Journal of
Comparative Criminal Jurisprudence
www.jccj.ir

Volume 6, Issue 3, 2026

Comparison of the Measures in the Criminal Policy of Iran and the United States in Dealing with Cybercrimes; Emphasizing the Teachings of Control Theory

Reza Shamsi[1], Seyedeh Zahra Habibi[2*], Samira Golkhandan[3], Akbar Rajabi[3]

1. PhD Student of Criminal Law and Criminology, Khom.C., Islamic Azad University, Khomein, Iran.

2. Assistant Professor, Department of Criminal Law and Criminology, CT.C., Islamic Azad University, Tehran, Iran. (Corresponding Author)

3. Assistant Professor, Department of Criminal Law and Criminology, Khom.C., Islamic Azad University, Tehran, Iran.

ARTICLE INFORMATION

Type of Article: ***Original Research***
Pages: ***40-55***

Corresponding Author's Info
ORCID: *0009-0006-0638-1897*
TELL: *+980000000000*
Email: *sz.habibi@iau.ac.ir*

Article history:

Received: *03 Feb 2025*

Revised: *31 Oct 2025*

Accepted: *02 Mar 2026*

Published online: *23 Sep 2026*

Keywords:
Criminal Policy, Cyber Crimes, Iran, America, Control Theory.

ABSTRACT

The premise of control theory is that people will commit crimes normally; unless the factor or factors prevent them from doing so; Therefore, the emphasis of this theory is on internal and external prevention tools. On the other hand, criminal policy in its full concept includes both punitive and repressive measures and preventive measures; The issue of how preventive measures can be effective in reducing new crimes such as cybercrimes; Examining the extent of the use of these measures in the criminal policy of dealing with these crimes pays attention, and since the criminal policy of the United States of America in dealing with cybercrimes is more up-to-date than other countries; This article compares the criminal policy of Iran and the United States in the use of criminal and preventive measures to deal with cybercrimes using descriptive-analytical methods and library tools. The findings of this article show that the American legislator, in relation to the crimes of fraud and cyber theft, has taken advantage of criminal measures in a minimal, exemplary and unique way by criminalizing examples and considering a specific punishment for each example. ; But besides that, he has also paid attention to preventive measures; In the case of Iran's criminal policy, the legislator has not acted very carefully with general and unjustified criminalization, criminalization and the use of criminal measures, and there is still a lot of work to be done to apply preventive measures using the teachings of control theory.

How to Cite This Article: Shamsi, R; Habibi, S. Z; Golkhandan, S & Rajabi, A (2026). "Comparison of the Measures in the Criminal Policy of Iran and the United States in Dealing with Cybercrimes; Emphasizing the Teachings of Control Theory". *Journal of Comparative Criminal Jurisprudence*, 6(3): 40-55.

فصلنامه فقه جزای تطبیقی
www.jccj.ir

دوره ششم، شماره سوم، پاییز ۱۴۰۵

مطالعه تطبیقی تدابیر سیاست جنایی ایران و آمریکا در مقابله با جرائم سایبری؛ با تأکید بر آموزه‌های نظریه کنترل

رضا شمسی[۱]، سیده زهرا حبیبی[۲]*، سمیرا گل‌خندان[۳]، اکبر رجبی[۳]

۱. دانشجوی دکترای حقوق جزا و جرم‌شناسی، واحد خمین، دانشگاه آزاد اسلامی، خمین، ایران.
۲. استادیار گروه حقوق جزا و جرم‌شناسی، واحد تهران مرکزی، دانشگاه آزاد اسلامی، تهران، ایران. (نویسنده مسؤول)
۳. استادیار گروه حقوق جزا و جرم‌شناسی، واحد خمین، دانشگاه آزاد اسلامی، خمین، ایران.

اطلاعات مقاله

نوع مقاله: پژوهشی
صفحات: ۵۵-۴۰

اطلاعات نویسنده مسؤول
کد ارکید: ۱۸۹۷-۰۶۳۸-۰۰۰۶-۰۰۰۹
تلفن: ۹۸۰۰۰۰۰۰۰۰۰+
ایمیل: sz.habibi@iau.ac.ir

سابقه مقاله:
تاریخ دریافت: ۱۴۰۳/۱۱/۱۵
تاریخ ویرایش: ۱۴۰۴/۰۸/۰۹
تاریخ پذیرش: ۱۴۰۴/۱۲/۱۱
تاریخ انتشار: ۱۴۰۵/۰۷/۰۱

واژگان کلیدی:
سیاست جنایی، جرائم سایبری، ایران، آمریکا، نظریه کنترل.

چکیده

پیش‌فرض نظریه‌ی کنترل آن است که اشخاص به‌صورت عادی مرتکب جرم خواهند شد؛ مگر آنکه، عامل یا عواملی آنها را از این امر بازدارد؛ لذا تأکید این نظریه بر ابزارهای پیشگیری درونی و بیرونی است. از سوی دیگر، سیاست جنایی در مفهوم کامل خود، هم تدابیر کیفری و سرکوبگر و هم تدابیر پیشگیرانه را در برمی‌گیرد؛ این مسأله که تدابیر پیشگیرانه تا چه میزان می‌توانند بر کاهش جرائم نوپدیدی چون جرائم سایبری مؤثر واقع شود؛ بررسی میزان بهره‌گیری از این تدابیر را در سیاست جنایی مقابله‌ای با این جرائم مورد توجه قرار می‌دهد و ازآنجاکه سیاست جنایی کشور آمریکا در مقابله با جرائم سایبری، به‌روزتر از سایر کشورهاست، این مقاله با روش توصیفی- تحلیلی و ابزار کتابخانه‌ای به مقایسه سیاست جنایی ایران و آمریکا در بهره‌گیری از تدابیر کیفری و پیشگیرانه برای مقابله با جرائم سایبری پرداخته است. یافته‌های این مقاله نشان می‌دهد که قانون‌گذار آمریکا، در رابطه با جرائم کلاه‌برداری و سرقت سایبری، با اقدام به جرم‌انگاری مصداقی و در نظر گرفتن مجازاتی خاص برای هر مصداق، از تدابیر کیفری به‌صورت حداقلی و مصداقی و منحصر بهره برده است، اما در کنار آن به تدابیر پیشگیرانه نیز توجه داشته است؛ درصورتی‌که در سیاست جنایی ایران، قانون‌گذار با جرم‌انگاری کلی و غیرمصداقی، در جرم‌انگاری و بهره‌گیری از تدابیر کیفری، خیلی دقیق عمل نکرده و برای به‌کارگیری تدابیر پیشگیرانه با بهره‌گیری از آموزه‌های نظریه کنترل نیز هنوز جای کار زیادی دارد.

مقدمه

نظریه‌ی کنترل از جمله نظریه‌هایی است که جامعه شناسان و جرم شناسان، برای خنثی ساختن جرم و یافتن منشأ کج‌رفتاری اشخاص در اجتماع مطرح نموده‌اند. این نظریه که از سوی صاحب‌نظرانی مانند **والترکلس، هیرشی** و دیگران مطرح شده بود، بعد از قرن بیستم میلادی، پا به عرصه‌ی وجود نهاد. مطابق این نظریه، وقتی می‌توان از ارتکاب جرم جلوگیری به‌عمل آورد که اشخاص در جامعه، مورد نظارت و کنترل قرار گیرند، زیرا کج‌رفتاری و ارتکاب جرم یک امر طبیعی است و در ماهیت اشخاص وجود دارد. باید سیستم و روش‌هایی را ایجاد کنیم تا از ارتکاب عمل خلاف قانون و عرف، جلوگیری کرده باشیم (خراسانی و همکاران، ۱۴۰۱: ۲۱). در این نظریه، دو نوع کنترل از سوی دانشمندان پیشنهاد گردیده است که با استفاده از عوامل محیطی، می‌توان کنترل درونی و کنترل بیرونی بر افراد را اعمال نمود. کنترل اجتماعی، از جمله نظریاتی است که در دو علم جامعه‌شناسی و جرم‌شناسی کاربرد داشته و هر دو این نظریه را مورد بررسی و توجه قرار داده است. (انصاری و همکاران، ۱۳۹۸: ۴۱). یکی از حوزه‌هایی که نظریه کنترل اجتماعی کاربرد دارد مربوط به جرائم رایانه‌ای است. جرم رایانه‌ای را فعالیتی مجرمانه با استفاده از فناوری‌های اینترنت و شبکه دانسته‌اند (سالارزهی و همکاران، ۱۳۹۰: ۱).

چالشی که سازمان قضایی با آن مواجه است، تعیین مجازات و کیفر برای مجرمان می‌باشد؛ زیرا قوانین جرائم رایانه‌ای متناسب با رشد فن‌آوری اطلاعات به‌روزرسانی نمی‌شوند و در نتیجه پس از وقوع جرم جدید، تعیین کیفر برای آن جرم توسط قانون‌گذار، کاری زمان‌بر و دشوار است. قوانین جرائم رایانه‌ای باید طوری تدوین شوند که همه‌شمول بوده و خلأ و حفره‌های قوانین را پوشش دهد. در همین راستا در سال ۱۳۸۸ قانون جرائم رایانه‌ای به تصویب و اجرا درآمد و مشکل خلأ تقنینی در مورد عنصر قانونی جرائم مذکور را در نظام حقوق کیفری مرتفع ساخت. جرائم رایانه‌ای حوزهٔ بسیار گسترده‌ای دارند و به فعالیتی گفته می‌شود که در آن کامپیوترها یا شبکه‌های ارتباطی ابزار، مقصد یا محل اجرای یک فعالیت مجرمانه و غیرقانونی می‌باشند. در هر عصر که علم جدیدی کشف می‌شود، مجرمین نیز از جلوه‌های نوین آن علم جهت ارتکاب جرم بهره‌برداری می‌کنند. تسهیل و تسریع در پیدا کردن کیفر برای جرائم جدید، پیدا کردن سابقه‌ی جرم، ردپای جرائم مرتبط و زنجیره‌ی بازداشت، آموزش از اهداف اصلی جلوه‌های جرائم رایانه‌ای می‌باشد.

آمار دقیقی در خصوص میزان تخلفات رایانه‌ای و اینترنتی در دست نیست، با این حال، گزارش‌های موجود از مرجع رسیدگی به جرائم رایانه‌ای و اینترنتی در ایران (پلیس فتا) و نیز گزارش‌های منتشر شده از منابع مختلف، نشانگر شیوع تخلفات رایانه‌ای در ایران می‌باشد. مسؤولان پلیس فتا، جرائم اینترنتی در ایران را در حال افزایش دانسته است. به استناد گزارش این واحد پلیس، ۸۱ درصد از مجرمین با انگیزه مالی، ۱۳ درصد با انگیزه غیر اخلاقی، ۳ درصد با انگیزه انتقام‌جویی، ۲ درصد با انگیزه سرگرمی و یک درصد با انگیزه‌های دیگر مرتکب جرائم رایانه‌ای شده‌اند. ۹۵ درصد از مرتکبین جرائم رایانه‌ای مرد و در گروه سنی ۱۸ تا ۳۵ سال قرار دارند. برداشت از حساب‌های بانکی و هتک حیثیت مهم‌ترین جرائم رایانه‌ای در ایران اعلام شده و بیشترین میزان جرائم رایانه‌ای به ترتیب در استان‌های تهران، خراسان، گیلان و مازندران بوده است (علیوردی‌نیا و همکاران، ۱۳۹۲: ۳۵).

با توجه به مسائل و مشکلات پیش‌گفته، سعی بر آن است تا در این تحقیق با بررسی سیاست جنایی کشور آمریکا، به‌عنوان کشور پیشرو در امر قانون‌گذاری جرائم سایبری، مدل سیاست جنایی مناسبی را که برگرفته از سیاست جنایی این کشور در رابطه با سرقت و کلاه‌برداری سایبری است ارائه شود تا شاید با الگو گرفتن از دیگر کشورها، سیاست جنایی مؤثر و کارآمدی در رابطه با این دو جرم در ایران تعریف و تبیین شود. از همین رو، برای رسیدن به قانونی کامل و ارائه راهکارهای عملی و به‌روز کردن قوانین موردنظر، علاوه‌بر اینکه باید شرایط اجتماعی و قانونی ایران مدنظر قرار گیرد، لازم است از دیدگاه‌های مختلف قانونی و قانون‌گذاری دیگر کشورها در پروسه جرم‌انگاری و تعیین مجازات جرم کلاه‌برداری اینترنتی کمک گرفت. همچنین، برای رسیدن به کمال مطلوب، طبیعتا باید قانون کشورمان را با کامل‌ترین و به‌روزترین قانون دنیا در زمینه کلاه‌برداری اینترنتی مقایسه کرد. به همین دلیل نیز

قانون فدرال جرائم رایانه‌ای آمریکا برای مقایسه با قانون جرائم رایانه‌ای ایران انتخاب شده است و علت انتخاب هم این است که طبق آمارهای جهانی و توضیحاتی که داده خواهد شد، قانون جرائم رایانه‌ای آمریکا به‌روزترین و کامل‌ترین قانون در دنیا در این زمینه است؛ لذا هدف تحقیق حاضر پاسخگویی به این سؤال اصلی است که میزان بهره‌گیری سیاست جنایی ایران و آمریکا از تدابیر کیفری و پیشگیرانه در مقابله با جرائم سایبری با بهره‌گیری از آموزه‌های نظریه کنترل، چقدر است؟

با نگاهی به تحقیقات انجام‌شده در این زمینه، مشخص می‌شود که عموم تحقیقات فقط بحث تعریف جرم و پیشگیری از کلاه‌برداری در ایران را مورد بررسی قرار داده‌اند و مطالعه تطبیقی و راهکارهای عملی و علمی در جهت پیشگیری از این دو جرم ارائه نشده است. در ادامه، به اختصار به تحقیقات و نتایج برخی از آنها اشاره می‌شود.

پایدارفر و همکاران (۱۴۰۱)، تحقیقی با عنوان مقایسه رکن مادی جرم کلاه‌برداری رایانه‌ای با سنتی انجام دادند. از حیث نتیجه، انتفاع مرتکب و ضرر به دیگری وجوه تشابه این دو بزه است اما بردن مال در کلاه‌برداری رایانه‌ای (برخلاف سنتی) جزو نتیجه حاصله در رکن مادی آن نبوده بلکه بخشی از رفتار حصری در قسمت دوم رفتار فیزیکی این جرم و موضوع آن بزه است.

دشتی و افشاری (۱۳۹۸)، تحقیقی با عنوان مطالعه تطبیقی جرائم سایبری در ایران و حقوق بین‌الملل انجام دادند. در این مقاله ماهیت فضای سایبر و ابزارهای ارتباطی، تعریف، تاریخچه، ویژگی و طبقه‌بندی آن مورد بررسی قرار می‌گیرد. خطرات احتمالی و جهانی‌شدن مقابله با جرائم سایبری از نکاتی بود که به‌عنوان نتیجه بحث مطرح شد.

انصاری و همکاران (۱۳۹۸)، تحقیقی با عنوان سیاست جنایی ایران و آمریکا در قبال جرائم کلاه‌برداری و سرقت سایبری انجام دادند. یافته‌ها نشان داد قانون‌گذار آمریکا، در رابطه با جرائم کلاه‌برداری و سرقت سایبری، اقدام به جرم‌انگاری مصداقی کرده و برای هرکدام مجازات خاص در نظر گرفته است، درصورتی‌که در سیستم حقوقی ایران، قانون‌گذار عنوان کرده اگر اعمال مندرج در مواد ۱۲ و ۱۳ قانون جرائم رایانه‌ای همراه با بردن یا ربودن مال دیگری شود، عنوان مجرمانه دارد و توجهی به انواع مصادیق این جرائم و تمایز آن‌ها نکرده است.

براتی و همکاران (۱۳۹۶)، تحقیقی با عنوان بررسی تطبیقی مصادیق جرائم حوزهٔ فضای مجازی در ایران، آمریکا و فرانسه انجام دادند. تجربه قانون‌گذاری سه کشور ایران، آمریکا و فرانسه علی‌رغم مشابهات آنها با یکدیگر (در شیوه شکلی قانون‌گذاری) دارای اختلافاتی نیز هست که این اختلافات، عمدتا به مبانی جرم‌انگاری برمی‌گردند. در این باب به نظر می‌رسد کشورهای فرانسه و آمریکا بر مبنای اصل لاضرر، جرم‌انگاری نموده و ایران بر اساس مقررات اسلامی به این مهم پرداخته است. علاوه بر این، می‌توان به رویکردی امنیتی در جرم‌انگاری جرائم حوزه فضای مجازی اشاره نمود که آمریکا از سال ۲۰۰۱ به بعد پیش گرفته است.

پورقهرمان (۱۳۹۶) تحقیقی با عنوان مطالعه‌ی تطبیقی سازوکارهای حمایت از بزه‌دیدگان جرائم رایانه‌ای در حقوق کیفری ایران و اسناد بین‌المللی با تأکید بر کنوانسیون بوداپست انجام داد. با بررسی قوانین کیفری ایران و اسناد بین‌المللی به‌ویژه کنوانسیون بوداپست و با لحاظ گونه‌شناسی حمایت‌ها مشخص می‌شود که سیاست جنایی ایران در قبال حمایت از بزه‌دیدگان جرائم رایانه‌ای افتراقی نبوده و سیاست پاسخ‌دهی غیرحمایتی و غیراختصاصی اعمال شده است و حتی نسبت به بزه‌دیدگان خاص که در اسناد بین‌المللی توجه مضاعفی شده است، در سیاست جنایی ایران چتر حمایتی از این گروه هم برداشته شده است.

رضوی‌فرد و موسوی (۱۳۹۵)، تحقیقی با عنوان مسئولیت کیفری در فضای سایبر در حقوق ایران انجام دادند. قانون‌گذار ایران فصل ششم از قانون جرائم رایانه‌ای را به موضوع مسئولیت کیفری اختصاص داده است و تغییری که قانون فوق‌الذکر ایجاد نموده شناسایی و ایجاد مسئولیت کیفری برای اشخاص حقوقی در محیط مجازی است.

انصاری و میلانی (۱۳۹۵)، تحقیقی با عنوان نقد سیاست جنایی ایران در قبال کلاه‌برداری اینترنتی انجام دادند. در بحث

پیشگیری روش‌هایی نیاز است تا بتوان از وقوع این جرم پیشگیری کرد. جنبهٔ فراملی بودن 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 پیشگیرانه‌ی دیگر کشورها باشد تا از این طریق، جنبه‌های مثبت این مباحث را وارد سیاست جنایی کشور شود.

آقابابایی و احمدی‌ناطور (۱۳۹۵)، تحقیقی با عنوان مطالعه تطبیقی جرائم علیه حریم خصوصی در فضای سایبری ایران و آلمان انجام دادند. مقایسهٔ مذکور نشان می‌دهد که حقوق ایران به لحاظ فقدان برخی از اصول حاکم بر داده‌های شخصی، کامل نبودن اصول پیش‌بینی‌شده و ارجاع برخی اصول به آیین‌نامه‌های گوناگون نقایص جدی دارد که باید از سوی مقنن بازنگری شود. از سوی دیگر، فقدان مقررات جامع در زمینهٔ حمایت از حریم خصوصی مانع از درک و اجرای صحیح حمایت از داده‌ها در دادگاه‌ها و مراجع اداری می‌شود.

رایجیان (۱۳۹۳)، تحقیقی با عنوان پیش‌گیری از جرائم رایانه‌ای از رهیافت‌های نظری تا رهیافت جهانی در پرتو رهنمود پیش‌گیری از جرم سازمان ملل متحد انجام دادند. مقاله‌ی حاضر، مسأله‌ی پیش‌گیری از جرائم رایانه‌ای را در دو محور اصلی بررسی می‌کند که عبارت‌اند: ۱) اتخاذپذیری رویکردهای پیش‌گیری مبتنی بر توسعه‌ی اجتماعی و مبتنی بر موقعیت‌های جرم‌زا که می‌توان آن را به‌عنوان «رهیافت‌های نظری» به این موضوع بررسی کرد؛ ۲) اصول راهبردی پیش‌گیری با محوریت سند رهنمود پیش‌گیری سازمان ملل متحد که می‌توان آن را جلوه‌ای از یک «رهیافت جهانی» یا رهیافتی در بستر جهانی‌شدن در نظر گرفت و تحلیل کرد.

سالارزهی و همکاران (۱۳۹۰)، تحقیقی با عنوان جرم‌شناسی رایانه‌ای در بستر تجارت الکترونیک و ارائه مدل پیشنهادی مقابله با جرائم رایانه‌ای انجام دادند. در این مقاله سعی شده است تا ابتدا با بیان مشکلات امنیتی سازمان‌ها در حوزهٔ فناوری اطلاعات و تجارت الکترونیک، مفاهیم، مصادیق و محدوده هر دو دسته از جرائم فنی و غیر فنی بیان شود، سپس با استراتژی‌های دفاعی سازمان در مقابل جرائم رایانه‌ای، پدیدهٔ نوظهور کالبدشکافی رایانه‌ای تشریح شده و در نهایت مدل منطقی پیشنهادی مقابله با جرائم رایانه‌ای ارائه شده است.

طارمی (۱۳۸۷)، در مقاله‌ای تحت عنوان طبقه‌بندی و آسیب‌شناسی جرائم رایانه‌ای با رویکردی حقوقی به انواع جرائم رایانه‌ای، خصوصیات و نیز چالش‌های مربوط به این جرائم می‌پردازند و راهکارهایی را جهت مقابله با این آسیب ارائه داده و به لوایح قانونی موجود در این زمینه و کاستی‌های آن تأکید کرده‌اند.

عالی‌پور (۱۳۸۳)، تحقیقی با عنوان کلاه‌برداری رایانه‌ای انجام داد. کلاه‌برداری رایانه‌ای چون در دنیای جدید به نام دنیای مجازی رایانه و اینترنت (فضای سایبر) با امکانات بی‌شماری تحقق می‌یابد فقط علیه انسان نیست و بلکه غالبا علیه سیستم رایانه‌ای و نرم‌افزارهای آن است و بنابراین شرط فریب قربانی در آن تا مرز حذف شدن تضعیف می‌شود. موضوع جرم کلاه‌برداری رایانه‌ای نیز فراتر از مال یا وسیله تحصیل مال است و شامل خدمات و امتیازات مالی و حتی داده‌های رایانه‌ای دارای ارزش مالی نیز می‌شود.

با بررسی‌های صورت گرفته در ادبیات تحقیق مشخص شد که موضوع کاربست یافته‌های نظریه کنترل در سیاست جنایی تقنینی ایران و آمریکا در حوزهٔ جرائم رایانه‌ای از دید پژوهشگران مغفول مانده است و این شکاف تحقیقاتی در پژوهش حاضر پوشش داده خواهد شد.

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

و طبقه‌بندی اطلاعات، از ابزارهای سنجش کتابخانه‌ای و اسنادی استفاده شده است.

۱- مفاهیم

۱-۱- جرائم سایبری

از اواسط دهه ۱۹۷۰، مطالعات تجربی در مورد جرم رایانه‌ای با استفاده از متدهای تحقیقاتی رشته جرم‌شناسی انجام شد. در دهه‌ی ۱۹۸۰، نظرات علمی و عمومی در مورد جرم رایانه‌ای به‌سرعت تغییر یافت و مشخص شد که جرم رایانه‌ای محدود به جرائم اقتصادی نبوده، بلکه همه تعرضات نسبت به همه منافع را شامل می‌شود. مثلا سوءاستفاده از رایانه بیمارستان یا تخلفات رایانه‌ای نسبت به حقوق خصوصی و فردی که جنبه اقتصادی ندارند و اساسا این موارد را جدا از جرم رایانه‌ای بررسی کرده‌اند. موج وسیعی از سرقت برنامه‌ها و سوءاستفاده‌ها از صندوق‌های پرداخت و استفاده از مخابرات، موجب شد انعطاف جامعه اطلاعاتی برانگیخته شده، نیاز برای استراتژی جدید امنیت داده‌پردازی و کنترل جرم احساس شود (براتی و همکاران، ۱۳۹۶: ۱۳۴).

در حال حاضر، بیشتر نظرها در زمینه جرائم رایانه‌ای به انتقال غیرقانونی سرمایه‌ها با استفاده از ابزار الکترونیکی، خرابکاری، ویروس‌ها، کرم‌های رایانه‌ای و همچنین، جعل اسناد با استفاده از رایانه معطوف است. خطر خرابکاری، مخصوصا در سال ۱۹۸۹ و زمانی آشکار شد که دادرسی‌های کیفری در جمهوری فدرال آلمان معلوم کرد که خرابکارانی با استفاده از شبکه‌های اطلاعاتی بین‌المللی به اطلاعاتی در آمریکا و انگلستان و دیگر کشورهای خارجی، دست‌یافته و حاصل کار خود را به کشور شوروی سابق فروخته‌اند. تقریبا در همان زمان (۱۹۸۸)، خطر ویروس‌ها و کرم‌ها هم معلوم شد. زمانی که (- Internet Worm) توسط یک دانشجوی آمریکایی ساخته شده بود، در طی چند روز نزدیک به ۶۰۰۰ سیستم رایانه‌ای را در اینترنت مختل کرد. بعد شکل‌های جدید بزهکاری در زمینه تکنیک‌های ارتباط سمعی-بصری (مثلا در زمینه سیستم مینیتل فرانسه و یا قسمت‌های ارتباط ماهواره‌ای) ادامه جرائم اطلاعات را افزایش دادند (انصاری و میلانی، ۱۳۹۵: ۵۳).

فضای سایبری در کنار نکات قوت و کارآمد خود و همچنین مهم و حیاتی بودن آن، محل فعالیت انسان‌های فرصت‌طلب نیز می‌باشد. یکی از جرائمی که در این محیط به وقوع می‌انجامد، سرقت اینترنتی است. پیشینه‌ی مقابله با جرم سرقت قدمتی برابر با تمدن بشری دارد و مقنن در خصوص مجازات این جرم، در قانون مجازات اسلامی پیش‌بینی کرده است. در عصر حاضر با توجه به رشد تکنولوژی رایانه‌ای و تحول اطلاعات و همچنین گسترش ارتباطات سایبری در چند دهه گذشته و متعاقبا سهولت ارتکاب جرائم مرتبط با فناوری‌های نوظهور که جرم سرقت اینترنتی جزء همین جرائم محسوب می‌شود، در کشورهای مختلف باعث ایجاد و اصلاحاتی در قوانین آن کشور شده است (اکبری، ۱۳۹۰: ۸۸).

در جهت پیشگیری و کاهش ارتکاب جرم توسط افرادی که سابقه‌دار نبوده و ویژگی‌های فضای سایبری باعث ترغیب آنها به ارتکاب جرم شده است، بایستی راهکارها که شامل دو روش پیشگیری وضعی و اجتماعی می‌باشد، با ایجاد فرهنگ بهره‌گیری از شبکه‌های سایبری، آموزشی و آگاه ساختن افراد جامعه توسط رسانه‌ها و... اقداماتی را انجام داد. سیاست جنایی از زمان ظهور انگاره‌های آن در لسان بانیان و نظریه‌پردازان، به‌نوعی تدوین خط‌مشی و اصول کلی راهبردی کنترل و پاسخ‌دهی سنجیده به جرم، در سایه‌ی به‌کارگیری ابزارهای ویژه و منطبق با شرایط خاص گفته شده است که همواره تحت تأثیر بنیادهای فکری و تئوری‌های برخاسته از آن‌ها، دستخوش تغییرات و تحولات بنیادین قرار گرفته است. از زمانی که **فوئر باخ** آلمانی در سال ۱۸۰۳ اصطلاح سیاست جنایی را در معنا و مفهوم مضیق سیاست کیفری، به مجموعه علوم جنایی وارد کرد (آقابابایی و احمدی‌ناطور، ۱۳۹۵: ۲۴)، پهنه‌ی گسترده‌ی عدالت کیفری، چاره‌اندیشی برای معضل جرم را جز در پرتوی به‌کارگیری اقدامات سنجیده و هدفمند دارای توفیق نمی‌یافت. لذا اهداف متولیان و متصدیان تشکیلات سیاست جنایی و مسیر تحول آن بر اساس نوع پاسخ‌دهی به جرم و پس از آن به‌کارگیری ابزار متناسب با وضعیت پیش‌آمده، تنظیم شد.

۲-۱- نظریه کنترل

نظریه‌ی کنترل از جمله نظریه‌هایی است که جامعه شناسان و جرم شناسان، برای خنثی ساختن عمل مجرمانه و یافتن منشأ کج‌رفتاری اشخاص در اجتماع مطرح نموده‌اند. این نظریه از سوی صاحب‌نظران مانند **والترکلس**، **هیرشی** و دیگران مطرح شده بود، بعد از قرن بیستم میلادی، پا به عرصه‌ی وجود نهاد. مطابق این نظریه، وقتی می‌توان از ارتکاب جرم جلوگیری به عمل آورد که اشخاص در جامعه، مورد نظارت و کنترل قرار گیرند، زیرا کج‌رفتاری و ارتکاب جرم یک امر طبیعی است و در ماهیت اشخاص وجود دارد. باید سیستم و روش‌هایی را ایجاد کنیم تا از ارتکاب عمل خلاف قانون و عرف، جلوگیری کرده باشیم. در این نظریه، دو نوع کنترل از سوی دانشمندان پیشنهاد گردیده است که با استفاده از عوامل محیطی، می‌توان کنترل درونی و کنترل بیرونی بر افراد را اعمال نمود. این کنترل‌ها را می‌توان از طریق کنترل و نظارت رسمی – قوانین و مقررات و... صورت می‌گیرد کنترل اجتماعی، از جمله نظریاتی است که در دو علم جامعه‌شناسی و جرم‌شناسی کاربرد داشته و هر دو، این نظریه را مورد بررسی و توجه قرار داده است. به سخن دیگر، نظریه‌های کنترل اجتماعی را می‌توان از دو بعد مورد واکاوی قرار داد. قبل از ابداع این نظریه (کنترل اجتماعی)، نظریه‌های دیگری در جرم‌شناسی مورد توجه جرم شناسان قرار گرفته بود؛ مثلا می‌توان به نظریات مکتب تحققی، خصوصا نظریه‌پرداز مشهور این مکتب، **لمبروزو** اشاره نمود. می‌توان ادعا کرد که دانشمندان این مکتب، بیشتر بر زیست‌شناسی و ساختار جسمانی توجه داشته‌اند. یا به عبارت دیگر، علت ارتکاب جرم را وجود اختلالات جسمانی مجرم می‌دانستند. به همین دلیل، بیشتر ژن‌ها و کروموزوم‌ها (شکل ظاهری مجرم)، مورد بررسی قرار می‌گرفت. مکاتب دیگر نیز در مورد علت ارتکاب جرم در مجرم، ابعاد دیگری را مورد بررسی قرار داده‌اند که هر صاحب‌نظر در این زمینه، نظر پردازی‌ها نموده است (اکبری، ۱۳۹۰: ۷۸)؛ مثلا آقای زیگموند فروید، بنیان‌گذار مکتب روان‌کاوی، معتقد بود که علت ارتکاب جرم در مجرمین، به خاطر به وجود آمدن اختلالات روانی و روحی است که مرتبط به گذشته‌ی فرد مجرم است، زیرا به نظر این دانشمند، مجرم فردی است که در گذشته، به آرزوهای خود دست نیافته و این برای وی به‌صورت عقده، تبدیل شده و ضمیر ناخودآگاهی در شخص به‌وجود آورده است. حال این ضمیر ناخودآگاه اوست که این‌گونه تبلور نموده و به‌صورت غیر ارادی، مرتکب جرم می‌شود؛ اما دانشمندانی مثل **تراویس هیرشی**، **دورکیم** و... نظریه‌های کنترل اجتماعی را به وجود آورده‌اند. اینان، پرسشی را که دانشمندان فوق، به‌عنوان مبنای جرم‌شناسی مطرح کرده بودند، به‌صورت برعکس درآورده و نظریاتی در این راستا ارائه کردند.

نظریه‌پردازان پیشین، به این عقیده بودند که علت و چرایی ارتکاب جرم را در مجرم واکاوی نمایند، زیرا آنان به این باور بودند که انسان متعارف و سالم، در اجتماع، مرتکب جرم نخواهد شد و مجرمینی‌که جرم را مرتکب می‌شوند، حتما اختلالاتی در جسم و روح آنان و همین‌طور رویدادهایی در اجتماعی‌که در آن زندگی می‌کنند، رخ داده است که اینان کج‌رفتار شده‌اند. با این وجود اما نظریه‌ی کنترل اجتماعی، برخلاف نظریه‌پردازان فوق معتقد است: «**اشخاص به‌صورت عادی مرتکب جرم خواهند شد و خطاکار بودن و ارتکاب جرم برای اشخاص، یک امر طبیعی است**». نظریه‌ی کنترل اجتماعی، علت و چرایی عدم ارتکاب جرم را مورد بحث و بررسی قرار داده است. به سخن دیگر، باید چه راه‌هایی در نظر گرفت تا افراد اجتماع جرم را انجام ندهند؟ زیرا اگر نظارت یا کنترلی نباشد، آن‌ها مرتکب جرم خواهند شد (انصاری، ۱۳۹۸: ۹۷).

جامعه، می‌تواند با درنظرگرفتن تفکیک قوا و ایجاد قوانین مناسب، سیاست جنایی مثبت به وجود آورده و از ارتکاب جرم جلوگیری نماید. البته باید خاطرنشان نمود که هر نظام حقوقی در میان کشورها، بخش جداگانه برای قوانین جزایی دارند؛ زیرا با توجه به شرایط، اوضاع حاکم بر اجتماع، عرف و اخلاق عامه سیاست جنایی خود را تغییر می‌دهند. برخی کشورها برای کنترل و نظارت شهروندان و اتباع، بیش‌تر اعمال کج را جرم‌انگاری نموده تا از این طریق اجتماع را منظم بدارند؛ اما برخی کشورها از راه‌های دیگر استفاده کرده و قوانین جزایی را برای حداقل کج‌رفتاری‌ها در نظر می‌گیرند. به عبارت حقوقی‌تر، اصل حداقل بودن یا اصل حداکثر بودن حقوق جزا را با توجه به شرایط و اوضاع جامعه عیار می‌سازند.

۳-۱- مفهوم پیشگیری

پیشگیری به‌طور عمده دارای دو مفهوم است؛ هم به معنای پیش‌دستی کردن و به جلوی چیزی رفتن و هم به معنای آگاه کردن و هشدار دادن است. اما در جرم‌شناسی پیشگیرانه، پیشگیری در معنای اول آن مورد استفاده قرار می‌گیرد، یعنی با به کار بردن متد و روش‌های مختلف به منظور جلوگیری از وقوع بزهکاری، هدف به جلوی جرم رفتن و پیشی گرفتن از بزهکاری است (احمدی، ۱۳۸۷: ۹۱-۹۰ و گسن، ۱۳۷۰: ۱۳۳). بر همین اساس، علمای حقوق جزا و جرم‌شناسی، دو مفهوم از پیشگیری را مورد توجه قرار داده‌اند و به تعریف و تبیین آن پرداخته‌اند که یکی از آنها، مفهوم موسع پیشگیری است و مقصود از آن هر اقدامی است که در مقابله با جرم و به منظور سد کردن ارتکاب آن باشد و جرم را کاهش دهد. طبق این تعریف از پیشگیری، می‌توان مواردی همچون مجازات بزهکار و ترمیم کردن خسارت وارد بر بزه‌دیده در فرآیند وقوع جرم را نام برد. این برداشت و استنباط از پیشگیری نزد افرادی همچون **انریکوفری** وجود داشته است؛ مقصود وی از این اصطلاحات همان اقدامات پیشگیرانه غیر کیفری است که جایگزین مجازات بوده و به عبارتی «هم‌عرض‌های کیفری» می‌باشند (نجفی ابرندآبادی، ۱۳۷۹: ۷۴۲). در مقابل مفهوم موسع پیشگیری، مفهوم مضیق پیشگیری قرار دارد که مقصود از آن مجموعه ابزار و وسایلی است که دولت برای مهار بهتر بزهکاری از دو طریق مورد استفاده قرار می‌دهد: از طریق حذف یا محدود کردن عوامل جرم‌زا و از طریق اعمال مدیریت مناسب نسبت به عوامل محیطی، فیزیکی و اجتماعی که به‌نوبه خود فرصت‌های مناسبی را برای ارتکاب جرم ایجاد می‌کنند (نجفی ابرندآبادی، ۱۳۷۹: ۷۵۰). در مفهوم مضیق پیشگیری، پیشگیری از تکرار جرم مدنظر نیست، بلکه مقصود مورد توجه قرار دادن وضعیت پیش جنایی و قبل از ارتکاب جرم است.

۲- تدابیر کیفری سیاست جنایی ایران و آمریکا در مقابله با جرائم سایبری

در رابطه با تحلیل سیاست جنایی تقنینی، با بررسی قوانین موجود در دو کشور مشخص شد که قانون جرائم رایانه‌ای ایران اقدامی در جهت مصداق شناسی و تفکیک آنها از هم نسبت به این جرائم انجام نداده و فقط یک سری اعمال را ذکر کرده و عنوان کرده است که چنانچه شخصی از طریق آن اعمال، مال دیگری را برباید یا ببرد، سارق یا کلاه‌بردار است. در طرف مقابل، در قانون جزای فدرال آمریکا، قانون‌گذار آن کشور در مواد مختلف و متعدد، اقدام به جرم‌انگاری جداگانه هر یک از مصادیق این جرائم کرده و مجازات آنها را نیز با توجه به شرایط و نتیجه جرم ارتکابی تعیین کرده است که این موضوع نشان‌دهندهٔ این است که می‌بایست میان مصادیق مختلف این جرائم تفاوت گذاشت تا بتوان نیازهای قانونی متناسب با پیشرفت فناوری را برای جامعه تأمین کرد و همچنین مجازات متناسب و بازدارنده را برای هرکدام، به‌طور جداگانه بکار برد.

ماده ۱۲ قانون جرائم رایانه‌ای، عنصر قانونی جرم سرقت سایبری است که در آن عنوان شده، هرکس داده‌های متعلق به دیگری را برباید، سارق محسوب می‌شود که این ماده ابهامات زیادی دارد و بر اساس آن نمی‌توان به تعریف دقیقی از سرقت سایبری دست‌یافت؛ چراکه برای رسیدن به تعریف مناسب، باید به مسائلی همچون مصادیق این جرم، شرایط وقوع و غیره توجه کرد. با نگاهی به این ماده، می‌توان دیگر عناصر تشکیل‌دهنده این جرم را تحلیل کرد و به‌دنبال آن، نقاط ضعف و قوت مادهٔ مربوطه را مشخص کرد. عنصر مادی سرقت سایبری و سنتی، شبیه به هم است که به‌دلیل جلوگیری از تکرار مکررات، فقط مواردی که سرقت سایبری را از سرقت سنتی جدا می‌سازد، ذکر خواهند شد. مورد اول این وجه تمایز، وسیله ارتکاب جرم است، دوم موضوع جرم و دیگری فضا و بستری است که امکان ارتکاب جرم در آن فراهم می‌شود. در اینجا وسیله ارتکاب جرم، رایانه است و موضوع سرقت سایبری، داده‌های دیجیتالی و بستر ارتکاب جرم، فضای سایبر است (خرم‌آبادی، ۱۳۸۶: ۸۴-۸۵).

الف) ماده ۱۳ قانون جرائم رایانه‌ای: ماده ۱۳ قانون جرائم رایانه‌ای که عنصر قانونی جرم کلاه‌برداری سایبری است، عنوان می‌کند: **«هر کس به‌طور غیرمجاز از سامانه‌های رایانه‌ای یا مخابراتی با ارتکاب اعمالی از قبیل وارد کردن، تغییر، محو، ایجاد یا توقیف کردن داده‌ها یا مختل کردن سامانه، وجه یا مال یا منفعت یا خدمات یا امتیازات مالی برای خود یا دیگری تحصیل کند ...».** کلاه‌بردار سایبری است.

با توجه به متن قانون مذکور، این موضوع مشخص می‌شود که قانون‌گذار ایران، تعریف کلاه‌برداری اینترنتی را از شکل سنتی گرفته است، درصورتی‌که در دیگر کشورها به‌دلیل وجود تفاوت بین موضوع کلاه‌برداری اینترنتی با نوع سنتی آن و همچنین کیفیات مجزا و متفاوت در شکل‌گیری این دو جرم، کلاه‌برداری اینترنتی را جرمی با تعریف و ماهیت جداگانه از کلاه‌برداری سنتی می‌دانند (بای و پورقهرمانی، ۱۳۸۸: ۳۰۴). به هر ترتیب، در ادامه سعی بر آن است تا بر اساس قانون مذکور، عناصر جرم کلاه‌برداری اینترنتی تفکیک و تحلیل شود. با بررسی ماده ۱۳ قانون جرائم رایانه‌ای، موارد زیر در مورد عنصر مادی جرم کلاه‌برداری اینترنتی قابل ذکر هستند:

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

۲. در خصوص کلاه‌برداری اینترنتی نیز، عمل مادی مرتکب، انجام اعمال متقلبانه بر روی سامانه‌های رایانه‌ای یا مخابراتی است و قانون‌گذار از باب تمثیل مصادیقی از این اعمال متقلبانه را احصاء کرده است، ولی این روش‌ها حصری نیست (اکبری، ۱۳۹۰: ۷).

۳. در کلاه‌برداری سنتی، تأثیر مانور متقلبانه بر بزه‌دیده از طریق فریب برای تحقق عنوان مجرمانه ضروری است، یعنی لازمه کلاه‌برداری، فریب خوردن شخص است (میرمحمدصادقی، ۱۳۸۶: ۱).

لازم به ذکر است که در قوانین بین‌المللی، کلاه‌برداری اینترنتی را جرمی می‌دانند که در آن اغفال و بردن مال شرط نیست، بلکه صرف ایراد ضرر به قصد به دست آوردن منافع مالی کافی است (سالاری شهر بابکی، ۱۳۹۳: ۲۶۴). در قانون ایران، تحقق جرم کلاه‌برداری و برخی جرائم مربوط، نیازمند فریب انسان زنده است (به استثنای کشورهایی همچون کانادا، فرانسه، هلند و اسکاتلند) (دزیانی، ۱۳۸۵: ۴۵). از همین رو، با توجه به بحث عنصر فریب شخص زنده، برخی از حقوقدانان معتقدند که فریب، مختص اشخاص حقیقی است و در مورد سامانه‌های رایانه‌ای و مخابراتی مصداق ندارد (خرم‌آبادی، ۱۳۸۶: ۱۰۳-۱۰۴).

ب) مواد ۱۰۲۸، ۱۰۲۸A، ۱۰۲۹، ۱۰۳۰، ۱۰۳۷ و ۱۳۴۳ قانون جزایی فدرال آمریکا: بخش ۱۸ قانون جزای فدرال آمریکا که بخش یا قانون جرائم سایبر نام دارد، انواع جرائم در این حوزه را با ذکر مصادیق و شرایط مورد نیاز جهت تحقق آنها به‌طور مفصل شرح داده که شش ماده آن مربوط به کلاه‌برداری اینترنتی و انواع صور آن می‌شود. پروسه قانونی تصویب این بخش تا سال ۱۹۸۵ طول کشید و سرانجام این اصلاحات در سال‌های ۱۹۸۸، ۱۹۸۹، ۱۹۹۰، ۱۹۹۱، ۱۹۹۲، ۲۰۰۱ و ۲۰۰۷ ادامه داشت تا در نهایت، قانون جرائم سایبر فعلی به تصویب کنگره رسید (مارشال و بیلی، ۲۰۰۷: ۲۰). بخش‌های مرتبط با کلاه‌برداری اینترنتی در قسمت ۱۸ قانون جزای آمریکا شامل مواد ۱۰۲۸، ۱۰۲۸A، ۱۰۲۹، ۱۰۳۰، ۱۰۳۷ و ۱۳۴۳ می‌شود که هرکدام مربوط به صور خاصی از سرقت و کلاه‌برداری است که در ادامه عناوین این مواد و توضیحات آنها ارائه خواهد شد، این عناوین شامل موارد زیر هستند (قانون جرائم سایبری آمریکا، ۲۰۰۸، بخش ۱۸):

- **ماده ۱۰۲۸) سرقت هویت و مشخصات دسترسی:** در این ماده عنوان شده، هر شخصی آگاهانه و بدون مجوز قانونی یک سند شناسایی، ویژگی‌های احراز هویت یا سند شناسایی جعلی تهیه و تولید کند، انتقال دهد یا تصرف کند، تحت عنوان سرقت هویت محاکمه می‌شود. در این ماده، بسته به چگونگی انجام جرم و عمل مرتکب حبس کمتر از ۲۰،۱۵ و ۳۰ سال در نظر گرفته است. همچنین، قانون‌گذار فدرال در ادامه اصلاحاتی را همچون «ساختن مدارک»، «مدارک هویت»، «مدارک غلط هویت»، «معنای هویت»، «کارت هویت شخصی» و غیره شرح و ویژگی‌های آنها را عنوان کرده است که این امر تکلیف مجریان قانون را در برخورد و رسیدگی با این جرم راحت‌تر می‌کند.

- **ماده ۱۰۲۸ A: سرقت هویت و اطلاعات هویتی همراه با خشونت:** در این ماده، منظور قانون‌گذار از سرقت هویت خشن، در جایی است که این سرقت هویت برای اعمال خشن از جمله جرائم مربوط به تروریسم و دیگر جرائم عمومی خشن بکار رفته است. بر اساس این ماده، منظور از جرائم خشن عمومی، جرائمی هستند که مربوط به انواع جنایات علیه انسان است که در این موارد، علاوه بر مجازات که برای آن جنایت در نظر گرفته می‌شود، بزهکار، برای این سرقت هویت به دو سال زندان

محکوم می‌شود و در جرائم مربوط به تروریسم، شخص بزهکار به مدت ۵ سال به زندان محکوم می‌شود (فینکلی، ۲۰۱۲: ۲).

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

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

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

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

۴. آگاهانه و با قصد فریب دادن، تجهیزات ایجاد ابزار را تولید و در آن تردد یا کنترل داشته باشد یا آنها را در اختیار داشته باشد (Gordon & Curtis, 2000: 16).

• **ماده ۱۰۳۰: کلاه‌برداری و جرائم وابسته در ارتباط با رایانه:** در این ماده عنوان شده، چنانچه شخص با داشتن دسترسی آگاهانه بدون مجوز به رایانه یا دسترسی بیش‌ازحد مجاز و به‌وسیله چنین دسترسی، اطلاعاتی که توسط ایالات‌متحده آمریکا و به موجب فرمان اجرایی یا اساسنامه به منظور دفاع ملی یا روابط خارجی یا هر نوع اطلاعات محدود دیگر تعریف شده در بند Y بخش ۱۱ قانون انرژی اتمی ۱۹۵۴ که نیاز به محافظت در برابر افشا دارد، به‌دلیل باور داشتن به اینکه اطلاعات به دست آمده به این روش را می‌توان برای آسیب زدن به ایالات‌متحده آمریکا مورد استفاده قرار داد، دریافت کند یا با هدف سود بردن از هر کشور خارجی از طریق ارتباط خودسرانه، ارائه و انتقال دهد یا باعث انتقال آن شود یا ارائه آن به افراد غیرمجاز یا نگهداری خودسرانه و عدم تحویل آن به افسر یا کارمند ایالات‌متحده که مجاز به تحویل آن است، کلاه‌برداری محسوب می‌شود. همچنین، دسترسی عمدی بدون مجوز یا دسترسی بیش‌ازحد مجاز و دریافت اطلاعات شامل اسناد مالی یک یا حاوی فایل سازمان گزارش دهنده مشتری در مورد یک مشتری مانند عباراتی که در قانون امور اعتباری تعریف شده است نیز جرم‌انگاری شده است (Gercke, 2012: 324).

• **ماده ۱۰۳۷: کلاه‌برداری و جرائم وابسته در ارتباط با نامه‌های الکترونیک:** در متن این ماده، قانون‌گذار توضیحاتی درباره عناصر جرم داده است که در ادامه، نکات کلیدی و مهم این ماده ذکر خواهد شد. در این ماده عنوان‌شده، به‌طورکلی هرکس که به نوعی در تجارت خارجی و بین ایالتی نقشی داشته باشد و آن شخص آگاهانه، به رایانه محافظت شده بدون مجوز، دسترسی داشته باشد و آگاهانه اقدام به شروع ارسال پیام‌های پست الکترونیکی تجاری چندگانه از این رایانه یا به چنین رایانه‌ای بکند، طبق این ماده مجازات می‌شود. در ادامه، قانون‌گذار صور دیگر این جرم را طبقه‌بندی می‌کند که به این شرح است: **«هرگاه شخصی از رایانه محافظت شده برای توزیع یا ارسال مجدد پیام‌های پست الکترونیک تجاری چندگانه با قصد فریب یا گمراه کردن دریافت‌کنندگان یا هر خدمت دسترسی اینترنتی به‌عنوان مبدأ چنین پیام‌هایی استفاده کند، یا با جعل اطلاعات اصلی در پیام‌های پست الکترونیک تجاری چندگانه و آغاز عمدی ارسال چنین پیام‌هایی یا با استفاده از اطلاعاتی که هویت ثبت‌کننده واقعی را جعل می‌کند، در این سایت‌ها ثبت‌نام و برای ۵ حساب پست الکترونیک یا تعداد بیشتر یا حساب‌های کاربری آنلاین یا دو یا چند نام دامنه و آغاز عمدی ارسال پیام‌های پست الکترونیکی از چنین ترکیبی از حساب‌ها یا دامنه‌ها مجازات خواهد شد»** (Wells, 2009, 283). همچنین، اگر شخص با قصد فریب اقدام به نشان دادن خود به‌صورت ثبت‌کننده یا جانشین مشروع او برای ثبت ۵ یا تعداد بیشتری از آدرس‌های پروتکل اینترنتی به دروغ بکند و برای آغاز عمدی ارسال پیام‌های پست الکترونیکی تجاری چندگانه از این آدرس‌ها برای توطئه و انجام آن، باید مجازات شود. این ماده برای کلاه‌برداری‌های مربوط، جرائمی از قبیل حبس و جزای نقدی در نظر گرفته است.

• **ماده ۱۳۴۳: کلاه‌برداری به‌وسیله سیم، رادیو و تلویزیون:** در این ماده، قانون‌گذار آمریکا هر کس را که طرح یا تصنعی ابداع کند یا حتی قصد ابداع را داشته باشد و این قصد یا این ساختن برای فریب یا کسب پول یا دارایی به‌وسیله جعل یا بازنمایی تقلبی

باشد یا موجب ارسال چیزی توسط سیم، رادیو و تلویزیون در تجارت خارجی یا بین ایالتی شود، هر نوشته یا سیگنال که به قصد اجرای چنین طرح یا تصنعی باشد باید جرم شناخته شود و مجازات شود که مجازات مندرج در این ماده شامل حبس کمتر از ۲۰ سال یا جریمه یا هر دو می‌شود و اگر این نقض قانون تأثیری روی یک مؤسسه مالی بگذارد، این شخص باید کمتر از ۱۰۰۰،۰۰۰ دلار جریمه شود و کمتر از ۳۰ سال زندانی شود یا به هر دو مجازات محکوم شود (Doyle, 2011: 2-1). همان‌طور که در بخش‌های قبلی عنوان شد، سیاست جنایی مشارکتی به دو گونه کنشی پیشگیرانه یا فعال) و واکنشی (پاسخگو یا منفعل) قابل تقسیم است. از همین رو، در نوع منفعل این نوع سیاست جنایی بحث پیشگیری ثانویه و ثالث نیز مطرح می‌شود که در ادامه به آنها پرداخته خواهد شد.

۳- تدابیر پیشگیرانه سیاست جنایی ایران و آمریکا در مقابله با جرائم سایبری با الگوبرداری از نظریه کنترل

۳-۱- پیشگیری اجتماعی

در این نوع پیشگیری، سعی بر این است که با افزایش آگاهی افراد و تربیت صحیح آنها، به‌ویژه قشر جوان و نوجوان جامعه و همچنین از بین بردن زمینه‌های اجتماعی وقوع جرم نظیر فقر و بیکاری، انگیزه‌های مجرمانه از مجرمان سلب شود (نجفی ابرندآبادی، ۱۳۸۲: ۱۲۰۸). همچنین، پیشگیری اجتماعی شامل اقدام‌هایی است که به‌طور مستقیم یا غیرمستقیم، هدفشان تأثیرگذاری بر شخصیت افراد است تا از سازمان دادن فعالیت خود حول انگیزه‌های بزهکارانه بپرهیزند (گسن، ۱۳۷۰: ۷۸). با توجه به تعاریف و مفاهیم ارائه شده، می‌توان پیشگیری اجتماعی را به دو دسته تقسیم‌بندی کرد؛ پیشگیری اجتماعی رشد مدار که سعی دارد چنانچه هر شخصی به هر دلیلی از خود نشانه‌هایی از بزهکاری را بروز داد، از طریق مداخله هر چه سریع‌تر در خود وی و محیط اطرافش از مزمن شدن بزهکاری در آینده جلوگیری کند و پیشگیری اجتماعی جامعه‌مدار که در پی خنثی‌سازی عوامل جرم‌زا در محیط اجتماعی است.

۳-۱-۱- پیشگیری اجتماعی رشدمدار اینترنتی

نکته بسیار مهم در برخورد و مبارزه با جرائم اینترنتی به‌ویژه کلاه‌برداری، استانداردهای فنی و اخلاق حرفه‌ای افراد است. بدین منظور که مسلما زمانی می‌توان از افراد انتظار عملکرد درستی داشت که به‌خوبی به وی تفهیم شود که چه تدابیر امنیتی باید به کار گیرد و چه اخلاق شغلی را رعایت کند (باستانی، ۱۳۹۰: ۱۲۸). طیف وسیعی از مجرمان و بزه‌دیدگان جرائم اینترنتی را افراد کم سن و سال، خصوصا نوجوانان تشکیل می‌دهند. از همین رو، از جمله تدابیر بسیار مؤثر در پیشگیری کلاه‌برداری اینترنتی، ارائه آموزش کافی و اطلاع‌رسانی به موقع است. آگاه ساختن افراد و ارائه آموزش‌های لازم در سنین کودکی و نوجوانی می‌تواند نقش شایان توجهی در مقابله با کلاه‌برداری اینترنتی داشته باشد.

۳-۱-۲- پیشگیری اجتماعی جامعه‌مدار سایبری

هدف از این تدابیر، جلوگیری از شکل‌گیری یا بروز انگیزه مجرمانه در عموم جامعه به‌وسیله دو اقدام اصلی است: ایجاد علاقه و آسان‌سازی بروز افکار مشروع و مفید و بر حذر داشتن از ناهنجاری‌های اینترنتی. یکی از مهم‌ترین راه‌های پیشگیری از کلاه‌برداری اینترنتی به‌وسیله پیشگیری اجتماعی جامعه‌مدار سایبری، از طریق آموزش‌های عمومی و رسانه‌های جمعی است. باید توجه داشت که اهمیت خاص تحقیق در زمینه رسانه و پیشگیری از وقوع جرم از آن روست که این وسیله تمامی زندگی انسان را در برمی‌گیرد. کارکرد رسانه‌های جمعی در مورد پیشگیری از کلاه‌برداری اینترنتی می‌تواند از طریق آگاه کردن مردم از پیامدهای ناگوار این جرم (چه بزهکار باشد، چه بزه‌دیده) و نیز دادن الگوهای مناسب رفتاری جهت جلوگیری از ارتکاب و تکرار آن باشد که از این طریق می‌توانند نقش مهمی در پیشگیری از جرم داشته باشند (دیندار و صدرنیا، ۱۳۸۸: ۴۰-۴۱). همچنین، اثربخشی هر چه بیشتر انواع راه‌های پیشگیری ذکرشده نسبت به کلاه‌برداری، نیازمند یک سیاست جنایی مشارکتی فعال است. از لحاظ مفهومی، سیاست جنایی مشارکتی، بررسی و مطالعه جایگاهی است که در سیاست جنایی یک کشور به جامعه مدنی و از طریق اعطای نقش به بزهکار، بزه‌دیده و به‌ویژه کل جامعه و مردم داده شده است (لازرژ، ۱۳۹۰: ۶۱). کارکرد این نوع از سیاست جنایی

نسبت به کلاه‌برداری اینترنتی، اقدامات در مرحله کشف جرم، تعقیب دادرسی و اجرای حکم را در برمی‌گیرد که با همکاری وسیع جامعه مدنی، نهادهای مردمی و نیروهای دولتی مانند پلیس، سازمان زندان‌ها و غیره با دستگاه قضایی انجام می‌شود (باصری، ۱۳۸۷: ۳۷).

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

۳-۲- پیشگیری وضعی

پیشگیری وضعی عبارت است از اقدامات پیشگیرانه معطوف به اوضاع و احوالی که جرائم ممکن است در آن وضعیت به وقوع بپیوندد، به‌طوری‌که هدف از این اقدامات، اتخاذ ترتیبی است که بهای ارتکاب عمل مجرمانه را برای مرتکب، بیش از سود حاصل از آن قرار دهد؛ چراکه از نظر طرفداران پیشگیری وضعی، انسان موجودی حسابگر است و سود و زیاد عملش را به‌طور فطری می‌سنجد. همچنین، این نوع پیشگیری سعی دارد تا با اتکا به آماج جرم یا بزه‌دیده به تبیین پیشگیری از جرم بپردازد. چهارچوب نظری این بحث به‌وسیله نظریه‌های مختلف «فرصت» بیان شده است. چنین اقداماتی در مورد جرم کلاه‌برداری اینترنتی شامل روش‌هایی همچون مصونیت بخشی به آماج، نظارت بر مراکز ارائه‌دهنده اینترنت، فیلترینگ و غیره می‌شود. این نوع پیشگیری خود نیز دارای نقاط ضعف و قوت است، اما مجال توضیح این موارد در این تحقیق نمی‌گنجد (نجیبیان، ۱۳۸۸: ۷۲-۶۹ و صفاری، ۱۳۸۱: ۱۹۴-۱۹۸). مخاطبان اصلی پیشگیری وضعی از جرم کلاه‌برداری اینترنتی، کسانی هستند که از تخصص و مهارت بالایی برخوردار نیستند و بیشتر سعی می‌کنند با امکاناتی که فضای اینترنت در اختیار آنها قرار می‌دهد مرتکب جرم شوند؛ نه اینکه خود دست به ابتکار عمل بزنند که در این صورت، همان‌طور که در ادامه توضیح داده خواهد شد، کاری از پیشگیری وضعی جهت مقابله با جرم کلاه‌برداری و سرقت اینترنتی ساخته نخواهد بود. البته این نکته را نباید از یاد برد که علیرغم تأثیرات مثبتی که پیشگیری وضعی در برابر کلاه‌برداری اینترنتی دارد، بعضا به‌دلیل ماهیت این جرم دارای نقاط ضعفی نیز است؛ از جمله این محدودیت‌ها، هزینه‌بر بودن و زمان‌گیر بودن این اقدامات، تفاوت در میزان دانش طرفین نسبت به اینترنت و تفاوت در به‌کارگیری روش‌ها چه در جهت فیلترینگ و چه در جهت اقداماتی ضد آن. در نهایت، از جمله اقداماتی که مبتنی بر این نوع پیشگیری است می‌توان به این موارد اشاره کرد؛ فیلترینگ، استفاده از پراکسی‌ها، استفاده از رمز ورود، کنترل موجودی حساب و نظارت بر فضای مجازی.

ج) اقدامات مبتنی بر پیشگیری وضعی در آمریکا: به‌دلیل ماهیت جرائم اینترنتی خصوصا کلاه‌برداری و سرقت اینترنتی، برنامه‌های پیشگیرانه در اکثر کشورهای دنیا با اتکا بر پیشگیری وضعی است. در کشور آمریکا علاوه‌بر دولت و ایالت‌ها، عموما شرکت‌های خصوصی مرتبط، پلیس فدرال، کمیسیون امنیت و اقتصاد و سازمان جاسوسی در این کار شرکت دارند. راهبردها و برنامه‌های کشور آمریکا در پیشگیری از جرم همان‌طور که گفته شد کلی است و البته، سازمان‌ها و نهادهای دولتی، برنامه‌هایی در این راستا طراحی کرده‌اند. این برنامه‌ها شامل تغییر نوع محافظت از دستگاه‌ها با استخدام افراد برای به وجود آوردن یک سیستم دفاعی جدید، همکاری با دیگر نهادهای سازمان‌ها و شرکت‌های خصوصی برای امنیت در فضای اینترنت، تمرکز بر روابط اینترنتی بین ایالات‌متحده آمریکا و دیگر کشورها، تلاش برای ارتقای امنیت فضای اینترنتی آمریکا و نوآوری در روش‌ها می‌شد. هرچند که این برنامه برای وزارت دفاع بود، اما مرکز دفاع جرائم سایبر که مسئول این تحقیقات بود به نوعی این اطلاعات و روش‌ها را بهبود بخشید و از این طریق مورد استفاده عمومی قرار داد (وزارت دفاع آمریکا، ۲۰۱۱: ۳).

در ماه می سال ۲۰۱۱، دفتر ریاست جمهوری آمریکا، راهبردی تحت عنوان «راهبرد جهانی برای فضای سایبر؛ امنیت، شکوفایی و آزادی در فضای مجازی» را به‌طور مکتوب درآورد و از این طریق امنیت و پیشگیری از جرائم در فضای مجازی در آمریکا را از طریق همکاری‌های بین‌المللی فراهم آورد. این راهبرد، پنج قاعده کلی داشت که شامل جلوگیری از جرم (بر همین اساس، همه دولت‌ها از جمله ایالات‌متحده آمریکا باید مجرمان اینترنتی را شناسایی و تعقیب کنند تا مطمئن شوند از جرم جلوگیری می‌شود و همچنین با مرکز تحقیقات مجرمان بین‌المللی همکاری داشته باشند)، ایجاد اولویت‌هایی که مستقیما در ارتباط با پیشگیری از جرائم سایبر، تحقیقات و دادرسی جرائم سایبر است، احترام به دارایی افراد، ارزش دادن به استقلال و خلوت اطلاعات مردم و تمرکز کردن بر آموزش مردم برای دفاع از خود در فضای اینترنت (کاخ سفید ایالات-متحده آمریکا، ۲۰۱۱: ۴۵). در رابطه با بحث پیشگیری و اقدامات انجام شده، نگاهی به قوانین مربوط نشان می‌دهد در کشور ایران، قانونی تحت عنوان قانون پیشگیری وجود دارد که متأسفانه، در آن راهکار و پیشنهادهایی در جهت پیشگیری از جرائم داده نشده و فقط صرفا به معرفی اعضا، نحوهٔ تشکیل و وظایف کارگروه‌ها اشاره شده است. از همین رو، در مورد هیچ نوع پیشگیری صحبت نشده است. درحالی‌که در قانون ملی پیشگیری از جرم آمریکا، انواع راهکارهای مبتنی بر پیشگیری وضعی، مرحله‌ای و اجتماعی لحاظ شده و قانون‌گذار، مسئولان مربوطه را به انجام تمام دستورالعمل‌های اجرایی و حمایتی، قبل و بعد از وقوع جرم موظف دانسته است.

نتیجه‌گیری

بررسی‌های انجام شده نشان می‌دهد که اولین عکس‌العمل قانون‌گذار ایران در مقابل جرائم رایانه‌ای در سال ۱۳۸۲ از طریق تصویب قانون مجازات جرائم نیروهای مسلح (مصوب ۱۳۸۲/۱۰/۰۹) در مجلس شورای اسلامی به عمل آمد. به موجب ماده ۱۳۱ این قانون، سرقت یا تخریب حامل‌های داده و سوءاستفاده مالی از طریق رایانه (کلاه‌برداری و اختلاس)، جعل اطلاعات و داده‌های رایانه‌ای و تسلیم و افشای غیرمجاز اطلاعات و داده‌ها به افرادی که صلاحیت سیاست جنایی ایران و آمریکا در قبال جرائم کلاه‌برداری و سرقت سایبری دسترسی به آن را ندارند، توسط نظامیان جرم تلقی و مرتکب حسب مورد به مجازات جرم ارتکابی محکوم می‌شود. واکنش بعدی قانونی مرتبط با جرائم رایانه‌ای از طریق تصویب قانون تجارت الکترونیکی (مصوب ۱۳۸۲/۱۰/۱۷) در مجلس شورای اسلامی به عمل آمده است. به موجب مواد ۶۶، ۶۷، ۶۸، ۶۹، ۷۴، ۷۵، ۷۶ و ۷۷ این قانون، کلاه‌برداری، جعل، دستیابی و افشای غیرمجاز اسرار تجاری، نقض حقوق مربوط به مالکیت معنوی (کپی‌رایت) و غیره که از طریق رایانه و در بستر تجارت الکترونیکی انجام شود، جرم تلقی و برای آن مجازات تعیین شده است. هر یک از قوانین مربوطه، در بستر خاص خود قابلیت اعمال دارند؛ مثلا قانون مطبوعات صرفا نسبت به جرائم رایانه‌ای ارتکابی در قالب نشریات الکترونیکی و قانون مجازات نیروهای مسلح صرفا در مورد بعضی از جرائم رایانه‌ای نظامیان و قانون تجارت الکترونیکی فقط در مورد برخی از جرائم رایانه‌ای ارتکابی در بستر تجارت الکترونیکی قابل اجرا هستند. طبق یافته‌ها، ماده ۱۲ و ۱۳ قانون جرائم رایانه‌ای ایران، ماده جامع و مانعی برای مقابله با کلاه‌برداری و سرقت سایبری نیست و نیاز است که قانون‌گذار ایران نسبت به رفع این مشکل اقدام کند که این اقدام می‌تواند با بهره‌گیری از سوابق دیگر کشورها در قانون‌گذاری از جمله آمریکا باشد تا به این شکل بتوان قانونی کامل و متناسب با شرایط کشور داشت.

یافته‌ها نشان داد در سیاست جنایی قضایی که در تصمیم‌ها و رویه‌های قضایی دادسراها و دادگاه‌ها منعکس می‌شود، قوه قضائیه با رویکرد پیشگیرانه در خصوص جرائم سایبری با کمک نهادهایی مانند مرکز ماهر (مرکز مدیریت امداد و هماهنگی عملیات رخداد) و مرکز آپا (مرکز آگاهی رسانه، پشتیبانی و امداد رایانه‌ای) و پلیس فتا فعالیت می‌نماید. به‌دلیل ماهیت جرائم اینترنتی خصوصا کلاه‌برداری و سرقت اینترنتی، برنامه‌های پیشگیرانه در امریکا با اتکا بر پیشگیری وضعی است. در کشور آمریکا علاوه بر دولت و ایالت‌ها، عموما شرکت‌های خصوصی مرتبط، پلیس فدرال، کمیسیون امنیت و اقتصاد و سازمان جاسوسی در این کار شرکت دارند. با توجه به اهداف و یافته‌های تحقیق، پیشنهادهایی به‌عنوان راهکارهای پیشگیری اجتماعی و وضعی از کلاه‌برداری و سرقت سایبری ارائه می‌شود.

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

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

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

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

• **تدبیر پالایه یا فیلترینگ:** فیلترینگ پورت‌ها از جمله مهم‌ترین عملیاتی است که توسط فایروال‌ها انجام می‌شود و سبب می‌شود اطلاعات و سراچه‌هایی که ممنوعه هستند از دسترس خارج گردند.

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

ملاحظات اخلاقی: موارد مربوط به اخلاق در پژوهش و نیز امانت‌داری در استناد به متون و ارجاعات مقاله تماما رعایت گردید.

تعارض منافع: تدوین این مقاله، فاقد هرگونه تعارض منافعی بوده است.

سهم نویسندگان: نگارش مقاله به‌صورت مشترک توسط نویسندگان انجام گرفته است.

تأمین اعتبار پژوهش: این پژوهش بدون تأمین اعتبار مالی سامان‌یافته است.

منابع و مآخذ

الف. منابع فارسی

– آقابابایی، حسین و احمدی‌ناطور، زهرا (۱۳۹۵). «مطالعه تطبیقی جرائم علیه حریم خصوصی در فضای سایبری ایران و آلمان». *مطالعات بین‌رشته‌ای در رسانه و فرهنگ*، ۶(۱): ۱- ۲۴.

– احمدی، حبیب (۱۳۸۷). *جامعه‌شناسی انحرافات*. تهران: انتشارات سمت.

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

– انصاری، جلال و میلانی، علیرضا (۱۳۹۵). «نقد سیاست جنایی ایران در قبال کلاه‌برداری اینترنتی». *حقوق جزا و سیاست جنایی (حقوق جزا و جرم‌شناسی سابق)*، ۱(۱): ۱۶۱- ۱۴۵.

– انصاری، جلال؛ عطازاده، سعید و قیومزاده، محمود (۱۳۹۸). «سیاست جنایی ایران و آمریکا در قبال جرائم کلاه‌برداری و سرقت سایبری (مقاله مروری)». *پژوهش‌های اطلاعاتی و جنایی*، ۱۴(۳ (مسلسل ۵۵)): ۱۳۱-۱۵۴.

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

– براتی، علی؛ اسلامی، محمد؛ رهبری، حسام‌الدین و یزدان‌پرست، پویا (۱۳۹۶). *بررسی تطبیقی مصادیق جرائم حوزه فضای مجازی در ایران، آمریکا و فرانسه*. همایش ملی پیشگیری از جرم در قلمرو مطالعات حقوق کیفری، علوم اجتماعی و انتظامی،کرج.

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

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

– پورقهرمان، بابک (۱۳۹۶). «مطالعه‌ی تطبیقی سازوکارهای حمایت از بزه‌دیدگان جرائم رایانه‌ای در حقوق کیفری ایران و اسناد بین‌المللی با تأکید بر کنوانسیون بوداپست». *پژوهشنامه حقوق کیفری*، ۸(۱): ۱–۳۶.

– خراسانی، سمیرا؛ مسعود، غلامحسین و شکرچی‌زاده، محسن (۱۴۰۱). «نگاه بومی به نظریه‌ی کنترل اجتماعی جرم با توجه به مبانی اسلامی– ایرانی». *پژوهش‌های حقوق جزا و جرم‌شناسی*، ۱۰(۲۰): ۳۱۷–۳۴۵.

– خرم‌آبادی، عبدالصمد (۱۳۸۶). «کلاه‌برداری رایانه‌ای از دیدگاه بین‌المللی و وضعیت ایران». *فصلنامه حقوق دانشگاه تهران*. ۲(۷۳): ۸۳–۱۱۲.

– دزیانی، محمدحسن (۱۳۸۵). «مقدمه‌ای بر سیاست جنایی ایران در باب جرائم سایبری». *قضاوت*، (۳۸): ۴۲–۴۸.

– دشتی، بیتا و افشاری، مریم (۱۳۹۸). «مطالعه تطبیقی جرائم سایبری در ایران و حقوق بین‌الملل». *پژوهشنامه حقوق تطبیقی*، ۳(۱): ۱۱۰–۸۳.

– رایجیان، مهرداد (۱۳۹۳). «پیشگیری از جرائم رایانه‌ای از رهیافت‌های نظری تا رهیافت جهانی در پرتو رهنمود پیش‌گیری از جرم سازمان ملل متحد». *مطالعات راهبردی سیاست‌گذاری عمومی*، ۵(۱۶): ۱۸۹–۲۱۶.

– رضوی‌فرد، بهزاد و موسوی، سید نعمت‌اله (۱۳۹۵). «مسئولیت کیفری در فضای سایبر در حقوق ایران». *فصلنامه پژوهش حقوق کیفری*، ۵(۱۶): ۲۹–۴۵.

– سالارزهی، حبیب‌اله؛ جمشیدی، محمدجواد و جمشیدی، محمدجعفر (۱۳۹۰). جرم‌شناسی *رایانه‌ای در بستر تجارت الکترونیک و ارائه مدل پیشنهادی مقابله با جرائم رایانه‌ای*. همایش منطقه‌ای چالش‌های جرائم رایانه‌ای در عصر امروز.

– سالاری شهربابکی، میرزا مهدی (۱۳۹۳). *کلاه‌برداری و ارکان متشکله آن*. تهران: میزان.

– صفاری، علی (۱۳۸۱). «مبانی نظری پیشگیری از وقوع جرم». *تحقیقات حقوقی*، دانشگاه شهید بهشتی، شماره ۳۴.

– طارمی، محمدحسین (۱۳۸۷). «طبقه‌بندی و آسیب‌شناسی جرائم رایانه‌ای». *مجله پگاه حوزه*، (۲۳۶): ۱۴–۲۴.

– علیوردی‌نیا، اکبر؛ ملک‌دار، اعظم و حسنی، محمدرضا (۱۳۹۲). «تخلفات رایانه‌ای در میان دانشجویان دانشگاه مازندران: آزمون تجربی نظریه یادگیری اجتماعی ایکرز». *مجله جامعه‌شناسی ایران*، ۱۵(۲): ۲۴–۵۶.

– کاخ سفید ایالات‌متحده آمریکا (۲۰۱۱). *راهبرد بین‌المللی برای فضای سایبری: شکوفایی، امنیت و گشودگی در جهانی شبکه‌ای*. واشنگتن دی.سی: کاخ سفید.

– گسن، ریموند (۱۳۷۰). *مقدمه‌ای بر جرم‌شناسی*. ترجمه مهدی کی‌نیا، تهران» نشر مترجم.

– لازرژ، کریستین (۱۳۹۰). *درآمدی بر سیاست جنایی*. مترجم: علی‌حسین نجفی ابرندآبادی، تهران: نشر میزان

– میرمحمدصادقی، حسین (۱۳۸۶). *حقوق کیفری اختصاصی (۲): جرائم علیه اموال و مالکیت*. تهران: نشر میزان.

– نجفی ابرندآبادی، علی‌حسین (۱۳۷۹). *تقریرات درس جرم‌شناسی پیشگیری، دوره دکتری حقوق جزا و جرم‌شناسی*، دانشگاه تربیت مدرس.

– نجفی ابرندآبادی، علی‌حسین (۱۳۸۲). تقریرات درس جرم‌شناسی (پیشگیری)، دوره کارشناسی ارشد حقوق کیفری و جرم‌شناسی، تنظیمی مهدی سیدزاده، نیمسال دوم تحصیلی ۱۳۸۲-۱۳۸۱.

– وزارت دفاع ایالات‌متحده آمریکا (۲۰۱۱). *گزارش سیاست سایبری وزارت دفاع: گزارشی به کنگره بر اساس قانون مجوز دفاع ملی برای سال مالی ۲۰۱۱، بخش ۹۳۴*. واشنگتن دی. سی: وزارت دفاع ایالات‌متحده آمریکا.

ب. منابع انگلیسی

- Doyle, Ch (2011). *Mail and Wire Fraud: An Abridged Overviwe of Federal Criminal Law*. Washington, D. C.: Congressional Research Service.

- Gercke, M (2012). *Understanding Cybercrime: Phenomena, Challenges and Legal Response*. Geneva: International Telecommunication Development Bureau.

- Gordon, G. R & Curtis, G. E (2000). *The Growing Global threat of Economic and Cyber Crime*. The National Fraud Center, Inc., In Conjunction Institute, Utica College.

- Wells, J. T (Eds.) (2009). *Computer Fraud Casebook: The Bytes That Bite*. Hoboken, NJ: John Wiley & Sons.