فصلنامه علمی تخصصی
پژوهش‌های بازاریابی اسلامی
دوره ۳، شماره ۲، بهار ۱۴۰۴

بررسی تطبیقی مسئولیت کیفری مرتکبان جرایم مالی و اقتصادی در حوزه فناوری اطلاعات و ارتباطات با تاکید بر قوانین جزایی ایران، آمریکا و فقه اسلامی

آزاده عرب زاده کفاش[۱]، سلامه ابوالحسنی[۲*]، سید باسم موالی زاده[۳]، آلبوعلی، امیر[۴]

[۱] دانشجوی دکتری، گروه حقوق جزا و جرم شناسی، پردیس علوم و تحقیقات خوزستان، دانشگاه آزاد اسلامی، اهواز، ایران.

[۲] استادیار، گروه حقوق جزا و جرم‌شناسی، واحد تهران شمال، دانشگاه آزاد اسلامی، تهران، ایران.

[۳] استادیار، گروه حقوق، واحد اهواز، دانشگاه آزاد اسلامی، اهواز، ایرا ن.

[۴] استادیار، گروه حقوق، واحد اهواز، دانشگاه آزاد اسلامی، اهواز، ایرا ن.

تاریخ دریافت: ۱۴۰۲/۰۲/۲۹ تاریخ پذیرش: ۱۴۰۳/۰۴/۱۱ تاریخ انتشار آنلاین: ۱۴۰۴/۰۱/۰۱

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 نشان‌دهنده دیدگاه تك‌بعدی سیاست جنایی ایران است. در همین راستا، پژوهش حاضر در نظر دارد با تطبیق سیاست جنایی ایران و آمریکا نحوه جرم‌انگاری جرائم مذکور را مورد تحلیل و بررسی قرار دهد.

روش: تحقیق حاضر با توجه به نحوه گردآوری داده‌ها به روش اسنادی بوده که در این راستا ضمن مطالعه منابع کتابخانه‌ای و اینترنتی داخلی و خارجی مرتبط با موضوع از جمله کتب، پایاننامه‌ها و مقالات معتبر علمی، قوانین حوزه 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 ۱۲و ۱۳ قانون جرائم رایانه‌ای همراه با بردن یا ربودن مال دیگری شود، عنوان مجرمانه دارد و توجه‌ای 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 یك 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 به منظور برطرف ساختن نقاط ضعف قانون در دستور کار مراجع ذی‌صلاح قرار گیرد.

واژه‌های کلیدی: سیاست جنایی، کلاهبرداری سایبری، سرقت سایبری، قانون جرائم رایانه‌ای، ایران، آمریکا.

* نویسنده مسئول: سلامه ابوالحسنی، ایمیل: salameh_abolhasani@yahoo .com

مقدمه

اینترنت مانند دیگر پدیده ها و ابزارهای علمی و فنی نوین با وجود مزایا و منافع بسیار زیادی که دارد موقعیت های مخاطره آمیز جدیدی نیز برای افراد در تمام سطوح جامعه به وجود آورده است . پدیده اینترنت به لحاظ ویژگی های منحصر به فرد خود از دو جهت بر وقوع جرایم تاثیر گذاشته است. اول اینکه امکان ارتکاب رفتارهای ضد اجتماعی جدیدی را به وجود آورده است که پیش از پدید آمدن فن آوری اطلاعات به هیچ وجه امکان پذیر نبوده و دوم این که ارتکاب رفتارهای مجرمانه مرسوم را تسهیل نموده و هزینه ارتکاب آنها را بسیار کاهش داده است.

با توجه به نقش ارایه دهندگان خدمات اینترنتی در تهیه ابزار و تسهیل وقوع جرایم اینترنتی، نظام های حقوقی بسیاری از کشورها، برای آن دسته از ارایه کنندگان خدمات اینترنتی که آگاهانه وقوع جرایم اینترنتی را تسهیل کرده و با وجود توانایی از وقوع جرایم پیشگیری نمی کنند، مسوولیت کیفری در نظر گرفته اند و تحت شرایطی آنها را قابل تعقیب و مجازات می دانند.

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 نتیجه 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 به روز 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 پروسه جرم انگاری و تعیین مجازات جرم کلاهبرداری اینترنتی کمك گرفت. همچنین، برای رسیدن به کمال مطلوب طبیعتاً باید قانون کشورمان را با کامل‌ترین و به‌روزترین قانون دنیا در زمینه 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 به طور جداگانه جرم‌انگاری کرده است. به طور 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 به طور جداگانه از این دو جرم، در قانون ذکر شده و برای هر کدام با توجه به شرایط و نتیجه به دست آمده، مجازات متناسب در نظر گرفته شده است که همین مطلب روند کشف جرم و تطابق عمل با ماده 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 مطالعه 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. ایزدی فر و پیردهی (۱۳۸۹) در تحقیقی با هدف بررسی اینکه آیا سرقت اینترنتی در زمره سرقت حدی محسوب می‌شود یا در زمره سرقت تعزیری، به این نتیجه رسیده‌اند که چون در سرقت اینترنتی، بردن مال به صورت فیزیکی و با دستان در عالم واقع انجام نمی‌شود، پس در رده تعزیرات قرار می‌گیرد. میرمحمد صادقی و شایگان (۱۳۸۹) نیز در تحقیقی با عنوان «بررسی تطبیقی کلاهبرداری سنتی و رایانه‌ای و مجازات آن در حقوق کیفری ایران»، به این نتیجه رسیده‌اند که کلاهبرداری سنتی و اینترنتی شباهت زیادی دارن،د اما موضوع جرم این دو، وجه تمایزشان است که در یکی مال آنها و در دیگری داده‌ها هستند. همچنین، میرمحمد صادقی و شایگان (۱۳۸۶) در تحقیقی با عنوان «راهکارهای مقابله با جرم کلاهبرداری رایانهای در حقوق کیفری ایران»، به این نتیجه رسیده‌اند که آنچه در مقابله غیرکیفری از کلاهبرداری اینترنتی مهم و کاربردی است، پیشگیری اجتماعی و وضعی است. خرم‌آبادی (۱۳۸۶) نیز در تحقیقی با عنوان «کلاهبرداری رایانهای از دیدگاه بین‌المللی و وضعیت ایران»، به این نتیجه رسیده است که مهمترین 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 به دو صورت کیفر و پیشگیری است (مارتی، ۱۳۹۳، ص. ۷-۹) یا تعریف لازرژ که سیاست جنایی را دربردارنده مطالعه اقدامها و تدابیری میداند که دولت و جامعه مدنی به طور مستقل یا با مشارکت هم برای سرکوب پدیده مجرمانه، پیشگیری از آن و حمایت بزهدیدگان مستقیم و غیرمستقیم پیش‌بینی میکنند (رمضانی و علیزاده،، ۱۳۹۲ ص ۱۲۶). در این مقاله به جهت اهمیت بیشتر، فقط به سیاست جنایی تقنینی 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 زمینه یك پدیده مجرمانه است که توسط قانونگذار تدوین میشود و بیانگر سیاست جنایی تقنینی آن کشور در رابطه با همان پدیده مجرمانه است (لعلی و معظمی،، ۱۳۹۶ص ۱۸۷). 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 کاهش 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، ص ۲۸۷).

مسئولیت کیفری: امروزه پاسخدهی کیفری تنها بر انسان برنا،آگاه و خردمند بار می گردد ولی از جهت پیشینی،داستان درازی دارد که می توان کیفر چیزهای بی جان و نیز جانداران را در این داستان دید. بررسی کوتاه این داستان در راستای پیش کشیدن بستر پاسخدهی در فضای سایبر بایسته است. در گذشته سرزنش‌پذیری رفتار،نوعی بود و از هرکه و هرچیزی سرچشمه می گرفت،از دید مردمان،ناپسند و کیفر شدنی به چشم می آمد. این باور در درازای سده ها همچنان در ناخودآگاه آدمیان مانده و گاه گاه از سر خشم،کودک،جاندار یا حتی چیزهای بی جان را به درشتی می رانند. در همین زمان ما نیز می توان دید که کودک را برای کار ناپسندش یا جاندار را به دلیل ناپیروی اش آزار می دهند. این آزار و به سخن راست تر این کیفر دهی در سده های پیشین رسمی و پذیرفته شده بود. در سفر احبار یهود (بند های ۲۹ الی۳۲) آمده است :"هرگاه گاو نری بوسیله ضربات شاخ،مرد یا زنی را به قتل رساند بایستی چنین گاوی سنگباران گردد و گوشتش خورده نشود،در این مورد صاحب گاو را مسئولیتی نیست. همچنین در قرن چهاردهم یک خوک نر و سه خوک ماده که خوک چران خود را کشته بودند به حکم فیلیپ دوم فرزند پادشاه فرانسه محکوم به اعدام شدند. "پس از دگرگونی های پدیدآمده در حقوق کیفری و روی آوردن به شناخت بیشتر انجام دهندگان بزه،پاسخدهی کیفری نه تنها در مرز رفتارهای آدمیان جای گرفت بلکه در این میان برخی از انسانها که از برنایی،خردمندی،و آگاهی بی بهره یا کم بهره بودند نیز از تنگنای پاسخدهی کیفری بیرون گذاشته شدند.

فضای سایبر دو سنجه جداگانه و رو در روی هم،در ارزیابی و شناخت مسئولیت کیفری بنیان نهاده است. نخست اینکه با فرمانرانی آزادی در این فضا در سنجش با فضای بیرونی،برای مسئول دانستن اشخاص حقیقی،افزون بر بود رکن های مسئولیت،باید

اندیشه شریرانه و خواست فرد در وارد کردن زیان به دیگری نیز در میان باشد. از این رو در این فضا پیش بینی بزه های غیر عمدی یا بزه های مطلق که نتیجه ای در بر نداشته باشد بخردانه نخواهد بود مگر اینکه بزه مطلق با ویژگی های دیگری همراه باشد که سرزنش پذیری رفتار یا بدخواهانه بودن اندیشه فاعل آن را نشان دهد مانند بزه دسترسی غیرمجاز به سامانه دیگری که یک رفتار بدون زیان بوده و به خودی خود بزه به شمار نمی رود مگر اینکه سامانه گفته شده دارای تدبیرهای حفاظتی و امنیتی باشد که دسترسی غیرمجاز به جهت این ویژگی،کیفر شدنی خواهد بود نه تنها به جهت انجام رفتار دسترسی[۱].

دوم اینکه با وابستگی همه کارها و برنامه ها به فضای فناوری اطلاعات،هررفتار ضد هنجار یا زیان آور در فضای سایبر می تواند به پیامدهای نگران کننده بینجامد که بیشتر آنها چهره گسترده و جهانی به خود می گیرند. همین پیامدها سبب شده است تا ویژگی آزاد بودن فضای سایبر در تنگنا قرار بگیرد و در سنجش با فضای بیرونی،رفتارهای مطلق یا غیر عمدی کاربران،خطرناک گردند. از این رو مسئولیت کیفری در فضای سایبر بر وارونه فضای بیرونی کمتر بر پایه سرزنش اخلاقی که بیشتر بر ستون زیان های دسته جمعی و حتی جهانی قرار دارد. بدین حال شمار بزه های فضای سایبر روز به روز در حال افزایش بوده و در میان آنها، رفتارهای غیر عمدی نیز رو به فزونی اند. همین رویکرد در قانون جرایم رایانه ای دیده می شود. چندانکه از هنگام دسترسی غیر مجاز به یک سامانه،هر رفتار شخص ممکن است عنوان های گوناگونی مانند جاسوسی،شنود، سرقت، تخریب و اختلال بیابد. جدا از فراوانی بزه ها در فضای سایبر که خود سبب گستردگی مسئولیت کیفری است،فراوانی اشخاص حقوقی در فضای سایبر نیز خود،مرزهای مسئولیت کیفری را گسترانیده است. اگر در فضای سنتی،مسئولیت کیفری اشخاص حقوقی هنوز جای گمان و پرسش دارد ولی در فضای سایبر که کنشگران بر جسته و بازیگران اصلی آن،اشخاص حقوقی اند. مسئولیت کیفری اینگونه اشخاص از بایسته های بنیادین حقوق کیفری سایبری است. هرچند فضای سایبر رهاورد دولت و به ویژه نیروی انتظامی ایالات متحده برای همه کشورهاست ولی نمی توان دولتها را دارنده و حتی کنترل گر آن دانست. به راستی که در سنجش هماوردی میان بخش خصوصی و بخش دولتی،باید فرمانروایان فضای سایبر را بخش خصوصی دانست. شرکت هایی مانند گوگل یا یاهو بدون پیوند مستقیم با دولتها حتی خود در مقام آموزش شیوه تعامل درست با فضای سایبر بر می آیند. چندانکه پا را فراتر گذاشته و دولتهای قدرتمندی چون چین را به جهت سرکوب آزادی ها در فضای سایبر هشدار می دهند[۲].

برخی کشورهای اقتدارگرا یا نامردم سالار شتاب و ظرفیت مبادلات اینترنتی را خود تعیین می کنند و می کوشند تا از گوشه های پنهان پیوندهای شهروندان سر در بیاورند. ولی روی هم رفته فضای سایبر با واسطه گری شرکت ها و اشخاص حقوقی در دسترس شهروندان قرار می گیرند. از این رو بر خلاف سپهر فیزیکی، فضای سایبر از پیش برای همگان آفریده نشده و در دسترس آنها قرار نمی گیرد. همین نکته،نقش اشخاص حقوقی را در فضای سایبر نشان می دهد و می توان گفت که در این فضا پیش از مسئولیت اشخاص حقیقی،مسئولیت اشخاص حقوقی پیش کشیده می شوند.

قانونگذار ایران نیز هرچند تا کنون در پیش بینی مسئولیت کیفری اشخاص حقوقی پر گمان بوده ولی نقش رسانه های اینترنتی(ارائه کنندگان خدمات اینترنتی) در فضای سایبر و شمار فراوان آنها، سبب شد تا با وجود انحصار گری دولت ایران در فضای سایبر، مسئولیت کیفری اشخاص حقوقی را به روشنی بپذیرد.

قانون جرایم رایانه ای سرانجام در سال ۱۳۸۸ تصویب شد تاکشور ما گامی دیگر درمبارزه با پدیده جرم بردارد. با تصویب این قانون دیگر لازم نیست قضات جرایم ارتکابی را باموادقانونی قبل از تصویب قانون جرایم رایانه ای تطبیق دهند. چه بسا این تلاش آنها ره به جایی نمی برد و نتیجه آن تباهی حقوق بزه دیدگان و جامعه در برابر بزهکاران می شد. اگرچه این قانون کاستی هایی دارد ولی همینکه کشور ما دارای قانونی برای جرایم رایانه ای شده است، جای بسی امیدواری به آینده داستان مبارزه همیشگی با بزهکاران

---

۱ . عالی پور، حسن . ۳۹۰) . حقوق کیفری فناوری اطلاعات، انتشارات خرسندی، چاپ اول، ص ۵۳ .

۲ . ابر شرکت گوگل رویکرد کشورهایی مانند ایران و چین نسبت به اینترنت و ارتباطات آزاد در آن را یک چالش فراروی خود می داند و به چنین کشورهایی انتقادات تندی وارد کرده است .ر .ک به وبگاه فارسی بی بی سی ۱ ۲ ۲۰۱۰

دارد. فصل ششم این قانون به یکی از بحث برانگیزترین مباحث حقوق کیفری یعنی مسئولیت کیفری اشخاص حقوقی مربوط می شود که می توان گفت در مقایسه با قوانین قبلی کاملتر نگاشته شده است.

بر پایه ماده ۱۹ قانون جرایم رایانه ای در موارد زیر چنانچه جرایم رایانه ای 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 رایانه ای شود.

ب)هرگاه مدیر شخص حقوقی دستور ارتکاب جرم رایانه ای صادر کرده و جرم به وقوع بپیوندد.

ج)هرگاه یکی از کارمندان شخص حقوقی با اطلاع مدیر یا در اثر عدم نظارت وی مرتکب جرم رایانه ای شود.

د)هرگاه تمام یا قسمتی از فعالیت شخص حقوقی به ارتکاب جرم رایانه ای اختصاص یافته باشد.

ماده پیش گفته،تشخیص مسئولیت کیفری اشخاص حقوقی از حقیقی را پیرو سه سنجه دانسته است که هر سه اینها باید در کنار هم وجود داشته باشند.

سنجه نخست آنکه بزه رایانه ای بنام شخص حقوقی انجام شود. شخص حقوقی هر شرکت یا موسسه ای است که به ثبت رسیده باشد. اگر شخص حقوقی به ثبت نرسیده باشد از نگاه قانون شخصیت نداشته و هر گروه یا هیأتی که در پیکره یک شرکت یا مؤسسه مرتکب بزه شود، بر پایه قاعده های عمومی حقوق کیفری پیگرد می شوند. با این حال به نظر می رسد که میان شخص حقوقی در حقوق کیفری با شخص حقوقی در روابط خصوصی و تجاری باید جدایی انداخت. در روابط تجاری،قانون تجارت به شرکت های تجاری شخصیت حقوقی بخشاییده است، همچنانکه ماده ۵۸۳ این قانون می گوید کلیه شرکت های تجاری مذکور در این قانون شخصیت حقوقی دارند. با وجود دیدگاههای گوناگون در این زمینه،این ماده و ماده ۵۸۴ نشان می دهد که قانون گذار شرکت تجاری به ثبت نرسیده را یک شخص حقوقی می داند ولی شرکت غیر تجاری را خیر. بر پایه ماده ۵۸۴ تشکیلات و مؤسساتی که برای مقاصد غیر تجاری تأسیس شده یا بشوند از تاریخ ثبت در دفتر ثبت مخصوصی که وزارت عدلیه معین خواهد کرد شخصیت حقوقی پیدا می کنند. حال با نگاه به قانون تجارت مصوب ۱۳۱۱ چهار گونه از شیوه شخصیت یابی را می توان دید؛ یکم:شرکت های دولتی و بلدی که به محض ایجاد شخصیت حقوقی دارند و این به جهت این است که دولت که خود دهنده شخصیت حقوقی به شرکت هاست در اینجا پدیدآورنده شرکت است. طبق ماده ۵۸۷ مؤسسات و تشکیلات بلدی و دولتی به محض ایجاد و بدون احتیاج به ثبت دارای شخصیت حقوقی می شوند.

دوم: شرکت‌های تجاری که با روی آوردن به ماده ۵۸۳ همچون شرکت‌های دولتی به محض بنیادگیری، شخصیت حقوقی دارند.

سوم:شرکت های غیر تجاری که برای شخصیت یابی باید به ثبت برسند و پیش از آن شخصیت حقوقی ندارند.

چهارم: شرکت‌های نامشروع از ریشه نمی‌توانند به عنوان شخص حقوقی به شمار آیند. طبق ماده ۵۸۶ قانون تجارت، مؤسسات و تشکیلاتی که مقاصد آنها مخالف با انتظامات عمومی یا نامشروع است نمی توان ثبت کرد. بنابراین بزه رایانه ای را یا شرکت های ثبت شده انجام می دهند یا شرکت های دولتی یا تجاری و در این حال شرکت های ثبت نشده از بار مسئولیت کیفری رهیده‌اند.

باید پذیرفت که در حقوق کیفری بر وارونه دیگر شاخه های حقوق، شرکت ها و مؤسسه ها موضوع حق و تکلیف مدنی نیستند بلکه باید از این نگاه به آنها نگریسته شود که یک اراده گروهی یا جمعی سبب انجام بزه شده است. خواه این گروه یا جمع در پیکره یک شرکت یا مؤسسه ثبت شده اند یا خیر ولی در هر حال شخص حقوقی به شمار می‌روند. به سخن دیگر در حقوق کیفری، شخص حقوقی را باید از جهت ماهیت،کارکرد و اراده مشترک سنجید و ثبت آن تنها یک شرط شکلی برای برخورداری از حق ها و تکلیف‌هاست.

سنجه دوم برای پاسخدهی کیفری شخص حقوقی،آنکه بزه رایانه ای در راستای سود آن شخص انجام شود و به سخن دیگر بزه باید بهره ای برای شرکت به همراه داشته باشد. این سنجه نشان می دهد که اگر در میان کارها و کنش های تجاری یا غیر تجاری شرکت،بزه رایانه ای نیز رخ دهد سبب مسئولیت کیفری شخص حقوقی نمی گردد مگر اینکه ثابت شود که انجام آن به سود شخص حقوقی بوده است. سود شخص حقوقی در اینجا نتیجه بزه رایانه ای نیست بلکه هدف و انگیزه انجام است و به دست آمدن سود برای

شخص حقوقی پرده از این هدف و انگیزه بر می دارد.

سنجه سوم برای مسئولیت، انجام رفتار از سوی کسان وابسته به شخص حقوقی است که می تواند به چهار حالت نمود پیدا کند:

اول- مرتکب جرم مدیر باشد- تبصره ۱ ماده ۱۹ مدیر را کسی تعریف می کندکه اختیار تصمیم گیری یا نمایندگی و یا نظارت بر شخص حقوقی را دارد. در ابتدا لازم است گفته شود؛ بهتر بود مقنّن به جای واژه "کسی" از واژه "شخصی" استفاده می کرد، چرا که اشخاص حقوقی نیز می توانند مدیر باشند[1]. از سوی دیگر مطابق این تعریف مجامع عمومی وبازرسان شرکت سهامی نیز مدیر محسوب می‌شوند. مطلب قابل ذکر این است که اگر اشخاص تصمیم گیرنده، بیش از یکی باشند، در صورتیکه هر یک به تنهایی اختیار تصمیم گیری داشته باشند، انجام جرم از سوی یکی از آنها برای تحقّق مسئولیت کیفری شخص حقوقی کافی است. ولی اگر به موجب مقرّرات حاکم برشخص حقوقی لازم باشدکه تصمیمات به اتفاق یا اکثریت اعضاگرفته شود،در این صورت چه کسی یا چه کسانی باید جرم را انجام دهند؟ یک تفسیر آن است که جرم را باید آن تعداد اشخاصی که رأی موافق آنها برای اتخاذ تصمیم در سازمان شخص حقوقی کافی است، بامشارکت هم انجام دهند.

زیرا یک نفراختیار تصمیم گیری ندارد و اجتماع مدیران است که می توانند تصمیم گیری کنند. از سوی دیگر مباشرین جرم، بایدمطابق قواعد عام جزایی،دارای مسئولیت کیفری شناخته شوند؛ برای مثال مستی یکی از اعضا در هنگام ارتکاب جرم، مانع تحقّق مفهوم مشارکت در جرم خواهد شد به شرطی که فقدان اوتعداد اشخاص شرکت کننده در جرم را از تعداد اشخاصی که رأی موافق آنها برای تصمیم گیری کافی است، کمتر نماید. این تفسیر گرچه به نفع متّهم خواهد بود، ولی راه را برای سوء استفاده اشخاص حقوقی بازخواهد کرد؛ برای مثال اگر هم اعضای هیئت مدیره با ارتکاب جرم موافق باشند وتنها یکی از آنها جرم را انجام دهد، شخص حقوقی طبق هیچ بند ماده ۱۹ قابل مجازات نیست، درحالیکه هیچ کس در شایستگی شخص حقوقی برای تحمل مجازات تردیدی نخواهد کرد. ازسوی دیگر این راه حل در مواردی کاربرد دارد که تعداد اعضای تصمیم گیرنده کم باشدتا بتوانند با مشارکت هم جرم را انجام دهند. ولی در مواردی که تعداد اعضا زیاد است؛ برای مثال مجامع عمومی سهامداران، تصور اینکه اکثریت یا تمام سهامداران با مشارکت هم جرم را انجام دهند مشکل است. در اینجا نمی توان تصور کردکه هیئت مدیره بتواند به شخصی نمایندگی دهد تا جرمی را به نام و حساب هیأت مدیره انجام دهد وآثار جرم دامنگیر هیأت مدیره شود. زیرا اعطای نمایندگی برای اعمال حقوقی است، در حالیکه ارتکاب جرم یک واقعه حقوقی است. از طرفی آثار جرم دامنگیر نماینده نیز می شودکه این برخلاف قواعد نمایندگی است. حتّی اگر هیأت مدیره به یکی از اعضای خود دستور ارتکاب جرمی را بدهد، باز عمل مشمول بند "الف"قرار نمی گیرد، بلکه مشمول بند "ج"خواهد بود. ولی اگر هیأت مدیره به موجب مقرّرات حاکم بر شخص حقوقی اختیار داشته باشد که اختیار تصمیم گیری را به یک نفر واگذار کند، در این صورت ارتکاب جرم توسط آن شخص برای تحقّق مسئولیت کیفری شخص حقوقی کافی است.

از سوی دیگر می توان گفت ماده منصرف به موردی است که تنها یک شخص در سازمان شخص حقوقی دارای اختیار تصمیم گیری است و یا اگر به بیش از یک تن اختیار تصمیم گیری داده شده است هر کدام به تنهایی اختیار تصمیم گیری دارند. ولی اگر تصمیمات باید به اتفاق یا اکثریت اعضا گرفته شود، ارتکاب جرم از سوی هریک از اعضا برای تحقّق مسئولیت کیفری شخص حقوقی کافی است . اشکال این تفسیر همان طور که گفته شد این است که یک نفر اختیار تصمیمگیری ندارد و اجتماع اعضاست که اختیار تصمیم گیری دارند. تفسیر سوم این است که در مورد مجامع عمومی جرم را باید آن تعداد اشخاصی که رأی موافق آنها برای اتخاذ تصمیم در سازمان شخص حقوقی کافی است، با مشارکت هم انجام دهند؛ ولی در مورد هیأت مدیره به معنای اخص (رکن اداره کننده) انجام جرم از سوی هر یک از اعضا کافی است. در مورد ناظر شخص حقوقی، حتّی اگر بیش از یک نفر باشند، ارتکاب جرم از سوی یکی از آنها برای تحقّق مسئولیت کیفری شخص حقوقی کافی است،زیرا در نظارت بحث رأی گیری و اکثریت

---

۱. ماده ۱۱۰ لایحه اصلاحی قانون تجارت، مصوب ۱۳۴۷.

در تصمیم گیری مطرح نمی شود، بنابراین حتّی اگروظیفه نظارت برعهده چندین شخص باشد، باز هم به هر یک از آنها عنوان ناظر اطلاق می شود. در صورتی که نماینده بیش از یک نفرباشد، اگر هر یک از نمایندگان به تنهایی اختیار نمایندگی داشته باشند، انجام جرم از سوی یکی از نمایندگان، برای تحقّق مسئولیت کیفری شخص حقوقی کافی است. ولی اگر هیچ کدام به تنهایی اختیار نمایندگی نداشته باشند، لازم است جرم به مباشرت همه نمایندگان انجام شود.

دوم-مرتکب جرم کارمند باشد- مطابق بند ب ماده ۱۹ شخص حقوقی وقتی از ارتکاب جرم توسط کارمند خود مسئولیت کیفری می یابد که کارمند جرم را در اثر عدم نظارت مدیر شخص حقوقی و یا با اطّلاع او انجام داده باشد. پرسشی که ممکن است مطرح شود این است که آیا صرف اطّلاع مدیر از ارتکاب جرم کافی است یا اینکه علاوه بر آگاهی از ارتکاب جرم، لازم است از ارتکاب جرم نیزرضایت داشته باشد؟ فرض کنید آبدارچی شرکت به مدیرشرکت اطّلاع می دهدکارمندی در حال تخریب داده های شرکت رقیب است، مدیر برای جلوگیری از ارتکاب جرم به اتاق کارمند مزبور می رود و بعد از بحث و جدل ودرگیری فیزیکی با کارمند، توسط ضربه ای که کارمند به سر او وارد می کند، بیهوش می شود ودر نهایت،کارمند جرم را به پایان می رساند؛ حال آیا به صرف اطّلاع مدیر از ارتکاب جرم می توان شخص حقوقی را دارای مسئولیت کیفری دانست؟ ظاهر ماده ۱۹ به پرسش فوق پاسخ مثبت می دهد؛ اما تفسیر به نفع متّهم و تفسیر منطقی ماده، پرسش بالا را با پاسخ منفی روبرو می کند. توضیح آنکه دلیل وضع بند" ب" این بوده که مدیر شخص حقوقی در صورت آگاهی مانع ارتکاب جرم شود وکارمندان شخص حقوقی با خیالی آسوده به سراغ جرم نروند. از طرفی مدیران نمایندگان شخص حقوقی هستندوتقصیرآنها تقصیر شخص حقوقی محسوب می شود؛در حالیکه در اینجا شخص حقوقی تقصیری مرتکب نشده است؛ چون مدیران تقصیری مرتکب نشده اند. آیا در این صورت می توان مدیری که در جلوگیری از ارتکاب جرم ناتوان بوده را به صرف آگاهی از ارتکاب جرم مقصر دانست و شخص حقوقی را مجازات کرد؟بنابراین لازم است ثابت شود که مدیر از ارتکاب جرم رضایت داشته است. مطلبی که باید به آن توجه کرد این است که اگر مدیری بداند کارمندی درحال ارتکاب

جرم است ولی نداند نوع جرم چیست یا اینکه کارمندی به مدیر اطّلاع دهدکه قصد ارتکاب جرمی رایانه ای را دارد بدون اینکه نوع جرم را بیان کند، با جمع بودن سایر شرایط، شخص حقوقی مسئولیت کیفری دارد. زیرا در اینجا عدم اقدام مدیردر کسب آگاهی از نوع جرم به معنی رضایت او به ارتکاب مطلق جرم بوده است. حال اگر کارمند به مدیر اطّلاع دهد که برای مثال قصد دارد داده های شرکتی را تخریب کند ولی کارمند جرم جعل را انجام دهد،آیا شخص حقوقی مسئولیت کیفری خواهد داشت؟همان طور که گفته شد بستگی به این امر دارد که آیا عدم اقدام مدیردرآگاهی از نوع جرم به معنی رضایت او به مطلق جرم بوده است یا خیر؟ در این مثال اگر اعتماد مدیر به گفته کارمند به حدی بوده است که عدم اقدام او را توجیه کند، شخص حقوقی مسئولیت نخواهد داشت. از سوی دیگر مدیر از ارتکاب جرم جعل بی اطّلاع بوده است و جرم تخریب داده نیز به وقوع نپیوسته تا بتوان گفت مدیر از جرم تخریب اطّلاع داشته است. مطلب قابل ذکر در مورد عدم نظارت مدیران است که این عدم نظارت باید ناشی از یک دلیل غیر موجه باشد. توضیح آنکه مقنّن عدم نظارت ناظررا به عنوان تقصیر ناظر و در نهایت تقصیر شخص حقوقی دانسته است . حال اگر ناظر برای عدم نظارت خود دلیل موجهی داشته باشد، آیا می توان گفت تقصیری مرتکب شده است؟ فرض کنید شخص "الف" که وظیفه داشته برکارمندان بخش معینی نظارت کند در اثر تصادف رانندگی بیهوش شده و چند روزی در این وضعیت باقی بماند؛در نتیجه این عدم نظارت، یکی ازکارمندان شرکت مرتکب جرمی شود. در این صورت آیا می توان گفت که ناظر در انجام وظیفه خود کوتاهی کرده است؟از سوی دیگرمحدوده نظارت ناظر باتوجه به مقرّرات حاکم بر شخص حقوقی مشخص می شود و نمی‌توان ناظر شخص حقوقی را در همه حال موظف به نظارت بر کارمندان دانست. برای مثال اگر کارمند شرکتی در خارج از ساعات کاری بدون اطّلاع ناظر شرکت به قصد سود رساندن به شرکتی که عضو آن است، داده های شرکت رقیب را تخریب کند، نمی توان گفت شرکت مسئولیت کیفری دارد، زیرا از حیطه نظارت ناظر بر کارمند خارج است. ولی اگر ناظر شرکت از ارتکاب جرم توسط کارمند با خبر باشد، حتّی اگر در خارج از ساعات کاری باشد، شخص حقوقی مسئولیت کیفری خواهد داشت.

آنچه لازم است مورد توجه قرار گیرد این است که اطّلاع هر یک از ارکان تصمیم گیرنده، نظارت کننده ونماینده از ارتکاب جرم کافی است ولی عدم نظارت شخصی ملاك است که به موجب مقرّرات حاکم بر شخص حقوقی این وظیفه را داشته باشد.

سوم- جرم با دستور مدیر ارتکاب یابد- پرسشی که ممکن است مطرح شود این است که اگر مدیر شخص حقوقی" الف " در سازمان شخص حقوقی "ب" نیز سمت مدیریت را داشته باشد و دستور ارتکاب جرمی را به یکی از کارکنان شخص حقوقی"ب" دهد تا جرمی را به نام و در راستای منافع شخص حقوقی"الف" انجام دهد،آیا در صورت تحقّق جرم،شخص حقوقی الف مسئولیت کیفری دارد؟

ظاهر بند ج ماده ۱۹ این برداشت را به ذهن متبادر می کند، اما فلسفه وضع این بند به پرسش بالا پاسخ منفی می دهد. زیرا علت وضع این بند جلوگیری از سوء استفاده مدیر از اختیار صدور دستوری است که شخص حقوقی به او اعطاکرده، در حالیکه مدیر اشخاص حقوقی "الف"و"ب" از اختیارات صدور دستوری که شخص حقوقی الف به او عطا کرده سوء استفاده نکرده است، ازاینرو عادلانه نیست که شخص حقوقی " الف " مجازات شود. بدین ترتیب می توان این چنین نتیجه گرفت که انجام دهنده دستور باید شخصی باشد که مدیر به موجب مقرّرات حاکم بر شخص حقوقی، اختیار صدور دستور به او را داشته باشد. پس اگر مدیر شرکتی به مستخدم منزل خود دستور انجام جرمی را بدهد، شرکتی که مدیر عضو آن است، مسئولیت کیفری نخواهد داشت؛چون اختیاری که مدیربرای صدور دستور به مستخدم دارد، به موجب مقرّرات حاکم بر شرکت به مدیر داده نشده است. پرسش دیگری که ممکن است مطرح می شود این است که اگر مدیر دستور ارتکاب جرم خاصی را صادر کند ولی کسی که دستور مدیر را انجام می دهد جرم دیگری را انجام دهد،آیا شخص حقوقی مسئولیت کیفری خواهد داشت؟ علاوه بر تفسیر به نفع متّهم، نمی توان گفت جرمی که انجام گرفته دستور مدیر است؛ در واقع ماهیت عمل ارتکابی، با دستور مدیر یکی نیست تا بتوان گفت جرم با دستور مدیر انجام گرفته است. در واقع مرتکب دستور مدیررا انجام نداده است. البته بایداحراز شود اعتماد مدیر به مأمور به اندازه ای بوده است که عدم نظارت مدیر را بر روند ارتکاب جرم توجیه کند. مگر اینکه کسی که جرم را انجام می دهد مدیر دیگری در سازمان شخص حقوقی باشد که در این صورت با جمع بودن سایر شرایط ماده ۱۹ خواهد شد. بنابراین شرط دوم این است که مأمورهمان جرمی را انجام دهدکه موضوع دستور مدیر بوده است. ولی اگر مدیر دستور ارتکاب مطلق جرم را داده باشد، در این صورت با جمع بودن سایر شرایط، شخص حقوقی مسئولیت کیفری خواهد داشت. از سوی دیگر عمل مشول بند ب نیز می تواند قرار گیرد به شرطی که انجام دهنده دستور،کارمند باشد؛ زیرا هرکس که دستور ارتکاب جرمی را می دهد از ارتکاب آن نیز اطّلاع دارد.

چهارم-تمام یا بخشی از فعالیت شخص حقوقی به ارتکاب جرم اختصاص یافته باشد_ تنها مطلب قابل ذکر در مورد این بند این است که منظور قانون گذار این بوده که شخص حقوقی با رعایت شرایط قانونی بوجود آمده است و بعد از کسب شخصیت، موضوع فعالیت خود را به ارتکاب جرم اختصاص داده باشد. زیرا به موجب قانون مدنی جهت قرارداد باید مشروع باشد، بنابراین قراردادی که موضوع آن ایجاد شخصیت حقوقی با هدف ارتکاب جرم باشد باطل است و در نتیجه شخصیتی بوجود نخواهد آمد.

به هر حال فضای سایبر هم سبب گسترش و نیرومندی اشخاص حقوقی و شرکت ها شده و هم زمینه مناسبی برای انجام بزه های مالی و اقتصادی فراهم ساخته است. همین نکته نیز در حقوق کیفری ایران،یکی از بزرگ ترین دگرگونی ها را پدیدآورده است و آن پذیرش مسئولیت کیفری اشخاص حقوقی است. هرچند سال های کنونی برخی مقرره های دیگر نیز به طور ویژه و محدود به این گونه از مسئولیت پرداخته اند ولی قانون جرایم رایانه ای راه را به گونه ای هموار ساخته که حتی در قانون مجازات اسلامی جدید در ماده ۲۰،مسئولیت کیفری اشخاص حقوقی با الگو برداری از قانون جرایم رایانه ای به رسمیت شناخته 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 تفکیك آنها از هم نسبت به این جرائم انجام نداده و فقط یك 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 یك از مصادیق این جرائم کرده و مجازات آنها را نیز با توجه به شرایط و نتیجه جرم ارتکابی تعیین کرده است که این موضوع نشان‌دهنده 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، به طور جداگانه بکار برد.

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

در این قسمت ابتدا ماده ۱۲ و ۱۳ قانون جرائم رایانه‌ای ایران مورد بررسی قرار می‌گیرد و سپس به تحلیل مواد ۱۳۴۳-۱۰۳۷-۱۰۲۸-۱۰۲۹-۱۰۳۰-۱۰۲۸A از بخش ۱۸ قانون جزایی فدرال آمریکا که به سرقت و کلاهبرداری سایبری اختصاص دارند، پرداخته می‌شود. ماده 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 تشکیل‌دهنده این جرم را تحلیل کرد و به دنبال آن نقاط ضعف و قوت ماده 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، وسیله ارتکاب جرم است، دوم موضوع جرم و دیگری فضا و بستری است که امکان ارتکاب جرم در آن فراهم می‌شود. در اینجا وسیله ارتکاب جرم، رایانه است و موضوع سرقت سایبری، داده‌های دیجیتالی و بستر ارتکاب جرم، فضای سایبر است (خرم‌آبادی،، ۱۳۸۶صص۸۴-۸۵).

الف) ماده ۱۳ قانون جرائم رایانه‌ای: ماده ۱۳ قانون جرائم رایانه ای که عنصر قانونی جرم کلاهبرداری سایبری است، عنوان می‌کند: «هرکس به طور 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،، ۱۳۹۰ص ۳۰۴). به هر ترتیب، در ادامه سعی بر آن است تا براساس قانون مذکور، عناصر جرم کلاهبرداری اینترنتی تفکیك و تحلیل شود. با بررسی ماده 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، ص ۷)؛

۳- در کلاهبرداری سنتی، تأثیر مانور متقلبانه بر بزه‌دیده از طریق فریب برای تحقق عنوان مجرمانه ضروری است، یعنی لازمه

کلاهبرداری، فریب خوردن شخص است(میرمحمدصادقی و شایگان،، ۱۳۸۶ص۱۱۲).

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،، ۱۳۹۳ص ۲۶۴). 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،، ۱۳۸۵ص ۴۵). 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،، ۱۳۸۶صص۱۰۴-۱۰۳).

ب) مواد ۱۰۲۹، ۱۰۳۰، ۱۰۳۷، ۱۰۲۸A، ۱۰۲۸ 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 به طور مفصل شرح داده که شش ماده آن مربوط به کلاهبرداری اینترنتی و انواع صور آن می‌شود. پروسه قانونی تصویب این بخش تا سال ۱۹۸۵ طول کشید و سرانجام این اصلاحات در سالهای ۲۰۰۷ و ۲۰۰۱، ۱۹۹۲، ۱۹۹۱، ۱۹۹۰، ۱۹۸۹، ۱۹۸۸ ادامه داشت تا در نهایت قانون، جرائم سایبر فعلی به تصویب کنگره رسید (مارشال و بیلی[1]، ۲۰۰۷، ص ۲۰). بخشهای مرتبط با کلاهبرداری اینترنتی در قسمت ۱۸ قانون جزای آمریکا شامل مواد ۱۰۳۷، ۱۰۲۸، ۱۰۳۰، ۱۰۲۹، ۱۰۲۸ 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).

- ماده ۱۰۲۸: سرقت هویت و مشخصات دسترسی: در این ماده عنوان شده، هر شخصی آگاهانه و بدون مجوز قانونی یك 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 ۲۰، ۱۵ و ۳۰ سال در نظر گرفته است. همچنین، قانون‌گذار فدرال در ادامه اصلاحاتی را همچون «ساختن مدارك»، «مدارك هویت»، « مدارك 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.

- ماده 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، ص ۲).

- ماده 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 به طور 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 یك سال و با چنین ابزاری هر چیزی به ارزش ۱۰۰۰ دلار یا بیشتر کسب کند؛

1. Marshall & Bailie
۲. Cybercrime Law of United States of America
۳. Finklea

۳- آگاهانه و با قصد فریب دادن، ۱۵یا 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[۱]، ۲۰۰۰، ص ۳۵).

- ماده 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 وسیله 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 تعریف شده 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 یك یا حاوی فایل سازمان گزارش دهنده مشتری در مورد یك مشتری مانند عباراتی که در قانون امور اعتباری تعریف شده است نیز جرم‌انگاری شده است(اتحادیه بین‌المللی ارتباطات[۲]، ۲۰۱۲، ص۳۲۴).

- ماده ۱۰۳۷: کلاهبرداری و جرائم وابسته در ارتباط با نامه‌های الکترونیك: در متن این ماده، قانون‌گذار توضیحاتی درباره عناصر جرم داده است که در ادامه، نکات کلیدی و مهم این ماده ذکر خواهد شد. در این ماده عنوان شده، به طور کلی هر کس که به نوعی در تجارت خارجی و بین ایالتی نقشی داشته باشد و آن شخص آگاهانه، به رایانه 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 رایانه محافظت شده برای توزیع یا ارسال مجدد پیامهای پست الکترونیك 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 الکترونیك تجاری چندگانه و آغاز عمدی ارسال چنین پیامهایی یا با استفاده از اطلاعاتی که هویت ثبت‌کننده واقعی را جعل می‌کند، در این سایت‌ها ثبت‌نام و برای ۵ حساب پست الکترونیك 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[۳]، ۲۰۰۹، ص ۲۸۳). همچنین، اگر شخص با قصد فریب اقدام به نشان دادن خود به صورت ثبت‌کننده یا جانشین مشروع او برای ثبت 5یا 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.

- ماده 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 وسیله جعل یا بازنمایی تقلبی 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 یك مؤسسه مالی بگذارد، این شخص باید کمتر از ۱/۰۰۰/۰۰۰

۱. The National Fraud Center

۲. International Telecommunication Union

۳. Twels

دلار جریمه شود و کمتر از ۳۰ سال زندانی شود یا به هر دو مجازات محکوم شود (دویل[1]، ۲۰۱۱، صص۲-۱).

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 گونه 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 به طور 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، صص. ۹۰-۹۱؛ گسن، ۱۳۷۰، ص ۱۳۳). 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،۱۳۷۹ص ۷۲۴). در مقابل مفهوم موسع پیشگیری، مفهوم مضیق پیشگیری قرار دارد که 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 نوبه خود فرصتهای مناسبی را برای ارتکاب جرم ایجاد می‌کنند(نجفی ابرندآبادی، ۱۳۷۹، ص. ۷۵۰). 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،،۱۳۸۲ص ۱۲۰۸). همچنین، پیشگیری اجتماعی شامل اقدامهایی است که به طور مستقیم یا غیرمستقیم، هدفشان تأثیرگذاری بر شخصیت افراد است تا از سازمان دادن فعالیت خود حول انگیزه‌های بزه‌کارانه بپرهیزند(گسن،،۱۳۷۰ص ۷۸). 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 به ویژه 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،،۱۳۹۰ص ۱۲۸). 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.

---

۱. Doyle

- پیشگیری اجتماعی جامعه مدار سایبری: هدف از این تدابیر، جلوگیری از شکل‌گیری یا بروز انگیزه مجرمانه در عموم جامعه به وسیله 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 وسیله پیشگیری اجتماعی جامعه‌مدار سایبری، از طریق آموزشهای عمومی و رسانه‌های جمعی است. باید توجه داشت که اهمیت خاص تحقیق در زمینه 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،،۱۳۸۸صص ۴۰-۴۱). همچنین، اثربخشی هر چه بیشتر انواع راههای پیشگیری ذکرشده نسبت به کلاهبرداری، نیازمند یك سیاست جنایی مشارکتی فعال است. از لحاظ مفهومی، سیاست جنایی مشارکتی، بررسی و مطالعه جایگاهی است که در سیاست جنایی یك کشور به جامعه مدنی و از طریق اعطای نقش به بزهکار، بزه‌دیده و به ویژه کل جامعه و مردم داده شده است (لازرژ،،۱۳۹۰ص ۶۱). کارکرد این نوع از سیاست جنایی نسبت به کلاهبرداری اینترنتی، اقدامات در مرحله کشف جرم، تعقیب دادرسی و اجرای حکم را در برمیگیرد که با همکاری وسیع جامعه مدنی، نهادهای مردمی و نیروهای دولتی مانند پلیس، سازمان زندانها و غیره با دستگاه قضایی انجام می‌شود(باصری،،۱۳۸۷ص ۳۷) پس از ارائه توضیحات مربوط به این بخش و با جمعبندی آن میتوان انتقادهایی را بر به کارگیری 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 پیشگیرانه معطوف به اوضاع و احوالی که جرائم ممکن است در آن وضعیت به وقوع بپیوندد، به طوری 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 به طور 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 ارائه‌دهنده 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، ۶۹-۷۲و صفاری، ۱۳۸۱، صص ۱۹۴-۱۹۸).

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 به کارگیری 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 یك 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 سایبری[۱] 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[۲]، ۲۰۱۱، ص ۳). در ماه می سال، ۲۰۱۱دفتر ریاست جمهوری آمریکا، راهبردی تحت عنوان «راهبرد جهانی برای فضای سایبر؛ امنیت، شکوفایی و آزادی در فضای مجازی» را به طور 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 قاعده کلی داشت که شامل جلوگیری از جرم (بر همین اساس، همه دولتها از جمله ایالات متحده 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[۳]، ۲۰۱۱، ص۴۵).

در رابطه با بحث پیشگیری و اقدامات انجام شده، 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، نحوه 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 جرم موظف دانسته است. در نهایت، برنامه 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 تسهیل‌کننده جرم	تدابیر امنیتی (Filtering) رمزگذاری پراکسیها (Proxy) کیبورد مجازی تدابیر مربوط به فیلترینگ
افزایش خطرات ارتکاب جرم	توسعه محافظت کمك 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 مشکوك مدیران بانکها

۱. Defense Cyber Crime Center

۲. U. S Department of Defense

۳. The white House

		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 به کارگیری 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 تحریك 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 کنترل شده

نتیجه گیری

پژوهش حاضر با هدف تطبیق سیاست جنایی ایران و آمریکا در خصوص نحوه 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 ماده ۱۳۱ این قانون، سرقت یا تخریب حاملهای داده و سوءاستفاده 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 یك 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، ص ۱۴۵).

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 دهه 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. اشکالی که در اینجا متوجه ماده ۱۲ و ۱۳ قانون جرائم رایانه‌ای است، این است که قانون‌گذار انواع مختلف کلاهبرداری و سرقت را در یك سطح دیده است، غافل از اینکه هر کدام از این اشکال با یکدیگر تفاوت دارند. لذا این تفاوتها هم به نحوه ارتکاب جرم و هم به وسیله ارتکاب جرم برمی‌گردد و از آن مهمتر، اثرات زیان‌باری که هر کدام از این روشها بر جای می‌گذارند، با هم متفاوت است. به همین جهت، شاید بتوان با انجام اصلاحاتی متناسب با شرایط اجتماعی و قانونی کشور، مدلی از قانون کشور آمریکا را در ایران اجرا کرد و بهتر است برای دستیابی به نتیجه مطلوب، انواع کلاهبرداری اینترنتی در چند ماده به طور جداگانه جرم‌انگاری شوند و برای هر کدام، مجازات متناسب در نظر 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 شکلی که باشند در نهایت در این دسته‌بندی قرار خواهند گرفت؛ افزایش تلاش و زحمت ارتکاب جرم، افزایش خطرات ارتکاب جرم، کاهش منافع ارتکاب جرم، کاهش تحریك ارتکاب جرم، از بین بردن بهانه‌های ارتکاب جرم و نصب تراشه‌های مخصوص برای تعیین میزان انطباق فعالیتها. هر کدام از این دسته‌بندی‌ها نیز مصداقهایی دارند؛ از جمله بحث فیلترینگ، کنترل موجودی حساب، کنترل مجرمان حرفه‌ای و جلوگیری از تکرار جرائم سازمان‌یافته، نظارت شبکهای، تدابیر امنیتی کدگذاری، امضای دیجیتال و رمزگذاری که همگی اینها در پیشگیری وضعی قرار می‌گیرند. در مورد پیشگیری 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 می‌توان در قوانین مربوطه مشاهده کرد و هم در رویه عملی نهادهای مربوط. در کشور آمریکا علاوه بر وجود قانون مدون فدرال جهت روشن شدن موضع قانون‌گذار نسبت به بحث پیشگیری، به ایالتها نیز اجازه داده شده که در پرتو قانون فدرال، راهکارهای پیشگیرانه متناسب با شرایط آن ایالت به تصویب و اجرا برسد.

در پایان می‌توان نتیجه گرفت که ماده ۱۲ و ۱۳ قانون جرائم رایانه‌ای ایران، ماده جامع و مانعی برای مقابله با کلاهبرداری و سرقت سایبری نیست و نیاز است که 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[۱]: فایروالها یکی از عناصر اساسی در نظام مهندسی امنیت اطلاعات هستند که استفاده از آنها به یك 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 به طور 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 ترافیك شبکه‌ای قبل از اینکه به شبکه وارد یا از آن خارج

---

۱. firewall

شود، قرار می‌گیرد و آن را میسنجد تا ببیند با سیاستهای امنیتی کاربر مطابقت دارد و سپس مشخص می‌کند که آیا به آن اجازه 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 قابل توجه برای کاربر، امنیت وب‌سایت است که رمزهای بانکی دزدیده نشود که بانکها برای ما این کار را انجام داده‌اند و صفحه کلید 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 دسترس خارج گردند.

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

– نظارت شبکه‌ای: این راهکار شاید بیش از آنکه یك اقدام پیشگیرانه باشد، از لحاظ بازدارندگی مورد توجه قرار می‌گیرد. در حالت فنی، ابزارها یا برنامه‌هایی بر روی سیستم نصب می‌شوند و کلیه 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، ص. ۱۰۶۵).

– 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 پیشینه کیفری و اجتماعی، کلیه تحرکات فرد موردنظر و اقدامات وی، اعم از اشتغال، سکونت، تردد، جابه‌جایی و معاملات دقیقاً در مکانیزم تعریف شده و به طور 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 انگیزه 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 اولیه محافظت اینترنتی در فضای سایبر قبل از وقوع هرگونه حمله رایانه‌ای و موقعیت خطر مطلع ساخت.

– نصب تراشه‌های مخصوص برای تعیین میزان انطباق فعالیتها: برای از بین بردن معاذیر در اقدامات قابل تصور در مورد حملات سایبری بر روی سیستمهای رایانه تراشه‌های مخصوص به منظور کنترل فعالیتهای سیستم عامل 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. فصلنامه مطالعات پیشگیری از جرم. ۶(۳)، صص ۱۱۰-۷۷.

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.

۱. Spagnoletti

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، بابك (۱۳۸۸). بررسی فقهی حقوقی جرائم رایانهای. قم: انتشارات پژوهشگاه علوم و فرهنگ اسلامی.

خرم‌آبادی، عبدالصمد(۱۳۸۶). کلاهبرداری رایانه‌ای از دیدگاه بین‌المللی و وضعیت ایران. فصلنامه حقوق دانشگاه تهران. ۲(۷۳)، صص . ۱۱۲ ۸۳.

دزیانی، محمدحسن (خرداد و تیر ۱۳۸۵). مقدمه‌ای بر سیاست جنایی ایران در باب جرائم سایبری. مجله قضاوت. شماره،۳۸صص . ۴۸-۴۲.

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. فصلنامه کارآگاه، ۷(۲۵) صص . ۱۶۲-۱۲۱.

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

شیعه علی، علی؛ زارع، وحید و زارع، مجتبی (۱۳۹۴). جایگاه سیاست جنایی مشارکتی واکنشی در مرحله تعقیب کیفری در حقوق ایران. مطالعات حقوق کیفری و جرمشناسی. ۲(۴ و ۵)، صص ۲۸۷-۳۱۰.

صابری، سیاوش و انصاری دوست، شیما (بهار ۱۳۹۶). جرائم رایانه‌ای در حقوق ایران. مطالعات علوم سیاسی، حقوق و فقه. ، ۳(۱ و ۲)، صص . ۱۴۹ -۱۴۱.

صفاری، علی (۱۳۸۱). انتقادات وارده به پیشگیری وضعی از جرم. مجله تحقیقات حقوقی. شماره ۳۵ و ۳۶. صص . ۱۹۳-۲۳۳.

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). صص . ۱۹۶-۱۸۵.

میر محمدصادقی، حسین و شایگان، محمد رسول (پاییز و زمستان ۱۳۸۶). راهکارهای مقابله با جرم کلاهبرداری رایانه‌ای در حقوق کیفری ایران. فصلنامه دیدگاههای حقوق قضایی. شماره ۴۲و ۴۳، صص . ۱۲۶-۱۰۹.

میرمحمدی صادقی، حسین و شایگان، محمد رسول (پاییز و زمستان ۱۳۸۹). بررسی تطبیقی کلاهبرداری سنتی و رایانه‌ای و مجازاتهای آنها در نظام حقوقی ایران. فصلنامه دیدگاه‌های حقوق قضایی. شماره ۵۱ و،۵۲صص . ۱۶۲-۱۳۷.

نجفی ابرندآبادی، علی حسین (۱۳۷۹). مباحثی در علوم جنایی؛ تقریرات درس جرمشناسی پیشگیری (محمدعلی بابایی، گردآورنده). دوره دکتری دانشگاه تربیت مدرس.

نجفی ابرندآبادی، علی حسین (۱۳۸۲). تقریرات درس جرمشناسی (رضا فانی، گردآورنده). دوره کارشناسی ارشد دانشگاه شهید بهشتی.

نجیبیان، علی (۱۳۸۸). موانع و محدودیتهای پیشگیری وضعی از ارتکاب جرم. پایان‌نامه کارشناسی ارشد رشته حقوق جزا و

جرم‌شناسی. دانشکده 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.

Finklea M. (2012). Kristin, Identity Theft: Trend and issue,published by congressional research service, Washington D. C.

International Telecommunication Union (2012). Understanding cybercrime: Phenomena, challenges and legal response,published by itu, Geneva.

Marshall, H. , Jarret & Bailie, W. (2007). michael, Prosecuting of cybercrime, published by legal education executive office for united states Attorneys, second edition, Department of justice,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.