مطالعات علوم سیاسی، حقوق و فقه
دوره ۱۰، شماره ۱، بهار ۱۴۰۳
صفحات ۹۹۶-۹۸۷

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

حمایت کیفری از حریم خصوصی در فضای سایبری ایران با تطبیق آمریکا

آزاده کلاسنگیانی
کارشناسی ارشد حقوق جزا و جرم‌شناسی دانشگاه روزبهان واحد ساری

چکیده
در عصر حاضر و با ظهور اینترنت و فراگیر شدن آن مشکلات جدیدی در رابطه با امنیت سایبری و جرم انگاری و مقابله و پیشگیری از جرائم سایبری به وجود آمده است. در بحث جرم انگاری 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 بیش‌ازپیش برای قانون‌گذار و مجریان قانون سخت کرده است کـه تشریح این موضوع در ادامه خواهد آمد. مشکل دیگر نیز بحث پیشگیری از این جـرائم و سازوکارهای مربوط به آن است؛ زیرا بحث در رابطه با انواع پیشگیری و تأثیر هر یک آن‌ها بر سرقت و کلاه‌برداری سایبری و همچنین ارائه راهکارهای متناسب با اوضاع اجتماعی و اقتصادی و غیره و مبتنی بر برنامه‌ای پیشـگیرانه امـری خطیـر اسـت کـه نیازمند کارهای علمی و عملی است. از همین رو، در ایـن مقاله فقط سیاست جنایی تقنینی و مشارکتی دو کشور ایران و آمریکا مـورد بررسـی قرار خواهـد گرفـت و دیگـر مدل‌های سیاست جنایی همچون سیاست جنایی قضـایی و اجرایـی مدنظر نگارندگان نمی‌باشند.

کلمات کلیدی: حمایت کیفری، حریم خصوصی، فضای سایبری

مقدمه

در رابطه با موضوع جرم انگاری و مقابله کیفری با این جرائم باید عنوان کرد قانون جرائم رایانه‌ای ایران در مواد ۱۲ و ۱۳ به جـرم انگـاری سـرقت و کلاه‌برداری سـایبری پرداخته است. با نگاه به این دو ماده، مشخص می‌شود که قانون‌گذار ایران بـا اسـتفاده از تعریف سنتی این جرائم، اقدام به جرم انگاری شکل سایبری آن‌ها کـرده اسـت. ایـن امـر فی النفسه مشکل اساسی در این زمینه نیست، بلکه عدم توجه قانون‌گذار بـه مصـادیق 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 جرم انگاری آنهاست؛ زیرا در عمل علی رغم تصویب قانون موردنظر و جرم انگاریو تعیین کردن مجازات برای جـرم کلاهبرداری اینترنتی، میزان این نوع جرم ها بـرای قبیل حبس و جزای نقدی در نظرهای مربـوط، جرائمـی کماکان رو به افزایش باورنکردنی اسـت. البتـه لازم به ذکر است که بحث ایراد در جرم انگاری تنها دلیل افزایش این آمار نیست بلکه مسائلی همچون ضعف در زیرساخت ها عدم یا کمبود آموزش مناسب آگاهی واطلاع ناکافی مردم در رابطه با محیط سایبری و خطرات آن و مسائلی از ایـن دسـت، مـیتواننـد بسیار مؤثر باشند. با توجه به مسائل و مشکلات پیش گفته، سعی بر آن است تا در این مقاله بـا بررسـی سیاست جنایی کشور آمریکا، به عنوان کشور پیشرو در امر قانونگذاری جرائم سـایبری، مدل سیاست جنایی مناسبی را که برگرفته از سیاست جنـایی ایـن کشـور در رابطـه بـا سرقت و کلاهبرداری سایبری است ارائه شود تا شاید با الگـو گـرفتن ازدیگـر کشـورها، 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 عملـی و بـه روز کردن قوانین موردنظر علاوه بر اینکه باید شرایط اجتماعی و قانونی ایران مدنظر قرار گیرد، لازم است از دیدگاه های مختلف قانونی و قانونگذاری دیگر کشورها در پروسه جرم انگاری و تعیین مجازات جرم کلاهبرداری اینترنتی کمک گرفت. همچنین، برای رسیدن به کمال مطلوب طبیعتاً باید قانون کشورمان را با کاملترین و به روزترین قانون دنیا در زمینه کلاهبرداری اینترنتی مقایسه کرد.

به همین دلیل نیز قانون فدرال جرائم رایانه‌ای آمریکا برای مقایسه با قانون جرائم رایانه ایران انتخاب شده است وعلت انتخاب هم ایـن اسـت کـه طبـق آمارهای جهانی و توضیحاتی که داده خواهد شد، قانون جرائم رایانه‌ای آمریکا به روزترین و کاملترین قانون در دنیا در این زمینه است. قانون جرائم سایبری فدرال آمریکا انواع مختلفی از کلاهبرداری و سرقت سـایبری را به طورجداگانه جرم انگاری کرده است. به طور مثال، عنـاوینی ماننـد کلاه‌برداری سـیم، تعدی به رایانه های دولتی، سرقت هویت و غیره که بـرای هـر کـدام تعریـف و مصـادیق جداگانه و همچنین مجازات جداگانه در نظر گرفته است. در قـانون کشـور آمریکـا صـور بیشتری به طور جداگانه از این دو جرم، در قانون ذکر شده و برای هر کدام بـا توجـه بـه شرایط و نتیجهٔ به دست آمده، مجازات متناسب در نظر گرفتـه شـده اسـت کـه همـین مطلب روند کشف جرم و تطـابق عمـل بـا مـادهٔ قـانونی مناسـب، دادرسـی، مجـازات و پیشگیری را بسیار آسان میکند. پرسش هایی که نگارندگان در این پژوهش به دنبال پاسخگویی به آن‌ها هسـتند، ایـن است که سیاست جنایی تقنینی ایـران و آمریکـا چگونـه جـرائم سـرقت و کلاه‌برداری سایبری را جرم انگاری کرده اند؟ 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 داده اند و مطالعهٔ تطبیقی وراهکارهای 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 پیر دهی (۱۳۸۹) در تحقیقی با هدف بررسی اینکه آیا سرقت اینترنتی در زمـره سـرقت حدی محسوب می‌شود مال به صورت فیزیکی و با دستان در عالم واقع انجـام نمـیشـود، پس در رده ی 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 رسیده اند که کلاهبرداری سنتی و اینترنتی شباهت زیـادی دارند اما موضوع جرم این دو وجه تمایزشان است که در یکی مال آن‌ها و در دیگـری داده هـا هستند. همچنین، میرمحمد صادقی و شایگان (۱۳۸۶) در تحقیقی با عنوان راهکارهای مقابله با جرم کلاه‌برداری رایانه ای در حقوق کیفری ایران به این نتیجه رسیده اند که آنچه در

مقابله غیرکیفری از کلاهبرداری اینترنتی مهم و کاربردی است، پیشگیری اجتماعی و وضعی است. خرم آبادی ۱۳۸۶ نیز در تحقیقی با عنوان کلاهبرداری رایانه‌ای از دیدگاه بین المللی و وضعیت ایران به این نتیجه رسیده است که مهمترین تفاوت کلاهبرداری سنتی و اینترنتی در این است که دراولی وجود عنصر اغفال ضروری است، اما کلاهبرداری اینترنتی بدون اغفال هم به وقوع می پیوندد.

سیاست جنایی

سیاست جنایی همان چاره اندیشی در رابطه با جرم است که به دوصورت کیفری و پیشگیری است (مارتی،۱۳۹۳ صص ۹-۷) یا تعریف لازرژ که سیاست جنایی را مستقل یا با طور تدابیری میداند که دولت و جامعهٔ مدنی به ها ودربردارندهٔ مطالعهٔ اقدام ها تدابیری میداند که دولت و جامعه ی مدنی به طور مستقل یا با مشارکت هم برای سرکوب پدیده مجرمانه، پیشگیری از آن و حمایت بزه دیدگان 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 زمینهٔ یک پدیدهٔ مجرمانه است که توسط قانون‌گذار تدوین می‌شود وبیانگر سیاست جنایی تقنینی آن کشور در رابطه با همان پدیدهٔ مجرمانه است (لعلی و معظمی،۱۳۹۶ ص. ۱۸۷). سیاست جنایی مشارکتی نیز بیانگر نقش و جایگاه مردم و نهادهای اجتماعی و غیردولتی در فرآیند کیفری است.

روش‌شناسی تحقیق

تحقیق حاضر با توجه به نحوهٔ گردآوری داده ها به روش اسنادی بوده و اطلاعات به دست آمده به صورت کیفی و مبتنی براستنتاج 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، مقاله ای 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 طبقه بندی اطلاعات، از ابزارهای سنجش کتابخانه ای و اسنادی استفاده شده است.

یافته های 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، سه بخش تحلیل مواد قانونی مرتبط، تبیین و ارائه راهکارها و مصادیق عملی پیشگیری اجتماعی و وضعی و مرحله ای 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 رایانه ای 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 کلاهبرداراست.

در طرف مقابل، در قانون جزای فدرال آمریکا، قانون‌گذار آن کشور در مواد مختلف و متعدد، اقدام به جرم نگاری 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 نشان دهندهٔ این است می بایست میان مصادیق مختلف این جرائم تفاوت گذاشت تا بتوان نیازهای قانونی متناسب با پیشرفت فناوری را برای جامعه تامین 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 جـرائم کالهبـرداری و سرقت سایبری در این قسمت ابتدا مادۀ ۱۲ و ۱۳ قانون جرائم رایانه‌ای ایران مورد بررسی قرار میگیرد و قـانون ۱۸ جزایی فدرال سپس به تحلیل مواد A-1028 ۱۰۲۸-۱۰۲۹ آمریکا که به سـرقت و کلاه‌برداری سـایبریاختصـاص دارنـد، پرداختـه می شود. مادۀ ۱۲ قانون جرائم رایانه‌ای، عنصر قانونی جرم سرقت سایبری است که در آن عنوان شده، هرکس داده های متعلق به دیگری را بربابد، سارق محسوب می‌شود که ایـن 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 جـرم، شرایط وقوع و غیره توجه کرد. با نگاهی به این ماده، میتوان دیگر عناصر تشکیل دهنـدۀ این جرم را تحلیل کرد و به دنبال آن نقاط ضعف و قوت مادۀ عنصر مادی سرقت سایبری و سنتی شبیه به هم است که به دلیـل مربوطه را مشـخص کـرد. سازد، مکررات، فقط مواردی که سرقت سایبری را از سرقسنتی جدا کرد تکـرار جلـوگیری ازذکر خواهنـد شد. مورد اول این وجه تمایز، وسیلۀ ارتکاب جرم است، دوم موضوع جرم و دیگری فضا و بستری است که امکان ارتکاب جرم در آن فراهم می‌شود.

در اینجـا وسیلۀ ارتکاب جرم، سایبرهای دیجیتـالی و بستر ارتکاب جرم، فضای سـرقت سـایبری، داده رایانه است و موضوع است (خرم آبادی،۱۳۸۶ صص.)۸۵-۸۴ ای که الف) ماده ۱۳ جرائم رایانه ای: دراین ماده جرائم رایانه ای که عنصر قانونی جرم کلاه‌برداری سایبری است عنوان میکند هر کس به طور غیر مجاز از سامانه رایانه ای یا مخابراتی با ارتکاب اعمالی از قبیل وارد کردن، تغییر، محـو، ایجـاد یـا توقیـف کـردن داده ها یا مختل کردن سامانه، وجه یا مال یا منفعت یا خدمات یـا امتیـازات مـالی بـرای خود یا دیگری تحصیل کند ... .» کلاهبردار سایبری است. با توجه به متن قانون مـذکور، این موضوع مشخص می‌شود که قانون‌گذار ایران، تعریف کلاهبرداری اینترنتی را از شکل سنتی گرفته است،

در صورتی که در دیگر کشورها به دلیل وجـود تفـاوت بـین موضـوع کلاهبرداری اینترنتی با نوع سنتی آن همچنین کیفیاتمجزا و متفاوت در شکل گیری این دو جرم کلاهبرداری اینترنتی را جرمی با تعریف و ماهیت جداگانـه از کلاه‌برداری سنتی می دانند (بای،۱۳۹۰ ص ۳۰۴) به هر ترتیـب، در ادامـه سـعی بـر آن اسـت تـا براساس قانون مذکور، عناصر جرم کلاهبرداری اینترنتی تفکیک و تحلیل شود بابررسی ماده ۱۳ قانون جرائم رایانه ای ای، 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 اعمـال متقلبانـه بـرروی سامانه های رایانه ای یا مخابراتی است و قانون‌گذار از باب تمثیـل مصـادیقی از ایـن ای یا مخابراتی است و قانونگذارهای رایانه روی سامانه (اکبـری،۱۳۹۰؛ ولی این روشهـا حصـری نیسـت اعمال متقلبانه را احصاءکرده است)

۳ - در کلاهبرداری سنتی، تأثیر مانور متقلبانه بر بزه دیده از طریـق فریـب بـرای تحقـق عنوان مجرمانه ضروری است، یعنی لازمه کلاه‌برداری، فریـب خـوردن شـخص اسـت (میرمحمدصادقی و شایگان،۱۳۸۶ ص)۱۱

لازم به ذکر است که درقوانین بین المللی، کلاهبرداری اینترنتی را جرمی میدانند که در آن اغفال و بردن مال شرط نیست، بلکه صرف ایراد ضـرر بـه قصـد بـه دسـت آوردن منافع مالی کافی است (سالری شهر بابکی،۱۳۹۳ ص)۲۶۴ در قانون ایران، تحقق جرم کلاهبرداری و برخی جرائم مربوط نیازمند فریب انسان زنده است (بـه اسـتثنای، کشورهایی همچون کانادا وفرانسه، هلند و اسکاتلند) (دزیـانی،۱۳۸۵ ص ۴۵) از همـین شخص زنده، برخی از حقوقدانان معتقدنـد کـه فریـب، مختص اشخاص حقیقی است و در مورد سامانه های رایانه‌ای و مخـابراتی مصـداق نـدارد (خرمآبادی،۱۳۸۶ صص).

ب)A۱۰۲۸،۱۳۴۳۱۰۲۸، ۱۰۳۷،۱۰۲۹ قانون جزایی فدرال آمریکا:

بخـش 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.

ماده ۱۰۲۸: سرقت هویت و مشخصات دسترسی: 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 هویـت محاکمـه می‌شود. در

این ماده، بسته به چگونگی انجام جرم و عمل مرتکب حبس کمتر از ۲۰، ۱۵ و ۳۰ سال در نظر گرفته همچنین، قانون‌گذار فدرال در ادامه اصالحاتی را همچون «ساختن مدرک» مدارک هویت «کـارت معنـای هویـت» «مدارک غلط هویت» «هویت» مجریان قانون را در برخورد و رسیدگی با ویژگیهای آن‌ها را عنوان کرده است که این امر تکلیـف این جرم راحت تر میکند.

۱۰۲۸: سرقت هویت و اطالعات هویتی همراه با خشونت: منظور قانون‌گذار از سرقت هویت خشن، در جایی است که این سرقت هویت برای اعمال خشن از جملهجرائم مربوط به تروریسم و دیگر جرائم عمومی خشن بکار رفته اسـت. براسـاس این ماده، منظور از جرائم خشن عمومی، جرائمی هستند که مربوط به انواع جنایات علیه 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 جـرائم مربـوط بـه تروریسم، شخص بزهکار به مدت ۵ سال به زندان محکـوم می‌شود

ماده ۱۰۲۹: کلاهبرداری و جرائم وابسته در ارتباط با وسایل دسترسی: قانون‌گذار هرکس را که دست به ساختن، استفاده کردن یا داد و ستد آگاهانـه و بـا قصـد متقلبانه کرده است. ازجرم، مجرم قلمـداد در وسایل دسترسی متقلبانه بزند، در حاالت مختلف از نوع خلاصه نام برد:

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

۲ - آگاهانه و با قصد فریب دادن، از یکی ابزارهای دسترسی بدون مجوز تردد یا اسـتفاده کند با چنین ابزاری هر چیزی بـه ارزش ۱۰۰۰ دلار یا بیشتر کسب کند

۳ - آگاهانـه و بـا قصـد فریـب دادن،۱۵ یـا تعـداد بیشـتری ابـزار تقلـب یـا ابزارهـای دسترسی های غیرمجاز داشته باشد؛

۴ - آگاهانه و با قصد فریب دادن، تجهیزات ایجاد ابزار را تولید و در آن تـردد یـا کنتـرل داشته باشد یا آن‌ها را در اختیار داشته باشد.

ماده ۱۰۳۰: کلاهبرداری و جرائم وابسته در ارتباط با رایانه: چنانچه شخص با داشتن دسترسی آگاهانه بدون مجوز به رایانه یا دسترسی بیش از حـد مجاز و به وسیلۀ چنین دسترسی، اطلاعاتی که توسط ایاالت متحده آمریکا و به موجـب 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 نیـاز بـه محافظـت در برابر افشا دارد، به دلیل باور داشتن به اینکه اطلاعـات بـه دسـت آمـده بـه ایـن روش را میتوان برای آسیب زدن به ایاالت متحده آمریکا مورد استفاده قرار داد، دریافت کند یـا با هدف سود بردن از هر کشور خارجی از طریق ارتباط خودسرانه، ارائه و انتقال دهـد یـا باعث انتقال آن شود یا ارائه آن به افراد غیرمجاز یا نگهداری خودسرانه و عدم تحویل آن به افسر یا کارمند ایاالت متحده که مجاز بـه تحویـل آن اسـت، کلاهبرداری محسـوب می‌شود. همچنین، دسترسی عمدی بدون مجوز یا دسترسی بیش از حد مجاز و دریافت اطلاعات شامل اسناد مالی یک یا حاوی فایل سازمان گزارش دهنـدۀ مشـتری در مـورد یک مشتری مانند عباراتی که در قانون امور اعتباری تعریف شده است نیـز جـرم انگـاری شده است.

ماده ۱۰۳۷: کلاهبرداری و جرائم وابسته در ارتباط با نامه های الکترونیک: قانون‌گذار توضیحاتی دربارۀ 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 کـه بـه نـوعی در تجارت خارجی وبین ایالتی نقشی داشته باشد و آن شخص آگاهانه، به رایانـۀ محافظـت شده بدون مجوز، الکترونیکی تجاری به شروع ارسال پیـامهـای پسـت دسترسی داشته باشد و آگاهانه اقدام به پست پیام چندگانه از این رایانه یا بـه چنـین رایانـهای بکنـد، طبـق ایـن مـاده مجازات می‌شود.

در ادامه، قانون‌گذار صور دیگر این جرم را طبقه بندی میکند که به این شرح است: هرگاه شخصی از رایانۀ محافظت شده برای توزیع یا ارسال مجـدد پیـام هـای پست الکترونیک تجاری چندگانه با قصد فریب یا گمراه کردن دریافت اطلاعات اصلی در پیامهای پست الکترونیک تجارت هـایی اسـتفاده کنـد، یـا بـا جعـل اطلاعات اصلی پست پیام چندگانه و آغاز عمدی ارسال چنین پیامهاییبا استفاده از اطلاعاتی ک هویت ثبت کننده واقعی را جعل مـی کنـد، در ایـن سایتها ثبت نام و برای حساب پست الکترونیک یا تعداد بیشترهای پسـت آنالین یا دو یا چند نام دامنه و آغاز عمدی ارسال پیام پست الکترونیکـی از چنـین ترکیبی از حسابها یا دامنه ها مجازات خواهد شد. همچنین، اگر شخص با قصد فریب اقدام به نشان دادن خود بـه صـورت

ثبت کننده یا جانشین مشروع او برای ثبت ۵ یا تعداد بیشتری از آدرس های پروتکل اینترنتی به دروغ بکند و برای آغاز عمدی ارسال پیام های پست الکترونیکی تجاری چندگانه ازاین آدرس ها برای توطئه و انجام آن، باید مجازات شود. این ماده برای کلاهبردارهای مربوط جرایمی از قبیل حبس و جزای نقدی در نظر گرفته است. تحلیل سیاست جنایی مشارکتی ایران و آمریکا نسبت به سرقت و کلاهبرداری سایبریهمانطور 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 پرداخت 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 وروشهای مختلف به منظور جلوگیری از وقوع بزهکاری، هدف به جلوی جرم رفتن و پیشی گرفتن از بزهکاری است بر همین اساس، علمای حقوق جزا و جرمشناسی، دو مفهوم ازپیشگیری را مورد توجه قرار داده اند و به تعریف و تبیین آن پرداخته اند 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 بزهکار و ترمیم کردن خسارت وارد بر بزه دیده در فرآیند وقوع جرم را نام برد.

این برداشت و استنباط از پیشگیری نزد افرادی همچون انریکوفری وجود داشته است؛ مقصود ویاز این اصطالحات همان اقدامات پیشگیرانه غیرکیفری است که جایگزین مجازات بوده و به عبارتی «هم عرض های کیفری» می باشند.

در مقابل مفهوم موسع پیشگیری، مفهوم مضیق پیشگیری قرار دارد که مقصود از آن مجموعه ابزارو 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.

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 اینناست که با افزایش آگاهی افراد و تربیت صحیح آن‌ها، به ویژه قشر جوان و نوجوان جامعه اجتماعی وقوع جرم نظیر فقر و بیکاری، انگیزه همچنین از بین بردن زمینه پیشگیری اجتماعی شامل اقدامهایی است که همچنین، مجرمانه از مجرمان سلب شود بهطور مستقیم یا غیرمستقیم، هدفشان تأثیرگذاری بر شخصیت افراد است تا از سازمان دادن فعالیت خود حول انگیزه های بزهکارانه بپرهیزند با توجه به تعاریف و مفاهیم ارائه شده، میتوان پیشگیری اجتماعی را به دو دسته تقسیم بندی کرد؛ پیشگیری اجتماعی رشد مدار که سعی دارد چنانچه هر شخصی به هر دلیلی از خود نشانه های بزهکاری را بروز داد به هر طریق مداخله هر چه سریعتر در خود وی و محیط اطرافش از مزمن شدن بزهکاری در آینده جلوگیری کند و پیشگیری اجتماعی جامعه مدار که درپی خنثی سازی عوامل جرم زا در محیط اجتماعی است. پیشگیری اجتماعی رشد مدار اینترنتی نکته بسیار مهم در برخورد و مبارزه اینترنتی به ویژه کلاهبرداری، استانداردهای فنی و اخالق 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 اخالق شغلی را رعایت کند طیف وسیعی از مجرمان و بزه دیدگان 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 اطلاع رسانی 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 شکل گیری یا بروز انگیزۀ مجرمانه در عموم جامعه به وسیلۀ دو اقـدام اصـلی اسـت: ایجـاد علاقـه و آسان سازی بروز افکار مـشروع و مفید و بر حذر داشـتن از ناهنجاریهای اینترنتی. یکـی از مهمترین راههای پیشگیری از کلاهبرداری اینترنتی یه وسیله ی پیشگیری اجـــتماعی طریق آموزشهای عمومی و رسانه های جمعی است. باید توجـه داشت که اهمیت خاص تحقیق در زمینۀ رسانه و پیشگیری از وقوع جـرم از آن روسـت کـه این وسیله تمامی زندگی انسان را در برمیگیرد.

کارکرد رسانه های جمعی در مـورد پیشگیری از کلاهبرداری اینترنتی میتواند از طریق آگاه کردن مردم از پیامدهای نـاگوارالگوهـای مناسـب رفتـاری جهـت جلوگیری از ارتکاب و تکرار آن باشد که از این طریق میتوانند نقش مهمی در پیشگیری از جرم داشـته بـاشند همچنین، اثربخشی هـر چه بیشتر انواع راه های پیشگیری ذکرشده نسبت به کلاهبرداری، نیازمند یـک سیاسـت جنـایی مشـارکتیفعال است. سیاست جنایی مشارکتی بررسـی و مطالعۀ جایگاهی است که در سیاست جـنایی یـک کشور بـه جامعـۀ مـدنی و از طریـق اعطای نقش به بزهکار، بزهدیده و به ویـژه کـل جامعه و مردم داده شـده اســت. کارکرد ایـن نـوع از سیاست جنایی نسـبت بـه کلاهبرداری اینترنتـی، اقدامات در مرحلۀ کشف جـرم، تـعقیب دادرسی و اجرای حکم را در برمیگیـرد کـه بـا همکاری وسیع جامعۀ مدنی، نـهادهای مـردمی و نیروهای دولتی مانند پلـیس، سـازمان زندان ها و غیره با دستگاه قضایی انجام می‌شود.

پس از ارائه توضیحات مربوط به این بخش و با جمع بندی آن میتوان انتقادهایی را بر به کارگیری این نوع پیشگیری در ایران وارد دانست؛ برنامه هایی که در ایران مبتنی بر این نوع پیشگیری هستند، عموماً با محوریت مسئولیت دولت یـا وزارت ارتباطـاتو فنـاوری اطلاعات و وزارت ارشاد است. برای اثربخشی بیشتر این نوع پیشـگیری درکلاهبـرداری اینترنتی، لازم است به سیاست جنایی مشارکتی بهای بیشتری داد و مردم را بـه عنـوان عضوی توجه قرار ها کرد که این امر نیز متأسفانه کمتر مـورد مؤثر در این نوع پیشگیری وارد برنامه گرفته است.

ب) اقدامات مبتنی بر پیشگیری وضعی در ایـران: پیشـگیری وضـعی عبـارت اسـت از اقدامات پیشگیرانۀ معطوف به اوضاع و احوالی که جرائم ممکن است در آن وضـعیت بـه 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 دهـد؛ چراکـه از نظـر طرفـداران پیشگیریوضعی، طـور فطـری انسان موجودی حسابگر است و سود و زیاد عملش را بـه طور فطری میسنجد همچنین این نوع پیشگیری سعی دارد تا با اتکا به آماج جرم یا بـزهدیـده بـه تبیین پیشگیری از جرم بپردازدچهارچوب نظری این بحث به وسیله نظریه هایی مختلف فرصت بیان شده است همچنین اقداماتی در مـورد جـرم کلاهبرداری اینترنتـی شـامل مصونیت بخشی به روش های همچون، نظـارت بـر مراکـز ارائـه آمـاج، و اینترنت و فیلترینگ و غیره می‌شود این نوع پیشگیری خود نیز دارای نقاط ضعف و قوت است، اما مجال توضیح این موارد در این تحقیـق نمـی گنجـد.

مخاطبان اصلی پیشگیری وضعی از جرم کلاهبرداری اینترنتی، کسانی هستند کـه از تخصص و مهارت باالیی برخوردار نیستند و بیشتر سعی میکنند با امکاناتی کـه فضـای اینترنت در اختیارانها میگذارد مرتکب جرم شوند؛ نه اینکه خود دسـت بـه ابتکـاربزنند، همانطور که در ادامه توضیح داده خواهـد شـد، کـاری از پیشگیری وضعی جهت مقابله با جرم کالاهبرداری و سرقت اینترنتی ساخته نخواهد بود. البته این نکته را نباید از یاد برد که علیرغم تأثیرات مثبتی که پیشگیری وضعی دربرابـر کلاهبرداری اینترنتی دارد بعضا به دلیل ماهیت این جرم دارای نقاط ضعفی نیز است؛ از جمله این محدودیت ها، هزینه بربودن و زمانگیر بودن ایـن اقـدامات، تفـاوت در میـزان دانش طرفین نسبت به اینترنت و تفاوت در به کارگیری روشها چه در جهت فیلترینگ و چه در جهت ضد آن در نهایـت، از جمله اقداماتی پیشگیری است میتوان به این موارد اشاره کرد؛ فیلترینگ، استفاده از پراکسی ها، استفاده از رمز ورود، کنترل موجودی حساب و نظارت بر فضای مجازی

ج) اقدامات مبتنی بر پیشگیری وضعی در آمریکا: بـه دلیـل ماهیـت جـرائم اینترنتـی خصوصا کلاهبرداری و سرقت اینترنتی، برنامه های پیشگیرانه در اکثر کشورهای دنیـا بـه اتکا بر پیشگیری وضعی اسـت. در کشـور آمریکـا عـلاوه بـر دولـت و ایالـتهـا، عمومـاً شرکت های خصوصـی مـرتبط، پلـیس فـدرال، کمیسـیون امنیـت و اقتصـاد و سـازمان جاسوسی در این کار ازشرکت دارند راهبردها و برنامه های کشور آمریکـا در پیشـگیری از جرم همانطور که گفته شد. کلی است و البته،

سازمان ها و نهادهای دولتی، برنامه هایی در این راستا طراحی کرده اند. این برنامه ها شامل تغییر نوع محافظت از سیستم ها با استخدام افراد برای امنیت در فضای اینترنت به تمرکز بر روابط اینترنتی بین ایاالت 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 که مسئول این تحقیقات ها نوعی این اطلاعات و روشها را بهبود بخشید و از این طریق مورد استفاده عمومی قرار داد در ماه می سال،۲۰۱۱ دفترریاست جمهوری امریکا راهبردی تحت عنوان راهبرد جهانی برای فضای سایبری 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 بین المللی فراهم آورد. این راهبرد، (بر همین اساس، همهٔ دولتها از جمله جلوگیری از جرم پنج قاعدهٔ کلی داشت که شامل ایاالت متحدهٔ آمریکا باید مجرمان اینترنتی را شناسایی و تعقیب کنند تا مطمئن شوند از جرم جلوگیری می‌شود وهمچنین با مرکز تحقیقات مجرمان بین المللی همکاری داشته باشند)، ایجاد که مستقیماً در ارتباط با پیشگیری از جرائم سایبر، تحقیقات و دادرسی جرائم هایی اولویت 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 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 ها اشاره نشده است.

از اعضا، نحوهٔ تشکیل و وظایف کارگروه اشاره شده است در مورد هیچ نوع پیشگیری صحبت نشده است. در حالی که در قانون ملی پیشگیری ازجرم آمریکا، انواع راهکارهای مبتنی بر پیشگیری وضعی، مرحله ای و اجتماعی لحاظ شده و قانون‌گذار، مسئولان مربوطه را به انجام تمام دستورالعمل های اجرایی و حمایتی، قبل و بعد از وقوع جرم موظف دانسته است.

نتیجه گیری

پژوهش حاضر با هدف تطبیق سیاست جنایی ایران و آمریکا در خصوص نحوهٔجرم انگاری سرقت و کلاهبرداری سایبری انجام شده است و بررسیهای انجام شده نشان میدهد که اولین عکس العمل قانون‌گذار ایران در مقابل جرائم رایانهای در سال ۱۳۸۲ از طریق تصویب قانون مجازات جرائم نیروهای مسلح (مصوب ۰۹/۱۰/۱۳۸۲) در مجلس شورای اسلامی به عمل آمد. به موجب ماده ی ۱۳۱ این قانون سرقت یا تخریب حامل داده و سوءاستفادهٔ مالی از طریق رایانه (کلاه‌برداری و اختلاس)، جعل اطلاعات وداده های رایانه ای، و تسلیم و افشای غیرمجاز اطلاعات و داده ها افرادی که صلاحیت دسترسی به آن را ندارند، توسط نظامیان جرم تلقی و مرتکب حسب مورد به مجازات جرم ارتکابی می‌شود. واکنش بعدی قانونی مرتبط با جرائم رایانه‌ای از طریق تصویب قانون تجارت الکترونیکی مصوب (۱۷/۱۰/۱۳۸۲) در مجلس شورای اسلامی به عمل آمده است. به موجب مواد ۶۷،۶۸،۶۹،۷۴،۷۵،۷۶ ۷۷ و ۶۶ این قانون کلاهبرداری، جعل، دستیابی و افشای غیرمجاز اسرار تجاری، نقض حقوق مربوط مالکیت معنوی (کپی رایت) و غیره که از طریق رایانه و در بستر تجارت به الکترونیکی انجام شود، جرم تلقی و برای آن مجازات تعیین شده است.

هر یک از قوانین مربوطه، در بستر خاص خود قابلیت اعمال دارند؛ مثلا قانون مطبوعات صرفاً نسبت به جرائم رایانه‌ای ارتکابی در قالب نشریات الکترونیکی و مجازات نیروهای مسلح ای صرفاً در مورد بعضی از جرائم رایانه نظامیان و قانون تجارت الکترونیکی فقط در مورد برخی از جرائم رایانه‌ای ارتکابی در بستر تجارت الکترونیکی قابل اجرا هستند با این سیاست جنایی تقنینی ایران نسبت به کلاهبرداری سرقت اینترنتی مشخص شد؛ اما برخالف این روند در ایران، قانونگذاران آمریکایی از سال ها قبل یعنی از اوایل دهۀ ۸۰ میالدی 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 جرم انگاری سرقت کلاهبرداری اینترنتی ذکر شده اند و برای هر کدام از آن‌ها با توجه

بـه شـرایط و نوع جرم مجازات متناسبی در نظر گرفته شده اسـت همـین نـوع قـانون نویسـی، یعنـی تقسیم بـندی اشکال مختلف کلاهبرداری اینترنتی سبب شده تا موردی از قلم نیفتد و جرم انگاری تمامی حاالت قانونی، کامل شکل بگیرد در قانون جرائم رایانه‌ای ایران، که عنصر قانونی مبارزه با کلاهبرداری اینترنتـی اسـت، قانون‌گذار فقط به ذکر افعالی همچون تغییر، محو و غیره بسنده کرده انجام این افعـال در فضای اینترنت برای فریب و به دست آوردن پول باشد، جرم انگاری کرده اسـت اشکالی که در اینجا متوجه مادۀ ۱۲ و ۱۳ قانون جـرائم رایانه‌ای 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 تفاوت ها هم به نحوه ی ارتکاب جرم هم به وسیله ارتکاب جرم بر میگردد و از آن مهمتر، اثرات زیانباری که هر کـدام از ایـن روش ها 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 درایران اجرا کرد و بهتر است برای دستیابی به نتیجۀ مطلوب، انواع کلاه‌برداری اینترنتـی در چند ماده به طور جداگانه جرم انگاری 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 مرحله ای در سیاست جنایی ایران عمالً جایی ندارد یا حداقل، توجه به آن نمیشود. برنامه مبتنی پیشگیری وضعی از این جرائم به هر شـکلی که باشند در نهایت در این دسته بندی قـرار خواهنـد گرفـت؛ افـزایش تـلاش و زحمـت ارتکاب جرم، افزایش خطرات ارتکاب جرم، کاهش منافع ارتکاب جرم کـاهش تحریـک ارتکاب جرم از بین بردن بهانه ارتکاب جـرم و نصب تراشههای مخصوص برای تعیین میزان انطباق فعالیت های، هر کدام از این دسته بندی ها نیز مصـداق هایی دارند ؛ از جملـه بحث فیلترینگ، کنترل موجودی حساب، کنترل مجرمان حرفهای جلـوگیری از تکـرار جرائم سازمان یافتـه، نظـارت شـبکه ای، تـدابیر امنیتـی کدگـذاری، امضـای دیجیتـال و رمزگذاری که همگی اینها در پیشگیری وضـعی قـرار مـیگیرنـد. در مـورد پیشـگیری مرحله ای موضوع قدری متفاوت است این تفاوت به برنامه‌ایران و آمریکا برمیگردد؛

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 رویۀ عملی نهادهای مربوط. در کشور آمریکا علاوه بر وجود قانون مدون فدرال جهت روشن شدن موضع قانون‌گذار نسبت بحـث پیشـگیری، بـه ایالت ها 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 مادۀ ۱۲ و ۱۳ قانون جـرائم رایانه‌ای ایـران، مـادۀ جامع و مانعی برای مقابله بـا کلاه‌برداری و سـرقت سـایبری نیسـت و نیـاز اسـت کـه قانون‌گذار ایران نسبت به رفع این مشکل اقدام کند که این اقدام میتواند با بهره گیری از سوابق دیگر کشورها در قانونگذاری ازجمله آمریکا باشد تا به ایـن شـکل بتـوان قـانونی کامل و متناسب با شرایط کشور داشت با اهداف و یافته های تحقیق، پیشنهادهایی به عنـوان راهکارهـای پیشـگیری اجتماعی و وضعی ازکلاهبرداری وسرقت سایبری ارائه می‌شود.

- افزایش تلاش و زحمت ارتکاب جرم کلاه‌برداری و سـرقت سـایبری از طریـق تـدبیر امنیتی دیوار آتش: فایروال ها یکی از عناصر اساس در نظام مهندسی امنیت اطلاعات هستند در دنیـای امنیـت اطالعـات و استفاده از آن‌ها به یک ضرورت اجتناب ناپـذیر است.

- تدابیر امنیتی کدگذاری و امضای دیجیتال و پسورد: در این روش، براساس معیارهـایی خاص، ازورود اشخاص ناشناس یا فاقد اعتبار جلوگیری می‌شود. این اقدام به ویژه بـرای زنان و کودکان یا اشخاصی که به هـر دلیـل آسـیب پذیر سودمند است بپردازند چراکه بدون آنکه فرصت شناسایی خود را به مجرمـان اینترنتـی بدهنـد، مـیتواننـد به فعالیت های شبکه ای بپردازند.

- پراکسی: در اینجا، از پراکسی به معنی پروسهای یاد می‌شود که در راه ترافیک شبکهای قبل ازاینکه به شبکه وارد یا از آن خارج شود، قرار میگیرد و آن را میسنجد تا ببیند با ازسیاست های امنیتی کاربر مطابقت دارد و سپس مشخص میکند که آیا به آن اجازۀ عبور از فایروال را بدهد یا خیر. بسته های مورد قبول به سرور موردنظر ارسال و بسـته هـای 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 نرم افزارهای جاسوسی به کار میرود. در زمانی که از سایت های بانکی خرید می‌شود، بیشترین بخش قابل توجه برای کاربر، امنیت وبسایت است که رمزهای بانکی دزدیده نشود که بانک ها برای ما این کار را انجام داده اند و صفحه کلید مجازی را گذاشته اند.

- تدبیر پالایه یا فیلترینگ: فیلترینگ پورتها از جمله مهمترین عملیاتی است که توسط فایروال ها انجام می‌شود و سبب می‌شود اطلاعات و سایت هایی 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. نمونهٔ سادهٔ این اقدام به کارگیری گذرواژه است که، در گذشته و اکنون جایگاه خود را حفظ کرده است به این ترتیب، تنهاکسانی حق بهره برداری از یک سیستم یا سایت را خواهند داشت که گذرواژهٔ مربوط را دریافت کنند.

منابع

۱. توانگر حمیدرضا، کاربرد آزمایش پزشکی قانونی DNA (نمونه برداری نگهداری، نمونه ها،) مجله علمی پزشکی قانونی، سال چهارم، دی و بهمن،۱۳۹۳ شماره ۱۵

۲. جعفری. امین تشخیص هویت ژنتیکی در پرتو علوم جنایی (فصلنامه حقوق پزشکی، تهران، ۱۳۹۳)

۳. سلطانی لرگانی، احمد، ارزیابی کارایی زیست فناوری در کشف علمی جرائم (با تأکید برفناوری،DNA) انتشارات کارآگاه، بهار ۶. ش ۱۳۹۱

۴. فخرز، میررحیم، کاربرد بیولوژی درعلوم جنایی دو ماهنامه کارآگاه

۵. مؤذن زادگان، حسنعلی، عظیمی فر، بابک؛ اخلاق زیستی از منظر حقوقی، فلسفی و علمی، چاپ دوم، انتشارات سمت، تهران،۱۳۹۱.

۶. نجابتی مهدی: پلیسعلمی (کشف علمی جرائم،) تهران، انتشارات سمت، چاپ سوم،۱۳۹۰