حقوق جزا و سیاست جنایی
دورهٔ ۱، شمارهٔ ۱، بهار و تابستان ۱۳۹۵
صفحات ۱۶۴ ـ ۱۴۵

ISSN: 2008-8418
https://jclp.ut.ac.ir

نقد سیاست جنایی ایران در قبال کلاهبرداری اینترنتی

جلال انصاری[۱*]، علیرضا میلانی[۲]

۱. دانشجوی دکتری حقوق جزا و جرم‌شناسی، دانشگاه آزاد اسلامی، واحد ساوه، ساوه، ایران
۲. استادیار، گروه حقوق، دانشگاه آزاد اسلامی، واحد اسلامشهر، اسلامشهر، ایران

(تاریخ دریافت: ۹۴/۱۲/۰۸؛ تاریخ پذیرش: ۹۵/۰۵/۰۳)

چکیده

جرم کلاهبرداری اینترنتی جزء جرائم نوین است و این مسئله سبب شده است کشورها در قانون‌گذاری و در پیشگیری از این جرم و مقابله با آن، با مشکلات فراوانی روبه‌رو شوند. منشأ این مشکلات در ماهیت متفاوت جرم کلاهبرداری اینترنتی نسبت به کلاهبرداری سنتی است، مباحثی مانند تفاوت در محیط ارتکاب این جرائم و همچنین، تفاوت وسایل ارتکاب جرم، سبب شده است نیاز به قانونی مجزا برای مبارزه با جرم کلاهبرداری اینترنتی بیش‌ازپیش احساس شود که این مسئله با تصویب قانون جرائم رایانه‌ای تقریباً برطرف شده است. همچنین، در بحث پیشگیری نیز روش‌هایی نیاز است تا بتوان از وقوع این جرم پیشگیری کرد. جنبهٔ فراملی‌بودن این جرم سبب می‌شود برای مقابلهٔ بهتر با آن، کشورها همکاری خود را در این زمینه بیشتر کنند. در ایران این همکاری‌ها می‌تواند به‌کارگیری الگوی قانونی و برنامه‌های پیشگیرانهٔ دیگر کشورها باشد تا از این طریق، جنبه‌های مثبت این مباحث را وارد سیاست جنایی کشور شود.

کلیدواژگان

برنامه‌های پیشگیرانه، تدابیر کیفری، فضای سایبری، کلاهبرداری اینترنتی.

* نویسندهٔ مسئول، رایانامه: jalalansari@yahoo.com

مقدمه

با توجه به گسترش روزافزون اینترنت در جهان و ایران، و ضریب نفوذ بالای آن در جوامع امروزی، علاوه بر روش‌های به‌کارگیری درست آن، بزهکاری‌هایی که اساس آن بر اینترنت است، نیز روبه‌افزایش است. در دههٔ اخیر به‌علت گسترش باورنکردنی اینترنت در جهان، کشورهای توسعه‌یافته و کشورهای درحال‌توسعه، بر اساس ضریب نفوذ اینترنت در کشورشان، با تبهکاری‌ها و بزهکاری‌های متعددی مواجهند. تنوع و میزان جرائم در کشورهای مختلف به سطح فرهنگی آن جامعه، میزان سواد و عوامل اجتماعی و غیره بستگی دارد. اما عموماً جرائم مالی یا همان جرائم علیه اموال و مالکیت که در فضای مجازی (اینترنت) اتفاق می‌افتد، در اغلب کشورها در صدر میزان این نوع جرائم قرار دارد. البته خود این جرم نیز صور مختلفی دارد که کلاهبرداری سایبری (اینترنتی) به علت گوناگونی در روش‌های اجرای آن و فراوانی افرادی که مورد بزه قرار می‌گیرند، بیشترین آمار را در جرائم علیه اموال در فضای اینترنت به خود اختصاص داده است. در این زمینه باید توجه کرد با اینکه در ایران ورود اینترنت به دههٔ ۱۳۷۰ بازمی‌گردد، اولین جرم در فضای کامپیوتری و اینترنت در سال ۱۳۸۱ اتفاق افتاد،[1] که شروعی برای جرائم اینترنتی در ایران بود. به‌طوری که از آن سال به بعد، این نوع جرائم به‌ویژه جرم کلاهبرداری اینترنتی افزایش یافت و علت آن هم نبود قانونی مناسب و بازدارنده بود. بر این اساس، مؤثرترین قانون آن زمان، یعنی قانون تجارت الکترونیکی در سال ۱۳۸۲ تصویب شد که البته نواقص و کمبودهای زیادی داشت و همین امر باعث شد میزان این جرائم روزبه‌روز بیشتر شود. این مسئله باعث شد قانون‌گذار این خلأ قانونی را بیش‌ازپیش احساس کند و بر این اساس، در سال ۱۳۸۸ قانون جرائم رایانه‌ای به تصویب مجلس شورای اسلامی رسید. این قانون تا حدی خلأ قانونی مورد نظر را در آن برههٔ زمانی پوشش داد، ولی متأسفانه در آن فقط یک ماده به جرم کلاهبرداری اینترنتی تخصیص داده

۱. برگرفته از سایت باشگاه خبرنگاران جوان، کد خبر ٤٠٥٨٦٢٩، ۲۷ مرداد ۱۳۹۱

شده بود که در آن هم تعریفی درست از کلاهبرداری اینترنتی و صور آن بیان نشده و به تعریف کلاهبرداری سنتی بسنده کرده بود.

جرم‌انگاری کلاهبرداری اینترنتی، مبانی و چالش‌ها

بر اساس آثار بعضی از حقوق‌دانان، گروهی معتقدند جرم کلاهبرداری اینترنتی، ساختاری شبیه کلاهبرداری سنتی دارد و نیازی به تعریف جدید و تغییر در دیدگاه جرم‌شناسی مرتبط با این دو نیست (Benner, 2010, p.73; Gercke, 2012, p.11; Chung, Schjolberg & Ghernaouti, 2011, p.4 ;2010, pp.241-246). برخی نیز معتقدند در بحث پیشگیری و جرم‌شناختی باید بین این دو جرم تفاوت قائل شد (Kleve et al., 2011, pp.162–167; Kerr, 2010, p.1584). با تحلیل نظرهای یادشده، به نظر می‌رسد، نظر گروه دوم کاربردی‌تر و با واقعیت همخوانی بیشتری دارد. پس از بیان این توضیحات، در ادامه، روند تاریخی تکامل سیاست جنایی ایران را نسبت به کلاهبرداری اینترنتی بررسی خواهیم کرد. دربارهٔ تاریخچهٔ وقوع کلاهبرداری اینترنتی در ایران باید بیان کرد با توجه به اینکه کاربرد کامپیوتر و اینترنت در ایران از ابتدای ورود آن تا دههٔ ۱۳۷۰ بسیار محدود بوده است، جرائم اینترنتی سابقهٔ زیادی در ایران ندارد. طبق بررسی‌های انجام‌گرفته، وقوع جرم کامپیوتری به‌تدریج از دههٔ ۱۳۷۰ در ایران شروع شد که متأسفانه آمار دقیقی در این زمینه نیز در دست نمی‌باشد (خرم‌آبادی، ۱۳۸٤، ص١٤).[1] از همین رو، قانون‌گذار در سال ۱۳۷۹ در برابر برخی جرائم کامپیوتری واکنش نشان داد و با الحاق تبصرهٔ ۳ به مادهٔ ۱ قانون مطبوعات، مقرر کرد «کلیهٔ نشریات الکترونیکی مشمول مواد این قانون است». این قانون را می‌توان اولین واکنش قانونی ایران در برابر بعضی از جرائم کامپیوتری دانست. دومین واکنش قانونی ایران در مقابل جرائم کامپیوتری، وضع «قانون حمایت از حقوق پدیدآورندگان نرم‌افزارهای رایانه‌ای» بود که در تاریخ ۱۳۷۹/۱۰/٤ در مجلس شورای اسلامی تصویب شد. مادهٔ ۱۳ قانون یادشده، نقض حقوق

۱. همچنین، رجوع کنید به وب‌سایت باشگاه خبرنگاران جوان، کد خبر ٤٠٥٨٦٢٩، ۲۷ مرداد ۱۳۹۱.

پدیدآورندگان آن دسته از نرم‌افزارهای رایانه‌ای را که مورد حمایت این قانون قرار گرفته‌اند، جرم تلقی کرده است. سومین واکنش قانون‌گذار ایران در مقابل جرائم کامپیوتری در سال ۱۳۸۲، تصویب قانون مجازات جرائم نیروهای مسلح مصوب ۱۳۸۲/۱۰/۹ مجلس شورای اسلامی بود. بر اساس مادهٔ ۱۳۱ این قانون، جعل اطلاعات و داده‌های رایانه‌ای،... و سوءاستفادهٔ مالی از طریق رایانه (کلاهبرداری و اختلاس) توسط نظامیان جرم تلقی شده و مرتکب حسب مورد، به مجازات جرم ارتکابی محکوم می‌شود. چهارمین واکنش قانونی مرتبط با جرائم رایانه‌ای، تصویب قانون تجارت الکترونیکی مصوب ۱۳۸۲/۱۰/۱۷ مجلس شورای اسلامی بود. بر اساس مواد ٦٦، ٦٧، ٦٨، ٦٩، ٧٤، ٧٥، ٧٦ و ٧٧ این قانون، کلاهبرداری، جعل و دستیابی و افشای غیرمجاز اسرار تجاری، نقض حقوق مربوط به مالکیت معنوی (کپی رایت) و غیره... که از طریق رایانه و در بستر تجارت الکترونیکی انجام گیرد، جرم تلقی شده، و برای آن مجازات تعیین شده است. شایان ذکر است هر یک از چهار قانون یادشده در بستر خاص خود قابلیت اعمال دارند. همان‌طور که از مطالب پیش‌گفته مشخص شد، در آن زمان برای مقابله با سایر جرائم اینترنتی قانونی کامل وجود نداشت، از همین رو، نیاز به یک قانون جامع در این زمینه بیش‌ازپیش احساس می‌شد، به این دلیل در سال ۱۳۸۸، بالاخره قانون جرائم رایانه‌ای تصویب شد و در مادهٔ ۱۳ آن کلاهبرداری اینترنتی جرم‌انگاری شد.

قانون جرائم رایانه‌ای و قانون تجارت الکترونیکی

تحلیل مادهٔ ۱۳ قانون جرائم رایانه‌ای

مادهٔ ۱۳ قانون جرائم رایانه‌ای به شرح ذیل کلاهبرداری مرتبط با رایانه و اینترنت را جرم‌انگاری کرده است: «هر کس به‌طور غیرمجاز از سامانه‌های رایانه‌ای یا مخابراتی با ارتکاب اعمالی از قبیل واردکردن، تغییر، محو، ایجاد یا توقیف‌کردن داده‌ها یا مختل‌کردن سامانه، وجه یا مال یا منفعت یا خدمات یا امتیازات مالی برای خود یا دیگری تحصیل کند، علاوه بر رد مال به صاحب آن، به حبس از یک سال تا پنج سال یا جزای نقدی از بیست میلیون ریال تا یکصد میلیون ریال یا هر دو مجازات محکوم خواهد شد».

با توجه به متن قانون یادشده، قانون‌گذار ایران، تعریف کلاهبرداری اینترنتی را از کلاهبرداری

سنتی گرفته است، در صورتی که در دیگر کشورها به‌دلیل وجود تفاوت بین موضوع کلاهبـرداری اینترنتی بـا نـوع سـنتی آن، همچنـین، کیفیـات مجـزا و متفـاوت در شـکل‌گیـری ایـن دو جـرم، کلاهبرداری اینترنتی را جرمی با تعریف و ماهیت جداگانه از کلاهبرداری سـنتی مـی‌داننـد (بـای، ۱۳۸۸، ص۳۰٤). در ادامه، بر اساس قانون یادشده، عناصر جـرم کلاهبـرداری اینترنتـی تفکیـک و تحلیل می‌شود.

ابتدا، عنصر مادی کلاهبرداری اینترنتی تحلیل می‌شود. با بررسی مادهٔ ۱۳ قانون جرائم رایانه‌ای، موارد ذیل دربارهٔ عنصر مادی جرم کلاهبرداری اینترنتی مشخص می‌شود:

۱. مرتکب می‌تواند هر کسی اعم از نظامی یا غیرنظامی، ایرانی یا خارجی باشد. وجـود سـمت خاصی نیز برای شخص مرتکب شرط نشده است.

۲. در کلاهبرداری سنتی انجام‌دادن مانور متقلبانه برای تحقق عنوان مجرمانه ضروری اسـت. در زمینهٔ کلاهبرداری اینترنتی نیز، عمل مادی مرتکب، انجام‌دادن اعمال متقلبانه در سامانه‌هـای رایانه‌ای یا مخابراتی است و قانون‌گذار برای مثال، مصادیقی از این اعمال متقلبانه را احصـا کرده است، ولی این روش‌ها حصری نیست (اکبری، ۱۳۹۰، ص۷).

۳. در کلاهبرداری سنتی، تأثیر مانور متقلبانه بر بزه‌دیده از طریـق فریـب، بـرای تحقـق عنـوان مجرمانه ضروری است، یعنی لازمهٔ کلاهبرداری فریب‌خوردن شخص است.

شایان ذکر است قوانین بین‌المللی کلاهبرداری اینترنتی را جرمی می‌دانند که در آن اغفال و بردن مال شرط نیست، بلکه صرف ایراد ضرر به قصد به‌دست‌آوردن منافع مالی کافی است (سالاری شهر بابکی، ۱۳۹۳، ص۲٦٤). در ادامه، باید گفت در قانون ایران برای تحقق جرم کلاهبرداری و برخی جرائم مربوط، الزاماً فـریب انسان زنده باید اتفاق افتد (دزیانی، ۱۳۸۵، ص٤٥). از همین رو، با توجه به بحث عنصر فریب شخص زنـده، اخـتلاف‌نظرهـایی بـین حقوق‌دانان به‌وجود آمده است، به این ترتیب که برخی حقوق‌دانان معتقدند فریب مخـتص اشخاص حقیقی است و دربارهٔ سامانه‌های رایانه‌ای و مخابراتی مصداق ندارد (خرم‌آبـادی، ۱۳۸٦، ص۱۰۳و۱۰٤)، اما برخی دیگر فریب‌خـوردن سـامانه‌هـای اینترنتـی را نیـز ممکـن

می‌دانند و از این حیث، کلاهبرداری اینترنتی را مشابه کلاهبرداری سنتی می‌دانند (نوری، ۱۳۸۳، ص۲۳). در این زمینه به نظر می‌رسد، دیدگاه اخیر کاربردی‌تر است. در واقع، کلاهبردار با فریب سامانه، مال دیگران را می‌برد.

٤. عمل مرتکب باید به‌طور غیرمجاز انجام گرفته باشد.

۵. این جرم مقید به نتیجه است. قانون‌گذار حصول حداقل یکی از نتایج ذیل را برای تحقق جرم ضروری دانسته است: تحصیل وجه، مال، منفعت و خدمات برای خود یا دیگری.

تحلیل مادهٔ ٦٧ قانون تجارت الکترونیکی

در ابتدای این قسمت عنصر مادی جرم کلاهبرداری اینترنتی مادهٔ ٦٧ قانون تجارت الکترونیکی و سپس، عنصر معنوی آن تحلیل و بررسی خواهد شد. این ماده، عنصر مادی سوءاستفاده در کلاهبرداری اینترنتی را به این شرح بیان کرده است: اقدامات و دستکاری‌های غیرمجاز و غیرقانونی که شامل مصادیق زیر است (گلدوزیان، ۱۳۹۱، ص۲): الف) واردکردن داده‌ها و اطلاعات اعم از صحیح و کذب؛ ب) تغییر غیرمجاز داده‌ها و اطلاعات رایانه‌ای؛ ج) محو داده‌ها یا اطلاعات رایانه‌ای و مخابراتی؛ د) توقف داده‌ها و اطلاعات رایانه‌ای: ایجاد وقفه در سیستم رایانه‌ای ممکن است موقت یا دائمی باشد. مانند متوقف‌کردن دستور پرداخت وجه به شخصی؛ هـ) مداخله در کارکرد سیستم رایانه.

دربارهٔ موارد یادشده، شایان ذکر است، وقتی این کار به تحصیل مال یا امتیاز منجر شود، جرم کلاهبرداری اینترنتی محقق می‌شود.

دربارهٔ عنصر معنوی جرم کلاهبرداری رایانه‌ای موضوع مادهٔ ٦٧ قانون تجارت الکترونیکی، باید گفت شباهت آن با عنصر معنوی جرم کلاهبرداری موضوع مادهٔ ۱ قانون تشدید مجازات مرتکبین اختلاس و ارتشا و کلاهبرداری محرز است. بنابراین، عنصر معنوی این جرم نیز از سه جزء علم مرتکب، سوءنیت عام و سوءنیت خاص تشکیل شده است. نتیجه اینکه قانون‌گذار در مادهٔ ٦٧ قانون تجارت الکترونیکی نه‌تنها نتوانسته است کلاهبرداری کامپیوتری محض را به‌درستی جرم‌انگاری کند، بلکه موجب شده است دو نوع مجازات برای کلاهبرداری کامپیوتری کلاسیک

وجود داشته باشد، که یکی مادهٔ ٦٧ قانون تجارت الکترونیکی است و دیگری مادهٔ ۱ قانون تشدید مجازات مرتکبین اختلاس و ارتشا و کلاهبرداری است (خرم‌آبادی، ۱۳۸٦، ص۱۰٤). از طرفی دیگر، با توجه به سکوت قانون‌گذار تا به امروز، در مقام جمع بین دو مادهٔ ۱۳ قانون جرائم رایانه‌ای و مادهٔ ٦٧ قانون تجارت الکترونیکی، می‌توان گفت هیچ‌یک ناسخ دیگری نیست.

برنامه‌های پیشگیرانه در برابر کلاهبرداری اینترنتی در ایران

به‌دلیل تأثیر علوم مربوط به جرم‌شناسی در پیشگیری از جرم، و به علت گسترش و بعضاً به‌وجودآمدن شکل جدید جرائم و پیچیده‌ترشدن آن‌ها، مباحث مربوط به پیشگیری همیشه در حال تغییر و روبه‌رشد است (Junger, 2011, p.2). دربارهٔ پیشگیری غیرکیفری باید توجه کرد پیشگیری از ارتکاب جرم، که با مداخلهٔ غیرکیفری انجام می‌گیرد، از این نوع است (صدیق، ۱۳۸۵، ص۲۱٦). دربارهٔ نوع‌شناسی پیشگیری غیرکیفری از کلاهبرداری اینترنتی در ایران نیز، باید بیان کرد این نوع پیشگیری دو نوع است، پیشگیری اجتماعی و پیشگیری وضعی (نجفی ابرندآبادی، ۱۳۸۱، ص۷۵۰). پس از آشنایی با کلیات و مفاهیم پیشگیری، در ادامه، سعی بر آن است تا برنامه‌های پیشگیرانه موردی ایران دربارهٔ کلاهبرداری اینترنتی توضیح داده شود.

برنامه‌های مبتنی بر پیشگیری وضعی از کلاهبرداری اینترنتی در ایران

پیشگیری وضعی عبارت است از اقدامات پیشگیرانهٔ معطوف به اوضاع و احوالی که جرائم ممکن است در آن وضعیت به وقوع بپیوندد، به‌طوری که هدف از این اقدامات، اتخاذ ترتیبی است که بهای ارتکاب عمل مجرمانه را برای مرتکب، بیش از سود حاصل از آن قرار دهد. زیرا از نظر طرفداران پیشگیری وضعی، انسان موجودی حسابگر است و سود و زیاد عملش را به‌طور فطری می‌سنجد.

اقدامات مبتنی بر این نوع پیشگیری دربارهٔ جرم کلاهبرداری اینترنتی شامل روش‌هایی مانند نظارت بر مراکز عرضه‌کنندهٔ اینترنت، فیلترینگ و غیره است. در ادامه، باید بیان کرد این نوع پیشگیری اساساً بزه‌دیده‌محور است. بنابراین، با پیشگیری اجتماعی که بزهکار را در کانون توجه

خود قرار می‌دهد، متفاوت است، هر چند در اینجا مجرم به‌طور غیرمستقیم مطرح است (نجفی ایرندآبادی، ۱۳۸۲-۱۳۸۱، ص۱۷۱). پس از این توضیحات مختصر دربارهٔ پیشگیری وضعی، باید بیان کرد با اینکه عملی‌کردن این نوع پیشگیری دربارهٔ جرائم اینترنتی به‌ویژه کلاهبرداری اینترنتی بسیار مشکل است، باز هم جایگاه خاصی در سیاست جنایی کشورها برای مقابله با این جرم دارد و برخلاف کاستی‌های ذاتی این نوع پیشگیری، در بعضی موارد کارایی دارد (صفاری، ۱۳۸۱، ص۲۳۳-۱۹۳؛ نجفی ابرندآبادی، ۱۳۸۳، ص۵۵۹).

به هر ترتیب، مصادیق این نوع پیشگیری برای مقابله با کلاهبرداری اینترنتی در ایران عموماً به پنج دسته طبقه‌بندی می‌شود که در جدول ۱ بیان شده است.

جدول ۱. طبقه‌بندی مصادیق پیشگیری وضعی از جرم کلاهبرداری اینترنتی

محور اصلی	محورهای فرعی	مصادیق مرتبط با کلاهبرداری اینترنتی
افزایش زحمت ارتکاب جرم	۱. سخت‌کردن آماج جرم	* تدابیر امنیتی (Filtering)
	۲. کنترل دسترسی به آماج جرم	* رمزگذاری و پسورد
	۳. غربال خروجی‌ها	* پراکسی‌ها (Proxy)
	٤. منحرف‌کردن بزهکار از آماج جرم	* کیبورد مجاز
	۵. کنترل وسایل تسهیل‌کنندهٔ جرم	* تدابیر مربوط به فیلترینگ
افزایش خطرات ارتکاب جرم	۱. توسعهٔ محافظت	* تدابیر صدور مجوز
	۲. کمک به نظارت طبیعی	* نصب دوربین‌های مداربسته
	۳. کاهش گمنامی	* کنترل مجرمان حرفه‌ای
	٤. استفاده از مدیران محلی	* جلوگیری از تکرار جرائم سازمان‌یافته
	۵. تقویت نظارت رسمی	* بررسی گزارش مشکوک مدیران بانک‌ها و آموزش آن‌ها
	٦. گشت‌زنی مجازی پلیسی	* نظارت، مانند نظارت بر چت‌روم‌ها
کاهش منافع	۱. جابه‌جایی آماج جرم	* کم‌کردن و کنترل موجودی
	۲. شناساندن یا نشانه‌گذاری	* استفاده از شناسه برای کاربران
	۳. حذف یا کاهش جذابیت	* ارائهٔ فهرست بدون اطلاعات
	٤. سخت‌کردن دسترسی	* به‌کارگیری گذرواژه
کاهش تحریکات	۱. کاهش سرخوردگی و استرس	* تدابیر مربوط به روان‌کاوی و روان‌درمانی از طریق آزمایش
	۲. دوری از تحقیر	
	۳. کاستن وسوسه‌های ارتکاب جرم	

ادامهٔ جدول ۱. طبقه‌بندی مصادیق پیشگیری وضعی از جرم کلاهبرداری اینترنتی

محور اصلی	محورهای فرعی	مصادیق مرتبط با کلاهبرداری اینترنتی
حذف معاذیر	۱. برقراری مقررات	* مقررات ثبت نام الکترونیکی توسط سرورها
	۲. تحریک وجدان و آگاهی	* درج راهنمایی‌ها وهشدارها
	۳. کنترل (پایش) رهاکننده‌ها یا رهاکننده‌های کنترل‌شده	* نصب تراشه‌های مخصوص برای تعیین میزان انطباق فعالیت‌ها
	٤. تسهیل رعایت قوانین	* ارائهٔ خدمات بیشتراز طریق روش‌های کنترل‌شده

در جدول ۱ انواع راه‌های پیشگیرانهٔ وضعی مورد استفاده در ایران را بیان کردیم. در ادامه، آن‌ها را نقد می‌کنیم. به‌طور طبیعی، بر هر یک از این روش‌ها نقد جداگانه و بعضاً مشترکی وارد است، که عموماً به نحوهٔ اجرا یا اطلاع‌رسانی دربارهٔ آن برمی‌گردد.

از جمله مهم‌ترین انتقادهای وارده در این زمینه، به مصادیق موجود در محور اصلی افزایش زحمت ارتکاب جرم و افزایش خطرات ارتکاب جرم برمی‌گردد. علت این است که این دو محور عملاً تشکیل‌دهندهٔ عمده‌ترین بخش مربوط به برنامه‌های مبتنی بر پیشگیری وضعی از کلاهبرداری اینترنتی در سیاست جنایی ایران هستند. با نگاهی به جدول ۱ و مصادیق مربوط، می‌توان سیاست جنایی ایران در این زمینه را به این شرح نقد کرد و ایراد گرفت که برای مثال، در بحث به‌کارگیری فیلترینگ و گذرواژه‌ها، مهم‌ترین نقد وارده این است که از طرفی، مسئولان سعی در اجرای فیلترینگ به‌طور تخصصی و کلی دارند، اما از طرف دیگر، آماده‌سازی زیرساخت‌های موجود برای این کار را کمتر مورد توجه قرار می‌دهند، به‌طوری که امروزه در جامعه شاهدیم بحث فیلترینگ به موضوعی سلیقه‌ای تبدیل شده است و آیین‌نامه یا دستورالعملی مشخص و مدون برای آن وجود ندارد و صرفاً بر اساس یک‌سری مسائل عمومی و سلیقه‌ای انجام می‌گیرد. موضوع مهم‌تر اینکه به‌دلیل موضوعات یادشده، متأسفانه به‌کارگیری برنامه‌های گذر از فیلتر در جامعه روبه‌افزایش است. البته موضوع به‌کارگیری این ابزارها نیز، از مهم‌ترین نقدهایی است که می‌توان بیان کرد. به این شرح که چرا با وجود صرف هزینه‌های هنگفت و صرف وقت فراوان برای فیلترینگ سایت‌های نامناسب، باید به‌راحتی برنامه‌های گذر از فیلتر قابل دسترسی و خرید باشد و عملاً همهٔ زحمات برای فیلترینگ زیر سؤال برود.

نقد دیگر نیز که می‌توان به برنامه‌های مبتنی بر پیشگیری وضعی در ایران وارد کرد، مربوط به بحث ناکافی‌بودن میزان آگاهی مردم و مدیران ارگان‌های مختلف هنگام مواجهه با کلاهبرداری اینترنتی است که این مسئله نیز طبیعتاً مربوط می‌شود به اینکه ارگان‌های مسئول به این مورد کمتر توجه کرده‌اند، به‌طوری که برای مثال، میزان آگاهی افراد از اینکه انواع مختلف کلاهبرداری اینترنتی چطور رخ می‌دهد و چه مواردی می‌تواند مشکوک باشد، پایین‌تر از حد معمول است، هر چند در سال‌های اخیر سعی شده است از طریق رسانه‌های جمعی و روزنامه و کتاب، سطح آگاهی مردم بالا برود، هنوز هم راه بسیار طولانی برای رسیدن به کمال مطلوب در این زمینه در پیش است.

برنامه‌های مبتنی بر پیشگیری اجتماعی

در این نوع پیشگیری سعی شده است با افزایش آگاهی افراد و تربیت صحیح آن‌ها، به‌ویژه قشر جوان و نوجوان جامعه، و همچنین، ازبین‌بردن زمینه‌های اجتماعی وقوع جرم، مانند فقر و بیکاری، انگیزه‌های مجرمانه از مجرمان سلب شود (نجفی ابرندآبادی، ۱۳۸۲، ص۱۲۰۸). در تعریفی دیگر از این نوع پیشگیری، بیان شده است «پیشگیری اجتماعی شامل اقدام‌هایی است که به‌طور مستقیم یا غیرمستقیم، هدفشان تأثیرگذاری بر شخصیت افراد است، تا از سازمان‌دادن فعالیت خود حول انگیزه‌های بزهکارانه بپرهیزند» (کی‌نیا، ۱۳۷۰، ص۷۸). با توجه به تعریف‌ها و مفاهیم یادشده، می‌توان پیشگیری اجتماعی را به دو دسته تقسیم کرد:

۱. پیشگیری اجتماعی رشدمدار، که سعی می‌کند اگر شخصی به هر دلیلی نشانه‌هایی از بزهکاری را بروز داد، از طریق مداخلهٔ سریع در او و محیط اطرافش از مزمن‌شدن بزهکاری در آینده جلوگیری کند.

۲. پیشگیری اجتماعی جامعه‌دار، که در پی خنثی‌سازی عوامل جرم‌زا در محیط اجتماعی است.

الف) پیشگیری اجتماعی رشدمدار اینترنتی

نکتهٔ بسیار مهم در برخورد و مبارزه با جرائم اینترنتی، به‌ویژه کلاهبرداری، استانداردهای فنی و اخلاق حرفه‌ای افراد است. بدین منظور که مسلماً زمانی می‌توان از فرد انتظار عملکرد درستی داشت که به‌خوبی به وی تفهیم شود چه تدابیر امنیتی باید به‌کار گیرد و چه اخلاق شغلی را رعایت کند (باستانی، ۱۳۸۳، ص۱۲۰). همان‌طور که می‌دانیم، طیف وسیعی از مجرمان و بزه‌دیدگان جرائم اینترنتی را افراد کم‌سن و سال، به‌ویژه نوجوانان تشکیل می‌دهند، از همین رو، از جمله تدابیر بسیار مؤثر در پیشگیری کلاهبرداری اینترنتی، ارائهٔ آموزش کافی و اطلاع‌رسانی به‌موقع است. آگاه‌کردن افراد و ارائهٔ آموزش‌های لازم در سنین کودکی و نوجوانی، می‌تواند نقش شایان توجهی در مقابله با کلاهبرداری اینترنتی داشته باشد. به همین دلیل، اولین محیطی که توجه مسئولان پیشگیری رشد مدار را جلب می‌کند، خانواده و به دنبال آن، پدر و مادر و بعد از آنان، دوستان، مربیان و دیگر مسئولان آموزشی و تربیتی است. به همین دلیل، اگر بتوان ابتدا توصیه‌ها و آموزش‌های لازم را به والدین منتقل و آن‌ها را با خطرها و در عین حال مزایا و مطلوبیت‌های فضای اینترنتی آشنا کرد، می‌توان امیدوار بود تا حد زیادی اهداف این تدابیر به ثمر بنشیند. متأسفانه این نوع پیشگیری نیز در کشورمان به‌طور شایسته، مورد توجه قرار نمی‌گیرد، هر چند امروزه در مدارس و بعضاً محیط خانواده تلاش‌هایی برای آموزش افراد در این زمینه انجام گرفته است، متأسفانه برنامه‌ای هدفمند و یکپارچه در این زمینه وجود ندارد، تا بتوان با توجه به آن آموزش افراد را پیگیری کرد.

ب) پیشگیری اجتماعی جامعه‌مدار سایبری

هدف از این تدابیر، جلوگیری از شکل‌گیری یا بروز انگیزهٔ مجرمانه در عموم جامعه به‌وسیلهٔ دو اقدام اصلی است، ۱. ایجاد علاقه و آسان‌کردن بروز افکار مشروع و مفید؛ ۲. دورکردن از ناهنجاری‌های اینترنتی.

از مهم‌ترین راه‌های پیشگیری از کلاهبرداری اینترنتی به‌وسیلهٔ پیشگیری اجتماعی جامعه‌مدار سایبری از طریق آموزش‌های عمومی و رسانه‌های جمعی است. باید توجه کرد

اهمیت خاص تحقیق در زمینهٔ رسانه و پیشگیری از وقوع جرم، از آن روست که این وسیله همهٔ زندگی انسان را دربرمی‌گیرد. کارکرد رسانه‌های جمعی دربارهٔ پیشگیری از کلاهبرداری اینترنتی می‌تواند از طریق آگاه‌کردن مردم از پیامدهای ناگوار این جرم (چه بزهکار باشد، چه بزه‌دیده) و نیز طراحی الگوهای مناسب رفتاری برای جلوگیری از ارتکاب و تکرار آن باشد، که از این طریق می‌توانند نقش مهمی در پیشگیری از جرم داشته باشند. (دیندار فرکوش، ۱۳۸۸، ص۴۱-۴۰). همچنین، برای اثربخشی بیشتر راه‌های پیشگیری از کلاهبرداری یادشده، به سیاست جنایی مشارکتی فعال نیازمندیم. از لحاظ مفهومی، سیاست جنایی مشارکتی، بررسی و مطالعهٔ جایگاهی است که در سیاست جنایی یک کشور به جامعهٔ مدنی و از طریق اعطای نقش به بزهکار، بزه‌دیده و به‌ویژه کل جامعه و مردم داده شده است (لازرژ[1]، ۱۳۹۰، ص۶۱). کارکرد این نوع سیاست جنایی نسبت به کلاهبرداری اینترنتی، اقدامات در مرحلهٔ کشف جرم، تعقیب دادرسی و اجرای حکم را دربرمی‌گیرد که با همکاری وسیع جامعهٔ مدنی، نهادهای مردمی و نیروهای دولتی مانند پلیس، سازمان زندان‌ها و جز آن با دستگاه قضایی انجام می‌گیرد (باصری، ۱۳۸۷، ص۳۷).

با جمع‌بندی توضیحاتی که بیان شد، می‌توان انتقاداتی را بر به‌کارگیری این نوع پیشگیری در ایران وارد دانست. برنامه‌هایی که در کشورمان مبتنی بر این نوع پیشگیری هستند، عموماً با محوریت مسئولیت دولت یا وزارت ارتباطات و فناوری اطلاعات و وزارت ارشاد است. همان‌طور که گفته شد، برای اثربخشی بیشتر این نوع پیشگیری از کلاهبرداری اینترنتی، باید 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.

برنامه‌های مبتنی بر پیشگیری مرحله‌ای

این نوع پیشگیری شامل پیشگیری‌های اولیه، ثانویه و ثالث می‌شود که در ادامه آن‌ها را تشریح خواهیم کرد.

1. Lazerges

پیشگیری اولیه

ابتدا باید بیان شود در ایران برنامه‌های پیشگیری عموماً کلی و مربوط به همهٔ جرائم است. البته می‌توان برنامه‌های مرتبط با پیشگیری اولیه را برای مقابله با کلاهبرداری اینترنتی در ایران یافت. ابتدا بهتر است تعریفی از این نوع پیشگیری بیان شود. پیشگیری اولیه، راهکارهایی را شامل می‌شود که از آن‌ها در زمینه‌های اجتماعی و اقتصادی، و دیگر زمینه‌های سیاست عمومی برای تأثیرگذاری بر موقعیت‌های ایجاد جرم و علل ریشه‌ای ارتکاب جرم به‌کار گرفته می‌شود (خسروشاهی، ۱۳۹۰، ص۱۲). از جملهٔ این برنامه‌های کلی که دربارهٔ کلاهبرداری اینترنتی نیز در کشورمان به‌کار گرفته می‌شود، می‌توان به ساخت فیلم‌های آموزشی، ایجاد سایت‌های آموزشی از طرف پلیس فتا و معاونت پیشگیری از جرم قوهٔ قضاییه و دیگر سایت‌هایی که توسط اشخاص عادی ایجاد شده است که در آن‌ها با ارائهٔ آموزش‌های لازم از جمله اعتمادنکردن به افراد در دادن رمز عبور کارت‌های اعتباری و نشان‌دادن انواع روش‌های کلاهبرداری از جمله فیشینگ و فارمینگ، از ارتکاب جرم کلاهبرداری اینترنتی پیشگیری شود. خوشبختانه به‌کارگیری برنامه‌هایی مبتنی بر این نوع پیشگیری از کلاهبرداری اینترنتی در حال رشد و بهبود است که آثار آن را می‌توان در رسانه‌های جمعی و سایر تبلیغات مشاهده کرد. شایان ذکر است یکی از مزایای این نوع پیشگیری توجه به همهٔ افراد جامعه است، به همین دلیل، نباید توجه به افراد کم‌سن و سال را، که بیشترین آمار را بین کاربران اینترنت دارند، در برنامه‌های پیشگیری اولیه از یاد برد (کاظمیان، ۱۳۸۸، ص۲٤۱).

پیشگیری ثانویه

پیشگیری ثانویه، مجموعهٔ تدابیر و اقداماتی است که در زمینهٔ بزهکاران و بزه‌دیدگان بالقوه، یعنی کسانی اعمال می‌شود که وضعیت خاص آنان باعث می‌شود بیشتر از سایرین در معرض خطر بزهکاری یا بزه‌دیدگی قرار گیرند، مانند تدابیر پیشگیرانهٔ مربوط به افراد هکر یا افرادی که توانایی نفوذ به سیستم‌های کامپیوتری را دارند. پیشگیری ثانویه، پیشگیری برای خنثی‌کردن حالت‌های خطرناک است. در این نوع پیشگیری، بر ایجاد تغییر در افراد، پیش از ارتکاب جرم توسط آن‌ها

تمرکز می‌شود. رفتارهای ضداجتماعی یا منحرفانه مانند فعالیت‌های نادرست و مجرمانه در اینترنت، ایجاد وب‌سایت‌های غیراخلاقی، یا مجرمانه، هک‌کردن سایت‌ها و جز آن، از جملهٔ این عوامل هشداردهنده‌اند که اگر پیش از اینکه جدی‌تر شوند و به یک زندگی مجرمانه یا بزه‌دیدگی منجر شوند، متوقف شوند، اقدامی برای پیشگیری ثانویه انجام گرفته است (صبوری‌پور، ۱۳۸۸، ص۳۳). با بررسی قوانین و وضع حاکم بر سیستم قضایی یا پلیس، و با بررسی لایحهٔ پیشگیری از وقوع جرم، درمی‌یابیم از این نوع پیشگیری غفلت شده است و فقط در بند ب مادهٔ ۸ این لایحه حمایت از افراد در معرض بزه‌دیدگی در نظر گرفته شده است، در صورتی که کنترل و بعضاً حمایت و آموزش افرادی که در معرض ارتکاب بزه کلاهبرداری اینترنتی‌اند با وجود سختی کار، می‌تواند مؤثر باشد، هر چند این نوع پیشگیری نسبت به پیشگیری اولیه و وضعی کارکرد کمتری دارد، زیرا به‌طور طبیعی، شناسایی حالت خطرناک افراد به‌ویژه در زمینهٔ کلاهبرداری اینترنتی بسیار سخت است. اصولاً بیان راهکار و تنظیم برنامهٔ مبتنی بر پیشگیری ثانویه بسیار سخت است، اما راهکارهایی را می‌توان با بهره‌گیری از کاربرد این پیشگیری در جرم کلاهبرداری اینترنتی بیان کرد. این راهکارها می‌توانند کارگاه‌های آموزشی باشند. البته شایان توجه است کارکرد این کارگاه‌های آموزشی با کارکرد کارگاه‌هایی که در پیشگیری اولیه وجود دارد، متفاوت است. زیرا در کارگاه‌های آموزشی که بر اساس پیشگیری اولیه به‌وجود آمده‌اند، همهٔ افراد جامعه مورد خطاب‌اند و همه می‌توانند شرکت کنند، اما در کارگاه‌هایی که برای پیشگیری از کلاهبرداری اینترنتی و بر اساس پیشگیری ثانویه ایجاد شده است، فقط افراد خاصی که بیان شد، می‌توانند حضور یابند تا با آموزش‌های لازم آن‌ها را از جرم دور کنیم و حالت خطرناک آن‌ها از بین ببریم.

پیشگیری ثالث

این نوع پیشگیری شامل اقداماتی می‌شود که در صورت انفجار بحران و مشخص‌شدن توالی فاسد آن و تبدیل‌شدن حالت خطرناک به مجرمیت، برای جلوگیری از استمرار و تداوم بزهکاری و مزمن‌شدن آن و پیشگیری از تکرار جرم توسط فرد، به‌کار گرفته می‌شود. بنابراین، اگر بخواهیم طبقه‌بندی تفکیکی بیان کنیم، باید گفت پیشگیری‌های اولیه و ثانویه، از جمله اقدامات پیشگیرانهٔ

معمول در جرم‌شناسی هستند و نوع ثالث آن شامل تدابیر بازپرورانه در جرم‌شناسی بالینی است. (کپوزی و آرگراس[1]، ۱۳۸٦، ص۲۰۲). پیشگیری از تکرار و تعدد جرم (پیشگیری ثالث) عموماً توسط پلیس و دیگر عوامل نظام عدالت کیفری انجام می‌گیرد (خسروشاهی و نمامیان، ۱۳۹۰، ص۱۳). این سیاست که بر اساس خصوصیات مجرمان و نوع جرائم و با توجه به شرایط مختلف بزهکار، اعمال می‌شود، نقش بسزایی در کاهش آمار تکرارکنندگان جرم داشته است، که متأسفانه در ایران کمتر به آن توجه می‌شود یا اصلاً به آن توجهی نمی‌شود. نمود عملی در این زمینه را نمی‌توان در ایران به‌طور منسجم یافت. با توجه به توضیحات بیان‌شده، از جمله مصادیقی که می‌توان دربارهٔ پیشگیری ثالث از کلاهبرداری اینترنتی بیان کرد، به این شرح است که برای مثال در آمریکا همهٔ کلاهبرداران اینترنتی و هکرها پرونده‌ای دارند که وضعیت آن‌ها اعم از نوع کلاهبرداری و اعمال آن‌ها را مشخص می‌کند و به همین دلیل، در مواقعی که تکرار جرم کلاهبرداری اینترنتی توسط مجرم رخ می‌دهد، می‌توانند برنامه‌ای مناسب برای خنثی‌کردن میل وی به تکرار جرم و ناتوان‌کردن وی در تکرار جرم به‌کار گرفته و از این طریق، برنامه‌های مبتنی بر پیشگیری ثالث را در زمینهٔ این جرم به‌کار گیرند. اما در مقابل مشاهده می‌شود در ایران پرونده‌سازی و توجه به کسانی که کلاهبرداری اینترنتی را انجام داده‌اند، مورد غفلت قرار گرفته یا به آن کمتر اهمیت داده شده است که همین ضعف در شناسایی و پرونده‌سازی برای کلاهبرداران اینترنتی سبب شد تا پیشگیری ثالث از کلاهبرداری اینترنتی در ایران مورد غفلت قرار گیرد.

نتیجه

با توجه به اینکه کاربرد رایانه و اینترنت در ایران از ابتدای ورود آن تا اواخر دههٔ ۱۳۷۰ بسیار محدود بوده است، کلاهبرداری اینترنتی سابقهٔ زیادی در ایران ندارد و اگر احیاناً جرمی در این زمینه واقع شده باشد، گزارشی از آن منتشر نشده است. این کند و طولانی‌بودن روند نفوذ اینترنت

1. Ceposy & Rgross

در آن سال‌ها سبب شد سیاست جنایی تقنینی ما به‌کندی خود را با جرم کلاهبرداری اینترنتی وفق دهد.

با نگاهی به سیاست جنایی تقنینی ایران در گذشته، مشخص می‌شود روند شکل‌گیری آن نسبت به جرم کلاهبرداری اینترنتی در سه مرحله بوده است. مرحلهٔ اول قانون مجازات جرائم نیروهای مسلح مصوب ۸۲/۱۰/۹ بود، که در آن سوءاستفاده مالی از طریق رایانه (کلاهبرداری و اختلاس) توسط نظامیان جرم تلقی می‌شد و مرحلهٔ دوم قانون تجارت الکترونیکی مصوب ۸۲/۱۰/۱۷ بود که در آن بیان شده بود، کلاهبرداری و... که از طریق رایانه و در بستر تجارت الکترونیکی انجام گیرد، جرم تلقی می‌شود. مرحلهٔ پایانی سیر تکمیلی سیاست جنایی تقنینی ایران نسبت به کلاهبرداری اینترنتی، مادهٔ ۱۳ قانون جرائم رایانه‌ای مصوب ۱۳۸۸ است، که با وجود نوآوری از نظر جرم‌انگاری کلاهبرداری اینترنتی، نقاط ضعفی نیز دارد. مهم‌ترین اشکالی که در اینجا به مادهٔ ۱۳ قانون جرائم رایانه‌ای وارد است، این است که قانون‌گذار انواع مختلف کلاهبرداری را در یک سطح دیده، غافل از اینکه هر یک از این اشکال با یکدیگر تفاوت دارند، بنابراین، این تفاوت‌ها هم به نحوهٔ ارتکاب جرم و هم به‌وسیلهٔ ارتکاب جرم برمی‌گردد و از آن مهم‌تر آثار زیانباری که هر یک از این روش‌ها بر جای می‌گذارند، متفاوت است. به همین دلیل، شاید بتوان با انجام‌دادن اصلاحاتی متناسب با شرایط اجتماعی و قانونی کشور، قانون را اصلاح کرد. دربارهٔ بحث پیشگیری از کلاهبرداری اینترنتی در ایران با توجه به مطالب پیش‌گفته، مشخص شد در کشور ایران بیشترین تأکید بر پیشگیری وضعی و اجتماعی است و در مرحلهٔ بعد، پیشگیری مرحله‌ای قرار دارد. دربارهٔ برنامه‌های مبتنی بر پیشگیری وضعی از کلاهبرداری اینترنتی باید بیان کرد این برنامه‌ها به روش فیلترینگ، کنترل موجودی حساب و جز آن که همگی این‌ها در سرفصل پیشگیری وضعی قرار گرفته، انجام می‌گیرد. اما در زمینهٔ پیشگیری مرحله‌ای موضوع قدری متفاوت است، این تفاوت به برنامه‌های ایران در مقابل مجرمان برمی‌گردد، به‌طوری که در ایران به این نوع پیشگیری بسیار کمتر از انواع دیگر پیشگیری توجه می‌شود که علت این مسئله را هم می‌توان در قوانین مربوطه و هم در رویهٔ عملی ارگان‌های مرتبط مشاهده کرد. به این دلایل، به

آموزش اولیهٔ مردم برای پیشگیری از کلاهبرداری اینترنتی و همچنین، آموزش و کمک به اشخاص درمعرض‌ارتکاب کلاهبرداری اینترنتی و خنثی‌کردن میل به تکرار جرم در کلاهبرداران اینترنتی با سابقهٔ تکرار توجه کمتری می‌شود. از طرفی دیگر، دربارهٔ پیشگیری اجتماعی از کلاهبرداری اینترنتی، ایران وضع مناسب‌تری دارد. همان‌طور که در بخش‌های قبل بیان شد، یکی از عناصر مهم در سیاست جنایی، پیشگیری از جرم است و از ابزارهای مهم پیشگیری از جرم ، رسانه‌های گروهی است. با توجه به نقش مهم رسانه و تأثیر مثبت آن در پیشگیری از جرم ، در سیاست جنایی ایران نیز برای رسانه، جایگاهی در نظر گرفته شده است. با وجودی که رسانه‌ها می‌توانند نقش بسیاری در پیشگیری جرم ایفا کنند و دولت‌ها می‌توانند برای رسیدن به اهداف خود به‌راحتی این ابزرا را به‌کار گیرند و هزینهٔ خود در مبارزه با جرم را کاهش دهند، جایگاه واقعی رسانه، در سیاست جنایی ایران در نظر گرفته نشده است. همچنین، شایان ذکر است که در سیاست جنایی قضایی ایران نیز، نمی‌توان از میان رویه‌ها و آرا به‌طور مستقیم، نقشی برای پیشگیری اجتماعی رسانه یافت، اما در قوانین، نقشی برای پیشگیری از جرم، برای قوهٔ قضاییه ، در سه مرحلهٔ پیش از وقوع جرم، مرحلهٔ وقوع جرم و پس از وقوع آن در نظر گرفته شده و رسانه نیز به‌عنوان ابزاری در دست قوهٔ قضاییه، در مراحل مختلف، پیش‌بینی شده است که کمک بسیاری به قوهٔ قضاییه در پیشگیری از کلاهبرداری اینترنتی می‌کند.

در پایان این بحث، می‌توان نتیجه گرفت مادهٔ ۱۳ قانون جرائم رایانه‌ای ایران، مادهٔ کاملی برای مبارزه با کلاهبرداری اینترنتی نیست و نیاز است قانون‌گذار محترم نسبت به رفع این مشکل اقدام کند و این اقدام می‌تواند با بهره‌گیری از سوابق دیگر کشورها در قانون‌گذاری باشد، تا بتوان قانونی کامل و متناسب با کشور خودمان داشته باشیم. دربارهٔ پیشگیری از کلاهبرداری اینترنتی نیز ایرادهایی مانند نبود برنامه‌های مشخص و منسجم، وارد است که رفع این ایرادها نیز نیازمند یک برنامه‌ای جامع، مشخص و اجراشدنی است.

منابع و مآخذ

۱. اکبری، عباسعلی (۱۳۹۰). *کلاهبرداری رایانه‌ای جلوه‌ای نوین و متمایز از بزهکاری سنتی. مجموعه مقالات همایش منطقه‌ای چالش‌های جرائم رایانه‌ای در عصر امروز* (صفحات ١٤-١)، مراغه، دانشگاه آزاد اسلامی واحد مراغه.

۲. بـاصری، علی‌اکبر (۱۳۸۷). *سیاست جنایی قضایی کودکان و نوجوانان (در حقوق داخلی و اسناد بین‌المللی)*. تـهران: خـرسندی.

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

٤. جـمشیدی، علیرضا (۱۳۹۰). *سیاست جنایی مشارکتی*. تهران: میزان.

۵. خرم‌آبادی، عبدالصمد (١٣٨٤) *جرائم فناوری و اطلاعات*. رسالهٔ دکتری، رشتهٔ حقوق جزا و جرم‌شناسی، دانشکدهٔ حقوق، دانشگاه تهران.

٦. خرم‌آبادی، عبدالصمد (١٣٨٦). کلاهبرداری رایانه‌ای از دیدگاه بین‌المللی و وضعیت ایران. *فصل‌نامهٔ حقوق مجلهٔ دانشکدهٔ حقوق و علوم سیاسی دانشگاه تهران*، سال ۷۳، شمارهٔ۲، صفحات ۱۱۲-۸۳.

۷. خسروشاهی، قدرت‌الله، نمامیان، پیمان و شکربیگی، علیرضا (۱۳۹۰). پیشگیری از جرم در پرتو آموزه‌های دینی. *نشریهٔ مهندسی فرهنگی*، سال ٦، شماره‌های ۵۷ و ۵۸، صفحات ۲۳-۸.

۸. دزیانی، محمدحسن (۱۳۸۵). مقدمه‌ای بر سیاست جنایی ایران در باب جرائم سایبری. *قضاوت*، شمارهٔ ۳۸ (خردادماه و تیرماه)، صفحات ٤٨-٤٢.

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

۱۰. رشادتی، جعفر (۱۳۸۷). *پیشگیری از جرم در قرآن کریم*. تهران: دفتر تحقیقات کاربردی پلیس پیشگیری ناجا.

۱۱.زیبر، اولریش (۱۳۹۰). جرائم *رایانه‌ای*. ترجمهٔ محمدعلی نـوری، رضا نخجوانی، مصطفی بختیاروند و احمد رحیمی مقدم، تهران: انتشارات گنج دانـش.
۱۲.سالاری شهر بابکی، میرزا مهدی (۱۳۹۳). *کلاهبرداری و ارکان متشکلهٔ آن*. تهران: میزان.
۱۳.صبوری‌پور، مهدی (۱۳۸۸). *رویکرد تطبیقی به پیشگیری از جرم (گزارش مرحلهٔ سوم طرح تحقیقاتی تدوین پیش‌نویس سیاست‌های کلی پیشگیری از جرم و اصلاح مجرمین)*. کمیسیون حقوقی و قضایی دبیرخانه مجمع تشخیص مصلحت نظام، صفحات ۱۲۰-۱.
۱٤.صفاری، علی (۱۳۸۱). انتقادات وارده به پیشگیری از جرم. م*جلهٔ تحقیقات حقوقی*، شماره‌های ۳۵ و ۳٦، صفحات ۲۳٤-۱۹۳.
۱۵.کاظمیان، لیلا (۱۳۸۸). *مجموعه مقالات نخستین همایش ملی پیشگیری ازجرم؛ پیشگیری از تکرار جرم و بزه‌دیدگی با تأکید بر نقش پلیس*. جلد اول، تهران: انتشارات معاونت آموزش ناجا.
۱٦.کپوزی، دیوید و آرگراس، داگلاس (۱۳۸٦). رهیافت‌هایی به پیشگیری. *فصل‌نامهٔ مطالعات پیشگیری از جرم*، سال ۲، شمارهٔ ۵، صفحات ۲۱۳-۱۹۱.
۱۷.گسن، ریموند (۱۳۸۸). *جرم‌شناسی کاربردی*. ترجمهٔ مهدی کی‌نیا،تهران: انتشارات مجد.
۱۸.گسن، موریس (۱۳۹٤). *اصول جرم‌شناسی*. ترجمهٔ میرروح‌اللّه صدیق، تهران: انتشارات دادگستر.
۱۹.گلدوزیان، ایرج (۱۳۹۱). کلاهبرداری رایانه‌ای. *مجلهٔ حقوقی مجد*، صفحات ۱۱-۱.
۲۰.لازرژ، کریستین (۱۳۹۰). *درآمدی بـر سـیاست جنایی*. ترجمهٔ علی‌حسین نـجفی ابـرندآبادی، تهران: میزان.
۲۱.نجفی ابرند آبادی، علی‌حسین (۱۳۸۲). *تقریرات درس جرم‌شناسی*. دورهٔ کارشناسی ارشد دانشگاه شهید بهشتی. گردآورنده رضا فانی.
۲۲.نجفی ابرندآبادی، علی‌حسین (۱۳۸۱). *تقریرات درس جرم‌شناسی*. دورهٔ کارشناسی ارشد مجتمع آموزشی عالی قم، گردآورنده مهدی سیدزاده.

۲۳.نجفی ابرندآبادی، علی‌حسین (۱۳۸۳). پیشگیری عادلانه از جرم در علوم جنایی. مجموعه *مقالات در تجلیل از استاد آشوری*، تهران: انتشارات سمت.

24. Brenner, W.S. (2010). *Cybercrime criminal threats from cyberspace*. Santa Barbara: Praeger.
25. **C**hung, Y.C. (2010). The computer fraud and abuse act. *Harvard Journal of Law And Technology*, 24(1), 222- 256.
26. Gercke, M. (2012). *Understanding cybercrime: Phenomena, challenges and legal response*. Geneva: ITU.
27. Junger, M. (2011). Cyber crime science. *Journal of Twente University*, (19), 1-55.
28. Kerr, S.O. (2010). Vagueness challenges to the computer fraud and abuse act. *Journal of Minnesota Law Review*, 94 (5), 1561-1587.
29. Kirwan, G. & Power, A. (2013). *Cybercrime: The psychology of online offenders*. Massachusetts: Cambridge University.
30. Kleve, P., De Mulder, R. & Van Noortwijk, K. (2011). *The definition of cyber crime. Computer Law & Security Review Journal*, 27(2), 162 – 167.
31. Schjolberg, S. & Ghernaouti-Helie, S. (2011). *A global treaty on cybersecurity and cybercrime*. Stålfjæra: Aitoslo.