

# مکانیسم پیشگیری از کلاهبرداری رفاهی در فضای مجازی<sup>۱</sup>

اکرم محمدزاده<sup>۲</sup> جمال بیگی<sup>۳</sup> فاطمه احدی<sup>۴</sup>

## چکیده

منظور از کلاهبرداری رفاهی در این مقاله، فریب دادن و توسل به وسایل و حیل متقلبانه نهادهای دولتی برای اخذ امتیازات رفاهی بیشتر است. هدف از این مقاله مطالعه و تبیین همه جانبه مکانیسم پیشگیری از کلاهبرداری رفاهی در فضای مجازی است. با توجه به ماهیت موضوع، پژوهش حاضر از نظر هدف کاربردی و به لحاظ گردآوری اطلاعات به روش اسنادی و از طریق مطالعه منابع معتبر انجام شده و اطلاعات به دست آمده به صورت توصیفی - تحلیلی مورد تجزیه و تحلیل قرار گرفته است. یافته ها این پژوهش حاکی از راهکارهای پیشگیرانه غیر کیفری (اجتماعی و وضعی) بصورت توأمان می تواند در پیشگیری از جرم کلاهبرداری رفاهی در فضای مجازی مناسب باشد. پیشگیری غیر کیفری از کلاهبرداری رفاهی در فضای مجازی از طریق پیشگیری اجتماعی و جامعه شناختی در قالب پیشگیری رشد مدار کلاهبرداری رفاهی در فضای مجازی و پیشگیری جامعه مدار کلاهبرداری رفاهی در فضای مجازی به صورت ارائه برنامه های خانواده مدار، تدابیر آموزشی و تربیتی فضای مجازی، بالا بردن سواد رسانه ای، اطلاع رسانی و فرهنگ سازی، کنترل و نظارت، بهبود شرایط اقتصادی، تدوین کدهای رفتاری، پیشگیری وضعی هم در قالب تدابیر امنیتی دیوارهای آتشین، تدابیر پالایش (فیلترینگ) و تدابیر نظارتی، انجام خواهد شد. پلیس فتا با شیوه های پیشنهادی این پژوهش می تواند نقش موثری در کشف جرم کلاهبرداری رفاهی در فضای مجازی داشته، تا برخورد به هنگام با مجرمان از بروز جرم کلاهبرداری رفاهی در این فضا پیشگیری کند.

**واژگان کلیدی:** کلاهبرداری رفاهی، فضای مجازی، پیشگیری اجتماعی، پیشگیری وضعی

<sup>۱</sup> این مقاله مستخرج از رساله دکتری با عنوان "بررسی تطبیقی کلاهبرداری رفاهی در حقوق ایران و انگلستان" است.

<sup>۲</sup> اکرم محمدزاده، دانشجوی دکترای حقوق کیفری و جرم شناسی، واحد مراغه، دانشگاه آزاد اسلامی، مراغه a.mohamadzade094@gmail.com

<sup>۳</sup> جمال بیگی، دانشیار، گروه آموزشی حقوق جزا و جرم شناسی، واحد مراغه، دانشگاه آزاد اسلامی، مراغه، ایران (نویسنده مسئول) jamalbeigi@iau-maragheh.ac.ir

<sup>۴</sup> فاطمه احدی، استادیار، گروه آموزشی حقوق جزا و جرم شناسی، واحد مراغه، دانشگاه آزاد اسلامی، مراغه، ایران Ahadi-223@yahoo.com

فناوری اطلاعات تحولات شگرفی در روند فعالیت جامعه بشری به وجود آورده است، به گونه ای که زندگی امروزی بدون استفاده از آن با دشواری های فراوانی مواجه است. تغییرات در فناوری رسانه و ظهور شبکه های نوین ارتباطی سبب رسوخ بیشتر فناوری در زندگی انسان ها و تشکیل دنیای جدیدی به نام فضای مجازی یا سایبری شده است. امروز فضای مجازی به طور بسزایی در ارتباطات جهانی نقش ایفا می کند و به صورت روز افزونی با زندگی مردم همبستگی یافته است (حسین نژاد، ۱۳۹۸، ۵).

رشد فزاینده استفاده از فضای مجازی در کشور، آن چنان است که این پدیده، بر کلیه شئون و ابعاد زندگی در سال های اخیر تاثیر مستقیم و غیر مستقیم گذاشته است تا بدان جا که به دلیل اهمیت ساماندهی و نظارت بر فضای مجازی، رهبر معظم انقلاب، دستور تشکیل شورای عالی مجازی را در تاریخ ۱۷ اسفند ۱۳۹۰ صادر کردند (خلج آبادی فراهانی، ۱۳۹۸، ۱۲۹). شبکه اینترنت و فضای مجازی تبدیل به جزء جدانشدنی در امور شخصی، خانوادگی، سازمانی، دولتی و حتی روابط بین المللی شده است. افزایش استفاده از فضای مجازی در سطح جهان، چالش های بسیاری را در مدیریت و قانون گذاری آن ایجاد کرده است. راهبری فضای مجازی، موضوعات گسترده ای (از جمله: امور اجرایی فنی، مباحث کلان عمومی هم چون نظارت بر اینترنت و ...) را در برمی گیرد (کاشانی و همکاران، ۱۳۹۶، ۲۹). پیشرفت و همه گیری فضای سایبر و اینترنت، جرائم رایانه ای خسارت های سنگینی به اقتصاد می رساند و این مسئله تهدیدی برای امنیت ملی و رفاه اجتماعی مردم به شمار می آید (رضایی و همکاران، ۱۴۰۰، ۱۱۶).

بررسی ها نشان می دهد جرایم فضای مجازی در ایران نیز به موازات سایر کشورها در حال شکل گیری، رشد و گسترش بوده و روز به روز بزرگ تر و پیچیدگی آن ها افزوده می شود که آمار اعلام شده توسط پلیس آگاهی ناجا، نشان دهنده گستردگی آن است. مطابق بررسی ها کاربران ایرانی در فضای مجازی با تهدید هایی در خصوص حریم خصوصی مواجه هستند. هم چنین به طور کلی تهدیدها و آسیب های امنیتی در فضای مجازی جعل و سرقت هویت، انتشار بدافزارها، سرقت و سوء استفاده از افشای اطلاعات و داده های شخصی، دسترسی غیرمجاز به داده های محافظت شده، سرقت مالی، اعتیاد الکترونیکی، گسترش روابط نامشروع، شایعه پراکنی، ایجاد شبهات دینی و سیاسی، تمایا به ارتکاب جرایم، کم رنگ شدن هنجارهای اجتماعی و هویت فردی و دیگر موارد مشابه هستند که در سال های اخیر، با گسترش استفاده از فضای مجازی در جامعه ایرانی ایجاد شده اند (نعیمی، ۱۳۹۶، ۳).

یکی از این جرائم رایانه ای که در فضای مجازی به راحتی تحقق می یابد، جرم کلاهبرداری رفاهی است. منظور از کلاهبرداری رفاهی، فریب دادن نهادهای دولتی برای اخذ امتیازهای رفاهی بیشتر است. (وایت و هنیس، ۱۳۸۶، ۱۱۵).<sup>۱</sup>

<sup>۱</sup> Wait hanis

بروز پدیده مجرمانه کلاهبرداری رفاهی در فضای مجازی که کشف آن زمان و هزینه های زیادی در پی خواهد داشت؛ در این میان پیشگیری، تدابیری است که از پایه مانع از رخداد جرم شده و از ریشه باعلل پیدایی بزه و جرم، مبارزه می کند (عشایری و همکاران، ۱۳۹۷، ۳۳). مانند هر جرم دیگری پیشگیری از وقوع این جرایم بسیار باصرفه تر و کم هزینه تر از طی فرآیند رسیدگی کیفری آن ها و تحمل خسارات بی شمار است (دستور و همکاران، ۱۳۹۳، ۵۸). از طرفی اولین و مهم ترین وظیفه پلیس پیش از مقابله با جرایم، پیشگیری از وقوع آن است (محمدی، ۱۳۹۸، ۹۸). از این رو در بهمن ماه ۱۳۸۹ نیروی انتظامی جمهوری اسلامی ایران، با تشکیل پلیس فضای تولید و تبادل اطلاعات (فتا) به مقابله و پیشگیری از جرایم سایبری پرداخته است (محمدی، ۱۳۹۸، ۹۶). تعامل و همکاری موثر میان پلیس و سازمان های مختلف می تواند در جهت نیل به اجرایی ساختن فرآیند پیشگیری از جرایم به ویژه جرایم سایبری کمک کند. هم چنین ارائه آموزش همگانی و شناسایی و آموزش های خاص به افراد و هم چنین سازمان هایی که احتمال می رود در معرض جرایم سایبری قرار گیرند یکی دیگر از شیوه های پیشگیری از این جرایم است که توسط پلیس انجام می شود (جعفری و همکاران، ۱۳۹۷، ۹۵).

هدف اصلی این تحقیق، بیان مفهوم کلاهبرداری رفاهی و جلوه های ارتکاب آن در فضای مجازی، مکانیسم های پیشگیری غیر کیفری از کلاهبرداری رفاهی در فضای مجازی از طریق پیشگیری اجتماعی در قالب پیشگیری رشدمدار کلاهبرداری رفاهی در فضای مجازی و پیشگیری جامعه مدار کلاهبرداری رفاهی در فضای مجازی به صورت ارائه برنامه های خانواده مدار، تدابیر آموزشی و تربیتی فضای مجازی، بالا بردن سواد رسانه ای، اطلاع رسانی و فرهنگ سازی، کنترل و نظارت، بهبود شرایط اقتصادی، تدوین کدهای رفتاری، پیشگیری وضعی هم در قالب تدابیر امنیتی دیوارهای آتشین، تدابیر پالایش (فیلترینگ) و تدابیر نظارتی انجام خواهد شد.

### پیشینه تحقیق

در خصوص موضوع مقاله منابع مستقلی وجود ندارد اما منابع زیر نزدیک به موضوع می باشند:

۱- **اوجاقلو و زندی (۱۴۰۰)**، در مقاله اش با عنوان: **«پیشگیری از کلاهبرداری سایبری در سیاست جنائی ایران با نگاهی به رویه قضایی»** معتقدند. پیشگیری از کلاهبرداری در فضای مجازی را در دو محور پیشگیری کیفری و غیر کیفری مورد بررسی قرار داده است و مجازات های مواد ۶۷ قانون تجارت الکترونیک و ماده ۷۴۱ قانون مجازات اسلامی را مورد توجه قرار داده است و معتقد است در رویه قضایی به دلیل عدم فهم یکسان قضات و به دلیل عدم تخصص کافی در زمینه سایبر موجب تشتت آراء در این زمینه شده است همچنین ایشان معتقدند علاوه بر اقدام کیفری که قانونگذار برای این مجرمین در نظر گرفته باید روش ها و اقدامات غیر کیفری هم به کار برد.

۲- **اسماعیلی کریزی و کاظمی گلوردی (۱۴۰۰)**، در مقاله اش با عنوان: **«پیشگیری از جرائم خاص انتظامی و نظامی در سیاست جنائی ایران»** معتقدند. راه های پیشگیری از جرائم خاص نظامی و انتظامی

در سیاست جنائی ایران در دو بعد پیشگیری کیفری و پیشگیری غیر کیفری قابل انجام است. تمرکز بیش از حد فرماندهان و مسئولین بر نظم و انضباط در محیط پادگان و توجه ویژه به کنترل و ورود و خروج افراد، منجر به کاهش رویکردهای پیشگیری اجتماعی و استفاده از روش های پیشگیری وضعی از جرائم خاص نظامی و انتظامی است.

۳- **محمدزده و بیگی و احدی (۱۴۰۰)**، در مقاله اش با عنوان: «**مبانی فقهی و حقوقی جرم انگاری**

**کلاهبرداری رفاهی در ایران**» معتقدند. در کلاهبرداری رفاهی رفتار ارتكابی خود به خود جرم است چون کسب امتیازات رفاهی و مالی غیر قانونی از دولت جرم است. از آن جا که این امتیازات رفاهی و مالی از دولت مستحق افرادی که دارای شرایط امتیازات رفاهی و مالی می باشند است، نه اشخاصی که با جعل مدارک خود را شایسته آن امتیازات می داند. بنابراین این رفتارها جرم انگاری شده اند و هر گاه این وصف در رفتار مرتکب وجود داشت، مستحق مجازات خواهد بود و حاکم باید او را به یکی از مجازات های تعزیری که آن را مناسب تشخیص می دهد محکوم کند.

۴- **شاه محمدی و زلفی (۱۴۰۰)**، در مقاله اش با عنوان: «**شناسایی و اولویت بندی شیوه های نظارت بر**

**جرایم در فضای مجازی**» معتقدند کشف و پیشگیری از جرایم در فضای مجازی مستلزم شناسایی شیوه های نظارت بر جرایم در این فضا است تا بتوان از این طریق با نظارت موثر بر جرایم نسبت به کنترل جرایم در این فضا اقدام کرد.

۵- **توکلی، مرتضوی و کشاورز ترک (۱۳۹۹)**، در مقاله اش با عنوان: «**تعیین عوامل راهبردی موثر بر**

**پیشگیری از جرایم سایبری با رویکرد دلفی فازی**» معتقدند. مهم ترین عوامل راهبردی موثر بر پیشگیری از جرایم سایبری، در ۳۱ عامل و ۷ گروه شامل عوامل فرهنگی، عوامل اجتماعی، عوامل فنی، عوامل ایجابی، عوامل سلبی، عوامل درون سازمانی و عوامل برون سازمانی هستند. نتایج نشان داد فرهنگ سازی و تولید رسانه ای، آگاه سازی خانواده ها، استفاده از ابزارهای امنیتی توسط کاربران، در اختیار داشتن نیروهای متخصص و آموزش دیده از جمله عوامل موثر و نقش آفرین در پیشگیری از جرایم سایبری هستند که بایستی در طراحی و انتخاب برنامه ریزی های راهبردی مناسب مورد توجه ویژه قرار گیرند.

۶- **نظری منظم و مجیدی و هندیانی و وفادار (۱۳۹۸)**، در مقاله اش با عنوان: «**بررسی عوامل موثر بر**

**جرم کلاهبرداری در فضای سایبر**» معتقدند. جرم کلاهبرداری سایبری جرم علیه اموال می باشد. هم چنین همکاری پلیس با مقامات قضایی، تجهیزات مدرن، علم و آگاهی از علوم رایانه توسط کارآگاهان سایبری و.. در کشف جرم کلاهبرداری سایبری تاثیر دارد.

۷- **جعفری و سلیمانی (۱۳۹۷)**، در مقاله اش با عنوان: «**نقش پلیس در تامین امنیت و سالم سازی فضای**

**سایبر با رویکرد پیشگیری اجتماعی از جرایم سایبری**» چنین آورده است پیشگیری اجتماعی جامعه مدار عوامل اجتماعی جرم زا در یک جامعه معینی را مورد هدف قرار می دهد و اقداماتی که در این راستا به

اجرا در می آید با هدف از بین بردن زمینه های اجتماعی ایجاد کننده انگیزه های مجرمانه است در این راستا راه کارهای مختلفی را می توان پیشنهاد کرد که عبارتند از: فرهنگ سازی، نظارت، آموزش، تدوین کد های رفتاری و حل مسائل و مشکلات اقتصادی.

۸- **دیمیتری پرسیا دیوید، مارکوس ماتئاس کتوب و آلن مرمود (۲۰۲۰)**<sup>۱</sup>، در پژوهش خود با عنوان: «**جذب دانش برای امنیت سایبری: نقش آگاهی و باورهای انسانی**» به مطالعه روند فعلی مدیریت، کاربرد، نظارت و اهمیت رسانه های اجتماعی در شرکت های ملی از طریق مصاحبه های نظرخواهی با شاغلان در ۱۰۰ تا ۵۰۰ شرکت آمریکایی که از نظر فروش درصد قرار داشتند پرداخت. یافته ها نشان می دهد که در استفاده و اهمیت درک شده رسانه های اجتماعی بین شاغلین شکاف عظیمی وجود دارد و این که روند آگاهی و درک ارزش بالقوه این رسانه در بین غیر کاربران به منظور پذیرش کند می باشد. علاوه بر این، مسیرهای جدیدی برای تحقیق و تمرین در استفاده از رسانه های اجتماعی به دلیل مدیریت موضوعات آشکار شد. رسانه های اجتماعی و شبکه های آنلاین شخصی در نحوه ارتباط هم زمان اقصی نقاط دنیا با هم انقلاب و دگرگونی ایجاد کرده است.

۹- **شوکان، عبدیژامی، عثمانوف و عبداکیموف (۲۰۱۹)**<sup>۲</sup>، پژوهشی با عنوان: «**کنترل جرم در حوزه فناوری های اطلاعاتی در جمهوری ترکیه**» انجام داده اند. یافته ها حاکی از سیاست مداوم آموزش برای کارمندان امنیت سایبری است به طوری که کاربران و متخصصان امنیت سایبری کشور می بایست با پیچیدگی ها و نوآوری های عرصه فناوری سایبر به صورت پیوسته و مداوم آشنا باشند تا از این روزنه، به نحو شایسته ای از جرایم سایبری پیشگیری و بر فضای سایبر نظارت موثر و پیشگیرانه اعمال کنند.

۱۰- **شیندر و کروس (۲۰۱۹)**<sup>۳</sup>، پژوهشی با عنوان: «**درک پیشگیری از وقوع جرایم سایبری پرداخته اند.** برابر یافته؛ درک مفاهیم اولیه امنیتی از جرایم سایبری، مزیت مشخصی در برقراری ارتباط هوشمندانه به کارکنان فناوری اطلاعات می دهد؛ در این رستا یک متخصص امنیت شبکه خوب یا یک مامور خوب پیشگیری از وقوع جرم، می داند که هر برنامه امنیتی باید چند لایه باشد تا بتواند موثر واقع شود. این موارد شامل امنیت داده های ذخیره شده بر روی دیسک ها، امنیت داده های افراد و کاربران در شبکه و وسیله ای برای تایید هویت کاربران، رایانه ها و سایر اشخاصی است که به منابع شبکه دسترسی دارند.

بررسی تحقیقات انجام شده در زمینه پیشینه پژوهش نشان می دهد که هر یک مباحث مختلفی را در مورد مسئله پژوهش دنبال کرده اند و با وجود آن که تحقیقاتی در رابطه با پیشگیری با جرایم سایبری انجام شده است. این تحقیق به صورت جامع تر و از یک زاویه جدید به موضوع مکانیسم پیشگیری از کلاهبرداری رفاهی در فضای مجازی

<sup>۱</sup>. Dimitri Percia David, Marcus Matthias Keupp, Alain Mermoud

<sup>۲</sup>. Snukan, Abdiznam, Ospanovand Abdakimov

<sup>۳</sup>. Sninder and Cross

پرداخته است. حال سؤال این است که به چه نحوی یا مکانیسم‌هایی می‌توان از وقوع جرم کلاهبرداری رفاهی در فضای مجازی پیشگیری کرد؟ آیا برای مقابله با جرم کلاهبرداری رفاهی همانند سایر رفتارهای مجرمانه می‌توان قواعد کلی یا تکنیک‌های پیشگیری غیر کیفری را در این زمینه مورد اجرا گذاشت؟

## ۱- مفهوم کلاهبرداری رفاهی و جلوه‌های آن

### ۱-۱- مفهوم کلاهبرداری رفاهی

کلاهبرداری در مفهوم کلاسیک و معمول آن، که موضوع ماده ۱ قانون تشدید است به « اعمال حیله و تقلب که منتهی به فریب دیگری و بردن مال او گردد» تعریف می‌شود (آقای نی و همکاران، ۱۳۹۷، ۳۷). برخی نیز کلاهبرداری را « بردن مال دیگری از طریق توسل توأم با سونیت به وسایل یا علمیات متقلبانه» (میرمحمد صادقی، ۱۳۹۶، ۵۶). تعریف نموده اند اما منظور از کلاهبرداری رفاهی، فریب دادن نهادهای دولتی برای اخذ امتیازهای رفاهی بیشتر است. (وایت و هنیس، ۱۳۸۶، ۱۵۱).<sup>۱</sup> اگر فرد فکر کند که در موقعیت اقتصادی مغلوب یا پایین باقی خواهد ماند و امکان ترقی و تغییری در جایگاه اجتماعی وی، پیش نخواهد آمد و به عبارت دیگر فکر کند موقعیت اقتصادی ثابت باقی خواهد ماند، این تفکر او را سوق می‌دهد به این که راهکاری برای این وضعیت خود بیابد. یکی از این پاسخ‌ها ارتکاب جرم و تشکیل خرده فرهنگ مجرمانه برای دستیابی به اهداف است. (نجفی ابرندآبادی، ۱۳۸۴، ۷۴). برخلاف تحلیل‌های علت شناختی گذشته، عده‌ای از نویسندگان معاصر، ارتکاب جرم کلاهبرداری را با نظریه «نظریه فرصت جرم» تبیین می‌کنند. این نظریه نسبت به نقش شخصیت در گذر از اندیشه به فعل، بی‌اعتنا است، افزایش میزان کلاهبرداری در وضعیت کنونی را، با رشد و توسعه قابل توجه فرصت‌های کلاهبرداری توجیه می‌کند (گسن، ۱۳۹۸، ۱۰۰).<sup>۲</sup>

کلاهبرداری رفاهی به دریافت یا استفاده نادرست از کمک‌های عمومی یا مزایای ارائه شده از طریق برنامه‌های دولتی که برای کمک به افراد کم‌درآمد، ناتوان یا افراد مسن ارائه می‌شود، اشاره دارد.

کلاهبرداری رفاهی یا کمک‌های عمومی می‌تواند اشکال مختلفی داشته باشد، از جمله تقلب دریافت‌کننده، تقلب در صورت حساب، تقلب ارائه‌دهنده، انواع دیگر کلاهبرداری (pirius, ۲۰۲۱, p۷۸۱).<sup>۳</sup> در کلاهبرداری رفاهی مفاهیم اخلاق گرایانه «شایسته بودن» زیربنای آن است و سیاست‌های رفاهی اساساً با تقاطع جنسیت، طبقه و نژاد مرتبط است (Semmelhack, ۲۰۲۱, p۴۴).<sup>۴</sup> دو مشکل مهم در برنامه‌های کمک‌های رفاهی وجود دارد: شیوع تقلب در رفاه و پذیرش ناقص، به موجب آن افراد فقیر واجد شرایطی به مطالبه مزایای رفاهی ندارند. گرچه ننگ رفاهی در درک ظهور

<sup>۱</sup> Wait hanis

<sup>۲</sup> Gassin

<sup>۳</sup> pirius

<sup>۴</sup> Semmelhack

کلاهبرداری رفاهی و پذیرش ناقص اهمیت دارد که تعامل پویا بین مدعیان واجد شرایط و غیر واجد شرایط نیز در تعیین انگ رفاه اهمیت دارند. (Itaya, Kurta, 2021, p41).<sup>۱</sup>

برای اثبات جرم کلاهبرداری رفاهی عدم افشای یک واقعیت مادی، دولت باید دو عنصر زیر را بدون تردید معقول اثبات کند:

۱. (متهم) عمداً با اظهارات نادرست، ارائه نادرست، جعل هویت یا سایر ابزارهای متقلبانه نتوانسته یک واقعیت مادی را فاش کند.

۲. این واقعیت برای تعیین صلاحیت (متهم) برای دریافت کمک‌های عمومی از هر برنامه کمک مورد استفاده قرار گیرد. متقلبانه به معنای قصد یا هدف سرکوب حقیقت یا ارتکاب فریب است.

«کلاهبرداری» شامل وارد کردن سوابق متقلبانه به سیستم رایانه‌ای، استفاده غیرمجاز از امکانات رایانه‌ای، تغییر یا تخریب عمدی یا عمدی اطلاعات یا فایل‌های رایانه‌ای، سرقت ابزارهای مالی، داده‌ها و سایر دارایی‌های است.

«کمک یا کمک» به معنای کمک، کمک یا تسهیل است.

علماً یعنی با علم و درک واقعی از حقایق یا حقیقت.

آگاهانه به معنای عملی است که بااراده و عمد انجام شود و نه از روی اشتباه یا تصادف یا دلیل بی‌گناه دیگر.

به هر حال، افرادی که در سطوح پایین‌تر نردبان اقتصادی-اجتماعی قرار دارند، به احتمال زیاد فرصت‌های محدود شده بیشتری را نسبت به آنانی که از خانواده‌های ثروتمند یا مرفه هستند، تجربه خواهند کرد. به عنوان نمونه، یکی از شرایط متقاضیان دریافت مسکن مهر در شهر تهران، سابقه سکونت پنج ساله متقاضیان بود تا بتوانند از مسکن مهرشهرهای جدید اطراف تهران استفاده کنند؛ اما در ابتدای ثبت نام مسکن مهر، مدارکی که ثابت می‌کرد متقاضیان شرایط مسکن مهر را دارند، به راحتی با جعل یک اجاره‌نامه قابل دسترس بود و تعداد قابل توجهی توانستند با جعل مدارک، برای مسکن مهر ثبت نام کنند. سرانجام دولت در سال جاری اعلام کرد که اجاره‌نامه را برای احراز شرایط پنج ساله سکونت، قبول ندارد و باید مدارکی از جمله شناسنامه فرزند، برای اثبات سکونت ارائه شود و بدین ترتیب بخش قابل توجهی از متقاضیان در آستانه تحویل واحدها حذف شدند.

## ۲-۱- جلوه‌های کلاهبرداری رفاهی در فضای مجاری

در این قسمت سعی شده موضوعاتی که امکان کلاهبرداری در فضای مجازی را دارد مورد بررسی قرار گیرد.

<sup>۱</sup> Itaya, Kurta

۲-۱-۱- کلاهبرداری بیمه ای: ممکن است کلاهبرداری در فضای مجازی با موضوع بیمه باشد. امروزه صنعت بیمه جایگاه خود را به عنوان یکی از ستون های اصلی جامعه مدرن تثبیت کرده است اما بدون شک صنعت بیمه جایگاه فعلی خود را در آینده حفظ و حتی مستحکم تر خواهد کرد. اما یکی از معضلات مهم در صنعت بیمه، کلاهبرداری بیمه ای یا سوء استفاده بیمه ای است نه تنها سود آوری بیمه گران را در معرض خطر قرار می دهد. بلکه بر کل مجموعه صنعت بیمه تأثیر منفی می گذارد و ممکن است برای ساختارهای شکل یافته اجتماعی و اقتصادی بسیار مضر باشد. اعتقاد بر این است که کلاهبرداری بیمه ای هزینه ها را در برخی رشته های بیمه ای هم چون اتومبیل، آتش سوزی و درمان به طور قابل ملاحظه افزایش می دهد. در مجموع کلاهبرداری تهدیدی بنیادی برای شالوده بیمه و کار کردهای آن می باشد (رشیدی، ۱۳۸۶، ۲۹). کلاهبرداری بیمه ای یعنی اعلام عمدی خسارت های جعلی، اعلام خسارات بیش از مقدار واقعی آن، یا هر روش دیگر برای به دست آوردن مبلغی بیش از آن چه که بیمه گذار قانوناً مستحق دریافت آن باشد.

بیمه یک رابطه مبتنی بر قرارداد است که بر اساس آن بیمه گر با بیمه گذار توافق می کند در قبال پرداخت حق بیمه از طرف بیمه گذار، به نمایندگی از او تامین مالی برای پوشش خسارت یک نفع بیمه پذیر (خسارت ناشی از یک یا چند حادثه تعریف شده ولی نامطمئن که در آینده رخ می دهد)، پس از این که ادعای خسارت به طور رسمی از طرف شخص زیان دیده (خود بیمه گذار یا شخص ثالث) مطرح شد، را انجام دهد. تمام اشخاص درگیر در این قرارداد در هر لحظه به طور قانونی باید با طرف مقابل بر اساس اصل حد اعلای حسن نیت عمل کنند. این اصل آن ها را ملزم می کند که تمام اطلاعات اساسی و عمده ای که بر آن ها مکشوف می شود را به گونه ای متقابل افشا کنند. بیمه گر علاوه بر بیان روشن و صریح در صدور بیمه نامه در مورد این که چه ریسک هایی باید پوشش داده شود و به چه ریسک هایی پوشش داده نمی شود، هنگام پرداخت خسارت نیز با همکاری یا خسارت دیده و پرداخت جبرانی به موقع، سریع و استاندارد های حرفه ای پذیرفته شده و اخلاقیات عمل کند. عدم وجود حسن نیت به معنی کلاهبرداری نیست. اگر چه معنای دقیق کلاهبرداری در سیستمهای حقوقی متفاوت است. اما در اصطلاح حقوقی بطور کلی عمل کلاهبرداری از سوی هر کدام از طرف های قرارداد باید دارای شرایط آن باشد و از طرفی فرد کلاهبردار باید سوء نیت داشته باشد. برای صدق عنوان مجرمانه بر فعل یا ترک فعل علاوه بر عنصر قانونی و مادی نیازمند به عنصر معنوی نیز می باشد؛ چرا که هر عملی بدون اراده و قصد مجرمانه؛ بودنش منتفی خواهد شد، به علت فقدان عنصر معنوی عمل ارتكابی حتی در جرائم مادی صرف نیز قانون گذار عنصر معنوی را لحاظ کرده است. (صبری، ۱۳۹۴، ۱۱۳).

بنابراین سوء نیت و کلاهبرداری در صنعت بیمه باعث عمل نامطلوبی که سوء استفاده بیمه ای نامیده می شود، می گردد. سوء استفاده بیمه ای به عملی گفته می شود که از بیمه در راهی مخالف هدف آن یا مخالف قانون استفاده شود. اگر چه کلاهبرداری در قوانین معنای خاص دارد، اما مفهوم کلاهبرداری بیمه ای در عمل غالباً به صورتی که شامل سوء استفاده بیمه ای نیز باشد بدون دلالت بر پیامدهای مستقیم قانونی بکار برده می شود. نامتقارن بودن اطلاعات پایه اصلی کلاهبرداری بیمه ای می باشد.



۲-۱-۲- ازدواج ها و طلاق های کاسب کارانه در ایران: خانواده در ایران یکی از اصلی ترین نهادهای اجتماعی نام گرفته است همان طور که « ازدواج رکن ماندگار خانواده ایرانی است» (آزاد ملکی، ۱۳۹۵، ۱۴۴). هر نوع تحلیل از خانواده در ایران بدون ارجاع به دو پدیده ازدواج و طلاق ناکافی به نظر می رسد. این در حالی است که ازدواج ها و طلاق های کاسب کارانه جدا شدن ازدواج و طلاق در صورت رسمی و حقوقی آن را از خانواده به عنوان نهادی اجتماعی نشان می دهند. به عبارت دیگر ازدواج ها و طلاق های کاسب کارانه برهم زننده ارتباط عرفی و حقوقی هستند که میان خانواده و این دو پدیده وجود دارد. ولیکن در تعریفی کلی می توان گفت که در ازدواج کاسب کارانه فرد به صورت رسمی ازدواج می کند اما تشکیل خانواده را هدف خود از ازدواج نمی داند و در طلاق کاسب کارانه فرد طلاق می گیرد اما انگیزه خود را از طلاق، پایان دادن به خانواده ای که تشکیل داده است بیان نمی کند. از این منظر ازدواج و طلاق کاسب کارانه در ربط با نهاد خانواده پروبلماتیزه شده و پیامدهای پیش بینی نشده آن در وهله اول گریبانگیر نهادهای حقوقی و اجرایی می شود. در حالی که هدف از وضع قواعد تسهیل کننده ازدواج و طلاق کاسب کارانه در بدو امر حمایت از نهاد خانواده بوده است. به این ترتیب بررسی ازدواج ها و طلاق های کاسب کارانه نشان از نظم جدیدی دارد که در آن قواعد حمایت کننده خانواده نافی انسجام آن شده و در نهایت نکاح و طلاق ارتباط خود را با نهاد خانواده از دست می دهند (اعتمادی فرد و همکاران، ۱۴۰۰، ۱۱۸).

ازدواج ها و طلاق های کاسب کارانه محدود به چند مورد خاص نیستند، بلکه در ایران متنوع تر و پیچیده تر از تصور اولیه بوده و به همیت دلیل شناسایی آن ها نیز به سادگی امکان پذیر نیست. علی رغم این تکررات تمامی ازدواج ها و طلاق هایی که در این مطالعه تحت عنوان ازدواج و طلاق کاسب کارانه بررسی شده اند واجد جنبه ای مشترک هستند: ازدواج بدون قصد تشکیل خانواده و طلاق بدون انگیزه پایان بخشیدن به تداوم نهاد خانواده. (وهر، ۱۳۹۲، ۱۴۰). در صورتی که این نوع ازدواج ها و طلاق ها در فضای مجازی صورت گیرد بی تردید نوعی ارتباط با موضوع مقاله حاضر دارد طلاق ها و ازدواج هایی که با هدف استخدام یا اخذ معافیت از خدمت برای فرزندان، مهاجرت به خارج، طلاق زوجین برای دریافت مستمری پدر فوت شده ی زوجه و... صورت می گیرد.

در هر یک از موارد ازدواج و طلاق کاسب کارانه- علی رغم آنکه جرمی رخ نداده و فرد نیز تحت هیچ کدام از عناوین مجرمانه قابل تعقیب نیست- نهاد حقوقی حامی ازدواج یا طلاق کاسب کارانه خواهد بوده و امکانات رسیدن به آن را برای ایجاد، استحکام و انتظام خانواده به تحریر درآمده سبب شده اند تا در مرتبه اول ازدواج و مقررات ناظر بر آن تنها به فرم هایی بدل شوند که در داخل آن ها هیچ نشانی از قصد و تلاش طرفین برای شکل دادن به خانواده وجود نداشته باشد. در حقیقت، آن چه مبنا و مورد توجه است « قرارداد نکاح» و آثار آن است و نه «نهاد خانواده» به این ترتیب هر چند این قواعد برای به جا آوردن خانواده تنظیم شده اند (اعتمادی فر و همکاران، ۱۳۰، ۱۴۰۰).

## ۲- مبانی پیشگیری از کلاهبرداری رفاهی در فضای مجازی

### ۲-۱- تضرر افراد

کلاهبرداری در همه حالات چه در فضای حقیقی یا فضای مجازی موجب تضرر افراد از طریق بردن اموال آنها می شود. کلاهبرداری بزهی مرکب و رکن مادی آن چند جزئی است. اولین جزء رکن مادی آن، توسل بزهکار به وسایل متقلبانه است. با توجه به پیشرفت علم و فناوری و افزایش آگاهی مردم، بر تنوع و پیچیدگی وسایل متقلبانه روزبه روز افزوده میشود و امروزه بزهکاران از رایانه و فضای مجازی برای فریب مردم استفاده میکنند. دومین جزء رکن مادی، اغفال بزه‌دیده است؛ یعنی بزه‌دیده بر اساس علل و عوامل مختلفی فریب خورده و در مرحله‌ی بعد اموالش را با رضایت خود در اختیار بزهکار قرار میدهد. (خسرو شاهی و همکاران، ۱۳۹۵، ۴۵).

با توجه به اینکه در کلاهبرداری افراد فریب خورده و اموال خود را در اختیار کلاهبردار قرار می دهند در واقع ضرر مالی به افراد می رسد که در این راستا افراد اموالی که با زحمت بسیار به دست آورده بودند را با دست خود به کلاهبردار می دهند. در فضای مجازی با توجه به اینکه افراد همدیگر را نمی بینند احتمال توسل به وسایل متقلبانه و تضرر مالی افراد زیاد است این در حالی است که علاوه بر قوانین جاری در منابع معتبر فقهی تضرر افراد مذموم شمرده شده و به عنوان یک قاعده بیان می شود. معنای قاعده لاضرر این است که در اسلام هیچ ضرر و اضرائی وجود ندارد. از این قاعده با عناوین دیگری نیز یاد شده است. تعبیری همچون قاعده ضرر، قاعده ضرر و ضرار، قاعده لا ضرر و لا ضرار و قاعده نفی ضرر (مشکینی، ۱۳۸۶، ۲۰۳).

### ۲-۲- نظم عمومی در اجتماع

نظم عمومی در جامعه ایجاب می کند برای اینکه افراد بتوانند در جامعه به عنوان یک شهروند از تمام فضای امکانات استفاده کنند باید اعتماد کامل داشته باشند که مکانیزمی وجود دارد که از آنها حمایت می کند و کلاهبردار قابل تعقیب و قابل کنترل است در غیر این صورت افراد در فضای مجازی اعتماد به همدیگر نخواهند داشت با توجه به اینکه امروزه بیشتر معاملات در فضای مجازی است چه بسا نظم عمومی بیشترین ارتباط را با فضای مجازی و کنترل و مدیریت و پیشگیری از وقوع جرم در فضای مجازی را داشته باشد.

نظم عمومی مشتمل بر ارزش ها و مصالح عالی جامعه مفهومی شناخته شده در نظام های حقوقی ملی است کارکرد مهم نظم عمومی ملی تحدید اصلی آزادی قراردادی و ممانعت از اجرا شروط مخالف نظم عمومی است. گفته می شود متولی نظم عمومی ملی محاکم هستند. (حدادی، ۱۳۸۹، ۱۸۲).

مفهوم نظم عمومی از جمله مفاهیمی است که تعریف آن به لحاظ منطقی دارای اوصاف سهل و ممتنع است دشواری تعریف این مفهوم سبب شده است تا در نوشته های مربوط به نظم عمومی مطالب بسیاری به تعاریف و نظرهای مختلف

راجع به آن اختصاص یابد دکتر جعفر لنگرودی (۱۳۹۲) نظم عمومی را اینگونه تعریف کرده است: مجموعه ی سازمانهای حقوقی و قواعد مربوط به حسن جریان امور راجع به اداره یک کشور یا راجع به حفظ امنیت و اخلاق در روابط بین افراد به طوریکه افراد نتوانند از طریق قراردادهای خصوصی از آن تجاوز کنند. بنابراین برای حفظ نظم عمومی در جامعه لازم است جرائم کلاهبرداری رفاهی پیشگیری و مورد کنترل قرار گیرد.

### ۳- تکنیک های پیشگیری اجتماعی از جرم کلاهبرداری رفاهی در فضای مجازی

پیشگیری اولین و بهترین گام در یک پدیده روی طولانی به سوی اینترنتی باز، شفاف، آزاد و درعین حال امن است. پیشگیری از جرائم مجازی باید باهدف مختل کردن این نوع جرائم، دستگیری مجرمین و ضبط سودهای غیرقانونی ناشی از آن مورد توجه قرار گیرد. چنین اهدافی تنها با اجرای قانون حاصل نمی شود، بلکه نیاز به تلاش تلفیقی تمامی سازمانهای وابسته به دولت، دستگاههای مجری قانون، بخش های خصوصی، شهروندان و... دارد (محمدی و همکاران، ۱۳۹۵، ۳۳).

در این قسمت از تحقیق به ارائه راهکارها یا سازوکارهای پیشگیری اعم از پیشگیری اجتماعی جامعه مدار و پیشگیری رشد مدار از وقوع جرم کلاهبرداری رفاهی در فضای مجازی، با یکایک تکنیک های پیشگیرانه می پردازیم.

یکی از مهم ترین راه های پیشگیری از کلاهبرداری سایبری از جمله کلاهبرداری رفاهی در فضای مجازی به وسیله پیشگیری اجتماعی جامعه مدار سایبری از طریق آموزش های عمومی و رسانه های 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 برمی گیرد. کارکرد رسانه های جمعی در مورد پیشگیری از کلاهبرداری سایبری می تواند از طریق آگاه کردن مردم از پیامدهای ناگوار این جرم (چه بزهکار باشد، چه بزه دیده) و نیز دادن الگوهای مناسب رفتاری جهت جلوگیری از ارتکاب و تکرار آن باشد که از این طریق می توانند نقش مهمی در پیشگیری از جرم داشته باشند (انصاری و همکاران، ۱۳۹۸، ۱۴۳).

در زمینه اقدامات پیشگیرانه در حوزه پیشگیری اجتماعی از (جرم کلاهبرداری رفاهی در فضای مجازی) مسئله آموزش کاربران اینترنت، اعم از کاربران خانگی و کارکنان خانگی و کارکنان ادارات و فرهنگ سازی در جامعه، مؤثرترین عامل در انصراف بزهکاران بالقوه از ارتکاب جرم در محیط سایبر است. کاربران خانگی و کارکنان ادارات که با تأسیسات رایانه ای و مخابراتی مخصوصاً در مراکز حساس سروکار دارند، باید در زمینه امنیت سایبری باهدف تربیت نیروی انسانی ممتاز و متعهد، مباحث مربوط به امنیت، شامل امنیت شبکه، امنیت در سرویس های وب، امنیت سامانه عامل، رمزنگاری، تحلیل بدافزار، مهندسی اجتماعی معکوس، ردگیری در فضای سایبری و امنیت سامانه های تلفن همراه، آموزش و آگاهی کافی داشته باشند (قدیر و همکاران، ۱۳۹۸، ۲۴۴).

تدابیر و اقدامات پیشگیری اجتماعی به دودسته تقسیم می شوند: زمانی که تأثیر گذاری بر محیط های پیرامون انسان مدنظر است که اصطلاحاً پیشگیری جامعه مدار یا محیط اجتماعی گفته می شود و زمانی که تأثیر گذاری در مراحل مختلف رشد

کودک و نوجوان ناسازگار منحرف یا بزهکار اعمال می‌شود که پیشگیری فردمدار با رشد مدار گفته می‌شود (پور قهرمانی، ۱۳۹۵:۸۱). حال پرسش این است که این نوع پیشگیری در مورد جرم کلاهبرداری رفاهی در فضای مجازی قابلیت اجرا را دارد یا خیر؟ به نظر می‌رسد پیشگیری محیطی بستگی به نوع جرم، شرایط و اقتضائات محیطی، تدابیر خاص خود را می‌طلبد و یک امر ثابت و کلی که شامل تمامی جرائم باشد نیست بلکه یک امر نسبی تلقی می‌شود و بسته به نوع و ویژگی‌های هر جرمی ممکن است تدابیر متفاوتی اتخاذ شود و جرم کلاهبرداری رفاهی هم از این قاعده مستثنی نیست.

از راهکارهای دیگر پیشگیری جامعه مدار می‌توان به دیجیتالی کردن محتواهای فرهنگی نام برد که در کشور کانادا و در کنار برنامه‌های تولید محتوای فرهنگی دیجیتال مورد پشتیبانی قرار گرفته و برنامه‌ها، طرح‌ها و پروژه‌های فراوانی را در راستای دیجیتالی سازی محتواهای فرهنگی کشور هم چون آثار هنری و فرهنگی و آثار فرهنگی فاخر و دسترس‌پذیر ساختن آن‌ها، تأسیس و راه‌اندازی کرده است (عاملی، ۱۳۹۰، ۳۶۴). با توجه به موضوع و ماهیت جرم کلاهبرداری رفاهی اهم تدابیر و مؤلفه‌هایی که می‌تواند به‌عنوان پیشگیری اجتماعی جامعه مدار و پیشگیری اجتماعی رشد مدار از وقوع جرم کلاهبرداری رفاهی در فضای مجازی تلقی شود.

### ۳-۱-۳- تدابیر پیشگیری اجتماعی جامعه مدار از جرم کلاهبرداری رفاهی در فضای مجازی

۳-۱-۱-۳- فرهنگ‌سازی: اولین گام در پیشگیری از جرم کلاهبرداری رفاهی در فضای مجازی فرهنگ‌سازی است. فرهنگ فناوری اطلاعات باید به‌گونه‌ای هدایت شود که هر کاربر بداند چگونه از رایانه استفاده کند و چگونه از اینترنت و رایانه به‌عنوان ابزار مثبت استفاده شود چنانچه کاربران ملاحظه کنند که با ورود به شبکه اینترنت یا فضای مجازی می‌توانند امور خود را به‌طور بهینه پیش ببرند و این تحول مثبت را در زندگی‌شان احساس کنند اولویت کاربری‌شان در فضای مجازی را به امور بیهوده اختصاص ندهند؛ مانند بسیاری از خدمات دولت الکترونیکی و بانکداری الکترونیکی که به نحوی غالب مردم با چگونگی بهره‌برداری از این گونه سیستم‌ها آشنایی اجمالی دارند که به‌عنوان تکنولوژی رفع نیازهای زندگی افراد تلقی شده است. بر این اساس با توجه به‌ضرورت کاربرد استفاده از رایانه و اینترنت در عصر امروز، مناسب است که عموم کاربران شیوه استفاده صحیح از آن را بیاموزند و از آنجا که محیط سایبری حاوی انواع اطلاعات مبتنی بر فرهنگ‌ها و اعتقادات گوناگون و متناسب با سنین مختلف است و به‌خصوص محتواهای مضر و نامناسب به‌راحتی در دسترس است لازم است فرهنگ محیط سایبری محقق شود.

خوشبختانه سیاست جنایی جمهوری اسلامی ایران در این زمینه بعد از انقلاب به‌طور کلی در زمینه فرهنگ‌سازی مسیر خوبی را طی کرده است. در مقدمه قانون اساسی و بند دوم اصل سوم به نحوی به نقش رسانه‌های جمعی در پیشگیری از بزهکاری توجه شده است در مقدمه قانون اساسی آمده است: «وسایل ارتباط جمعی (رادیو و تلویزیون) باید در جهت روند تکاملی انقلاب اسلامی در خدمت اشاعه فرهنگ اسلامی قرار گیرد و در این زمینه از برخورد سالم اندیشه‌های متفاوت بهره جوید و از اشاعه و ترویج خصلت‌های تخریبی و ضد اسلامی جدا پرهیز کند» بند دوم اصل سوم قانون اساسی نیز «بالا بردن سطح

آگاهی‌های عمومی در هر زمینه با استفاده صحیح از مطبوعات، رسانه‌های گروهی و وسایل دیگر» را از وظایف دولت جمهوری اسلامی ایران برشمرد. از آنجا که رایانه به‌نوعی جزو رسانه‌های گروهی محسوب می‌شود. توجه به فرهنگ‌سازی به‌خصوص در فضای مجازی می‌تواند نقش مؤثری در پیشگیری از جرم کلاهبرداری رفاهی در فضای مجازی داشته باشد (پور قهرمانی، ۱۳۹۷، ۳۵).

۲-۱-۳. **کنترل و نظارت** «موضوع کنترل و نظارت در پیشگیری از وقوع جرم کلاهبرداری رفاهی در فضای مجازی هم می‌تواند کاربرد داشته باشد. کنترل و نظارت یعنی تلاشی منظم در جهت رسیدن به اهداف استاندارد و جلوگیری از انحرافات غیرمسئولانه و غیرقانونی است. از حیاتی‌ترین ارکان هر سیستم و مجموعه سالم و کارآمد، وجود یک نظام کامل و دقیق نظارت و بازرسی است. آنچه می‌تواند انسان را از خطا آگاه کند و ضعف او را به قوت و جاهل او را به آگاهی مبدل سازد نظارت «انس آن‌های صالح»، «دلسوز و آگاه» بر کار دیگران است بنابراین ضرورت «نظارت» انکارناپذیر است و هر قدر این ابزار با کمال دقت، متانت، عدالت و با رعایت شرایط آن به کار رود تأثیر و اهمیت آن بیشتر مشخص خواهد شد (جلالی، ۱۳۸۹، ۱۰). «نظارت باعث می‌شود که افراد مستعد یا در معرض ارتکاب جرم در اندیشه مجرمانه خود وجود نظارت را مورد توجه قرار دهند و چه بسا به خاطر ترس از نظارت که احتمال مقابله با جرم و کشف آن را افزایش می‌دهد از ارتکاب جرم منصرف شوند» (Marilyn, ۲۰۰۵, p۷۰).<sup>۱</sup>

البته منظور از نظارت در اینجا صرفاً نظارت مراجع رسمی نیست بلکه نظارت عمومی که همان امر به معروف و نهی از منکر است را هم شامل می‌شود<sup>۲</sup> این نوع نظارت امروزه به‌عنوان پیشگیری مشارکتی که خود یکی از شاخه‌های سیاست جنایی مشارکتی است شناخته می‌شود. نظارت و کنترل صرفاً نظارت عمومی را شامل نمی‌شود بلکه نظارت و کنترل افراد بر افراد را نیز شامل می‌شود به‌عبارت دیگر این نظارت در محیط خانواده می‌تواند واقع شود تا در محیط جامعه و نیز ممکن است در محیط رسمی هم صورت گیرد.

لازم به ذکر است که نقش نظارتی سازمان‌های مردم‌نهاد در پیشگیری از جرائم رایانه‌ای را نباید از نظر دور داشت. سازمان‌های مردم‌نهاد یکی از مهم‌ترین ابزارهای نهادینه کردن نظارت عمومی در دنیای معاصرند و از توانایی‌ها و قابلیت‌های آن‌ها در تمام شیوه‌های نوین پیشگیری از جرم استفاده می‌کنند. این سازمان‌ها جایگاه رفیعی در ساماندهی نظارت عمومی بر پدیده مجرمانه دارند و کلیه برنامه‌های پیشگیری مشارکتی در سطوح ملی و محلی بر پایه مشارکت فعال آن‌ها تدوین و اجرا می‌شود به‌نحوی که تمام تصمیم‌گیری‌ها و اقدامات مربوط به این موضوع مشارکت می‌جویند و عضو فعال‌های جمعی و شوراهای پیشگیری از جرم هستند (رستمی، ۱۳۸۷، ۵۷).

<sup>۱</sup> Marilyn

<sup>۲</sup> نظارت انواع و اقسام مختلفی دارد که عبارت‌اند از: نظارت فرد، نظارت گروهی، نظارت عمومی، نظارت رسمی... (محسن شیخی، ۱۳۸۱، ۱۶۱).

در نهایت باید گفت که کنترل و نظارت‌های زمانی در حوزه پیشگیری از جرم کلاهبرداری رفاهی در فضای مجازی می‌تواند مؤثر باشد که در این راستا عواملی از فناوری‌های اطلاعات که به‌نوعی تهدید در این زمینه محسوب می‌شوند تضعیف گردیده و حالت اجرایی و کاربردی نظارت و کنترل‌ها دقیق‌تر و فرصت‌ها تقویت گردند.

**۳-۱-۳- بهبود شرایط اقتصادی:** وضعیت اقتصادی نامناسب افراد در جامعه می‌تواند باعث وقوع بسیاری از جرائم در دنیای فیزیکی و سایبری باشند. به‌عنوان نمونه، فردی را در نظر بگیرید که پس از سپری نمودن مراحل تحصیلی و کسب تخصص لازم در رشته کامپیوتر، به دنبال شغلی مناسب در بازار می‌گردد. حال اگر وی با فقر اقتصادی و وضعیتی نابسامان روبرو شود و نتواند تخصص خود در راه مشروع بکار گیرد. به‌طور حتم متمایل به انجام اعمال غیرقانونی خواهد شد. از این رو، می‌توان وظیفه دولت را اتخاذ یک سیاست اقتصادی مناسب به‌منظور کاهش دامنه ارتکاب جرائم و خسارت ناشی از آن است که تنها منجر به کاهش جرائم سایبر بلکه نرخ کلی جرائم را نیز به کاهش می‌دهد. این امر با استفاده از روش‌های علمی و تخصص به همراه ارائه تحلیل مناسب از وضعیت اقتصادی افراد جامعه، اقداماتی برای از بین بردن فقر و بیکاری و به‌ویژه ایجاد فرصت‌های شغلی اشخاص تحصیل کرده میسر شده و کمک می‌کند که از تخصص این افراد به‌طور شایسته و مناسب استفاده شود.

قانون اساسی جمهوری اسلامی ایران در قالب اصل سوم و بندهای شانزده‌گانه آن در جهت نیل به این هدف و ایجاد امکانات مناسب در زمینه‌های مادی و معنوی، وظایفی را برای دولت تعیین کرده است که بر اساس آن‌ها تبعیضات ناروا از بین رفته و اقتصاد صحیح و عادلانه پی‌ریزی شود تا رفاه عمومی ایجاد شده، هر نوع محرومیت در زمینه‌های تغذیه و مسکن و کار تعمیم بیمه از بین رود (جعفری و همکاران، ۱۳۹۷، ۱۰۵). به نظر می‌رسد بهبود شرایط اقتصادی یا مالی تا حدودی هم می‌تواند در جهت از بین بردن تحقق جرم کلاهبرداری رفاهی در فضای مجازی مؤثر باشد.

**۳-۱-۴- تدوین کدهای رفتاری و افزایش عزت نفس:** یکی دیگر از طرق پیشگیری اجتماعی جامعه مدار در حوزه جرم کلاهبرداری رفاهی در فضای مجازی، تدوین «کدهای رفتاری»<sup>۱</sup> برای مشاغل گوناگون و الزام به آگاهی از مفاد آن است. به‌طور کلی با کدهای رفتاری می‌توان گروه‌های ویژه‌های و خاصی را که تعهد و وظیفه‌ای به آن‌ها سپرده شده است، در مقابل کارها و اعمال خود، مسئول و پاسخگو نگه داشت. از جمله آن‌ها گروه‌های شغلی و حرفه‌ای هستند که در حوزه‌های مختلف به کار و فعالیت می‌پردازند و چون که به متصدیان شبکه‌ای خود اطلاعات و داده‌های واجد ارزش و اعتبار را واگذار کرده‌اند تا با رعایت سه اصل محرمانه بودن<sup>۲</sup>، تمامیت<sup>۳</sup> و دسترس‌پذیری<sup>۴</sup> در فضای سایبر منتشر و توزیع کنند، ضروری است مناسب و متناسب با حرفه و شغل، نوع و میزان اطلاعات آن‌ها و دیگر شرایط کد رفتاری مربوط و مرتبط را برای آن‌ها تدوین کنند (منفرد و همکاران، ۱۳۹۱، ۱۴۲). کدهای رفتاری مقنن را از حجم زیاد

<sup>۱</sup> Codes of Conduct

<sup>۲</sup> confidentiality

<sup>۳</sup> Integrity

<sup>۴</sup> Availability

تقنین نجات می‌دهد. صنوف از جمله صنف رایانه‌ای؛ مخابراتی و... با خودتنظیمی<sup>۱</sup> باید‌ها و نباید‌ها شغلی را تعریف می‌کنند و این کار سبب ترویج اخلاق رایانه‌ای می‌شود که در اسناد جهانی «اعلامیه اصول، ایجاد و ساخت جامعه اطلاعاتی، چالش جهانی هزاره جدید»<sup>۲</sup> (با ۶۷ ماده) و «طرح اقدام»<sup>۳</sup> (با ۲۹ ماده و یازده خط عمل) در سال ۲۰۰۳ در ژنو و نیز در اسناد «تعهد تونس» و «دستور جلسه تونس برای جامعه اطلاعاتی»<sup>۴</sup> (سال ۲۰۰۵) مورد تأکید قرار گرفته است.

«هرچند به نظر برخی هیچ‌گاه کد رفتاری در کشورمان نوشته نشد» (دزیانی، ۱۳۸۵، ۱۷). ولی نظر می‌رسد که این ادعا با این کلیت صحیح به نظر نمی‌رسد، چراکه شورای عالی انقلاب فرهنگی پیرو تصویب ابلاغ سیاست‌های کلی نظام درباره شبکه‌های اطلاع‌رسانی رایانه‌ای از سوی مقام معظم رهبری، آیین‌نامه واحدهای ارائه‌کننده خدمات اطلاع‌رسانی و اینترنت رسا<sup>۵</sup> ISP و آیین‌نامه دفاتر خدمات اینترنت (Coffeenet) را تصویب و ابلاغ کرد که بر اساس محتوای آیین‌نامه‌های فوق می‌توان آن‌ها را جزو کدهای رفتاری نامید<sup>۶</sup>

همچنین افزایش عزن نفس در افراد به خودی خود باعث می‌شود افراد طمع نداشته باشند و به جرائم مالی سوق پیدانکنند کمبودهای مالی و اقتصادی در بیشتر موارد باعث سوق افراد به جرائم مالی می‌شود.

## ۲-۳- تدابیر پیشگیری اجتماعی رشدمدار از کلاهبرداری رفاهی در فضای مجازی

آگاه کردن کودکان از مخاطرات و سوءاستفاده‌های احتمالی و ضرورت حفظ حریم شخصی، اولین گام در آموزش نحوه استفاده سالم از شبکه‌های مجازی است؛ بنابراین ضروری است که به کودکان آموزش داده شود که چنانچه مشکلی در فضای مجازی پیش آمد، چه اقداماتی باید انجام دهند. والدین می‌توانند با انجام فعالیت‌های مشترک در اینترنت نظیر جستجو و یادگیری مطالب جدید، فرصتی را برای حضور خود در کنار فرزندشان، در هنگام استفاده از شبکه‌های مجازی فراهم کنند (کرامتی معز، ۱۳۹۷، ۱۶۷).

<sup>۱</sup>Self- regulation

<sup>۲</sup> Itu

<sup>۳</sup> Tunis commitment

<sup>۴</sup> Tunis agenda for the information socit

<sup>۵</sup> Internet Servica provider

<sup>۶</sup> هم‌چنین در این زمینه می‌توان به آیین‌نامه «ساماندهی فعالیت سایت‌های اینترنتی» مصوب ۱۳۸۵/۵/۲۹ هیئت‌وزیران، «آیین‌نامه ساماندهی و توسعه رسانه‌ها و فعالیت‌های فرهنگی دیجیتال» مصوب ۱۳۸۹/۵/۲۴ هیئت‌وزیران، «آیین‌نامه تأمین، توزیع و عرضه خدمات اینترنت و اینترنت ملی» مصوب ۱۳۸۵/۵/۱ کمیسیون تنظیم مقررات و ارتباطات، «آیین‌نامه ارائه خدمات پیام چندرسانه‌ای» مصوب ۱۳۸۷/۶/۲۵ کمیسیون تنظیم مقررات و ارتباطات، «آیین‌نامه ساماندهی فعالیت و نظارت بر فروشگاه‌های مجازی» مصوب ۱۳۸۸/۹/۲۱ وزارت بازرگانی و آیین‌نامه «آیین‌نامه تأسیس و فعالیت بانک‌های مجازی» مصوب ۱۳۹۰/۲/۲۷ شورای پول و اعتبار اشاره کرد.

از این رو، اتخاذ تدابیر و سیاست‌هایی در زمینه پیشگیری اجتماعی رشد مدار می‌تواند زمینه‌های شکل‌گیری کلاهبرداری رفاهی در فضای مجازی را کم‌رنگ نماید. این امر که امنیت همواره در کنار آموزش امکان‌پذیر است، امروزه به یک امر مهم در پیشگیری از جرم بدل شده و در سیاست‌های دولت‌ها نقش پررنگی ایفا می‌کند.

### ۳-۳- تکنیک‌های پیشگیری وضعی از جرم کلاهبرداری رفاهی در فضای مجازی

پیشگیری وضعی به‌عنوان یکی از شیوه‌های پیشگیری از جرم، درصد است تا با تعبیر وضعیت فرد یا وضعیت محیط بیرونی، مانند مکان و زمان، از ارتکاب جرم از سوی افراد جلوگیری کند (میر خلیلی، ۱۳۹۹، ۱۹). یا پیشگیری وضعی شامل مجموعه اقدامات و تدابیری است که به سمت تسلط بر محیط و شرایط پیرامونی جرم (وضعیت مشرف بر جرم) و مهار آن متمایل است. این امر از یک سو، از طریق کاهش وضعیت‌های ماقبل بزهکاری، یعنی وضعیت‌های پیش‌جنایی که وقوع جرم را مساعد و تسهیل می‌کند، انجام می‌شود و از سوی دیگر، با افزایش خطر شناسایی و احتمال دستگیری بزهکاران، از وقوع جرم جلوگیری می‌نماید؛ بنابراین، پیشگیری وضعی بیشتر با حمایت از آماج‌های جرم و نیز بزه دیدگان بالقوه و اعمال تدابیر فنی، به دنبال پیشگیری از بزه دیدگی افراد یا آماج‌ها در برابر بزهکاران است که در نهایت و به‌طور غیرمستقیم، کاهش بزهکاری نتیجه آن خواهد بود (پیکا، ۱۳۹۹، ۱۴۰).<sup>۱</sup>

پیشگیری وضعی شامل اقدامات و روش‌هایی برای کاهش فرصت است به‌نحوی که:

۱. به سوی شکل کاملاً خاصی از جرم نشانه می‌رود؛
۲. متضمن طراحی و مدیریت محیط بلا واسطه (صحنه و محل وقوع جرم) یا همان نظارت و تحت نفوذ در آوردن هرچه پایدارتر و سازمان‌یافته‌تر محل وقوع جرم است. رود؛
۳. زحمات و خطرات ناشی از اقدام برای ارتکاب جرم را افزایش داده و سود حاصله؛ در نظر مرتکب را کاهش می‌دهد (دارابی، ۱۳۹۵، ۱۳۱).

به‌منظور پیشگیری از خسارت کلان احتمالی از جرم کلاهبرداری رفاهی، پیشگیری وضعی یا موقعیت مدار یکی از بهترین و مؤثرترین گزینه‌های تأمین امنیت به شمار می‌آید. بسیاری از تکنیک‌های پیشنهادی تدابیر موقعیت مدار قابلیت کاربست در فضای مجازی را دارا هستند و با استفاده از ابزارهای فناوری اطاعات و ارتباطات می‌توان آن‌ها را در این فضا به کار بست.

۳-۳-۱- تدابیر امنیتی دیوار آتشین: دیواره‌های آتشین<sup>۲</sup> یکی از مؤثرترین و مهم‌ترین روش‌های پیاده‌سازی مصونیت شبکه هستند قادرند تا حد زیادی از دسترسی غیرمجاز دنیای بیرون به منابع داخلی جلوگیری کنند. دیواره‌های آتش، مانند

<sup>۱</sup> pika

<sup>۲</sup> دیواره‌های آتشین در اصطلاح علوم رایانه‌ای عبارت است از: یک سامانه ایمنی برای محافظت از شبکه یک سازمان در مقابل تهدیدهای خارجی هم چون نفوذ گران که از شبکه‌های خارجی هم چون اینترنت وارد می‌شوند. دیوار آتش که به‌طور معمول،



خندق‌های دور قلعه‌های دوران قرون وسطی عمل می‌کنند. خندق دور قلعه باعث می‌شود نفوذ به قلعه مشکل باشد (پور قهرمانی، ۱۳۹۵، ۹۷).

یکی از مهم‌ترین تدابیر صیانت از آماج بزه به‌ویژه در جرم کلاهبرداری رفاهی از طریق دشوار سازی دسترسی، دیوارهای آتشین هستند. این دیوارها که در دو نوع سخت‌افزاری و نرم‌افزاری موجود هستند، به‌مثابه محافظی عمل می‌کنند که از دسترسی غیرمجاز به شبکه‌های داخلی و خروج اطلاعات پیشگیری می‌کنند. نظارت و مسدودسازی دسترسی به شبکه بر اساس تطبیق ورودی‌ها با الگوی های غیرمجاز تعیین شده صورت می‌گیرد. بدین صورت که در یک فرآیند کلی، درخواست‌های دسترسی به شبکه داخلی را در پوشه‌ای ذخیره کرده، آن را با الگوها مقایسه می‌کند و در صورتی که موارد غیرمجازی را مشاهده نماید، کاربر را مطلع خواهد نمود برای دیوارهای آتش پیکربندی‌ها و کاربردهای مختلفی وجود دارد: صافی‌ها، تقویت‌کننده‌های برنامه‌های کاربردی، رمزگذاری، ایجاد منطقه غیرنظامی و سایر موارد مشابه که سبب افزایش ضریب امنیتی آن‌ها می‌شود (فرهادی آلاشتی، ۱۳۹۵، ۴۴). به نظر می‌رسد اگر نیروی انتظامی و پلیس در زمینه پیشگیری از کلاهبرداری رفاهی در فضای مجازی از این گونه تدابیر استفاده کنند، بسیار مفید و مؤثر خواهد بود.

۲-۳-۳- تدابیر پالایشی<sup>۱</sup>: یکی دیگر از روش‌های دشوار سازی دسترسی به آماج جرم، استفاده از پالایشگرها<sup>۲</sup> است. همان‌گونه که از نام این تدابیر پیداست، اجازه‌ی دسترسی به برخی و یا تمام محتویات موجود در شبکه را نخواهند داد و با توجه به الگوهای تعیین شده محتویات خاصی را غربال خواهند کرد. پالایشگرها بر اساس فهرست سفید<sup>۳</sup> یا فهرست سیاهی<sup>۴</sup> که برای آن‌ها تعیین می‌شود، فعالیت می‌کنند. «فهرست سفید، اجازه‌ی دسترسی به مشخصات تعیین شده را می‌دهد. در حالی که فهرست سیاه اجازه‌ی دسترسی به مشخصات تعیین شده را نخواهد داد» (Schwabak, ۲۰۰۶, p1۷۳).<sup>۵</sup>

---

ترکیبی از سخت‌افزارهای و نرم‌افزارهای است، از ارتباط مستقیم کامپیوترهای عضو شبکه داخلی با شبکه‌های خارجی و برعکس جلوگیری می‌کند (ماه پیشانیان، ۱۳۹۷، ۹۷).

### <sup>۱</sup> Filtering

<sup>۲</sup> برخی تعاریف پالایش یا فیلترینگ را در معنای عام و خاص به‌کاربرده‌اند. در معنای عام پالایش عبارت از فناوری‌هایی که از دستیابی به انواع خاص محتوا یا بسته ویژه‌ای از محتوای اینترنتی در دسترسی، جلوگیری به عمل می‌آورد؛ اما تعریف خاص، فیلترینگ عبارت است از جلوگیری از دسترسی به اطلاعات بر مبنای محتوای اطلاعات و نه آدرس سایت. در حقیقت معنای خاص پالایش، در مقابل مسدود کردن به کار می‌رود. طبق این تفکیک هنگامی که دسترسی به کل یک سایت بر اساس آدرس آن سایت ممنوع می‌شود، آن سایت مسدود (بلاک) شده و در صورتی که بخشی از محتوای آن ممنوع شده باشد پالایش گشته است (کرامتی معزو همکاران، ۱۳۹۷، ۷۸).

### <sup>۳</sup> . Whitelist

### <sup>۴</sup> .Blacklist

<sup>۵</sup> . Schwabac

موردی همچون نام دامنه<sup>۱</sup>، نشانی پروتکل اینترنت<sup>۲</sup>، مکان‌یاب یکنواخت منبع وب<sup>۳</sup>، کلید واژگان و یا تصاویر موردنظر در این فهرست‌ها گنجانیده می‌شوند و منجر به دسترسی و یا عدم دسترسی کاربران به محتویات موردنظر خواهند شد.

به‌عنوان نمونه، چنانچه واژه‌ی پورنو در فهرست سیاه پالایشگری قرار گیرد، از دسترسی کاربران به محتویات مرتبط با آن واژه (اعم از فیلم، عکس، نوشتار...) جلوگیری خواهد کرد. لازم به ذکر است، زمانی دقت پالایشگرها بالا می‌رود که از چندین مؤلفه برای سلب و یا محدودیت دسترسی به شبکه استفاده شود. به‌عنوان نمونه، چنانچه پالایشگری صرفاً بر اساس مکان‌یاب یکنواخت منبع وب تنظیم شده باشد، تنها می‌تواند درخواست‌هایی که در رابطه با این نشانی است را مسدود نماید و چنانچه کاربر شماره‌ی پروتکل اینترنت آن نشانی را وارد کند، اجازه دسترسی به وی داده خواهد شد. از همین رو، امروزه سعی بر این است که برای تأمین امنیت حداکثری، پالایشگرهای چند مؤلفه‌ای جایگزین پالایشگرهای تک مؤلفه‌ای شوند. پالایشگرها نیز همچون دیواره‌های آتشین می‌توانند در سطوح خرد همچون صیانت از کاربران خانگی و مراکز آموزشی و یا در سطوح کلان همچون صیانت از سازمان‌ها و افراد یک کشور مورد استفاده قرار گیرند. همچنین، پالایشگرها می‌توانند از سوی کاربران نهایی، ارائه‌دهندگان خدمات دسترسی حضوری (کافی‌نت‌ها) یا ارائه‌دهنده خدمات اینترنتی، از سوی ایجادکننده نقطه‌ی تماس بین‌المللی و بر روی موتور جستجو اعمال شوند (خانعلی پور و همکاران، ۱۳۹۰، ۱۲۷).

بر مبنای نظام حقوقی کشورمان، بالاترین سطح کاربرست این تدابیر در بعد داخلی لازم‌الاجرا است. بر اساس ماده ۷۴۹ قانون مجازات اسلامی بخش تعزیرات (ماده ۲۱ قانون جرائم رایانه‌ای مصوب ۱۳۸۸)، ارائه‌دهندگان خدمات دسترسی یا همان میزبان‌های داخلی، موظف به کاربرست پالایشگرها می‌باشند. طبق این ماده: ارائه‌دهندگان خدمات دسترسی موظف‌اند طبق ضوابط فنی و فهرست مقرر از سوی کارگروه (کمیته) تعیین مصادیق موضوع ماده ذیل محتوای مجرمانه که در چارچوب قانون تنظیم شده است، اعم از محتوای ناشی از جرائم رایانه‌ای و محتوایی که برای ارتکاب جرائم رایانه‌ای به کار می‌رود را پالایش (فیلتر) کنند. در صورتی که عمداً از پالایش (فیلتر) محتوای مجرمانه خودداری کنند، منحل خواهند شد و چنانچه از روی بی‌احتیاطی و بی‌مبالاتی زمینه دسترسی به محتوای غیرقانونی را فراهم آورند، در مرتبه نخست به جزای نقدی از بیست میلیون ریال تا یکصد میلیون ریال و در مرتبه دوم، به جزای نقدی از یکصد میلیون ریال تا یک میلیارد ریال و در مرتبه سوم، به یک تا سه سال تعطیلی موقت محکوم خواهند شد (سبزواری نژاد و همکاران، ۱۳۹۹، ۱۷). در برخی از موارد ماهیت مجرمانه و یا غیر مجرمانه‌ی برخی از اطلاعات برای نرم‌افزارهای پالایشگر قابل تشخیص نبوده و چنانچه مشتقات محتویات موردنظر، در لیست سیاه قرار داشته باشند، نرم‌افزار دسترسی به این محتویات را غیرممکن خواهد ساخت که اصطلاحاً به این گونه محتویات، «موضوعات خاکستری» و به این حالات «پالایش بیش از اندازه» گفته می‌شود

---

<sup>۱</sup>. Domain Name System

<sup>۲</sup>. Internet protocol Address

<sup>۳</sup>. Jniform Resource locator

(فرهادی آلاشتی، ۱۳۹۵، ۱۴۸). به عبارت بهتر، مشکل از آنجایی آغاز می‌شود که در بسیاری از موارد با ترکیبی از داده‌های قانونی و غیرقانونی روبه‌رو هستیم. عدم توانایی نرم‌افزارهای پالایشگر در تشخیص داده‌های قانونی از غیرقانونی و زمان‌بر بودن رفع کاستی‌ها توسط عامل انسانی، نتیجه‌ای جز عدم دسترسی به تعداد بی‌شماری از محتویات قانونی برای مدت‌زمان خاص را در پی ندارد. به همین دلیل، در بسیاری از موارد داده‌های قانونی نیز به همراه داده‌ها غیرقانونی، در زمره‌ی اطلاعات غیرمجاز قرار می‌گیرد و تا تشخیص اشتباه و رفع آن، کاربران قادر به دسترسی به اطلاعات موردنظر خود نیستند (سبزواری نژاد و همکاران، ۱۳۹۹، ۱۸).

۳-۳-۳- **تدابیر نظارتی:** یکی از مهم‌ترین راهبردهای پیشگیری وضعی در حوزه جرم کلاهبرداری رفاهی، تدابیری است که سعی در کنترل و نظارت دارد. از این رو نظارت در محیط سایر نیز مانند نظارت در محیط مادی از راهکارهایی است که علاوه بر کشف سریع‌تر جرائم ارتكابی می‌تواند از ارتكاب آن‌ها نیز پیشگیری می‌کند.

شورای عالی فضای مجازی و پلیس فتا، نهادهایی هستند که در جهت سامان‌دهی فضای مجازی نقش‌آفرینی می‌کند و می‌تواند از طریق ایجاد محدودیت‌های دسترسی به فضای مجازی و هم‌چنین اعمال نظارت و کنترل در این فضا در امر پیشگیری از بزه‌کاری و بزه دیدگی نقش مهمی داشته باشند (منصورآبادی و همکاران، ۱۴۰۰، ۴۷).

### نتیجه‌گیری

در راستای پیشگیری از جرم کلاهبرداری رفاهی در فضای مجازی، استفاده از تکنیک‌های پیشگیرانه غیر کیفری (اجتماعی و وضعی) در کاهش جرم ارتكابی لازم است. اما فن‌های پیشگیری اجتماعی جامعه مدار و رشد مدار که عوامل اجتماعی جرم‌زا در یک جامعه معینی را مورد هدف قرار می‌دهند، یا اقداماتی که در این راستا به اجرا درمی‌آید با هدف از بین بردن زمینه‌های اجتماعی ایجادکننده انگیزه‌های مجرمانه است، در این راستا راهکارهای مختلفی را می‌توان بررسی کرد که عبارت‌اند از فرهنگ‌سازی، نظارت، آموزش، تدوین کدهای رفتاری و حل مسائل و مشکلات اقتصادی. آموزش دادن در زمینه‌های افزایش ابزارهای حفاظتی و امنیتی و نوع و نحوه‌ی کار آبی و به‌کارگیری آن‌ها و جدی گرفتن هشدارها از این قبیل است. آگاه ساختن از خطرات رفتار زیان‌بار در غیرقانونی آنلاین و یادگیری نحوه حفاظت از خود و دیگر کاربران اینترنت در برابر آن‌هاست. اما در روش پیشگیری وضعی از جمله تدابیر امنیتی دیوار آتشین، تدابیر پالایشی، تدابیر نظارتی می‌توان وضعیت‌های زمانی و مکانی جرم کلاهبرداری رفاهی را در فضای مجازی را کنترل نمود و با اعمال غیر قهرآمیز و غیر کیفری افراد بزه‌کار را از دسترسی به آماج جرم دور نموده و هم‌چنین فرصت ارتكاب جرم کلاهبرداری رفاهی و منافع حاصله از ارتكاب جرم توسط افراد نابهنجار را کاهش داد. که این روش یا مکانیسم پیشگیری با توجه به شرایط کلاهبرداری رفاهی در فضای مجازی بیشتر از روش‌های دیگر قابلیت اجرایی یا استفاده را دارد.

اما فن‌های پیشگیری اجتماعی جامعه مدار و رشد مدار که عوامل اجتماعی جرم‌زا در یک جامعه معینی را مورد هدف قرار می‌دهند، یا اقداماتی که در این راستا به اجرا درمی‌آید با هدف از بین بردن زمینه‌های اجتماعی ایجادکننده انگیزه‌های

مجرمانه است، در این راستا راهکارهای مختلفی را می‌توان بررسی کرد. که عبارت‌اند از فرهنگ‌سازی، نظارت، آموزش، تدوین کدهای رفتاری و حل مسائل و مشکلات اقتصادی، آموزش دادن در زمینه های افزارهای و ابزارهای حفاظتی و امنیتی و نوع و نحوه‌ی کار آیی و به‌کارگیری آن‌ها و جدی گرفتن هشدارها از این قبیل است. آگاه ساختن از خطرات رفتار زیان‌بار در غیرقانونی آنلاین و یادگیری نحوه حفاظت از خود و دیگر کاربران اینترنت در برابر آن‌ها است.

البته موارد فوق زمانی نتیجه‌بخش خواهد بود که سازوکارهای اجرایی آن‌ها و متولیان امر مشخص و با همکاری هم و ترکیبی از راهکارهای پیشگیرانه وضعی و اجتماعی به‌صورت توأمان در پیشگیری از وقوع جرم کلاهبرداری رفاهی در فضای مجازی می‌تواند کمک و مناسب باشد.

### پیشنهادها

- ۱- اجرای برنامه های پلیس محور به صورت نظارت های مجازی (الکترونیکی) و فیزیکی یا میدانی در مناطقی که کلاهبرداری رفاهی در فضای حقیقی و مجازی آمار قابل توجهی دارد.
- ۲- کمک گرفتن از راهنمایی و ارشاد قضات، وکلا، دفترخانه های ازدواج و طلاق، مراکز مشاوره و دفتر خدمات قضایی مبنی بر علت اصلی طلاق ها و ازدواج های کاسب کارانه در ایران.
- ۳- راهنمایی از اداره ثبت احوال کشور در مورد فاصله زمانی ازدواج ها و طلاق، گرفتن شناسنامه جدید در پاک کردن نام همسران یا شوهران که در کشف جرم کلاهبرداری رفاهی و حتی پیشگیری می تواند موثر باشد.
- ۴- نظارت های فیزیکی از طرف کمیته امداد یا بهزیستی یا تامین اجتماعی بعد از ثبت نام در این مراکز.
- ۵- کمک گرفتن از بانک ملی کشور در جهت اخذ تسهیلات وام های ازدواج، پرداخت بیمه در سازمان تامین اجتماعی.
- ۶- برخی مجرمین کلاهبرداری رفاهی به‌صورت آنی و بدون سابقه تصمیم، مرتکب جرم در فضای مجازی می‌شوند لذا اعمال تدابیر پیشگیری وضعی و اجتماعی بر روی فضای مجازی در ارتباط با این افراد نتایج مطلوبی به همراه خواهد داشت.
- ۷- توجه و تأکید بیشتر به فرهنگ‌سازی و جامعه‌پذیری و تدابیر نظارتی مناسب و متناسب مردم جامعه برای تربیت و پرورش شهروندان قانون‌مدار و قانونمند.

### منابع و مآخذ

- آقایی نیا، حسین، رستمی، هادی (۱۳۹۷). حقوق کیفری اختصاصی، جرایم علیه اموال و مالکیت، چاپ دوم، تهران، میزان.
- آزاد ملکی، تقی (۱۳۹۵). تغییرات، چالش ها و آینده خانواده ایرانی، تهران، تیسرا.
- اسدی فرد، محمد، ذوالفقاری، حسین، دعاگویان، داود و هندیابی، عبدالله (۱۳۹۶). مولفه های و شاخص های تعاملات اجتماعی پلیس در مدیریت انتظامی از جرم، فصلنامه علمی انتظام اجتماعی، شماره ۴.
- اسماعیلی کریزی، علی احمری، حسین؛ کاظمی گلوردی (۱۴۰۰). پیشگیری از جرائم خاص انتظامی و نظامی در سیاست جنایی ایران، فصلنامه علمی مطالعات پیشگیری از جرم، ۱۶ (۵۹) ۲۰۷-۱۹۱.
- اکبری جبلی، سعید (۱۳۹۹). پلیس و روبروهای پیشگیری از وقوع جرم. نشریه علمی دانش انتظامی سیستان و بلوچستان، شماره ۱۱.
- اعتمادی فرد، مهدی، نجمی، آلاء (۱۴۰۰). ازدواج ها و طلاق های کاسب کارانه در ایران (مطالعه جامعه شناسانه ی فرم حقوقی در نهاد خانواده)، فصلنامه مطالعات جامعه شناختی، دوره ۲۸، شماره یک ۱۳۹-۱۱۷.
- اوجاقلو، صالح؛ زندی، محمدرضا (۱۴۰۰). پیشگیری از کلاهبرداری سایبری در سیاست جنایی ایران با نگاهی به رویه قضایی، فصلنامه علمی مطالعات پیشگیری از جرم. ۱۶ (۵۸) ۲۶۱-۲۴۳.
- انصاری، جلال؛ عطا زاده، سعید؛ قیوم زاده، محمود (۱۳۹۸). سیاست جنایی ایران و آمریکا در قبال جرائم، فصلنامه پژوهش های اطلاعاتی و جنایی، ۱۴ (۵۵) ۱۳۱-۱۵۴.
- خسرو شاهی، قدرت، مظاهری کوهانستانی، معمار، ثریا، عبداللهی، الهام (۱۳۹۵) نقش بزه دیده در تحقق جرم کلاهبرداری و راه کارهای پیشگیری از آن، فصلنامه علمی و تخصصی مجله حقوقی معاونت فرهنگی دانشگاه اصفهان، دوره ۳، شماره ۱.
- جعفری لنگرودی، محمدجعفر. (۱۳۹۲). ترمینولوژی حقوق. تهران، انتشارات گنج دانش.
- حدادی، مهدی. (۱۳۸۹). مقایسه مفهوم و کارکرد نظم عمومی در نظام حقوقی بین الملل با نظام های حقوقی ملی، مطالعات حقوق خصوصی، شماره ۱۶، صص ۱۵۷.
- پورقهرمانی، بابک (۱۳۹۷). پیشگیری جامعه مدار از وقوع جرایم رایانه ای و متولیان آن در حقوق ایران، فصلنامه علمی ترویجی مطالعات پیشگیری از جرم، سال ۱۳، شماره ۴۹.
- ورقهرمانی، بابک (۱۳۹۵). سیاست جنایی ایران در قبال جرایم رایانه ای: مطالعه تطبیقی با اسناد بین المللی. چاپ اول. تهران تهران: موسسه مطالعات و پژوهش های حقوقی (شهر دانش).
- بیکا، ژرژ (۱۳۹۹). جرم شناسی، ترجمه علی حسین نجفی ابرند آبادی، انتشارات میزان.
- تقی زاده، ابراهیم (۱۳۹۰). فضاهای مجازی (آسیب ها، رویکردها و راهکارها)، فصلنامه حقوقی مجد، شماره ۱۶.
- توکلی، فخرالدین، شاه محمدی، غلامرضا (۱۳۹۷). تاثیر مدیریت فناوری اطلاعات در پی جویی جرایم سایبری، فصلنامه پژوهش های اطلاعاتی و جنایی، ۱۳ (۵۰)، ۱۴۸-۱۲۹.

- جلالی، علی اکبر (۱۳۸۹). نظارت همگانی، عامل پیشگیری از جرایم در فضای مجازی، فصلنامه کارآگاه، دوره دوم، سال شوم، شماره ۱۲.
- جعفری، مریم؛ سلیمانی، فرزاد (۱۳۹۷). نقش پلیس در تامین امنیت و سالم سازی فضای سایبر با رویکرد پیشگیری اجتماعی از جرایم سایبری، فصلنامه دانش اجتماعی زنجان، شماره ۲۹.
- حسین نژاد، مجتبی (۱۳۹۸). بررسی فقهی بغی در فضای مجازی، فصلنامه پژوهش های فقه و حقوق اسلامی، ۱۵ (۵۵)، ۷۴-۵۳.
- خانعلی پور و اجاره گاه، سکینه (۱۳۹۰). پیشگیری فنی از جرم. چاپ اول. تهران: بنیاد حقوقی میزان.
- خلیج آبادی فراهانی، فریده (۱۳۹۸). مواجهه با محتوای خارج عرف جنسی (پورنوگرافی) در اینترنت و فضای مجازی و تاثیرات رفتاری در نوجوانان در تهران، مجله خانواده پژوهشی، ۱۵ (۵۷)، ۱۵۳-۱۲۷.
- دارابی، شهرداد (۱۳۹۵). پیشگیری از جرم در مدل مردم سالار سیاست جنایی، چاپ اول. تهران: بنیاد حقوقی میزان.
- درویشی، صیاد (۱۳۹۶). بررسی دانش و مهارت مورد نیاز پلیس در پیشگیری وضعی از جرم. فصلنامه پژوهش های دانش انتظامی، ۱۹ (۷۱)، ۴۷-۶۸.
- دستور، علی و ملکی، عزیزالله (۱۳۹۳). وظایف پلیس در پیشگیری از جرایم سایبری (موانع و چالش ها). فصلنامه علمی دانش انتظامی مرکزی، ۶ (۶)، ۳۷-۶۴.
- دزیانی، محمد حسن (۱۳۸۵). مقدمه ای بر سیاست جنایی ایران در باب جرایم سایبری، مجله قضاوت، شماره ۳۸، ۴۲-۴۸.
- ذبیح اله نژاد، وحید (۱۳۹۶). نقش پلیس فتا در پیشگیری وضعی و پیشگیری اجتماعی از جرایم سایبری، فصلنامه دانش انتظامی البرز، سال پنجم، شماره ۱، ۶۷-۸۹.
- ذوالفقاری، حسین، صیدال، فعال (۱۳۹۳). بررسی نقش پلیس در پیشگیری اجتماعی از جرم، فصلنامه مطالعات امنیت اجتماعی، شماره ۴۱.
- رستمی، هادی (۱۳۹۸). کلاهبرداری رایانه ای؛ تاملی بر ارکان جرم و آثار آن. آموزه های حقوق کیفری. ۱۶ (۱۸): ۵۱-۸۱.
- رشیدی، رامین (۱۳۸۶). کلاهبرداری بیمه ای: مقایسه و چالش های تازه های جهان بیمه، دی و بهمن ماه، شماره ۱۱۶-۱۱۵.
- رشیدی، رامین (۱۳۹۰) و مقدمه ای بر نقشه راه و صنعت بیمه در مواجهه با ریسک های پنهان (ریسک کلاهبرداری)، تازه های جهان بیمه، شماره ۱۰.
- رضایی، احمد، رضایی، محسن، خطیبی، سجاد (۱۴۰۰). بازنگری نقش و عملکرد پلیس در فضای مجازی با تاکید بر آموزش و انتظام بخشی، نشریه علمی انتظام اجتماعی، شماره ۱۳. ۱۱۵-۱۴۰.

- سبزواری نژاد، حجت، رضازاده سلطان آباد، محمد، (۱۳۹۹). پیشگیری غیر کیفری از تهدیدات امنیت ملی در راستای تروریسم سایبری، فصلنامه علمی پژوهش های جرم شناختی پلیس، ۱(۱) ۲۵-۱.
- شاه محمدی، غلامرضا، زلفی، حمید(۱۴۰۰). شناسایی و اولویت بندی شیوه های نظارت بر جرایم در فضای مجازی، فصلنامه پژوهش های اطلاعاتی و جنایی، ۱۴(۶۴)، ۱۱۰-۸۷.
- عاملی، سید سعید رضا(۱۳۹۰). رویکرد دو فضایی به آسیب ها، جرایم، قوانین و سیاست های فضای مجازی. چاپ اول. تهران: موسسه انتشارات امیرکبیر.
- عشایری، طاهّا، نامیان، فاطمه(۱۳۹۷). فرا تحلیل عوامل موثر بر پیشگیری از وقوع جرم، فصلنامه پژوهش های مدیریت انتظامی ۱۴(۱)، ۵۴-۳۳.
- فرهادی آلاشتی، زهرا(۱۳۹۵). پیشگیری وضعی از جرایم سایبری راهکارها و چالش ها. چاپ اول. تهران: بنیاد حقوقی میزان.
- قدیر، محسن و کاظمی فروشان، حسین(۱۳۹۸). بررسی تطبیقی حقوق کیفری ایران با اسناد بین المللی در زمینه مقابله و پیشگیری از وقوع تروریسم سایبری. حقوق بین المللی. ۳۶(۶۰) ۲۶۷-۲۳۷.
- کاشانی، بهزاد و کاسمانی، اکبر(۱۳۹۶). شناسایی و طبقه بندی زمینه های سیاست گذاری عمومی فضای مجازی، فصلنامه پژوهش های ارتباطی، ۲۴(۴)، ۲۷-۵۳.
- کرامتی معز، هادی و میر خلیلی، سید محمود(۱۳۹۹). نقد سیاست های پالایش (فیلترینگ) در پیشگیری از بزه دیدگی نوجوانان در شبکه های اجتماعی مجازی به عنوان محیطی نوین از جغرافیای انسانی. نگرش های نو در جغرافیای انسانی. ۱۲(۴۶): ۹۶-۵۷.
- گسن، ریمون(۱۳۸۹). جرم شناسی بزهکاری اقتصاد، ترجمه شهرام ابراهیمی، چاپ اول، تهران، انتشارات میزان.
- ماه پیشانیان، مهسا(۱۳۹۰). فضای سایبر و شیوه های نوین درگیری ایالات متحده آمریکا با جمهوری اسلامی. مطالعات فرهنگ و ارتباطات. ۱۲(۱۳): ۱۲۱-۹۵.
- محسن شیخی، علی اکبر(۱۳۸۱). نظارت و بازرسی، چاپ اول، قم، معاونت و آموزش ستاد ولی فقیه در سپاه.
- محمدزاده، اکرم و بیگی، جمال و احدی، فاطمه(۱۴۰۰). مبانی فقهی و حقوقی جرم انگاری کلاهبرداری رفاهی در ایران، فصلنامه علمی فقه و مبانی حقوق اسلامی دانشگاه آزاد اسلامی واحد بناب، دوره ۱۵، شماره ۴.
- محمدی، سهیلا و جوانبخت، محمد(۱۳۹۵). فضای سایبری امن (بررسی نقش پلیس و ارائه شیوه های کاربردی پیشگیری از جرایم سایبری). دانش انتظامی خراسان رضوی، ۸(۳۳)، ۲۵-۴۸.
- محمدی، علی(۱۳۹۸)، نقش و جایگاه پلیس در سیاست جنایی ایران در پیشگیری از جرایم سایبری، فصلنامه دانش انتظامی خراسان جنوبی، ۸(۱)، ۹۶-۱۱۵.

- منصور آبادی، عباس، میرخلیلی، سید محمود و کرامتی معز، هادی (۱۴۰۰). پیشگیری از بزه دیدگی کودکان در شبکه های اجتماعی مجازی با تاکید بر نقش نظارتی شواری عالی فضای مجازی و پلیس فتا. مطالعات بین المللی پلیس. ۱۲(۴۶):۵۲-۲۹.
- منفرد، محبوبه و جلالی فراهانی، امیرحسین (۱۳۹۱). کدهای رفتاری و پیشگیری از بزهکاری، پژوهش نامه حقوق کیفری. ۳(۲):۱۰۵-۱۳۴.
- محمد نسل، غلامرضا (۱۳۹۹). کلیات پیشگیری از جرم. چاپ دوم. تهران: بنیاد حقوقی میزان.
- میر خلیلی، سید محمود (۱۳۹۷). جرم شناسی. چاپ اول. قم انتشارات پژوهشگاه حوزه و دانشگاه.
- میر خلیلی، سید محمود، کرامتی معز، هادی و چاووشی، محمد صادق (۱۳۹۷). پیشگیری از ریزومیک شدن جرایم در فضاهای شهری با تاکید بر سرمایه اجتماعی. مطالعات شهر ایرانی اسلامی. ویژه نامه (۳۱): ۱۲۴-۱۱۵.
- میر محمد صادقی، حسین، (۱۳۹۶). حقوق کیفری اختصاصی (۲)، جرایم علیه اموال و مالکیت، چاپ پنجاهم، تهران، میزان.
- مشکینی، علی، (۱۳۶۸) اصطلاحات الاصول، قم، انتشارات علی ابن ابی طالب.
- نجفی ابرند آبادی، علی حسین (۱۳۸۴). مباحثی در علوم جنایی تقریرات درس جرم شناسی، تهیه و تنظیم فاطمه قناد.
- نجفی توانا، علی (۱۳۹۴). جرم شناسی، تهران، انتشارات آموزش و سنجش، چاپ سوم.
- نظری منظم، مهدی؛ مجیدی، عبدالله؛ هندیانی، عبدالله؛ وفادار، حسین (۱۳۹۸). بررسی عوامل موثر بر جرم کلاهبرداری در فضای سایبر، فصلنامه پژوهش های دانش انتظامی. ۲۱، شماره ۲.
- نعیمی، محمد رضا (۱۳۹۶). بررسی تاثیر استفاده از اینترنت و فضای مجازی در احساس امنیت اجتماعی و تغییر سبک زندگی جوانان استان گلستان (فرصت ها، چالش ها و راهکارها). طرح پژوهشی. وزارت ورزش و جوانان. اداره کل ورزش و جوانان استان گلستان. شورای مطالعات و پژوهش های راهبردی.
- واعظ، زهرا (۱۳۹۰). پس لرزه پیامک های یارانه ای، روزنامه دنیای اقتصاد، ۲۶۰۶، شماره ۲۳.
- وایت، راب، هینس، فیونا (۱۳۸۶). درامدی بر جرم و جرم شناسی، ترجمه روح الله صدیق بطحانی، چاپ دوم، تهران، نشر دادگستر.
- وبر، ماکس (۱۳۹۲). روش شناسی علوم اجتماعی، ترجمه حسن چاوشیان، تهران مرکز.
- Dimirt percia David, MarcusMatthias Keup, Alain Mermoud (۲۰۲۰). Knowledge absorption for cyber-security; The role of human beliefs.
- Jun-ichi Itaya, Kenichi Kurita, October ۲۰۲۱, Replicator Evolution of Welfare Stigma: Welfare Fraud vs. Incomplete Take-Up, CESifo Working Paper No. ۸۶۲۱, pp. ۱-۴۱.



- Isabelle Semmelhack , Lisa Guenther , 30 June 2021, Beyond 'Deserving:' An Examination of the Moral Regulatory Function of Welfare Policing During the COVID-19 Pandemic, pp 1-48.
- Rebecca Pirius, 2021, Welfare Fraud.  
<https://www.criminaldefenselawyer.com/resources/welfare-fraud.htm>. 2021.
- Schwabach, Aaron. (2006). Internet and the Law: Technology, Society and Compromises, United States or America: ABC-CLIO.
- Snukan, Aliya, Abdizhami, Aitugan. Ospanov, Gulnar and Abdakimov, Dana (2019). Crime control in the sphere of information technologies in the Republic of Turkey, Digital Investigation, Volume 30, September 2019, Pages 94-100.
- Marilyn, A, Campbell (2005), Cyber bullying: An old problem in a new guise? Australian Journal of Guidance and Counseling.
- <https://www.criminaldefenselawyer.com/resources/welfare-fraud.htm>. 2022.

### **Mechanism for preventing welfare fraud in cyberspace**

#### **Abstra**

Welfare fraud means deceiving government institutions to obtain more welfare benefits. The purpose of this article is to comprehensively study and explain the mechanism of welfare fraud prevention in cyberspace. According to the nature of the subject, the present research has been conducted in terms of practical purpose and in terms of collecting information by documentary method and through the study of reliable sources, and the obtained information has been analyzed in a descriptive-analytical manner. This research indicates that non-criminal preventive solutions (social and situational) can be suitable in preventing the crime of welfare fraud in cyberspace. Non-criminal prevention of welfare fraud in cyberspace through social prevention in the form of preventing the growth of welfare fraud documents in cyberspace and community-oriented prevention of welfare fraud in cyberspace in the form of providing family-oriented programs, educational and training measures in cyberspace, increasing media literacy, informing And culture building, control and monitoring, improvement of economic conditions, development of codes of conduct, situational prevention in the form of firewall security measures, filtering measures and monitoring measures will be done.

**Keywords: welfare fraud, cyberspace, social prevention, situational prevention.**

.