فصلنامهٔ پژوهش‌های اطلاعاتی و جنایی، سال چهاردهم
شمارهٔ سوم، پاییز ۱۳۹۸

سیاست جنایی ایران و آمریکا در قبال جرائم کلاهبرداری و سرقت سایبری

نوع مقاله: مروری

تاریخ دریافت: ۹۸/۰۲/۱۰ تاریخ پذیرش: ۹۸/۰۵/۲۵

از صفحهٔ ۱۳۱ تا ۱۵۴

جلال انصاری[۱]، سعید عطازاده[۲]، محمود قیوم زاده[۳]

چکیده

زمینه و هدف: قانون‌گذار ایران در راستای مقابله با سرقت و کلاهبرداری سایبری، اقدام به جرم‌انگاری آن بدون توجه به لزوم تعیین مجازات متناسب کرده که این موضوع نشان‌دهندهٔ دیدگاه تک‌بعدی سیاست جنایی ایران است. در همین راستا، پژوهش حاضر در نظر دارد با تطبیق سیاست جنایی ایران و آمریکا نحوهٔ جرم‌انگاری جرائم مذکور را مورد تحلیل و بررسی قرار دهد.

روش: تحقیق حاضر با توجه به نحوهٔ گردآوری داده‌ها به روش اسنادی بوده که در این راستا ضمن مطالعهٔ منابع کتابخانه‌ای و اینترنتی داخلی و خارجی مرتبط با موضوع از جمله کتب، پایان‌نامه‌ها و مقالات معتبر علمی، قوانین حوزهٔ جرائم کلاهبرداری و سرقت سایبری ایران و آمریکا به صورت تطبیقی مطالعه و مورد تجزیه و تحلیل قرار گرفته است.

یافته‌ها: یافته‌ها نشان داد قانون‌گذار آمریکا، در رابطه با جرائم کلاهبرداری و سرقت سایبری، اقدام به جرم‌انگاری مصداقی کرده و برای هرکدام مجازات خاص در نظر گرفته است، در صورتی که در سیستم حقوقی ایران، قانون‌گذار عنوان کرده اگر اعمال مندرج در مواد ۱۲ و ۱۳ قانون جرائم رایانه‌ای همراه با بردن یا ربودن مال دیگری شود، عنوان مجرمانه دارد و توجهی به انواع مصادیق این جرائم و تمایز آن‌ها نکرده است.

نتیجه‌گیری: برای داشتن قانونی کارآمد و پیشگیرانه در ایران در رابطه با جرائم کلاهبرداری و سرقت سایبری، توجه به بخشی از سیاست جنایی آمریکا شامل جرم‌انگاری مصادیق مختلف و ذکر تعاریف هر یک از این جرائم مثل فیشینگ، می‌تواند در صورت بومی‌سازی، مؤثر و کارآمد باشد، لذا پیشنهاد می‌شود اقدامات لازم در جهت اصلاح قانون جرائم کلاهبرداری و سرقت سایبری به‌منظور برطرف ساختن نقاط ضعف قانون در دستور کار مراجع ذی‌صلاح قرار گیرد.

کلید واژه‌ها: سیاست جنایی، کلاهبرداری سایبری، سرقت سایبری، قانون جرائم رایانه‌ای، ایران، آمریکا.

استناد: انصاری، جلال؛ عطازاده، سعید و قیوم‌زاده، محمود (پاییز ۱۳۹۸). سیاست جنایی ایران و آمریکا در قبال جرائم کلاهبرداری و سرقت سایبری. *فصلنامهٔ پژوهش‌های اطلاعاتی و جنایی*. ۱۴(۵۵)، صص ۱۵۴-۱۳۱.

۱. دانش‌آموختهٔ دکتری حقوق کیفری و جرم‌شناسی دانشگاه آزاد اسلامی واحد ساوه، Jalalansari@yahoo.com

۲. استادیار حقوق جزا و جرم‌شناسی پژوهشگاه علوم انتظامی و مطالعات اجتماعی ناجا، نویسندهٔ مسئول: saeidbahjat@yahoo.com

۳. استاد گروه فقه و مبانی حقوق دانشگاه آزاد اسلامی واحد ساوه، maarefteacher@yahoo.com

مقدمه

در عصر حاضر و با ظهور اینترنت و فراگیر شدن آن مشکلات جدیدی در رابطه با امنیت سایبری، جرم‌انگاری، مقابله و پیشگیری از جرائم سایبری به وجود آمده است. در بحث جرم‌انگاری و مقابله با این جرائم و مسائل مرتبط با آن‌ها باید عنوان کرد که به دلیل پیچیدگی و مصادیق گوناگون، همچنین تغییرات مداومی که در روش ارتکاب این جرائم اتفاق می‌افتد، کار را بیش از پیش برای قانون‌گذار و مجریان قانون سخت کرده است که تشریح این موضوع در ادامه خواهد آمد. مشکل دیگر نیز بحث پیشگیری از این جرائم و سازوکارهای مربوط به آن است؛ زیرا بحث در رابطه با انواع پیشگیری و تأثیر هر یک از آن‌ها بر سرقت و کلاهبرداری سایبری و همچنین ارائه راهکارهای متناسب با اوضاع اجتماعی و اقتصادی و غیره و مبتنی بر برنامه‌های پیشگیرانه امری خطیر است که نیازمند کارهای علمی و عملی است. از همین رو، در این مقاله فقط سیاست جنایی تقنینی و مشارکتی دو کشور ایران و آمریکا مورد بررسی قرار خواهد گرفت و دیگر مدل‌های سیاست جنایی همچون سیاست جنایی قضایی و اجرایی مدنظر نگارندگان نمی‌باشند.

در رابطه با موضوع جرم‌انگاری و مقابله کیفری با این جرائم باید عنوان کرد، قانون جرائم رایانه‌ای ایران در مواد ۱۲ و ۱۳ به جرم‌انگاری سرقت و کلاهبرداری سایبری پرداخته است. با نگاه به این دو ماده، مشخص می‌شود که قانون‌گذار ایران با استفاده از تعریف سنتی این جرائم، اقدام به جرم‌انگاری شکل سایبری آن‌ها کرده است. این امر فی‌النفسه مشکل اساسی در این زمینه نیست، بلکه عدم توجه قانون‌گذار به مصادیق گوناگون این جرائم و چگونگی به وقوع پیوستن این جرائم و حتی در نظر نگرفتن نتیجهٔ حاصل شده از کلاهبرداری و سرقت سایبری مشکل اساسی در جرم‌انگاری آن‌هاست؛ زیرا در عمل، علیرغم تصویب قانون موردنظر و جرم‌انگاری و تعیین کردن مجازات برای جرم کلاهبرداری اینترنتی، میزان این نوع جرم کماکان رو به افزایش باورنکردنی است. البته لازم به ذکر است که بحث ایراد در جرم‌انگاری، تنها دلیل افزایش این آمار نیست، بلکه مسائلی همچون ضعف در زیرساخت‌ها، عدم یا کمبود آموزش مناسب، آگاهی و اطلاع ناکافی مردم در رابطه با محیط سایبر و خطرات آن و مسائلی از این دست، می‌توانند بسیار مؤثر باشند.

با توجه به مسائل و مشکلات پیش‌گفته، سعی بر آن است تا در این مقاله با بررسی سیاست جنایی کشور آمریکا، به عنوان کشور پیشرو در امر قانون‌گذاری جرائم سایبری، مدل سیاست جنایی مناسبی را که برگرفته از سیاست جنایی این کشور در رابطه با سرقت و کلاهبرداری سایبری است ارائه شود تا شاید با الگو گرفتن از دیگر کشورها، سیاست جنایی مؤثر و کارآمدی در رابطه با این دو جرم در ایران تعریف و تبیین شود. از همین رو، برای رسیدن به قانونی کامل و ارائه راهکارهای عملی و به‌روز کردن قوانین موردنظر، علاوه بر اینکه باید شرایط اجتماعی و قانونی ایران مدنظر قرار گیرد، لازم است از دیدگاه‌های مختلف قانونی و قانون‌گذاری دیگر کشورها در پروسهٔ جرم انگاری و تعیین مجازات جرم کلاهبرداری اینترنتی کمک گرفت. همچنین، برای رسیدن به کمال مطلوب طبیعتاً باید قانون کشورمان را با کامل‌ترین و به‌روزترین قانون دنیا در زمینهٔ کلاهبرداری اینترنتی مقایسه کرد. به همین دلیل نیز قانون فدرال جرائم رایانه‌ای آمریکا برای مقایسه با قانون جرائم رایانه‌ای ایران انتخاب شده است و علت انتخاب هم این است که طبق آمارهای جهانی و توضیحاتی که داده خواهد شد، قانون جرائم رایانه‌ای آمریکا به‌روزترین و کامل‌ترین قانون در دنیا در این زمینه است.

قانون جرائم سایبری فدرال آمریکا انواع مختلفی از کلاهبرداری و سرقت سایبری را به‌طور جداگانه جرم‌انگاری کرده است. به‌طور مثال، عناوینی مانند کلاهبرداری سیم، تعدی به رایانه‌های دولتی، سرقت هویت و غیره که برای هر کدام تعریف و مصادیق جداگانه و همچنین مجازات جداگانه در نظر گرفته است. در قانون کشور آمریکا صور بیشتری به‌طور جداگانه از این دو جرم، در قانون ذکر شده و برای هر کدام با توجه به شرایط و نتیجهٔ به دست آمده، مجازات متناسب در نظر گرفته شده است که همین مطلب روند کشف جرم و تطابق عمل با مادهٔ قانونی مناسب، دادرسی، مجازات و پیشگیری را بسیار آسان می‌کند.

پرسش‌هایی که نگارندگان در این پژوهش به دنبال پاسخگویی به آن‌ها هستند، این است که سیاست جنایی تقنینی ایران و آمریکا چگونه جرائم سرقت و کلاهبرداری سایبری را جرم‌انگاری کرده‌اند؟ و راهکارهای پیشگیری اجتماعی و وضعی از کلاهبرداری و سرقت سایبری چیست؟

با نگاهی به تحقیقات انجام شده در این زمینه مشخص می‌شود که عموم تحقیقات فقط بحث تعریف جرم و پیشگیری از کلاهبرداری در ایران را مورد بررسی قرار داده‌اند و

مطالعهٔ تطبیقی و راهکارهای عملی و علمی در جهت پیشگیری از این دو جرم ارائه نشده است. در ادامه، به اختصار به تحقیقات و نتایج برخی از آن‌ها اشاره می‌شود. ایـزدی فـر و پیردهی (۱۳۸۹) در تحقیقی با هدف بررسی اینکه آیا سرقت اینترنتی در زمـرهٔ سـرقت حدی محسوب می‌شود یا در زمرهٔ سرقت تعزیری، به این نتیجه رسیده‌اند کـه چـون در سرقت اینترنتی، بردن مال به صورت فیزیکی و با دستان در عالم واقع انجـام نمـی‌شـود، پس در ردهٔ تعزیرات قرار می‌گیرد. میرمحمد صادقی و شایگان (۱۳۸۹) نیز در تحقیقی با عنوان «بررسی تطبیقی کلاهبرداری سنتی و رایانه‌ای و مجازات آن در حقوق کیفـری ایران»، به این نتیجه رسیده‌اند که کلاهبرداری سنتی و اینترنتی شباهت زیـادی دارن،د اما موضوع جرم این دو، وجه تمایزشان است که در یکی مال آن‌ها و در دیگـری داده‌هـا هستند. همچنین، میرمحمد صادقی و شایگان (۱۳۸۶) در تحقیقی با عنوان «راهکارهای مقابله با جرم کلاهبرداری رایانه‌ای در حقوق کیفری ایران»، به این نتیجه رسیده‌انـد کـه آنچه در مقابلهٔ غیرکیفری از کلاهبرداری اینترنتـی مهـم و کـاربردی اسـت، پیشـگیری اجتماعی و وضعی است. خرم‌آبـادی (۱۳۸۶) نیـز در تحقیقـی بـا عنـوان «کلاهبـرداری رایانه‌ای از دیدگاه بین‌المللی و وضعیت ایران»، به این نتیجه رسیده است که مهـم‌تـرین تفاوت کلاهبرداری سنتی و اینترنتی در این است که در اولی وجود عنصر اغفال ضروری است، اما کلاهبرداری اینترنتی بدون اغفال هم به وقوع می‌پیوندد.

سیاست جنایی: سیاست جنایی همان تدبیر و چاره‌اندیشی در رابطه با جرم است که بـه دو صورت کیفر و پیشگیری است. (مارتی، ۱۳۹۳، صص۹-۷) یا *تعریف لازرژ که سیاست جنایی را دربردارندهٔ مطالعهٔ اقدام‌ها و تدابیری می‌داند که دولت و جامعهٔ مـدنی بـه‌طـور مستقل یا با مشارکت هم بـرای سـرکوب پدیـدهٔ مجرمانـه، پیشـگیری از آن و حمایـت بزه‌دیدگان مستقیم و غیرمسـتقیم پـیش‌بینـی مـی‌کننـد* (رمضـانی و علیـزاده، ۱۳۹۲، ص۱۲۶). در این مقاله به جهـت اهمیـت بیشـتر، فقـط بـه سیاسـت جنـایی تقنینـی و مشارکتی پرداخته خواهد شد. سیاست جنایی تقنینی به عنوان یکی از مصادیق سیاست جنایی، به معنای مجموع متون حقوقی اعم از کیفری و غیر کیفری در زمینهٔ یک پدیدهٔ مجرمانه است که توسط قانون‌گذار تدوین می‌شود و بیانگر سیاسـت جنـایی تقنینـی آن کشور در رابطه با همان پدیدهٔ مجرمانه است (لعلی و معظمی، ۱۳۹۶، ص۱۸۷). سیاست جنایی مشارکتی نیز بیانگر نقش و جایگاه مردم و نهادهای اجتماعی و غیردولتی در فرآیند کیفری است. هدف اصلی سیاست جنایی مشارکتی، پیشگیری از ارتکاب جرم یا کـاهش

آن از طریق فرهنگ‌سازی در رفتارهای اجتماعی و دخالت دادن مردم و نهادهای غیردولتی در فرآیند کیفری، پس از وقوع جرم است (شیعه علی، زارع و زارع، ۱۳۹۴، ص۲۸۷).

روش‌شناسی تحقیق

تحقیق حاضر با توجه به نحوهٔ گردآوری داده‌ها به روش اسنادی بوده و اطلاعات به دست آمده به صورت کیفی و مبتنی بر استنتاج محقق از منابع و متون بوده است. ماهیت موضوع ایجاب کرد تا با مطالعه و ترجمه متون لاتین و کنار هم قرار دادن آن‌ها با مطالب منابع فارسی، مقاله‌ای تطبیقی گردآوری شود. در این تحقیق، قانون مجازات فدرال و متن برنامهٔ ملی پیشگیری آمریکا توسط نگارندگان ترجمه شده و با قانون جرائم رایانه‌ای و قانون تشدید مجازات مرتکبان اختلاس، ارتشا و کلاهبرداری ایران تطبیق داده شده است. گردآوری و تجزیه تحلیل مطالب به این قوانین متکی بوده و برای به دست آوردن و طبقه‌بندی اطلاعات، از ابزارهای سنجش کتابخانه‌ای و اسنادی استفاده شده است.

یافته‌های تحقیق

پژوهش حاضر به دنبال یافتن مبانی حاکم بر سیاست جنایی تقنینی و مشارکتی ایران و آمریکا نسبت به کلاهبرداری و سرقت سایبری است. از همین رو، نتایج به دست آمده در این رابطه، در سه بخش تحلیل مواد قانونی مرتبط، تبیین و ارائه راهکارها و مصادیق عملی پیشگیری اجتماعی و وضعی و مرحله‌ای در تکمیل پیشگیری اجتماعی و همچنین تشریح انواع مصادیق این دو جرم، ارائه خواهد شد.

در رابطه با تحلیل سیاست جنایی تقنینی، با بررسی قوانین موجود در دو کشور مشخص شد که قانون جرائم رایانه‌ای ایران اقدامی در جهت مصداق شناسی و تفکیک آن‌ها از هم نسبت به این جرائم انجام نداده و فقط یک سری اعمال را ذکر کرده و عنوان کرده است که چنانچه شخصی از طریق آن اعمال، مال دیگری را برباید یا ببرد، سارق یا کلاهبردار است. در طرف مقابل، در قانون جزای فدرال آمریکا، قانون‌گذار آن کشور در مواد مختلف و متعدد، اقدام به جرم‌نگاری جداگانه هر یک از مصادیق این جرائم کرده و مجازات آن‌ها را نیز با توجه به شرایط و نتیجهٔ جرم ارتکابی تعیین کرده است که این

موضوع نشان‌دهندهٔ این است که می‌بایست میان مصادیق مختلف این جرائم تفاوت گذاشت تا بتوان نیازهای قانونی متناسب با پیشرفت فناوری را برای جامعه تأمین کرد و همچنین مجازات متناسب و بازدارنده را برای هر کدام، به‌طور جداگانه بکار برد.

تحلیل سیاست جنایی تقنینی ایران و آمریکا نسبت به جرائم کلاهبرداری و سرقت سایبری

در این قسمت ابتدا مادهٔ ۱۲ و ۱۳ قانون جرائم رایانه‌ای ایران مورد بررسی قرار می‌گیرد و سپس به تحلیل مواد ۱۰۲۸-۱۰۲۸A-۱۰۲۹-۱۰۳۰-۱۰۳۷-۱۳۴۳ از بخش ۱۸ قانون جزایی فدرال آمریکا که به سرقت و کلاهبرداری سایبری اختصاص دارند، پرداخته می‌شود. مادهٔ ۱۲ قانون جرائم رایانه‌ای، عنصر قانونی جرم سرقت سایبری است که در آن عنوان شده، هرکس داده‌های متعلق به دیگری را برباید، سارق محسوب می‌شود که این ماده ابهامات زیادی دارد و براساس آن نمی‌توان به تعریف دقیقی از سرقت سایبری دست یافت؛ چراکه برای رسیدن به تعریف مناسب، باید به مسائلی همچون مصادیق این جرم، شرایط وقوع و غیره توجه کرد. با نگاهی به این ماده، می‌توان دیگر عناصر تشکیل‌دهندهٔ این جرم را تحلیل کرد و به دنبال آن نقاط ضعف و قوت مادهٔ مربوطه را مشخص کرد. عنصر مادی سرقت سایبری و سنتی شبیه به هم است که به دلیل جلوگیری از تکرار مکررات، فقط مواردی که سرقت سایبری را از سرقت سنتی جدا می‌سازد، ذکر خواهند شد. مورد اول این وجه تمایز، وسیلهٔ ارتکاب جرم است، دوم موضوع جرم و دیگری فضا و بستری است که امکان ارتکاب جرم در آن فراهم می‌شود. در اینجا وسیلهٔ ارتکاب جرم، رایانه است و موضوع سرقت سایبری، داده‌های دیجیتالی و بستر ارتکاب جرم، فضای سایبر است (خرم‌آبادی، ۱۳۸۶، صص۸۵-۸۴).

الف) مادهٔ ۱۳ قانون جرائم رایانه‌ای: مادهٔ ۱۳ قانون جرائم رایانه‌ای که عنصر قانونی جرم کلاهبرداری سایبری است، عنوان می‌کند: «هرکس به‌طور غیرمجاز از سامانه‌های رایانه‌ای یا مخابراتی با ارتکاب اعمالی از قبیل وارد کردن، تغییر، محو، ایجاد یا توقیف کردن داده‌ها یا مختل کردن سامانه، وجه یا مال یا منفعت یا خدمات یا امتیازات مالی برای خود یا دیگری تحصیل کند ... .» کلاهبردار سایبری است. با توجه به متن قانون مذکور، این موضوع مشخص می‌شود که قانون‌گذار ایران، تعریف کلاهبرداری اینترنتی را از شکل سنتی گرفته است، در صورتی که در دیگر کشورها به دلیل وجود تفاوت بین موضوع کلاهبرداری اینترنتی با نوع سنتی آن و همچنین کیفیات مجزا و متفاوت در شکل‌گیری

این دو جرم، کلاهبرداری اینترنتی را جرمی با تعریف و ماهیت جداگانه از کلاهبرداری سنتی می‌دانند (بای، ۱۳۹۰، ص۳۰۴). به هر ترتیب، در ادامه سعی بر آن است تا براساس قانون مذکور، عناصر جرم کلاهبرداری اینترنتی تفکیک و تحلیل شود. با بررسی مادهٔ ۱۳ قانون جرائم رایانه‌ای، موارد زیر در مورد عنصر مادی جرم کلاهبرداری اینترنتی قابل ذکر هستند:

۱- مرتکب می‌تواند هرکسی اعم از نظامی یا غیرنظامی و ایرانی یا خارجی باشد؛

۲- در خصوص کلاهبرداری اینترنتی نیز، عمل مادی مرتکب، انجام اعمال متقلبانه بر روی سامانه‌های رایانه‌ای یا مخابراتی است و قانون‌گذار از باب تمثیل مصادیقی از این اعمال متقلبانه را احصاء کرده است، ولی این روش‌ها حصری نیست (اکبری، ۱۳۹۰، ص۷)؛

۳- در کلاهبرداری سنتی، تأثیر مانور متقلبانه بر بزه‌دیده از طریق فریب برای تحقق عنوان مجرمانه ضروری است، یعنی لازمهٔ کلاهبرداری، فریب خوردن شخص است (میرمحمدصادقی و شایگان، ۱۳۸۶، ص۱۱۲).

لازم به ذکر است که در قوانین بین‌المللی، کلاهبرداری اینترنتی را جرمی می‌دانند که در آن اغفال و بردن مال شرط نیست، بلکه صرف ایراد ضرر به قصد به دست آوردن منافع مالی کافی است (سالاری شهر بابکی، ۱۳۹۳، ص۲۶۴). در قانون ایران، تحقق جرم کلاهبرداری و برخی جرائم مربوط، نیازمند فریب انسان زنده است (به استثنای کشورهایی همچون کانادا، فرانسه، هلند و اسکاتلند) (دزیانی، ۱۳۸۵، ص۴۵). از همین رو، با توجه به بحث عنصر فریب شخص زنده، برخی از حقوقدانان معتقدند که فریب، مختص اشخاص حقیقی است و در مورد سامانه‌های رایانه‌ای و مخابراتی مصداق ندارد (خرم‌آبادی، ۱۳۸۶، صص۱۰۳-۱۰۴).

ب) مواد ۱۰۲۸، ۱۰۲۸A، ۱۰۲۹، ۱۰۳۰، ۱۰۳۷ و ۱۳۴۳ قانون جزایی فدرال آمریکا: بخش ۱۸ قانون جزای فدرال آمریکا که بخش یا قانون جرائم سایبر نام دارد، انواع جرائم در این حوزه را با ذکر مصادیق و شرایط موردنیاز جهت تحقق آن‌ها به‌طور مفصل شرح داده که شش مادهٔ آن مربوط به کلاهبرداری اینترنتی و انواع صور آن می‌شود. پروسهٔ قانونی تصویب این بخش تا سال ۱۹۸۵ طول کشید و سرانجام این اصلاحات در سال‌های

۱۹۸۸، ۱۹۸۹، ۱۹۹۰، ۱۹۹۱، ۱۹۹۲، ۲۰۰۱ و ۲۰۰۷ ادامه داشت تا در نهایت، قانون جرائم سایبر فعلی به تصویب کنگره رسید (مارشال و بیلی[1]، ۲۰۰۷، ص۲۰). بخش‌های مرتبط با کلاهبرداری اینترنتی در قسمت ۱۸ قانون جزای آمریکا شامل مواد ۱۰۲۸، ۱۰۲۸A، ۱۰۲۹، ۱۰۳۰، ۱۰۳۷ و ۱۳۴۳ می‌شود که هر کدام مربوط به صور خاصی از سرقت و کلاهبرداری است که در ادامه عناوین این مواد و توضیحات آن‌ها ارائه خواهد شد، این عناوین شامل موارد زیر هستند: (قانون جرائم سایبری آمریکا[2]، ۲۰۰۸، بخش۱۸).

- **مادهٔ ۱۰۲۸: سرقت هویت و مشخصات دسترسی:** در این ماده عنوان شده، هر شخصی آگاهانه و بدون مجوز قانونی یک سند شناسایی، ویژگی‌های احراز هویت یا سند شناسایی جعلی تهیه و تولید کند، انتقال دهد یا تصرف کند، تحت عنوان سرقت هویت محاکمه می‌شود. در این ماده، بسته به چگونگی انجام جرم و عمل مرتکب حبس کمتر از ۱۵، ۲۰ و ۳۰ سال در نظر گرفته است. همچنین، قانون‌گذار فدرال در ادامه اصلاحاتی را همچون «ساختن مدارک»، «مدارک هویت»، «مدارک غلط هویت»، «معنای هویت»، «کارت هویت شخصی» و غیره شرح و ویژگی‌های آن‌ها را عنوان کرده است که این امر تکلیف مجریان قانون را در برخورد و رسیدگی با این جرم راحت‌تر می‌کند.
- **مادهٔ ۱۰۲۸A: سرقت هویت و اطلاعات هویتی همراه با خشونت:** در این ماده، منظور قانون‌گذار از سرقت هویت خشن، در جایی است که این سرقت هویت برای اعمال خشن از جمله جرائم مربوط به تروریسم و دیگر جرائم عمومی خشن بکار رفته است. براساس این ماده، منظور از جرائم خشن عمومی، جرائمی هستند که مربوط به انواع جنایات علیه انسان است که در این موارد، علاوه بر مجازات که برای آن جنایت در نظر گرفته می‌شود، بزهکار، برای این سرقت هویت به دو سال زندان محکوم می‌شود و در جرائم مربوط به تروریسم، شخص بزهکار به مدت ۵ سال به زندان محکوم می‌شود (فینکلی[3]، ۲۰۱۲، ص۲).

1.Marshall & Bailie
2.Cybercrime Law of United States of America
3.Finklea

- **مادۀ ۱۰۲۹: کلاهبرداری و جرائم وابسته در ارتباط با وسایل دسترسی:** در این ماده، قانون‌گذار هرکس را که دست به ساختن، استفاده کردن یا دادوستد آگاهانه و با قصد متقلبانه در وسایل دسترسی متقلبانه بزند، در حالات مختلف از نوع جرم، مجرم قلمداد کرده است. از جمله این حالات که در متن ماده ذکر شده‌اند، می‌توان چند مورد را به‌طور خلاصه نام برد:

۱- آگاهانه و با قصد فریب دادن، یکی یا تعداد بیشتری از ابزارهای دسترسی به تقلب را تولید یا استفاده یا تردد کند؛

۲- آگاهانه و با قصد فریب دادن، از یکی ابزارهای دسترسی بدون مجوز تردد یا استفاده کند و در طی هر یک سال و با چنین ابزاری هر چیزی به ارزش ۱۰۰۰ دلار یا بیشتر کسب کند؛

۳- آگاهانه و با قصد فریب دادن، ۱۵ یا تعداد بیشتری ابزار تقلب یا ابزارهای دسترسی‌های غیرمجاز داشته باشد؛

۴- آگاهانه و با قصد فریب دادن، تجهیزات ایجاد ابزار را تولید و در آن تردد یا کنترل داشته باشد یا آن‌ها را در اختیار داشته باشد (مرکز ملی کلاهبرداری[1]، ۲۰۰۰، ص۳۵).

- **مادۀ ۱۰۳۰: کلاهبرداری و جرائم وابسته در ارتباط با رایانه:** در این ماده عنوان شده، چنانچه شخص با داشتن دسترسی آگاهانه بدون مجوز به رایانه یا دسترسی بیش از حد مجاز و به وسیلۀ چنین دسترسی، اطلاعاتی که توسط ایالات متحده آمریکا و به موجب فرمان اجرایی یا اساسنامه به منظور دفاع ملی یا روابط خارجی یا هر نوع اطلاعات محدود دیگر تعریف‌شده در بند Y بخش ۱۱ قانون انرژی اتمی ۱۹۵۴ که نیاز به محافظت در برابر افشا دارد، به دلیل باور داشتن به اینکه اطلاعات به دست آمده به این روش را می‌توان برای آسیب زدن به ایالات متحده آمریکا مورد استفاده قرار داد، دریافت کند یا با هدف سود بردن از هر کشور خارجی از طریق ارتباط خودسرانه، ارائه و انتقال دهد یا باعث انتقال آن شود یا ارائه آن به افراد غیرمجاز یا نگهداری خودسرانه و عدم تحویل آن به افسر یا کارمند ایالات متحده که مجاز به تحویل آن است، کلاهبرداری محسوب می‌شود. همچنین، دسترسی عمدی بدون مجوز یا دسترسی بیش از حد مجاز و دریافت اطلاعات شامل اسناد مالی یک یا حاوی فایل سازمان گزارش دهندۀ مشتری در مورد

1.The National Fraud Center

یک مشتری مانند عباراتی که در قانون امور اعتباری تعریف شده است نیز جرم‌انگاری شده است (اتحادیه بین‌المللی ارتباطات[1]، ۲۰۱۲، ص۳۲۴).

- **مادهٔ ۱۰۳۷: کلاهبرداری و جرائم وابسته در ارتباط با نامه‌های الکترونیک:** در متن این ماده، قانون‌گذار توضیحاتی دربارهٔ عناصر جرم داده است که در ادامه، نکات کلیدی و مهم این ماده ذکر خواهد شد. در این ماده عنوان شده، به‌طور کلی هر کس که به نوعی در تجارت خارجی و بین ایالتی نقشی داشته باشد و آن شخص آگاهانه، به رایانهٔ محافظت شده بدون مجوز، دسترسی داشته باشد و آگاهانه اقدام به شروع ارسال پیام‌های پست الکترونیکی تجاری چندگانه از این رایانه یا به چنین رایانه‌ای بکند، طبق این ماده مجازات می‌شود. در ادامه، قانون‌گذار صور دیگر این جرم را طبقه‌بندی می‌کند که به این شرح است: هرگاه شخصی از رایانهٔ محافظت شده برای توزیع یا ارسال مجدد پیام‌های پست الکترونیک تجاری چندگانه با قصد فریب یا گمراه کردن دریافت‌کنندگان یا هر خدمت دسترسی اینترنتی به عنوان مبدأ چنین پیام‌هایی استفاده کند، یا با جعل اطلاعات اصلی در پیام‌های پست الکترونیک تجاری چندگانه و آغاز عمدی ارسال چنین پیام‌هایی یا با استفاده از اطلاعاتی که هویت ثبت‌کنندهٔ واقعی را جعل می‌کند، در این سایت‌ها ثبت‌نام و برای ۵ حساب پست الکترونیک یا تعداد بیشتر یا حساب‌های کاربری آنلاین یا دو یا چند نام دامنه و آغاز عمدی ارسال پیام‌های پست الکترونیکی از چنین ترکیبی از حساب‌ها یا دامنه‌ها مجازات خواهد شد (تی ولز[2]، ۲۰۰۹، ص۲۸۳). همچنین، اگر شخص با قصد فریب اقدام به نشان دادن خود به صورت ثبت‌کننده یا جانشین مشروع او برای ثبت ۵ یا تعداد بیشتری از آدرس‌های پروتکل اینترنتی به دروغ بکند و برای آغاز عمدی ارسال پیام‌های پست الکترونیکی تجاری چندگانه از این آدرس‌ها برای توطئه و انجام آن، باید مجازات شود. این ماده برای کلاهبرداری‌های مربوط، جرائمی از قبیل حبس و جزای نقدی در نظر گرفته است.

- **مادهٔ ۱۳۴۳: کلاهبرداری به وسیله سیم، رادیو و تلویزیون:** در این ماده، قانون‌گذار آمریکا هرکس را که طرح یا تصنعی ابداع کند یا حتی قصد ابداع را داشته باشد و این قصد یا این ساختن برای فریب یا کسب پول یا دارایی به وسیلهٔ جعل یا بازنمایی تقلبی

1.International Telecommunication Union
2.Twels

باشد یا موجب ارسال چیزی توسط سیم، رادیو و تلویزیون در تجارت خارجی یا بین ایالتی شود، هر نوشته یا سیگنال که به قصد اجرای چنین طرح یا تصنعی باشد باید جرم شناخته شود و مجازات شود که مجازات مندرج در این ماده شامل حبس کمتر از ۲۰ سال یا جریمه یا هر دو می‌شود و اگر این نقض قانون تأثیری روی یک مؤسسهٔ مالی بگذارد، این شخص باید کمتر از ۱.۰۰۰.۰۰۰ دلار جریمه شود و کمتر از ۳۰ سال زندانی شود یا به هر دو مجازات محکوم شود (دویل[1]، ۲۰۱۱، صص۱-۲).

تحلیل سیاست جنایی مشارکتی ایران و آمریکا نسبت به سرقت و کلاهبرداری سایبری

همان‌طور که در بخش‌های قبلی عنوان شد، سیاست جنایی مشارکتی به دو گونهٔ کنشی (پیشگیرانه یا فعال) و واکنشی (پاسخگو یا منفعل) قابل تقسیم است. از همین رو، در نوع منفعل این نوع سیاست جنایی بحث پیشگیری ثانویه و ثالث نیز مطرح می‌شود که در ادامه به آن‌ها پرداخته خواهد شد.

پیشگیری به‌طور عمده دارای دو مفهوم است؛ هم به معنای پیش‌دستی کردن و به جلوی چیزی رفتن و هم به معنای آگاه کردن و هشدار دادن است. اما در جرم‌شناسی پیشگیرانه، پیشگیری در معنای اول آن مورد استفاده قرار می‌گیرد، یعنی با به کار بردن متد و روش‌های مختلف به منظور جلوگیری از وقوع بزهکاری، هدف به جلوی جرم رفتن و پیشی گرفتن از بزهکاری است (احمدی، ۱۳۸۷، صص۹۱-۹۰ و گسن، ۱۳۷۰، ص۱۳۳). بر همین اساس، علمای حقوق جزا و جرم‌شناسی، دو مفهوم از پیشگیری را مورد توجه قرار داده‌اند و به تعریف و تبیین آن پرداخته‌اند که یکی از آن‌ها، مفهوم موسع پیشگیری است و مقصود از آن هر اقدامی است که در مقابله با جرم و به منظور سد کردن ارتکاب آن باشد و جرم را کاهش دهد. طبق این تعریف از پیشگیری، می‌توان مواردی همچون مجازات بزهکار و ترمیم کردن خسارت وارد بر بزه‌دیده در فرآیند وقوع جرم را نام برد. این برداشت و استنباط از پیشگیری نزد افرادی همچون انریکوفری وجود داشته است؛ مقصود وی از این اصطلاحات همان اقدامات پیشگیرانه غیرکیفری است که جایگزین مجازات بوده و به عبارتی «هم‌عرض‌های کیفری» می‌باشند (نجفی ابرندآبادی، ۱۳۷۹، ص۷۴۲). در مقابل مفهوم موسع پیشگیری، مفهوم مضیق پیشگیری قرار دارد که

1.Doyle

مقصود از آن مجموعه ابزار و وسایلی است که دولت برای مهار بهتر بزهکاری از دو طریق مورد استفاده قرار می‌دهد: از طریق حذف یا محدود کردن عوامل جرم‌زا و از طریق اعمال مدیریت مناسب نسبت به عوامل محیطی، فیزیکی و اجتماعی که به نوبهٔ خود فرصت‌های مناسبی را برای ارتکاب جرم ایجاد می‌کنند (نجفی ابرندآبادی، ۱۳۷۹، ص۷۵۰). در مفهوم مضیق پیشگیری، پیشگیری از تکرار جرم مدنظر نیست، بلکه مقصود مورد توجه قرار دادن وضعیت پیش جنایی و قبل از ارتکاب جرم است.

الف) اقدامات مبتنی بر پیشگیری اجتماعی در ایران: در این نوع پیشگیری، سعی بر این است که با افزایش آگاهی افراد و تربیت صحیح آن‌ها، به ویژه قشر جوان و نوجوان جامعه و همچنین از بین بردن زمینه‌های اجتماعی وقوع جرم نظیر فقر و بیکاری، انگیزه‌های مجرمانه از مجرمان سلب شود (نجفی ابرندآبادی، ۱۳۸۲، ص۱۲۰۸). همچنین، پیشگیری اجتماعی شامل اقدام‌هایی است که به‌طور مستقیم یا غیرمستقیم، هدفشان تأثیرگذاری بر شخصیت افراد است تا از سازمان دادن فعالیت خود حول انگیزه‌های بزهکارانه بپرهیزند (گسن، ۱۳۷۰، ص۷۸). با توجه به تعاریف و مفاهیم ارائه شده، می‌توان پیشگیری اجتماعی را به دو دسته تقسیم‌بندی کرد؛ پیشگیری اجتماعی رشد مدار که سعی دارد چنانچه هر شخصی به هر دلیلی از خود نشانه‌هایی از بزهکاری را بروز داد، از طریق مداخله هر چه سریع‌تر در خود وی و محیط اطرافش از مزمن شدن بزهکاری در آینده جلوگیری کند و پیشگیری اجتماعی جامعه‌مدار که در پی خنثی‌سازی عوامل جرم‌زا در محیط اجتماعی است.

- **پیشگیری اجتماعی رشد مدار اینترنتی:** نکته بسیار مهم در برخورد و مبارزه با جرائم اینترنتی به‌ویژه کلاهبرداری، استانداردهای فنی و اخلاق حرفه‌ای افراد است. بدین منظور که مسلماً زمانی می‌توان از افراد انتظار عملکرد درستی داشت که به خوبی به وی تفهیم شود که چه تدابیر امنیتی باید به کار گیرد و چه اخلاق شغلی را رعایت کند (باستانی، ۱۳۹۰، ص۱۲۸). طیف وسیعی از مجرمان و بزه‌دیدگان جرائم اینترنتی را افراد کم سن و سال، خصوصاً نوجوانان تشکیل می‌دهند. از همین رو، از جمله تدابیر بسیار مؤثر در پیشگیری کلاهبرداری اینترنتی، ارائه آموزش کافی و اطلاع‌رسانی به موقع است. آگاه ساختن افراد و ارائه آموزش‌های لازم در سنین کودکی و نوجوانی می‌تواند نقش شایان توجهی در مقابله با کلاهبرداری اینترنتی داشته باشد.

- **پیشگیری اجتماعی جامعه مدار سایبری:** هدف از این تدابیر، جلوگیری از شکل‌گیری

یا بروز انگیزهٔ مجرمانه در عموم جامعه به وسیلهٔ دو اقدام اصلی است: ایجاد علاقه و آسان‌سازی بروز افکار مشروع و مفید و بر حذر داشتن از ناهنجاری‌های اینترنتی. یکی از مهم‌ترین راه‌های پیشگیری از کلاهبرداری اینترنتی به وسیلهٔ پیشگیری اجتماعی جامعه‌مدار سایبری، از طریق آموزش‌های عمومی و رسانه‌های جمعی است. باید توجه داشت که اهمیت خاص تحقیق در زمینهٔ رسانه و پیشگیری از وقوع جرم از آن روست که این وسیله تمامی زندگی انسان را در برمی‌گیرد. کارکرد رسانه‌های جمعی در مورد پیشگیری از کلاهبرداری اینترنتی می‌تواند از طریق آگاه کردن مردم از پیامدهای ناگوار این جرم (چه بزهکار باشد، چه بزه‌دیده) و نیز دادن الگوهای مناسب رفتاری جهت جلوگیری از ارتکاب و تکرار آن باشد که از این طریق می‌توانند نقش مهمی در پیشگیری از جرم داشته باشند (دیندار و صدرنیا، ۱۳۸۸، صص۴۱-۴۰). همچنین، اثربخشی هر چه بیشتر انواع راه‌های پیشگیری ذکرشده نسبت به کلاهبرداری، نیازمند یک سیاست جنایی مشارکتی فعال است. از لحاظ مفهومی، سیاست جنایی مشارکتی، بررسی و مطالعهٔ جایگاهی است که در سیاست جنایی یک کشور به جامعهٔ مدنی و از طریق اعطای نقش به بزهکار، بزه‌دیده و به ویژه کل جامعه و مردم داده شده است (لازرژ، ۱۳۹۰، ص۶۱). کارکرد این نوع از سیاست جنایی نسبت به کلاهبرداری اینترنتی، اقدامات در مرحلهٔ کشف جرم، تعقیب دادرسی و اجرای حکم را در برمی‌گیرد که با همکاری وسیع جامعهٔ مدنی، نهادهای مردمی و نیروهای دولتی مانند پلیس، سازمان زندان‌ها و غیره با دستگاه قضایی انجام می‌شود (باصری، ۱۳۸۷، ص۳۷).

پس از ارائه توضیحات مربوط به این بخش و با جمع‌بندی آن می‌توان انتقادهایی را بر به‌کارگیری این نوع پیشگیری در ایران وارد دانست؛ برنامه‌هایی که در ایران مبتنی بر این نوع پیشگیری هستند، عموماً با محوریت مسئولیت دولت یا وزارت ارتباطات و فناوری اطلاعات و وزارت ارشاد است. برای اثربخشی بیشتر این نوع پیشگیری در کلاهبرداری اینترنتی، لازم است به سیاست جنایی مشارکتی بهای بیشتری داد و مردم را به عنوان عضوی مؤثر در این نوع پیشگیری وارد برنامه‌ها کرد که این امر نیز متأسفانه کمتر مورد توجه قرار گرفته است.

ب) اقدامات مبتنی بر پیشگیری وضعی در ایران: پیشگیری وضعی عبارت است از اقدامات پیشگیرانهٔ معطوف به اوضاع و احوالی که جرائم ممکن است در آن وضعیت به وقوع بپیوندد، به‌طوری که هدف از این اقدامات، اتخاذ ترتیبی است که بهای ارتکاب عمل

مجرمانه را برای مرتکب، بیش از سود حاصل از آن قرار دهد؛ چراکه از نظر طرفداران پیشگیری وضعی، انسان موجودی حسابگر است و سود و زیاد عملش را به‌طور فطری می‌سنجد. همچنین، این نوع پیشگیری سعی دارد تا با اتکا به آماج جرم یا بزه‌دیده به تبیین پیشگیری از جرم بپردازد. چهارچوب نظری این بحث به وسیله نظریه‌های مختلف «فرصت» بیان شده است. چنین اقداماتی در مورد جرم کلاهبرداری اینترنتی شامل روش‌هایی همچون مصونیت بخشی به آماج، نظارت بر مراکز ارائه‌دهندهٔ اینترنت، فیلترینگ و غیره می‌شود. این نوع پیشگیری خود نیز دارای نقاط ضعف و قوت است، اما مجال توضیح این موارد در این تحقیق نمی‌گنجد (نجیبیان، ۱۳۸۸، صص۶۹-۷۲ و صفاری، ۱۳۸۱، صص۱۹۴-۱۹۸).

مخاطبان اصلی پیشگیری وضعی از جرم کلاهبرداری اینترنتی، کسانی هستند که از تخصص و مهارت بالایی برخوردار نیستند و بیشتر سعی می‌کنند با امکاناتی که فضای اینترنت در اختیار آن‌ها قرار می‌دهد مرتکب جرم شوند؛ نه اینکه خود دست به ابتکار عمل بزنند که در این صورت، همان‌طور که در ادامه توضیح داده خواهد شد، کاری از پیشگیری وضعی جهت مقابله با جرم کلاهبرداری و سرقت اینترنتی ساخته نخواهد بود. البته این نکته را نباید از یاد برد که علیرغم تأثیرات مثبتی که پیشگیری وضعی در برابر کلاهبرداری اینترنتی دارد، بعضاً به دلیل ماهیت این جرم دارای نقاط ضعفی نیز است؛ از جمله این محدودیت‌ها، هزینه‌بر بودن و زمان‌گیر بودن این اقدامات، تفاوت در میزان دانش طرفین نسبت به اینترنت و تفاوت در به‌کارگیری روش‌ها چه در جهت فیلترینگ و چه در جهت اقداماتی ضد آن. در نهایت، از جمله اقداماتی که مبتنی بر این نوع پیشگیری است می‌توان به این موارد اشاره کرد؛ فیلترینگ، استفاده از پراکسی‌ها، استفاده از رمز ورود، کنترل موجودی حساب و نظارت بر فضای مجازی.

ج) اقدامات مبتنی بر پیشگیری وضعی در آمریکا: به دلیل ماهیت جرائم اینترنتی خصوصاً کلاهبرداری و سرقت اینترنتی، برنامه‌های پیشگیرانه در اکثر کشورهای دنیا با اتکا بر پیشگیری وضعی است. در کشور آمریکا علاوه بر دولت و ایالت‌ها، عموماً شرکت‌های خصوصی مرتبط، پلیس فدرال، کمیسیون امنیت و اقتصاد و سازمان جاسوسی در این کار شرکت دارند. راهبردها و برنامه‌های کشور آمریکا در پیشگیری از جرم همان‌طور که گفته شد کلی است و البته، سازمان‌ها و نهادهای دولتی، برنامه‌هایی در این راستا طراحی کرده‌اند. این برنامه‌ها شامل تغییر نوع محافظت از سیستم‌ها با

استخدام افراد برای به وجود آوردن یک سیستم دفاعی جدید، همکاری با دیگر نهادها، سازمان‌ها و شرکت‌های خصوصی برای امنیت در فضای اینترنت، تمرکز بر روابط اینترنتی بین ایالات متحده آمریکا و دیگر کشورها، تلاش برای ارتقای امنیت فضای اینترنتی آمریکا و نوآوری در روش‌ها می‌شد. هر چند که این برنامه برای وزارت دفاع بود، اما مرکز دفاع جرائم سایبر[1] که مسئول این تحقیقات بود به نوعی این اطلاعات و روش‌ها را بهبود بخشید و از این طریق مورد استفاده عمومی قرار داد. (وزارت دفاع آمریکا[2]، ۲۰۱۱، ص۳) در ماه می سال ۲۰۱۱، دفتر ریاست جمهوری آمریکا، راهبردی تحت عنوان «راهبرد جهانی برای فضای سایبر؛ امنیت، شکوفایی و آزادی در فضای مجازی» را به‌طور مکتوب درآورد و از این طریق امنیت و پیشگیری از جرائم در فضای مجازی در آمریکا را از طریق همکاری‌های بین‌المللی فراهم آورد. این راهبرد، پنج قاعدهٔ کلی داشت که شامل جلوگیری از جرم (بر همین اساس، همهٔ دولت‌ها از جمله ایالات متحدهٔ آمریکا باید مجرمان اینترنتی را شناسایی و تعقیب کنند تا مطمئن شوند از جرم جلوگیری می‌شود و همچنین با مرکز تحقیقات مجرمان بین‌المللی همکاری داشته باشند)، ایجاد اولویت‌هایی که مستقیماً در ارتباط با پیشگیری از جرائم سایبر، تحقیقات و دادرسی جرائم سایبر است، احترام به دارایی افراد، ارزش دادن به استقلال و خلوت اطلاعات مردم و تمرکز کردن بر آموزش مردم برای دفاع از خود در فضای اینترنت (انتشارات کاخ سفید[3]، ۲۰۱۱، ص۴۵).

در رابطه با بحث پیشگیری و اقدامات انجام‌شده، نگاهی به قوانین مربوط نشان می‌دهد در کشور ایران، قانونی تحت عنوان قانون پیشگیری وجود دارد که متأسفانه، در آن راهکار و پیشنهادهایی در جهت پیشگیری از جرائم داده نشده و فقط صرفاً به معرفی اعضا، نحوهٔ تشکیل و وظایف کارگروه‌ها اشاره شده است. از همین رو، در مورد هیچ نوع پیشگیری صحبت نشده است. در حالی که در قانون ملی پیشگیری از جرم آمریکا، انواع راهکارهای مبتنی بر پیشگیری وضعی، مرحله‌ای و اجتماعی لحاظ شده و قانونگذار، مسئولان مربوطه را به انجام تمام دستورالعمل‌های اجرایی و حمایتی، قبل و بعد از وقوع

1.Defense Cyber Crime Center
2.U.S Department of Defense
3.The white House

جرم موظف دانسته است. در نهایت، برنامهٔ مبتنی بر پیشگیری وضعی از جرائم رایانه‌ای و سایبری در دو کشور ایران و آمریکا به شرح جدول ۱ قابل تبیین است.

جدول ۱ – راهکارهای پیشگیری وضعی از جرائم رایانه‌ای و سایبری در ایران و آمریکا

راهکار اصلی	راهکارهای فرعی	موارد مورد استفاده در سرقت و کلاهبرداری سایبری
افزایش زحمت ارتکاب جرم	سخت کردن آماج جرم کنترل دسترسی به آماج جرم غربال خروجی‌ها منحرف کردن بزهکار از آماج جرم کنترل وسایل تسهیل‌کنندهٔ جرم	تدابیر امنیتی (Filtering) رمزگذاری پراکسی‌ها (Proxy) کیبورد مجازی تدابیر مربوط به فیلترینگ
افزایش خطرات ارتکاب جرم	توسعهٔ محافظت کمک به نظارت طبیعی کاهش گمنامی استفاده از مدیران محلی گشت‌زنی مجازی پلیسی	تدابیر صدور مجوز نصب دوربین‌های مداربسته در کافی‌نت‌ها کنترل مجرمان حرفه‌ای جلوگیری از تکرار جرائم سازمان‌یافته بررسی گزارش مشکوک مدیران بانک‌ها نظارت مانند نظارت بر سایت‌های خریدوفروش
کاهش منافع	جابجایی آماج جرم شناساندن یا نشانه‌گذاری حذف یا کاهش جذابیت سخت کردن دسترسی	کم کردن و کنترل موجودی استفاده از شناسه برای کاربران ارائه فهرست بدون اطلاعات به‌کارگیری گذرواژه
کاهش تحریکات	کاهش سرخوردگی و استرس دوری از تحقیر کاستن وسوسه‌های ارتکاب جرم از طریق آزمایش‌های مربوط	تدابیر مربوط به روان‌کاوی و روان‌درمانی افراد مستعد ارتکاب جرم
حذف معاذیر	برقراری مقررات تحریک وجدان و آگاهی کنترل (پایش) رها کننده‌ها تسهیل رعایت قوانین	مقررات ثبت‌نام الکترونیکی توسط سرورها درج راهنمایی‌ها و هشدارها نصب تراشه‌های مخصوص برای تعیین میزان انطباق فعالیت‌ها ارائه خدمات از طریق روش‌های کنترل‌شده

نتیجه‌گیری

پژوهش حاضر با هدف تطبیق سیاست جنایی ایران و آمریکا در خصوص نحوهٔ جرم‌انگاری سرقت و کلاهبرداری سایبری انجام شده است و بررسی‌های انجام شده نشان می‌دهد که اولین عکس‌العمل قانون‌گذار ایران در مقابل جرائم رایانه‌ای در سال ۱۳۸۲ از طریق تصویب قانون مجازات جرائم نیروهای مسلح (مصوب ۱۳۸۲/۱۰/۰۹) در مجلس شورای اسلامی به عمل آمد. به موجب مادهٔ ۱۳۱ این قانون، سرقت یا تخریب حامل‌های داده و سوءاستفادهٔ مالی از طریق رایانه (کلاهبرداری و اختلاس)، جعل اطلاعات و داده‌های رایانه‌ای و تسلیم و افشای غیرمجاز اطلاعات و داده‌ها به افرادی که صلاحیت

دسترسی به آن را ندارند، توسط نظامیان جرم تلقی و مرتکب حسب مورد به مجازات جرم ارتکابی محکوم می‌شود. واکنش بعدی قانونی مرتبط با جرائم رایانه‌ای از طریق تصویب قانون تجارت الکترونیکی (مصوب ۱۳۸۲/۱۰/۱۷) در مجلس شورای اسلامی به عمل آمده است. به موجب مواد ۶۶، ۶۷، ۶۸، ۶۹، ۷۴، ۷۵، ۷۶ و ۷۷ این قانون، کلاهبرداری، جعل، دستیابی و افشای غیرمجاز اسرار تجاری، نقض حقوق مربوط به مالکیت معنوی (کپی‌رایت) و غیره که از طریق رایانه و در بستر تجارت الکترونیکی انجام شود، جرم تلقی و برای آن مجازات تعیین شده است. هر یک از قوانین مربوطه، در بستر خاص خود قابلیت اعمال دارند؛ مثلاً قانون مطبوعات صرفاً نسبت به جرائم رایانه‌ای ارتکابی در قالب نشریات الکترونیکی و قانون مجازات نیروهای مسلح صرفاً در مورد بعضی از جرائم رایانه‌ای نظامیان و قانون تجارت الکترونیکی فقط در مورد برخی از جرائم رایانه‌ای ارتکابی در بستر تجارت الکترونیکی قابل‌اجرا هستند (صابری و انصاری دوست، ۱۳۹۶، ص۱۴۵).

با این توضیحات، روند شکل‌گیری سیاست جنایی تقنینی ایران نسبت به کلاهبرداری و سرقت اینترنتی مشخص شد. اما برخلاف این روند در ایران، قانون‌گذاران آمریکایی از سال‌ها قبل یعنی از اوایل دهۀ ۸۰ میلادی در جهت تصویب قانون مرتبط گام برداشتند و از آن زمان تا به امروز، قانون جرائم سایبری آمریکا بیش از پنج بار تغییر کرده است که قانون فعلی در سال ۲۰۰۸ به تصویب رسید و تا الان نیز عنصر قانونی جرائم سایبری است. البته طرح اصلاح موادی از این قانون در حال حاضر در سنای آمریکا در حال بررسی است که از زمان تصویب و اجرایی شدن آن اطلاعی در دسترس نیست. بخش ۱۸ قانون جزای فدرال که به نام بخش جرائم سایبر شناخته می‌شود، در شش ماده به جرم‌انگاری سرقت و کلاهبرداری سایبری پرداخته است. در هر کدام از این مواد، صور مختلف کلاهبرداری اینترنتی ذکر شده‌اند و برای هر کدام از آن‌ها با توجه به شرایط و نوع جرم مجازات متناسبی در نظر گرفته شده است. همین نوع قانون‌نویسی، یعنی تقسیم‌بندی اشکال مختلف کلاهبرداری اینترنتی سبب شده تا موردی از قلم نیفتد و با جرم‌انگاری تمامی حالات قانونی، کامل شکل بگیرد.

در قانون جرائم رایانه‌ای ایران، که عنصر قانونی مبارزه با کلاهبرداری اینترنتی است، قانون‌گذار فقط به ذکر افعالی همچون تغییر، محو و غیره بسنده کرده و انجام این افعال در فضای اینترنت را اگر برای فریب و به دست آوردن پول باشد، جرم‌انگاری کرده است.

اِشکالی که در اینجا متوجه مادهٔ ۱۲ و ۱۳ قانون جـرائم رایانـه‌ای اسـت، ایـن اسـت کـه قانون‌گذار انواع مختلف کلاهبرداری و سرقت را در یک سطح دیده است، غافـل از اینکـه هر کدام از این اشکال با یکدیگر تفاوت دارند. لذا این تفاوت‌ها هم به نحوهٔارتکاب جـرم و هم به وسیلهٔ ارتکاب جرم برمی‌گردد و از آن مهم‌تر، اثرات زیان‌باری که هر کـدام از ایـن روش‌ها بر جای می‌گذارند، با هم متفاوت است. به همین جهـت، شـاید بتـوان بـا انجـام اصلاحاتی متناسب با شرایط اجتماعی و قانونی کشور، مدلی از قانون کشور آمریکـا را در ایران اجرا کرد و بهتر است برای دستیابی به نتیجهٔ مطلوب، انواع کلاهبـرداری اینترنتـی در چند ماده به‌طور جداگانه جرم‌انگاری شوند و برای هر کدام، مجازات متناسب در نظـر گرفته شود.

در مورد بحث پیشگیری از این جرائم، در ایران بیش‌ترین تأکید بر پیشگیری وضعی و اجتماعی است و پیشگیری مرحله‌ای در سیاست جنایی ایران عملاً جایی ندارد یا حداقل، توجهی به آن نمی‌شود. برنامه‌های مبتنی بر پیشگیری وضعی از این جرائم به هر شـکلی که باشند در نهایت در این دسته‌بندی قـرار خواهنـد گرفـت؛ افـزایش تـلاش و زحمـت ارتکاب جرم، افزایش خطرات ارتکاب جرم، کاهش منافع ارتکاب جـرم، کـاهش تحریـک ارتکاب جرم، از بین بردن بهانه‌های ارتکاب جرم و نصب تراشه‌های مخصوص برای تعیین میزان انطباق فعالیت‌ها. هر کدام از این دسته‌بندی‌ها نیز مصـداق‌هـایی دارنـد؛ از جملـه بحث فیلترینگ، کنترل موجودی حساب، کنترل مجرمان حرفه‌ای و جلـوگیری از تکـرار جرائم سازمان‌یافتـه، نظـارت شـبکه‌ای، تـدابیر امنیتـی کدگـذاری، امضـای دیجیتـال و رمزگذاری که همگی این‌ها در پیشگیری وضـعی قـرار مـی‌گیرنـد. در مـورد پیشـگیری مرحله‌ای موضوع قدری متفاوت است. این تفاوت به برنامه‌های ایران و آمریکا برمی‌گردد؛ چراکه دید این دو کشور به این نوع پیشگیری متفاوت است، به شکلی که در ایران به این نوع پیشگیری بسیار کمتر از آمریکا توجه می‌شود. این مسئله را هم می‌تـوان در قـوانین مربوطه مشاهده کرد و هم در رویهٔ عملی نهادهای مربوط. در کشور آمریکا علاوه بر وجود قانون مدون فدرال جهت روشن شدن موضع قانون‌گذار نسبت بـه بحـث پیشـگیری، بـه ایالت‌ها نیز اجازه داده شده که در پرتو قانون فدرال، راهکارهای پیشـگیرانه متناسـب بـا شرایط آن ایالت به تصویب و اجرا برسد.

در پایان می‌توان نتیجه گرفت که مادهٔ ۱۲ و ۱۳ قانون جـرائم رایانـه‌ای ایـران، مـادهٔ جامع و مانعی برای مقابله بـا کلاهبـرداری و سـرقت سـایبری نیسـت و نیـاز اسـت کـه

قانون‌گذار ایران نسبت به رفع این مشکل اقدام کند که این اقدام می‌تواند با بهره‌گیری از سوابق دیگر کشورها در قانون‌گذاری ازجمله آمریکا باشد تا به این شکل بتوان قانونی کامل و متناسب با شرایط کشور داشت.

با توجه به اهداف و یافته‌های تحقیق، پیشنهادهایی به عنوان راهکارهای پیشگیری اجتماعی و وضعی از کلاهبرداری و سرقت سایبری ارائه می‌شود.

- افزایش تلاش و زحمت ارتکاب جرم کلاهبرداری و سرقت سایبری از طریق تدبیر امنیتی دیوار آتش[1]: فایروال‌ها یکی از عناصر اساسی در نظام مهندسی امنیت اطلاعات هستند که استفاده از آن‌ها به یک ضرورت اجتناب‌ناپذیر در دنیای امنیت اطلاعات و رایانه تبدیل شده است.

- تدابیر امنیتی کدگذاری و امضای دیجیتال و پسورد: در این روش، براساس معیارهایی خاص، از ورود اشخاص ناشناس یا فاقد اعتبار جلوگیری می‌شود. این اقدام به ویژه برای زنان و کودکان یا به‌طور کلی اشخاصی که به هر دلیل آسیب‌پذیرند سودمند است؛ چراکه بدون آنکه فرصت شناسایی خود را به مجرمان اینترنتی بدهند، می‌توانند به فعالیت‌های شبکه‌ای بپردازند.

- پراکسی: در اینجا، از پراکسی به معنی پروسه‌ای یاد می‌شود که در راه ترافیک شبکه‌ای قبل از اینکه به شبکه وارد یا از آن خارج شود، قرار می‌گیرد و آن را می‌سنجد تا ببیند با سیاست‌های امنیتی کاربر مطابقت دارد و سپس مشخص می‌کند که آیا به آن اجازهٔ عبور از فایروال را بدهد یا خیر. بسته‌های مورد قبول به سرور موردنظر ارسال و بسته‌های رد شده، دور ریخته می‌شوند.

- استفاده از کیبورد مجازی: استفاده از این صفحه کلید برای جلوگیری از ثبت کلیدهای فشرده شده در صفحه کلید افراد توسط نرم‌افزارهای جاسوسی به کار می‌رود. در زمانی که از سایت‌های بانکی خرید می‌شود، بیش‌ترین بخش قابل‌توجه برای کاربر، امنیت وب‌سایت است که رمزهای بانکی دزدیده نشود که بانک‌ها برای ما این کار را انجام داده‌اند و صفحه‌کلید مجازی را گذاشته‌اند.

- تدبیر پالایه یا فیلترینگ: فیلترینگ پورت‌ها از جمله مهم‌ترین عملیاتی است که توسط فایروال‌ها انجام می‌شود و سبب می‌شود اطلاعات و سایت‌هایی که ممنوعه هستند از

1.firewall

دسترس خارج گردند.

- تدابیر صدور مجوز: در اینجا تلاش می‌شود براساس معیارهایی خاص، از ورود اشخاص ناشناس یا فاقد اعتبار جلوگیری شود. نمونهٔ سادهٔ این اقدام، به‌کارگیری گذرواژه است که در گذشته و اکنون جایگاه خود را حفظ کرده است. به این ترتیب، تنها کسانی حق بهره‌برداری از یک سیستم یا سایت را خواهند داشت که گذرواژهٔ مربوط را دریافت کنند.

- نظارت شبکه‌ای: این راهکار شاید بیش از آنکه یک اقدام پیشگیرانه باشد، از لحاظ بازدارندگی مورد توجه قرار می‌گیرد. در حالت فنی، ابزارها یا برنامه‌هایی بر روی سیستم نصب می‌شوند و کلیهٔ فعالیت‌های شبکه‌ای اشخاص، ضبط می‌شوند. شایان ذکر است در صورتی نظارت شبکه‌ای اثر بازدارنده خواهد داشت که کاربر بداند فعالیت‌هایش تحت نظارت قرار دارد؛ چراکه نظارت مخفی فقط برای جمع‌آوری ادله علیه متهم به کار می‌رود و هیچ اثر پیشگیرانه‌ای ندارد (اسپانولتی[1]، ۲۰۰۵، ص۱۰۶۵).

- کنترل مجرمان حرفه‌ای و جلوگیری از تکرار جرائم سازمان‌یافته: برنامه کنترل مجرمان حرفه‌ای و خروجی آن حداقل در بحث مرتبط با مجرمان سابقه‌دار، علاوه بر وجود پیشینهٔ کیفری و اجتماعی، کلیهٔ تحرکات فرد موردنظر و اقدامات وی، اعم از اشتغال، سکونت، تردد، جابه‌جایی و معاملات دقیقاً در مکانیزم تعریف شده و به‌طور مشخص تحت کنترل قرار گیرد.

- کنترل موجودی حساب: در اینجا کاربر با کم کردن موجودی حساب یا جابجایی موجودی باعث انصراف مجرم از کلاهبرداری اینترنتی می‌شود؛ چراکه با کاهش موجودی حساب، مجرم انگیزهٔ لازم را برای انجام اعمال بزهکاری با در نظر گرفتن میزان سود حاصله از دست می‌دهد و از ارتکاب جرم منصرف می‌شود.

- هرچه قدر آگاهی بیشتری در فضای رسانه‌ای به خصوص در صدا و سیما منتشر شود و خطرات این موضوعات بیشتر گوشزد شود، جامعه کمتر آسیب خواهد دید. لذا لازم است برای پیشگیری از این جرائم سایبری، با هشدارها و راهنمایی‌های لازم، کاربران را از اصول اولیهٔ محافظت اینترنتی در فضای سایبر قبل از وقوع هرگونه حملهٔ رایانه‌ای و موقعیت خطر مطلع ساخت.

- نصب تراشه‌های مخصوص برای تعیین میزان انطباق فعالیت‌ها: برای از بین بردن

1.Spagnoletti

معاذیر در اقدامات قابل‌تصور در مورد حملات سایبری بر روی سیستم‌های رایانه تراشه‌های مخصوص به منظور کنترل فعالیت‌های سیستم‌عامل و جلوگیری از دسترسی به منابع آن نصب می‌شود.

منابع

منابع فارسی

- احمدی، احمد (بهار ۱۳۸۷). نقض حریم خصوصی؛ چالشی فراروی پیشگیری وضعی از وقوع جرم. *فصلنامهٔ مطالعات پیشگیری از جرم*. ۶(۳)، صص۷۷-۱۱۰. بازیابی از: http://pishgiri.police.ir/uploads/fasl6-04_10503.pdf

- اکبری، عباسعلی (۱۳۹۰). کلاهبرداری رایانه‌ای؛ جلوه‌ای نوین و متمایز از بزهکاری سنتی. *مجموعه مقالات همایش منطقه‌ای چالش‌های جرائم رایانه‌ای در عصر امروز*. دانشگاه آزاد اسلامی واحد مراغه.

- باستانی، برومند (۱۳۹۰). *جرائم کامپیوتری و اینترنتی جلوه‌ای نوین از بزهکاری*. تهران: انتشارات بهنامی

- باصری، علی اکبر (۱۳۸۷). *سیاست جنایی قضایی کودکان و نوجوانان (در حقوق داخلی و اسناد بین‌المللی)*. تهران: خرسندی.

- بای، حسینعلی و پورقهرمانی، بابک (۱۳۸۸). *بررسی فقهی حقوقی جرائم رایانه‌ای*. قم: انتشارات پژوهشگاه علوم و فرهنگ اسلامی.

- خرم‌آبادی، عبدالصمد (۱۳۸۶). کلاهبرداری رایانه‌ای از دیدگاه بین‌المللی و وضعیت ایران. *فصلنامهٔ حقوق* دانشگاه تهران. ۲(۷۳)، صص۸۳-۱۱۲. بازیابی از: https://b2n.ir/270728

- دزیانی، محمدحسن (خرداد و تیر ۱۳۸۵). مقدمه‌ای بر سیاست جنایی ایران در باب جرائم سایبری. *مجله قضاوت*. شمارهٔ ۳۸، صص۴۲-۴۸. بازیابی از: https://www.noormags.ir/view/fa/articlepage/334352

- دلماس مارتی، می‌ری (۱۳۹۳). *نظام‌های بزرگ سیاست جنایی* (علی حسین نجفی ابرندآبادی، مترجم). تهران: نشر میزان.

- دیندار فرکوش، فیروز، صدرنیا، حسین (۱۳۸۸). *روابط عمومی و رسانه*. تهران: انتشارات سایه‌روشن.

- رمضانی، میریاسین و علیزاده، اکبر (۱۳۹۲). سیاست جنایی؛ ابزارها، مقامات و مراجع

دخیل در سیاست جنایی قضایی. *فصلنامهٔ کارآگاه*. ۷(۲۵)، صص۱۲۱-۱۶۲. بازیابی از: https://b2n.ir/518353

- سالاری شهر بابکی، میرزا مهدی (۱۳۹۳). *کلاهبرداری و ارکان متشکلهٔ آن*. تهران: میزان.

- شیعه علی، علی؛ زارع، وحید و زارع، مجتبی (۱۳۹۴). جایگاه سیاست جنایی مشارکتی واکنشی در مرحلهٔ تعقیب کیفری در حقوق ایران. *مطالعات حقوق کیفری و جرم‌شناسی*. ۲(۴و۵)، صص۲۸۷-۳۱۰. بازیابی از: https://jqclcs.ut.ac.ir/article_59075.html

- صابری، سیاوش و انصاری دوست، شیما (بهار ۱۳۹۶). جرائم رایانه‌ای در حقوق ایران. *مطالعات علوم سیاسی، حقوق و فقه*. ۳(۱/۲)، صص۱۴۱- ۱۴۹. بازیابی از: https://b2n.ir/018478

- صفاری، علی (۱۳۸۱). انتقادات وارده به پیشگیری وضعی از جرم. *مجلهٔ تحقیقات حقوقی*. شمارهٔ ۳۵ و ۳۶. صص۲۳۳-۱۹۳. بازیابی از: http://ensani.ir/fa/article/download/7156

- قانون تجارت الکترونیکی. مصوب ۱۳۸۲.

- قانون تشدید مجازات مرتکبان اختلاس، ارتشا و کلاهبرداری. مصوب ۱۳۶۷.

- قانون جرائم رایانه‌ای. مصوب ۱۳۸۸.

- گسن، ریموند (۱۳۷۰). *جرم‌شناسی کاربردی* (مهدی کی‌نیا، مترجم). تهران: نشر مترجم.

- لازرژ، کریستین (۱۳۹۰). *درآمدی بر سیاست جنایی* (علی حسین نجفی ابرندآبادی، مترجم). تهران: نشر میزان.

- لعلی، عاطفه و معظمی، شهلا (۱۳۹۶). سیاست جنایی تقنینی ایران در قبال بزه‌دیدگی زنان. *مطالعات علوم سیاسی، حقوق و فقه*. ۳(۱)، صص۱۸۵-۱۹۶. بازیابی از: https://www.noormags.ir/view/fa/articlepage/1206273

- میر محمدصادقی، حسین و شایگان، محمد رسول (پاییز و زمستان ۱۳۸۶). راهکارهای مقابله با جرم کلاهبرداری رایانه‌ای در حقوق کیفری ایران. *فصلنامهٔ دیدگاه‌های حقوق قضایی*. شمارهٔ ۴۲ و ۴۳، صص۱۰۹-۱۲۶. بازیابی از: http://jlviews.ir/files/site1/files/x_211.pdf

- میرمحمدی صادقی، حسین و شایگان، محمد رسول (پاییز و زمستان ۱۳۸۹). بررسی تطبیقی کلاهبرداری سنتی و رایانه‌ای و مجازات‌های آن‌ها در نظام حقوقی ایران. *فصلنامهٔ*

دیدگاه‌های حقوق قضایی. شمارهٔ ۵۱ و ۵۲، صص۱۳۷-۱۶۲. بازیابی از:
http://jlviews.ir/files/site1/files/x_247.pdf
- نجفی ابرندآبادی، علی حسین (۱۳۷۹). *مباحثی در علوم جنایی؛ تقریرات درس جرم‌شناسی پیشگیری* (محمدعلی بابایی، گردآورنده). دورهٔ دکتری دانشگاه تربیت مدرس.
- نجفی ابرندآبادی، علی حسین (۱۳۸۲). *تقریرات درس جرم‌شناسی* (رضا فانی، گردآورنده). دورهٔ کارشناسی ارشد دانشگاه شهید بهشتی.
- نجیبیان، علی (۱۳۸۸). *موانع و محدودیت‌های پیشگیری وضعی از ارتکاب جرم*. پایان‌نامهٔ کارشناسی ارشد رشتهٔ حقوق جزا و جرم‌شناسی. دانشکدهٔ علوم اجتماعی دانشگاه بین‌المللی امام خمینی (ره).

منابع انگلیسی

- Cybercrime law of united states of America (2008). available at: https://fas.org/sgp/crs/misc/97-1025.pdf
- Doyle, Charles (2011). Mail and Wire Fraud: A Brief Overview of Federal Criminal Law, published by congressional research service, Washington.
- Marshall, H., Jarret & Bailie, W. (2007). michael, Prosecuting of cyber crime, published by legal education executive office for united states Attorneys, second edition, Department of justice,Washington D.C.
- International Telecommunication Union (2012). Understanding cybercrime: Phenomena, challenges and legal response,published by itu, Geneva.
- Finklea M. (2012). Kristin, Identity Theft: Trend and issue,published by congressional research service, Washington D.C.
- Spagnoletti, Paolo (2005). Situational Crime Preventionand Cyber-crime investigation, eurocon, Europian union.
- The National Fraud Center (2000). the growing treat of cybercrimes, Ucla University, Los Angeles.
- The white House (2011). International strategy for cyberspace, washimgton D.C.
- Twels, Joseph (2009). computer fraud,published by john willey and son, new jersey.
- U.S. Department of Defense (july 2011). strategy for operating in cyberspace, washimgton D.C.