین‌المللی برای مقابله با جرایم سایبری ضروری است. مدل‌های مفهومی فضای سایبری کمک می‌کنند تا ابعاد مختلف این حوزه از جمله هویت، امنیت و تهدیدات به صورت نظام‌مند تحلیل شود و راهکارهای مناسبی برای مقابله با آسیب‌ها ارائه گردد.

مبانی نظری فضای سایبری نقش بنیادینی در توسعه و شکل‌دهی سیاست‌های امنیتی ایفا می‌کنند. این مبانی که شامل چارچوب‌های نظری، مدل‌های مفهومی و دکترین‌های سایبری هستند، به سیاستگذاران کمک می‌کنند تا با درک عمیق‌تر از ساختار، بازیگران، تهدیدات و ابعاد فضای سایبری، راهبردهای مؤثر و متناسب با شرایط محیطی و ملی تدوین کنند.

۴-مبانی نظری فضای سایبری بر توسعه سیاست‌های امنیتی

۴-۱- تبیین ساختار و عناصر فضای سایبری:

مبانی نظری، عناصر کلیدی فضای سایبری مانند شبکه‌ها، زیرساخت‌ها، بازیگران دولتی و غیردولتی، و تعاملات آن‌ها را شناسایی می‌کنند. این شناخت به سیاستگذاران امکان می‌دهد تا سیاست‌ها را بر اساس واقعیت‌های زیست‌بوم سایبری کشور و با در نظر گرفتن همه ذینفعان طراحی کنند. (جلالی‌فراهانی و باقریاصل، ۱۳۹۵)

۴-۲-ایجاد چارچوب حاکمیت شبکه‌ای:

نظریه‌های حاکمیت شبکه‌ای که در مبانی نظری مطرح می‌شوند، بر ضرورت هماهنگی بین نهادهای مختلف پژوهشی، دولتی و خصوصی تأکید دارند. این هماهنگی باعث تدوین سیاست‌های یکپارچه و نقشه راه فناوری‌های بومی امنیت سایبری می‌شود که امنیت ملی را تقویت می‌کند.

۴-۳-مدیریت عنصر انسانی و روانشناسی سایبری:

مبانی نظری روانشناسی سایبری به عنوان یکی از اجزای مهم فضای سایبری، نقش کلیدی عنصر انسانی را در امنیت سایبری برجسته می‌کند. شناخت رفتار کاربران، آموزش و فرهنگ‌سازی امنیتی از طریق این مبانی، سیاست‌های امنیتی را به سمت کاهش آسیب‌پذیری‌های انسانی هدایت می‌کند. (جلالی‌فراهانی، ۱۳۹۴)

۴-۴-تدوین دکترین سایبری

دکترین سایبری به عنوان مجموعه‌ای از اصول، قواعد و باورهای نظری و عملی، راهنمایی برای همسویی و همگرایی اقدامات راهبردی در حوزه امنیت سایبری فراهم می‌آورد. این دکترین‌ها بر اساس مبانی نظری، تجارب موفق گذشته و شرایط بومی تدوین می‌شوند و به سیاستگذاران کمک می‌کنند تا اولویت‌ها و خطوط راهنمای امنیتی را مشخص کنند.

۴-۵-توجه به ابعاد چندگانه فضای سایبری:

مبانی نظری فضای سایبری ابعاد مختلفی مانند دیپلماسی، اقتصادی، فرهنگی، اطلاعاتی و امنیتی را در نظر می‌گیرند. این نگاه چندبعدی باعث می‌شود سیاست‌های امنیتی نه تنها فنی بلکه جامع و متناسب با واقعیت‌های اجتماعی و سیاسی کشور باشند. (باستانی، ۱۳۹۳)

۴-۶-تقویت اعتماد عمومی و قانون‌مداری:

مبانی نظری حکمرانی سایبری بر اهمیت اعتماد عمومی و پذیرش مدل‌های حکمرانی تأکید دارند. این موضوع در تدوین سیاست‌های امنیتی اهمیت دارد زیرا بدون حمایت و همکاری افکار عمومی، اجرای سیاست‌ها با چالش مواجه می‌شود.

۷-جرم‌انگاری جرایم سایبری

جرم‌انگاری جرایم سایبری به معنای تعریف و تعیین رفتارهای مجرمانه در فضای مجازی و فناوری اطلاعات است که بر اساس آن، اعمالی که به صورت غیرمجاز در سامانه‌های رایانه‌ای یا مخابراتی انجام می‌شود، تحت پیگرد قانونی قرار می‌گیرند. این جرم‌ها شامل دسترسی غیرمجاز، تخریب داده‌ها، اختلال در سامانه‌ها، سوءاستفاده از اطلاعات و سایر رفتارهای مخرب در فضای سایبری می‌شوند.

مبانی جرم‌انگاری جرایم سایبری بر اساس فلسفه حقوق و هستی‌شناسی، شرط لازم برای جرم‌انگاری را حصول نتیجه و پیامد فرامجازی (خارج از فضای مجازی) می‌داند، به این معنا که کنش سایبری باید منجر به مداخله در آزادی یا حقوق شهروندان شود تا بتوان آن را جرم شناخت. شرط کافی نیز توجیه مداخله قانونی در آزادی افراد بر اساس اصول محدودکننده آزادی است. (آقایی نیا، ۱۳۹۲)

۷-۱-اصول جرم‌انگاری در فضای سایبر

اصول کلی و خاصی در جرم‌انگاری جرایم سایبری باید رعایت شود که شامل موارد زیر است:

اصل مشروعیت: هر رفتاری که جرم شناخته می‌شود باید بر اساس قانون باشد.

اصل ضرورت: جرم‌انگاری باید تنها در موارد ضروری و ناگزیر صورت گیرد.

رعایت حریم خصوصی و حقوق شهروندی: حقوق افراد در فضای سایبر باید محفوظ بماند.

تناسب جرم و مجازات: مجازات‌ها باید متناسب با نوع و شدت جرم باشد.

توجه به امکانات دستگاه عدالت کیفری و اقشار آسیب‌پذیر: در جرم‌انگاری باید به توانایی‌های اجرایی و حمایت از اقشار خاص توجه شود.

۷-۲-قانون جرایم رایانه‌ای در ایران

قانون جرایم رایانه‌ای ایران شامل ۵۶ ماده است که انواع جرایم رایانه‌ای را تعریف و برای آن مجازات تعیین کرده است. این قانون جرایمی مانند دسترسی غیرمجاز، تخریب داده‌ها، سوءاستفاده از اطلاعات، و جرایم مرتبط با کودکان را پوشش می‌دهد. رسیدگی به این جرایم معمولاً در دادگاه محل وقوع جرم انجام می‌شود و در صورت نامعلوم بودن محل وقوع جرم، دادسرای محل کشف جرم مسئول تحقیقات مقدماتی است. (آخوندی، ۱۳۹۹)

۷-۳-مجازات جرایم سایبری

بر اساس قانون جرایم رایانه‌ای، مجازات‌ها شامل حبس از ۹۱ روز تا یک سال و جریمه نقدی بین ۵ تا ۲۰ میلیون ریال است. این مجازات‌ها بسته به نوع جرم و شدت آن متفاوت است و هدف آن حفظ امنیت فضای سایبری و جلوگیری از تخلفات در این حوزه است.

۷-۴-سیاست جنایی ایران در زمینه جرایم سایبری

سیاست جنایی ایران در زمینه جرایم سایبری بر چند محور اصلی استوار است که شامل سیاست جنایی تقنینی، قضایی و مشارکتی می‌شود:

۷-۴-۱- سیاست جنایی تقنینی

این بخش وظیفه قانون‌گذاری را بر عهده دارد و در آن قوانین و مقررات مرتبط با جرایم سایبری تدوین شده‌اند. قانون‌گذار در ایران با تصویب قانون جرایم رایانه‌ای و مصوبات شورای عالی فضای مجازی، به طور صریح و ضمنی تدابیر فنی و قانونی را برای تأمین امنیت فضای سایبری پیش‌بینی کرده است. این سیاست بر پیشگیری از جرم و تضمین ضمانت اجرای سنگین برای مرتکبان جرایم سایبری تأکید دارد. (بولک ۱۳۹۵)

۷-۴-۲- سیاست جنایی قضایی

قوه قضائیه با رویکرد پیشگیرانه و مقابله‌ای در برابر جرایم سایبری فعالیت می‌کند. این سیاست شامل تصمیم‌گیری‌ها، رویه‌های دادسراها و دادگاه‌ها و همکاری با نهادهای تخصصی مانند مرکز مدیریت امداد و هماهنگی عملیات رخداد (ماهر)، مرکز آگاهی رسانه، پشتیبانی و امداد رایانه‌ای (آپا) و پلیس فتا است. هدف این سیاست، رسیدگی سریع و مؤثر به جرایم سایبری و کاهش بار دستگاه عدالت کیفری است.

۷-۴-۳-سیاست جنایی مشارکتی

این سیاست بر مشارکت جامعه مدنی، نهادهای غیر دولتی و مردم در پیشگیری و مقابله با جرایم سایبری تأکید دارد. از طریق آموزش، ارتقاء سواد دیجیتال، فرهنگ‌سازی و استفاده از فناوری‌های فنی مانند رمز عبور و نرم‌افزارهای ضد پایش، سعی می‌شود فضای سایبری سالم‌سازی شود. مشارکت مردم در گزارش‌دهی و نظارت بر ورودی‌ها و خروجی‌های اطلاعاتی از جمله راهکارهای این سیاست است که به پیشگیری مؤثرتر از وقوع جرم کمک می‌کند. (بولاغی و جمادی، ۱۳۹۳)

۷-۵-مسئولیت کیفری در محیط سایبری

تعاریف بسیار زیادی از آن ارائه داده‌اند. یکی از نویسندگان حقوق جزای کشورمان به‌طورکلی الزام شخص به پاسخگویی در قبال تعرض به دیگران یا نقض حقوقی که تحت عنوان حقوق آزادی‌های غربی و گاهاً تحت عنوان حقوق حمایتی جمعی و به‌منظور دفاع از جامعه ارائه می‌شود را مسئولیت کیفری قلمداد کرده است (باستانی، ۱۳۹۳). یکی دیگر از نویسندگان باتوجه به تعریف لغوی مسئولیت که به معنای موظف بودن به انجام کار معنا شده مسئولیت را نوعی التزام دانسته و معتقد است در قلمرو حقوق کیفری محتوای این التزام تقبل آثار و عواقب افعال محرمانه است، به عبارت صحیح‌تر تحمل مجازات که در قوانین کیفری سزای افعال سرزنش‌آمیز بر نظام به شمار می‌آید (جلالی‌فراهانی، ۱۳۹۴). البته مسئولیت کیفری را می‌توان از دیدگاه دیگری نیز معنا کرد و آن نه التزام به تقبل آثار و عواقب افعال مجرمانه که استحقاق و سزاواری تحمل این عواقب

است. مسئولیت کیفری در محیط سایبر نیز به معنای تقبل آثار ناشی از فعل مجرمانه فرد است که در محیط اینترنت به وقوع پیوسته بنابراین مسئولیت در محیط سایبر مفهومی جدای از سایر موارد مسئولیت ندارد. (باستانی، ۱۳۹۳)

در رابطه با مسئولیت کیفری اشخاص حقوقی نظرات مختلفی ارائه‌شده است، برخی از نویسندگان درصدد نفی آن برآمده‌اند و برخی دیگر با استناد به اینکه اشخاص حقوقی وجود واقعی دارند، بزه ارتکابی در برابر ایشان قابلیت استناد دارد و درنهایت اینکه برخی کیفرها را می‌توان در ارتباط این اشخاص مورداستفاده قرارداد معتقدند که اشخاص حقوقی مسئولیت کیفری دارند (روح‌الامینی ۱۳۸۷: ۱۳۳). در ایران موارد متعددی می‌توان ذکر نمود که بیانگر تمایل قانون‌گذار ایران در پذیرش مسئولیت کیفری برای اشخاص حقوقی است، شاید بتوان ماده ۲۲۰ قانون تجارت را به‌عنوان نخستین گام از پذیرش مسئولیت برای اشخاص حقوقی نام برد که به‌موجب آن مسئولیت تضامنی برای شرکت‌های ثبت‌نشده و عملی در نظر گرفته‌شده است، متن ماده‌واحده مربوط به ضبط اموال متعلق به احزابی که منحل می‌شوند نمونه دیگری از پذیرش مسئولیت کیفری اشخاص حقوقی در نظام حقوقی ایران است (دامغانی ۱۳۸۸: ۱۵) و درنهایت می‌توان به قانون جرایم رایانه‌ای استناد نمود که در این قانون مسئولیت کیفری اشخاص حقوقی صراحتاً موردپذیرش قرارگرفته است، از دیدگاه تطبیقی ماده ۱۰ کنوانسیون پالرمو که در رابطه با جرایم سازمان‌یافته فراملی به تصویب کشورهای عضو رسیده است، در این رابطه مقرر داشته: هر دولت عضو، منطبق با اصول حقوقی خود، تدابیر لازم جهت برقراری مسئولیت اشخاص حقوقی مشارکت‌کننده در ارتکاب جنایات شدیدی که یک گروه مجرم سازمان‌یافته نیز در آن‌ها دخالت دارد و نیز جرایم موضوع ۵، ۶، ۸ و ۳۲ این کنوانسیون اتخاذ خواهد نمود (باستانی، ۱۳۹۳)

مسئولیت اشخاص حقوقی می‌تواند کیفری، مدنی یا اداری باشد. این مسئولیت‌ها، به مسئولیت کیفری اشخاص حقیقی که مرتکب این جرایم شده‌اند، خدشه‌ای وارد نخواهد کرد.

در ژاپن تا سال ۱۹۳۲ تنها مدیران اشخاص حقوقی به نیابت از آن مسئول قلمداد می‌شدند، از سال ۱۹۳۲ نظام مسئولیت دوگانه یا ریوباتسوکایتی مسئولیت مشترک شخص حقوقی و مدیر را موردپذیرش قرارداد، مهم‌ترین مجازات قابل‌اعمال در نظام حقوقی این کشور در برابر اشخاص حقوقی جریمه است (کیوتو ۱۳۸۲: ۱۸۰). در حقوق جزای آمریکا، به خاطر پیچیدگی بیشتر حیات اجتماعی، شرکت‌های بزرگ صنعتی و تجارتی نمود و اهمیت فوق‌العاده‌ای به دست آورده‌اند؛ به همین خاطر مسئولیت جزایی اشخاص حقوقی از دیرباز پذیرفته‌شده است (آخوندی، ۱۳۹۹). اما مسئولیت کیفری به‌عنوان یک مفهوم حقوقی چه ارتباطی با سایر موارد مسئولیت دارد؟ پاسخ این سؤال درگرو بررسی مفهوم مسئولیت کیفری در کنار سایر موارد مسئولیت است.

۷-۶- مسئولیت کیفری در قانون جرایم رایانه‌ای ایران

قانون‌گذار ایران در قانون جرایم رایانه‌ای فصل ششم از قانون را به موضوع مسئولیت کیفری اختصاص داده است، شاید بتوان گفت مهم‌ترین تغییری که قانون فوق‌الذکر در رابطه با مسئولیت کیفری ایجاد نموده، شناسایی و ایجاد مسئولیت کیفری برای اشخاص حقوقی است، ماده ۱۹ و ۲۰ قانون فوق‌الذکر در رابطه با مسئولیت کیفری اشخاص حقوقی است. ماده ۱۹ مقرر می‌دارد: «در موارد زیر، چنانچه جرایم رایانه‌ای به نام شخص حقوقی و در راستای منافع آن ارتکاب یابد، شخص حقوقی دارای مسئولیت کیفری خواهد بود:

الف) هرگاه مدیر شخص حقوقی مرتکب جرم رایانه‌ای شود.

ب) هرگاه مدیر شخص حقوقی دستور ارتکاب جرم رایانه‌ای را صادر کند و جرم به وقوع پیوندد.

ج) هرگاه یکی از کارمندان شخص حقوقی بااطلاع مدیر یا در اثر عدم نظارت وی مرتکب جرم رایانه‌ای شود.
د) هرگاه تمام یا قسمتی از فعالیت شخص حقوقی به ارتکاب جرم رایانه‌ای اختصاص‌یافته باشد.
ماده ۲۰ نیز اشعار داشته: «اشخاص حقوقی موضوع ماده فوق، با توجه به شرایط و اوضاع‌واحوال جرم ارتکابی، میزان درآمد و نتایج حاصله از ارتکاب جرم، علاوه بر سه تا شش برابر حداکثر جزای نقدی جرم ارتکابی، به ترتیب ذیل محکوم خواهند شد:
الف) چنانچه حداکثر مجازات حبس آن جرم تا پنج سال حبس باشد، تعطیلی موقت شخص حقوقی از یک تا نُه ماه و در صورت تکرار جرم تعطیلی موقت شخص حقوقی از یک تا پنج سال.
ب) چنانچه حداکثر مجازات حبس آن جرم بیش از پنج سال حبس باشد، تعطیلی موقت شخص حقوقی از یک تا سه سال و در صورت تکرار جرم شخص حقوقی منحل خواهد شد.
در این رابطه ممکن است این سؤال مطرح شود که تأکید قانون‌گذار ایران بر بحث مسئولیت کیفری اشخاص حقوقی چه معنایی در پی دارد؟ و آثار آن چیست؟
یکی از مهم‌ترین سؤالاتی که ممکن است در این زمینه مطرح شود درواقع بحث شناخت مسئولیت کیفری برای اشخاص حقوقی و تأثیر آن بر مسئولیت افراد حقیقی است، آیا رویه قانون‌گذار ایران بر این بوده که اصل را بر مسئولیت کیفری اشخاص حقوقی قرار دهد؟ یا به دنبال نفی مسئولیت کیفری اشخاص حقیقی در محیط سایبر بوده است؟ پاسخ مطمئناً منفی است، با توجه به اینکه تبصره دو ماده ۱۹ مقرر می‌دارد: «مسئولیت کیفری شخص حقوقی مانع مجازات مرتکب نخواهد بود»، بنابراین اینکه قانون‌گذار ماده نخست از مبحث ششم قانون جرایم رایانه‌ای را به بحث مسئولیت کیفری اختصاص داده، به معنای نفی مسئولیت کیفری اشخاص حقیقی نیست.
مسئله دیگری که باید در این مقوله موردبررسی قرار بگیرد بحث تناسب مسئولیت‌ها و رابطه مسئولیت کیفری اشخاص حقیقی و حقوقی است، همان‌طور که گفتیم تبصره دو ماده ۱۹ مسئولیت کیفری اشخاص حقوقی را مانعی برای مجازات اشخاص حقیقی ندانسته، اما متن ماده فوق تا اندازه‌ای گمراه‌کننده است، زیرا عملاً صحبتی از ارتباط دو مسئولیت با یکدیگر نشده است، به‌هرحال باید اذعان داشت تا زمانی که کسی مسئولیت نداشته باشد اعمال مجازات بر ایشان امکان‌پذیر نیست، بنابراین متن تبصره ۲ فوق‌الذکر به معنای امکان وجود مسئولیت همزمان برای شخص حقوقی و اشخاص حقیقی عضو آن مجموعه است. بحث ارتباط میان مسئولیت اشخاص حقیقی و مسئولیت اشخاص حقوقی، به اشکال ارتباط میان این دو نوع مسئولیت می‌پردازد، باید توجه داشت که این دو مسئولیت از پیشینه و ریشه‌ی مشترکی برخوردارند، آن‌ها براثر نقض جدی تعهداتی که به‌طورکلی در برابر جامعه وجود دارند ایجاد می‌شوند .(Bonafe, 2009: 24) البته این دو مسئولیت عواقب یکسانی ندارند، به‌هرحال باید گفت که وجود مبنای مشترک به معنای آن نیست که قواعد کلی مسئولیت اشخاص حقیقی در رابطه با مسئولیت اشخاص حقوقی قابلیت کاربرد دارند، در اینجا تنها می‌توانیم به این مسئله اشاره‌کنیم که یکسان بودن این دو نوع مسئولیت در قواعد اولیه به معنای آن است که هر دو براثر نقض هنجارهای اساسی که موردحمایت جامعه است ایجاد می‌شوند، البته در قواعد ثانویه این ارتباط کمرنگ خواهد شد. درهرحال شناخت اشتراکات و ارتباط میان مسئولیت اشخاص بررسی مبانی مسئولیت در این زمینه است. (بولاغی و جمادی، ۱۳۹۳)

۸-عوامل رافع مسئولیت کیفری در محیط سایبری

مسئولیت کیفری «التزام به تقبل آثار عواقب افعال مجرمانه یا تحمل مجازاتی است که سزای افعال سرزنش‌آمیز بزهکار به‌شمار می‌آید؛ لکن به‌صرف ارتکاب جرم نمی‌توان بار مسئولیت را یک‌باره بر دوش مقصر گذاشت، بلکه پیش از آن باید بتوان او را

سزاوار تحمل این بار سنگین دانسته، تقصیری را که مرتکب شده‌است، نخست به‌حساب او گذاشت و سپس او را مؤاخذه کرد. توانایی پذیرفتن بار تقصیر را در اصطلاح حقوقدانان «قابلیت انتساب» می‌نامند و آن را به برخورداری فاعل از قدرت ادراک و اختیارتعریف کرده‌اند؛ بنابراین اگر مجرم مُدرِک یا مختار نباشد مسئول اعمال خود نیست. برای اینکه مسئولیت جزایی به معنای اخص کلمه وجود داشته باشد باید مجرم مرتکب تقصیری شده مجرمیت و این تقصیر قابل اسناد به او باشد (حبیب زاده، ۱۳۸۴: ۴۲-۴۱)، در این قبیل علل مسئولیت جزایی برای اعمال مجرم وجود ندارد، برای درک این مفهوم باید ابتدا معنای مسئولیت جزایی را درک نمود، مسئولیت جزایی را مسئولیت مرتکب جرمی از جرایم مصرح در قانون را گویند و شخص مسئول به یکی از مجازات‌های مقرر در قانون خواهد رسید، متضرر از جرم در این موارد اجتماع است (آقایی نیا، ۱۳۹۲)، به هر صورت علل رافع مسئولیت جزایی موجبات سلب مسئولیت بزهکار را فراهم می‌سازند در این موارد علیرغم آنکه جرم به وقوع پیوسته است اما به‌واسطه وجود شرایطی در خود شخص بزهکار مجرم مسئولیت نداشته و درنتیجه مجازاتی بر وی اعمال نخواهد شد، در رابطه با تفاوت ماهوی این علل با علل موجهه جرم باید گفت: عوامل رافع مسئولیت جزایی، جنبه خصوصی و شخصی و یا به عبارتی درونی دارند، دارد و ناشی از اهلیت و خصوصیات جسمی یا روانی مرتکب جرم است و دارای مظهر و منشأ درونی است. درحالی‌که علل مشروعیت ناشی از عوامل و شرایط خارجی است و قائم بر واقعه‌ای است که باعث حذف وصف مجرمانه از عمل مرتکب خواهد شد، ضمن آنکه خصوصیات جسمی و روانی مجرم در آن نقشی ندارد (شامبیاتی، ص۳۱۴)، عوامل رافع مسئولیت جزایی همچون یک امر شخصی است که قلمرو آن محدود به شخص مرتکب جرم است یعنی وجود آن تنها باعث عدم مسئولیت جزایی مجرم می‌شود و تأثیری در عدم مسئولیت جزایی شرکا و معاونین جرم ندارد درحالی‌که علل مشروعیت نسبت به کلیه شرکت‌کنندگان در جرم قابل‌اعمال است یعنی مشروعیت آن شامل شرکا و معاونین جرم نیز می‌شود. از دیگر تفاوت‌های این دو باید گفت که در علل رافع مسئولیت درواقع عنصر معنوی جرم محقق نشده و بدین ترتیب اصولاً جرمی تحقق‌نیافته است درحالی‌که در علل موجهه جرم عدم جرم شناختن عمل مجرمانه به علت رفع عنصر قانونی آن توسط متن دیگری از قانون است و درنهایت از دیدگاه هدف شناسی باید گفت علل رافع مسئولیت مدنی مرتکب را رفع نمی‌نماید زیرا هدف از وضع قواعد مربوط به عوامل رافع مسئولیت جزایی همان‌طوری که از عنوان آن برمی‌آید، برای از بین رفتن مسئولیت جزایی مرتکب جرم است. زیرا لازمه اعمال مجازات که فرع بر اثبات مسئولیت جزایی است، به‌منظور حفظ نظم و دفاع اجتماعی است و نمی‌تواند مسئولیت مدنی مرتکب جرم را از بین ببرد. درحالی‌که علل مشروطیت نه‌تنها موجب زوال مسئولیت جزایی و مسئولیت مدنی مرتکب جرم خواهد شد. یعنی عمل مجرمانه او را مشروع می‌سازد و باعث عدم مسئولیت جزایی و مدنی شرکا و معاونین جرم نیز خواهد شد (جلالی‌فراهانی، ۱۳۹۴).

قانون‌گذار ایران در قانون جرایم رایانه‌ای اشاره‌ای به عوامل رافع مسئولیت کیفری ننموده است بند ب ماده ۱۹ اشاره به دستور مدیر و نقش این دستور در ارتکاب جرم دارد که درواقع اشاره به علل موجه جرم دارد نه عوامل رافع مسئولیت کیفری، به‌هرحال باید اذعان داشت عوامل رافع مسئولیت در محیط سایبری تابع عوامل کلی رافع مسئولیت کیفری است، می‌توان این عوامل را در موضوعاتی مانند کودکی، جنون، اجبار معنوی و... دانست، بنابراین باید اذعان داشت که عوامل رافع مسئولیت در محیط سایبری همان عوامل کلی رافع مسئولیت جزایی هستند که معمولاً در متون حقوق کیفری عمومی موردبررسی قرار می‌گیرند.

اقتصاددانان بر این باورند که مجرم انسان عاقلی است و قبل از انتخاب جرم هزینه‌ها و فایده‌های ارتکاب آن را می‌سنجد. استفاده از آنالیز اقتصادی جرم با رویکردی متفاوت از سایر رویکردها نهایتا به دنبال کاهش جرم است چه از طریق دستگیری و مجازات مجرمین و چه با انتخاب راه‌های پیشگیری از جرم.

در این میان افزایش احتمال دستگیری و محکومیت می‌تواند در کاهش هزینه‌ی جرایم بسیار موثر باشد. نمونه این امر مطالعه ایست که در سال ۲۰۰۵ توسط "ملونی" تحت عنوان " عوامل موثر بر جرم در آرژانتین طی دهه۹۰" انجام شد. وی در این مطالعه به بررسی عوامل اقتصادی موثر بر نرخ جرم در آمریکا (۹۹-۱۹۹۰) می‌پردازد و اذعان می‌دارد که عوامل بازدارنده جرم اثرات معنی داری بر کاهش جرم در این کشور داشته است. او در مطالعه خود به این نتیجه می‌رسد که افزایش در احتمال دستگیری و محکومیت می‌تواند منجر به کاهش میزان جرم گردد. بدین شکل که افزایش تنها ۱۰ درصدی در احتمال دستگیری منجر به کاهش ۳/۳۸ درصدی در نرخ جرم شده و نیز افزایش ۱۰ درصدی در احتمال محکومیت نیز باعث کاهش ۲/۶۷ درصدی در نرخ جرم می‌شود. بنابراین با تغییر در وضعیت احتمال دستگیری و مجازات در جرایم سایبر نیز می توان به کاهش قابل توجه نرخ این جرایم رسید و پس از آن با تعیین مجازات های مناسب که گاه فاکتور شدت را با خود به همراه دارد و گاه فاکتور قطعیت را، از آمار این جرایم کاست. جهت گیری این بخش از کار، در راستای بررسی این احتمالات و چگونگی تاثیر گذاری آنها بر کاهش مطلوبیت جرم از طریق افزایش هزینه ها خواهد بود. بدین منظور این بخش در قالب سه فصل به عنوان هزینه های جرم ابتدائا به نقش احتمال دستگیری و پس از آن به تاثیر افزایش احتمال محکومیت و مجازات در افزایش هزینه های جرم می پردازد. (جلالی‌فراهانی، ۱۳۹۴ص ۴۶)

۸-۱-توان پلیسی و نقش آن در افزایش احتمال دستگیری

همراه با تاثیر شرایط اقتصادی بر میزان جرم، یکی از موضوعات اصلی که به خصوص"بکر" برآن تأکید کرده است، تاثیرگذاری عملکرد امنیتی و پلیسی بر سطح فعالیت بزهکارانه است. بهبود این عملکرد و افزایش توان امنیتی و پلیسی در کنار تمامی هزینه‌هایی که وجود دارد (نظیرهزینه‌های استخدام نیروی پلیس، آموزش آنها و هزینه‌های مربوط به ایجاد و بهره‌برداری از ایستگاه‌های پلیس که کاهش آمار کشف جرم می‌تواند بر ارزش‌گذاری آنها تأثیرگذار باشد)، نقش مهمی در کاهش آمار جرایم سایبر ایفا می‌کند (منبع پیشین).

به نظر می‌رسد سرمایه‌گذاری در این قسمت نسبت به مراحل دیگر دادرسی ثمربخش‌تر باشد زیرا معمولا هزینه‌های مرحله پلیسی (کشف جرم و دستگیری متهم) پایین است ولی منافع آن از حیث بازدارندگی زیاد است، در حالیکه برعکس، هزینه‌های مرحله صدور حکم و نهادهای اصلاحی و تربیتی زیاد است ولی منافع آن پایین.

حملات سایبری با سرعت فزاینده‌ای رو به رشد هستند در حالیکه سرعت کشف این جرایم متقارن با سرعت رشدشان پیشرفتی نکرده است. تحلیلی در سال ۲۰۱۲ توسط شرکت اچ پی انجام گرفته است که نشان می‌دهد حملات سایبری در سال ۲۰۱۲ به نسبت سال های پیش از آن دو برابر شده است و هزینه‌های اقتصادی ناشی از آن نیز در طول سه سال ۴۰ درصد افزایش داشته است. ۱ این در حالیست که کشف این جرایم پیشرفت قابل قبولی نداشته است. برای مثال میانگین زمان لازم برای مقابله با یک حمله سایبری در سال ۲۰۱۰، ۱۴ روز؛ در سال ۲۰۱۱، ۱۸ روز و در سال ۲۰۱۲ به ۲۴ روز افزایش پیدا کرده است. ۲ این امر نشان از ضعف توان مقابله ای در جرایم سایبر دارد. (منبع پیشین)

بدین شکل و با توجه به سرعت روز افزون این جرایم و همزمان ضعف توان مقابله با آن، مهارت و تخصص و نیز تجهیز نیروهای پلیس این حوزه به انواع آموزش ها و نیز جدیدترین برنامه‌ها و تکنیک‌های مقابله‌ای بیش از افزایش بودجه خودنمایی می‌کند. این مهم، امری است اساسی که خود از بسیاری هزینه‌های احتمالی جلوگیری می‌نماید همچنین از لحاظ ارعابی نیز بسیار حائز اهمیت است. بدین شکل اولین گام در مسیر تخصصی‌شدن واحد جرایم رایانه‌ای، تجهیز این واحدها به بخش های تخصص است. بخش هایی نظیر:

-مراقبت از کودکان؛

-آزمایشگاه قضایی جرایم رایانه‌ای؛

-آگاه سازی جامعه شامل مدارس، عموم جامعه، واحدهای حراست سازمان ها و...؛

-دریافت شکایت‌های اینترنتی، تخلفات تجاری، جاسوسی اطلاعاتی اعم از صنعتی/ تجاری (تخلفات مخابراتی، سرقت سخت افزار و نرم افزار) و...

امروزه بیشتر ادارات پلیس در سطح جهان از این بخش های تخصصی بهره می‌برند این کار بسیار می‌تواند در افزایش توان پلیسی، افزایش هزینه ارتکاب جرم و کاهش مطلوبیت جرایم سایبر موثر باشد.

اما پلیس در زمینه مقابله و پیگیری با این جرایم با چالشهای بسیاری مواجه است. چالش هایی که باعث شده فرآیند پیگیری به کندی پیش رود.

۸-۱-۱- اقدامات انجام گرفته به منظور افزایش توان پلیسی

تحلیل اقتصادی جرم با تأکید بر آنالیز عقلانی مجرم از ارتکاب یا عدم ارتکاب جرم، بر افزایش هزینه فعالیت مجرمانه تأکید دارد که این مهم نیز منوط است به افزایش کارایی نیروهای پلیسی و امنیتی. بدین منظور و با وجود همه مشکلاتی که پلیس در زمینه مقابله با جرایم سایبر با آن درگیر است، تا کنون اقدامات مفید زیادی در زمینه کنترل و مقابله با این جرایم انجام داده است. از مهمترین این اقدامات می‌توان به موارد زیر اشاره کرد:

۸-۱-۲-تشکیل مرکز بررسی جرایم سازمان یافته اینترنتی

رشد قارچ گونه جرائم سازمان یافته بین المللی و سوء استفاده از بستر اینترنت و سایر سامانه‌های ارتباطی جهت انجام اقدامات تروریستی، جاسوسی اینترنتی، پولشویی و تخریب نظام فرهنگی و اجتماعی جامعه و هتک حرمت و توهین به مقدسات دینی و ارزش‌های انقلابی از دلایل راه اندازی مرکز بررسی جرائم سازمان یافته بوده است. این سازمان در سال ۱۳۸۶ در زمینه تخصصی تر شدن پلیس و به منظور شناسایی و برخورد با جرائم مذکور با هماهنگی قوه قضائیه جمهوری اسلامی شکل گرفت. وظیفه این مرکز نظارت و بررسی جرائم سازمان یافته تروریستی، جاسوسی، اقتصادی و اجتماعی در فضای مجازی می‌باشد که با همکاری و هماهنگی سایر حوزه‌های اطلاعاتی و قضایی جهت بررسی تهدیدات و آسیب های شبکه جهانی اینترنت و سایر فناوریهای نوین از توان فنی و اطلاعاتی کارشناسان سپاه پاسداران و سایر متخصصین بهره گرفته و طبق اصل ۱۵۰ قانون اساسی در راستای نگهبانی از انقلاب و دستاوردهای آن فعالیت می نماید. شکل گیری چنین مراکزی باعث تسریع در فرآیند کشف و برخورد با جرایم سایبر خواهد شد. همچنین از مشغول شدن سایر مراکز با تنوع پرونده ها که کند شدن فرآیند رسیدگی را در پی دارد، جلوگیری می شود. با تسریع در رسیدگی هزینه انجام فعالیت مجرمانه افزایش خواهد یافت و در نتیجه از آمار این جرایم کاسته می شود. (مارک، ۱۳۷۵)

۸-۱-۳-تدوین قواعد کارآمد برای دفاتر خدمات اینترنتی

با توجه به اینکه حدود ۲۲ درصد از کاربران اینترنتی از کافی نت استفاده می کنند۱، پلیس به هدف برقراری امنیت کاربران در دفاتر خدمات اینترنتی دستورالعملی را تهیه و صاحبان این مراکز را ملزم به رعایت آنها می‌نماید. اقدامی که در جهت کشف و برخورد با این جرایم بسیار مفید و کارآمد خواهد بود که بر مبنای آن مدیران خدمات اینترنتی موظفند:

-پهنای باند مورد نیاز خود را الزاما از طریق شرکت‌های دارای پروانه‌ی ارائه کنندگان خدمات اینترنت (ISP) تأمین کنند.

- مدارک لازم در خصوص تأمین پهنای باند و رعایت شرایط عمومی را حسب مورد در اختیار بازرسان پلیس قرار دهند.

- اطلاعات هویتی کاربران (نظیر نام و نام خانوادگی، نام پدر، کد ملی، کد پستی، شماره تلفن تماس) را با دریافت مدارک شناسایی معتبر (ترجیحا" کارت ملی) ثبت و از ارائه خدمات به مراجعه کنندگانی که مدارک شناسایی ارائه نمی کنند خودداری کنند. [2]

- علاوه بر اطلاعات هویتی کاربران، سایر اطلاعات کاربری شامل روز و ساعت استفاده، IP اختصاص یافته و فایل وبلاگ سایت‌ها و صفحات رویت شده را ثبت و حداقل تا ۶ ماه نگهداری کنند.

-مانع از استفاده و در اختیار گذاشتن هر گونه ابزار دسترسی به سایت‌های فیلتر شده، مثل انواع فیلتر شکن‌های قابل نصب روی رایانه، یا معرفی سایت‌های فیلترشکن و خدمات گیرندگان و یا استفاده از هرگونهVPN۱ روی سیستم‌های رایانه‌ای دفاتر خدمات اینترنت شوند. (گرکی، مارکو، ۱۴۰۱):

-شرایطی را فراهم کنند که اطلاعات کاربر پیشین (شامل سایت‌ها، صفحات دیده شده، فعالیت ها، IDها آدرس‌های ایمیل و...) به محض قطع استفاده کاربر، از بین رفته و برای کاربران بعدی که از آن رایانه استفاده می‌کنند قابل بازیابی نباشد.

-رایانه‌های استفاده شده در مراکز خدمات اینترنت (کافی‌نت) بایستی الزاما در حالت کاربر محدود۲ در اختیار کاربران قرار گرفته و درگاه‌های ورودی سیستم رایانه‌ای شامل درگاه‌هایUSB ، کارت خوان‌ها و سایر درگاه‌هایی که امکان اتصال حافظه‌های جانبی به آن ها وجود دارد، به صورت نرم افزاری مسدود شود.

- هر روز در پایان ساعت کاری کافی‌نت، نسبت به وارسی سیستم‌های رایانه‌ها از نظر نصب نشدن نرم افزارهای مخرب، آلودگی به ویروس ها و بدافزارها و امحاء اطلاعات باقی مانده کاربران اقدام کنند.

-دوربین مدار بسته داخلی با قابلیت ضبط تمام وقت، نگهداری تصاویر و امکان بازبینی تا ۶ ماه نصب نمایند. و.... رعایت سلسله اقدامات مذکور توسط مدیران خدمات اینترنتی باعث خواهد شد تا با حذف یکی از پرطرفدارترین مراکز انجام فعالیت های خرابکارانه سایبری، به دلیل از دست رفتن محیطی امن برای ارتکاب جرم تمایل به ارتکاب جرم کاهش یافته و هزینه و ریسک انجام جرم افزون گردد و این همان چیزی است که تحلیل اقتصادی به دنبال آن است.

۸-۱-۴- راه اندازی آزمایشگاه بررسی ادله دیجیتال

با وجود همه مشکلات، در فضای مجازی هم ارتکاب جرم قابل ردیابی است و ادله کافی از ارتکاب جرم باقی می ماند. ادله‌ای که پلیس بر اساس آن، با بررسی سیستم‌های رایانه‌ای و مخابراتی مجرمان، توانایی کشف علمی جرایم در فضای مجازی را داشته باشد. بر همین اساس با استفاده از تجهیزات آزمایشگاهی، امکان بررسی ادله دیجیتال و بررسی فنی تجهیزات مجرمانه در ارتکاب جرم محقق شده است. پلیس این آزمایشگاه را به منظور بازیابی اطلاعات، سخت افزار، نرم افزار، رمز شکنی، مخابرات، تلفن همراه و مولتی مدیا راه اندازی کرده است که جزو موارد نادر فعال در حوزه سایبر است تا به راحتی بتواند ادله ای را که در فرایند رسیدگی و برای اثبات مجرمیت لازم است، بدست آورده و در شرایطی ایده آل نگهداری نماید. [3]

---

[2] - پایگاه اطلاع رسانی شرکت مهندسی شبکه گستر، گشت زنی شبانه روزی پلیس فتا در اینترنت، تاریخ انتشارخبر۱۲ بهمن ۱۳۹۲، برگرفته از http://blog.shabakeh.net/5413

[3] - پلیس فتا، مدیران کافی نت ها برای ساماندهی وضعیت مراکز خود تنها ۱۵ روز مهلت دارند، تاریخ انتشارخبر ۱۳ دی ۱۳۹۰، برگرفته از http://www.cyberpolice.ir/news/3001

۸-۱-۵-محدود کردن دامنه فعالیت مجرمان در فضای سایبر

هم‌اکنون امکانی فراهم شده که آدرس‌های اینترنتی که از طریق آنها به فعالیت‌های خرابکارانه مثل ارسال ویروس، نفوذ غیرمجاز و ارسال پیغام‌های مزاحم می پردازند، شناسایی و هرگونه فعالیت از طریق این آدرس‌ها به شدت محدود شود. برای مثال، امروزه سرورهای پست‌الکترونیک به صورت خودکار با پلیس سایبر برای دریافت یا حذف پیغام‌های ورودی مشورت می‌کنند. این امر باعث شده تا با حذف عوامل زمینه ساز وقوع جرم و محدود کردن فعالیت مجرمان سایبری از بسیاری از جرایم احتمالی جلوگیری گردد و در نتیجه مجرمان به راحتی نتوانند به اقدامات خرابکارانه شان دست بزنند. (گیدنز، ۱۳۹۷)

۸-۱-۶-گشت زنی شبانه روزی در اینترنت

این اقدام به منظور دشوار کردن ارتکاب جرائم و همچنین برای شناسایی حفره های امنیتی، عملکرد ارائه دهندگان اطلاعات بی نام در کافی نت ها، فروشندگان باگ های امنیتی و اطلاع رسانی را دنبال می‌کند. رصد مداوم فضای مجازی احساس امنیت کاذبی که در مجرمان به هنگام ارتکاب جرم وجود دارد را از بین برده و بدین شکل ریسک و هزینه انجام فعالیت مجرمانه را افزایش می دهد. (فرجی‌ها و دیگران، ۱۴۰۰)

۸-۱-۷-اتخاذ برخی تدابیر پیشگیرانه در زمینه آگاه سازی عمومی جامعه

بسیاری از جرایم سایبر به دلیل عدم آموزش و آگاهی کافی و لازم بزه دیدگان به وقوع می پیوندد. به منظور آگاه سازی افراد در این زمینه، ادارات پلیس حداقل به اقدامات زیر می‌پردازند:

برگزاری سخنرانی برای دانش آموزان، مربیان و اولیا؛ ارسال تذکرات ویژه برای مشترکین با پهنای باند وسیع تر؛ چاپ و نشر مواد فرهنگی در مدارس از طریق بروشور، برچسب و پوستر؛ همکاری با ISPs در ارسال تذکر به خاطیان شبکه اینترنت؛ همکاری با آموزش و پرورش در طراحی مباحث امنیتی؛ خلاقی در تهیه درس فناوری اطلاعات؛ سخنرانی برای کارکنان و مدیران صنایع و بنگاه های تجاری؛ گنجاندن متن قانون در کتب درسی؛ حضور در همایش های عمومی مرتبط با امنیت اطلاعات؛ حضور در نمایشگاه های رایانه ای با هدف آموزش و آگاه سازی؛ ایجاد رشته های تخصصی جهت تحصیل در دوره تحصیلات تکمیلی و آموزش عالی و... با توسل به اقدامات. [۴]

پیشگیرانه، نیل به مقصود نهایی تحلیل اقتصادی که همان افزایش هزینه جرم و کاهش سودمندی جرایم است بسیار راحت تر خواهد بود. به همین دلیل است که پیشگیری مورد توجه متصدیان امر و از اهم فعالیت هایشان قرار گرفته است. اگرچه که این مقدار کار کفایت نکرده و اقدامات جدی تری نیاز است اما همین مقدار کار نشان دهنده تمایل پلیس این حوزه به پیشرفت و افزایش توانایی و تخصص در برخورد با جرایم سایبر است. افزایش توان پلیسی و امنیتی از مباحث مهم در آنالیز اقتصادی و اولین چیزی است که مجرم سایبری در احتمالات اولیه خود در نظر می گیرد. تقویت توان این حوزه، در کاهش آمار این جرایم و نیز کاهش تمایل افراد به ارتکاب جرم در فضای مجازی بسیار موثر بوده و از بسیاری از جرایم جلوگیری خواهد کرد. (عاملی، ۱۳۹۶)

[۴] - پایگاه اطلاع رسانی شرکت مهندسی شبکه گستر، گشت زنی شبانه روزی پلیس فتا در اینترنت، تاریخ انتشارخبر۱۲ بهمن ۱۳۹۲، برگرفته از http://blog.shabakeh.net/5413

۹-نتیجه‌گیری

جرم‌انگاری جرایم سایبری باید بر مبنای اصول حقوقی و فلسفی دقیق صورت گیرد تا از تورم کیفری جلوگیری شده و حقوق شهروندان در فضای مجازی حفظ شود. قانون‌گذاری در این حوزه باید متناسب با ویژگی‌های خاص فضای سایبر باشد و ضمن رعایت حقوق فردی، به مقابله مؤثر با جرایم سایبری کمک کند در مجموع، جرم‌انگاری جرایم سایبری در ایران بر اساس قانون جرایم رایانه‌ای است که رفتارهای مجرمانه در فضای مجازی را تعریف و مجازات می‌کند و مبانی آن بر اصول حقوقی مانند ضرورت، مشروعیت و تناسب جرم و مجازات استوار است. سیاست جنایی ایران در زمینه جرایم سایبری ترکیبی از اقدامات قانونی، قضایی و مشارکتی است که با هدف پیشگیری، مقابله و تضمین امنیت فضای سایبری طراحی شده است. این سیاست‌ها با بهره‌گیری از قوانین مدون، نهادهای تخصصی قضایی و همکاری گسترده با جامعه مدنی، تلاش می‌کنند تا پاسخگویی مناسبی به تهدیدات نوظهور در فضای مجازی داشته باشند و از حقوق شهروندان در این فضا حفاظت کنند.

استفاده از ابزارها و وسایل نوین ارتباطی خصوصاً محیط سایبر و اینترنت، فرصت‌های جدید برای ارتکاب جرم مجرمین به وجود آورده است، در همین راستا چنانچه حقوق کیفری در درون هر جامعه‌ای نتواند متناسب با این پیشرفت‌ها تغییر پیدا کند، تبعاً جرایم و بزهکاری‌های زیادی به وجود می‌آید که بدون مجازات باقی خواهند ماند، شاید بتوان گفت که مهم‌ترین ابزارهایی که برای مبارزه با جرایم نوین در برابر حقوق جزا وجود دارد. راهکارهایی مانند جرم‌انگاری، ایجاد و توسعه مسئولیت کیفری، استفاده از راهکارهای نوین حل اختلاف و مجازات‌های نوین و... است، در رابطه با مسئولیت کیفری در جرایم سایبری قانون‌گذار ایران اقدام به توسیع و گسترش مسئولیت کیفری در برابر اشخاص حقوقی نموده است. تا قبل از تصویب قانون فوق‌الذکر بحث مسئولیت کیفری اشخاص حقوقی در قوانین کیفری ایران چندان مطرح نشده بود و قانون جرایم رایانه‌ای نخستین بار این موضوع یعنی مسئولیت کیفری اشخاص حقوقی را موردپذیرش قرارداده است، می‌دانیم بسیاری از جرایم رایانه‌ای معمولاً توسط اشخاص حقوقی واقع می‌شوند و این اقدام قانون‌گذار ایران در رابطه با ایجاد مسئولیت کیفری برای این اشخاص امری کاملاً طبیعی بوده و درواقع استفاده از ابزار گسترش مسئولیت کیفری برای مبارزه با جرایم جدید است، البته باید اذعان داشت که:

الف: مسئولیت کیفری اشخاص حقوقی به معنای نفی مسئولیت‌اشخاص حقیقی نیست.

ب: مسئولیت کیفری شخص حقوقی مانعی بر سر راه اعمال مجازات بر اشخاص حقیقی ایجاد نمی‌کند.

و درنهایت باید گفت در باب عوامل رافع مسئولیت کیفری در محیط سایبر این علل تابع عوامل کلی رافع مسئولیت می‌باشند، عواملی مانند کودکی و جنون از این موارد محسوب می‌شوند. جرایم سایبر به دلیل ویژگی‌هایی نظیر جهانی بودن، فقدان اهمیت زمان و مکان در ارتکاب آن، ناشناختگی، مجازی بودن، سود سرشار و بسیاری ویژگی‌های دیگر مورد تمایل بسیاری قرار می‌گیرد. به همین دلیل توسل به راهکارهایی که از میزان این جرایم بکاهد و مطلوبیت این جرایم را تقلیل دهد بسیار حائز اهمیت است. در این میان تحلیل اقتصادی جرایم سایبر با تأکید بر این که دلیل انجام یک جرم توسط مرتکب، کسب سود و منفعتی است که باید در ارتکاب آن باشد و در صورت حذف این سود و منفعت، از تمایل به ارتکاب جرم کاسته خواهد شد، به دنبال کاهش سودمندی و مطلوبیت در این جرایم است. اما وجود مشکلاتی نظیر کمبود تخصص ماموران کشف و تعقیب، عدم گزارش و همکاری بزه دیدگان، عدم کفایت قانون، فقدان توافقنامه‌ای بین‌المللی و بسیاری دلایل دیگر باعث شده است تا دستیابی به این هدف با چالش‌های بسیاری همراه گردد.

بدین شکل در راستای کاهش مطلوبیت و سودمندی جرایم سایبر و از سوی دیگر افزایش هزینه‌های شخصی این جرم برای مجرم، ابتدائا به دلیل وجود خلأهای بسیار در قوانین فعلی و عدم کفایت این قوانین، بایستی قبل از هر چیز قانون و مقررات

سختگیرانه‌ای را در این خصوص تصویب و اجرا کرد.

در گام بعد، از آنجاییکه طبق نظریه بازدارندگی مردم به طور قابل توجهی به انگیزه‌های اجتماعی ایجاد شده توسط سیستم دادگستری جنایی پاسخ می دهند، منابعی که جامعه صرف دستگیری، محکومیت و جریمه مجرمین می‌کند، را افزایش داد تا بتوان از مقدار و هزینه اجتماعی جرم کاست. به منظور دستیابی به این هدف، بایستی هزینه‌های جرم (احتمال دستگیری و مجازات) را تقویت کرد که این امر خود نیازمند افزایش توان پلیسی و قضایی در جهت افزایش کشف و برخورد قاطع و کارشناسانه با این جرایم است. در مرحله بعد از آنجاییکه روش های داخلی و صرفا ملی نمی‌تواند در برابر جرایم این چنینی کارایی لازم را داشته باشد نیاز است تا سطح همکاریها و هماهنگی های بین المللی افزایش یابد و برخوردی جهانی و همه جانبه شکل گیرد.

اما مهمترین مسأله در مقابله با افزایش هزینه‌های جرایم سایبر، مسئولیت‌پذیری دولت در سیاست گذاری کارشناسانه و همه‌سونگر برای تدوین سیاستها، قوانین و مقررات مناسب حمایتی، هدایتی، نظارتی است. در این مسیر بهره‌گیری از تمام توان علمی و اجرایی کشور، رویکرد میان رشته‌ای و میان بخشی ضروری است. به نظر می‌رسد که دولت باید با شناسایی کمبودها و فقدان قوانین، بسته به ارگان یا ارگان های درگیر، زمینه‌ساز تدوین قوانین شود.

منابع و مآخذ

۱. آخوندی، محمود، (۱۳۹۹)، آیین دادرسی کیفری جدید، انتشارات، دانشگاه تهران.

۲. آقایی نیا، حسین، (۱۳۹۲)، جرایم علیه اشخاص (جنایات) تهران، انتشارات بنیادحقوقی میزان، چاپ۱۱.

۳. باستانی، برومند، (۱۳۹۳) جرایم کامپیوتری و اینترنتی جلوه‌ای نوین از بزهکاری، تهران، نشر بهنامی، چاپ اول.

۴. بولاغی، رضا و جمادی، حبیب الله، (۱۳۹۳)، قانون آیین دادرسی کیفری نموداری مصوبات ۱۳۹۲ تهران، انتشارات نشر دانش چاپ ششم.

۵. بولک برنار، (۱۳۹۵) کیفرشناسی، علی حسین نجفی ابرندآبادی، تهران، انتشارات مجد، چاپ ششم.

۶. جلالی‌فراهانی، امیرحسین (۱۳۹۴)، پیشگیری وضعی از جرائم سایبری در پرتو موازین حقوق بشر، نشریه حقوق، شماره ۶، پاییز.

۷. جلالی‌فراهانی، امیرحسین و باقریاصل، رضا، (۱۳۹۵) پیشگیری اجتماعی از جرایم سایبر (راهکارهای اصولی برای نهادینه کردن اخلاق سایبری)، دومین همایش منطقه‌ای اخلاق و فناوری اطلاعات، مرکز تحقیقات مخابرات ایران.

۸. جلالی‌فراهانی، امیرحسین (۱۳۹۸) (مترجم) کنوانسیون جرایم سایبر و پروتکل الحاقی آن (به همراه گزارش‌های توجیهی)، معاونت حقوقی و توسعه قضایی قوه قضائیه

۹. جلالی‌فراهانی، امیرحسین، (۱۳۹۳) پیشگیری از جرائم رایانه ای، مجله حقوقی دادگستری، شمارهٔ ۴۷.

۱۰. جوان‌جعفری، عبدالرضا، (۱۳۹۹) جرایم سایبر و رویکرد افتراقی حقوق کیفری، مجله دانش و توسعه، سال هفدهم، شماره۳۴، اسفند.

۱۱. جوانشیر، سحر؛ پورقهرمانی، بابک (۱۳۹۸)، بررسی راه های پیشگیری و مقابله با جرائم سایبری، دومین کنفرانس ملی پدافند سایبری.

۱۲. حسینی، منیره (۱۳۹۵). نقش پلیس فتا در پیشگیری از جرایم رایانه ای، پایان نامه کارشناسی ارشد، دانشگاه آزاد اسلامی، واحد تهران مرکزی.

۱۳. حیدری، مسعود؛ شهبازی، امید؛ شیرانی، پویا (۱۳۹۷). چالش ها و فرصت های پیش روی پلیس در برخورد با جرایم سایبری، سال دوازدهم، شماره ۴۵.

۱۴. ریک، کاسپرسن، (۱۳۹۶) تعقیب بین‌المللی جرایم رایانه‌ای، ترجمه محمد حسن دزیانی، دبیرخانه شورای عالی انفورماتیک، سازمان برنامه و بودجه کشور.

۱۵. شیرزاد، کامران، (۱۳۹۹) جرایم رایانه‌ای از منظر حقوق جزای ایران و حقوق بین‌الملل، شرکت نشر بهینه فراگیر، چاپ اول.

۱۶. عاملی، سیدرضا (۱۳۹۶)، جزوه درسی مطالعات فضای مجازی، دوره کارشناسی، ترم اول سال تحصیلی ۹۶-۹۵.

۱۷. عبقری، آدینه (۱۳۹۷)، جرایم کامپیوتری جلوه نوینی از بزهکاری، پایان‌نامه کارشناسی‌ارشد، دانشکده حقوق دانشگاه تهران.

۱۸. فرجی‌ها، محمد و دیگران (۱۴۰۰) رویکرد چندنهادی به پیشگیری از جرم، تهران، نشر نیروی انتظامی جمهوری اسلامی ایران، معاونت آموزش، چاپ اول.

۱۹. گرکی، مارکو، جرایم سایبری (۱۴۰۱): راهنمایی برای کشورهای در حال توسعه، ترجمه مرتضی اکبری، نشر پلیس امنیت فضای تولید و تبادل اطلاعات ناجا، چاپ اول.

۲۰. گیدنز، آنتونی، (۱۳۹۷)، پیامد مدرنیت. ترجمه محسن ثلاثی. چاپ اول.

۲۱. مارک آنسل، (۱۳۷۵)، دفاع اجتماعی، ترجمه محمد آشوری و علی حسین نجفی ابرندآبادی (چاپ سوم: تهران، انتشارات دانشگاه تهران).

مطالعات علوم سیاسی، حقوق و فقه

دوره ۱۱، شماره ۱، بهار ۱۴۰۴، صفحات ۹۳۶-۹۱۸

Explanation of Cybercrimes and Cybercrimes and the Criminal Liability of Individuals in this Field

Mohsen Rostami

Master's degree in Criminal Law and Criminology, Islamic Azad University, Noorabad Mamasani Branch. Iran.

Abstract

Cybercrimes are illegal activities that are carried out through computers, the Internet, and cyberspace, and include information theft, hacking, cyber espionage, phishing, publishing illegal content, and sabotage in computer systems. With the spread of new technologies and the increased use of cyberspace, these crimes have become a serious threat to the security and rights of individuals. By approving the Computer Crimes Law, the Iranian legislator has criminalized these behaviors and determined the criminal liability of natural and legal persons in this field. The purpose of explaining cybercrimes and cybercrimes is to accurately recognize these crimes, determine the limits and criminal liability of perpetrators, and create an appropriate legal framework to combat them. Also, the aim is to identify the scope of criminal liability of individuals and legal entities in cyberspace and to ensure legal and social security in this area. Method: Study and analyze the existing laws and regulations in Iran, especially the computer crime law, examine the types of cybercrimes and the criminal liability related to them, and review the legal and criminological literature on cyberspace crimes and the criminal liability of individuals in this space. Findings: Cybercrimes include various types such as theft of personal and financial information, hacking systems, cyber espionage, phishing, publishing illegal content, and sabotage in computer systems. The punishment for these crimes varies depending on the type and severity of the crime, from imprisonment (from 91 days to several years) to fines and even execution in special cases. The Iranian computer crime law also recognizes the criminal liability of legal entities in cyberspace for the first time, and the sixth chapter of this law is dedicated to the issue of criminal liability. Criminal liability in cyberspace includes natural and legal persons, and the legislator emphasizes the creation of legal frameworks to combat these crimes. Results: Due to their specific complexities, cybercrimes and crimes related to cyberspace require precise criminalization and determination of specific criminal liability for natural and legal persons. Iran's computer crime law has taken an important step in this regard and, by determining penalties and responsibilities, has provided the basis for effective confrontation with these crimes. Recognizing and explaining criminal liability in cyberspace is essential for maintaining legal and social security .

Keywords: Cybercrimes, Cyberspace, Criminal Liability, Computer Crime Law, Cyber Espionage, Phishing