فصلنامه علمی
مطالعات حقوقی فضای مجازی
سال دوم | شماره سوم | پاییز ۱۴۰۲
وبگاه مجله: https://cyberlaw.maragheh.iau.ir

A Feasibility Study of Crime Prevention in the Dark Web

Zahra Rahpeik*
M.A. Graduate, Department of Criminal Law and Criminology, Farabi Campus, Tehran University, Tehran, Iran.
Hasan Alipuor
Assistant Professor, Department of Criminal Law and Criminology, Farabi Campus, Tehran University, Tehran, Iran.
Zrah002@gmail.com

DOI: 10.30495/CYBERLAW.2023.707603

Keywords:
Cyber Threat,
Dark Web,
Feasibility of Crime Prevention,
Situational Prevention,
Social Prevention.

Abstract

The dark web is an invisible part of the cyber space like an iceberg floating in the ocean, only the tip of which is visible and main and threatening part of the same invisible to the authorities. The first challenge of the dark web is the impossibility of identifying it in order to apply preventive measures as such that the issue of prevention, cyber threat, is behind the veil of ambiguity. The uncontrollability and lack of environmental boundaries is another challenge for crime prevention in the dark web. Finally, the arrangement of suitable solutions for this environment is proposed as the third aspect of crime prevention challenges. Using library and internet resources, this article tries to deal with the challenges of crime prevention on the dark web from the perspective of the prevention platform, the issue of prevention, and the preventive solutions. The results of the research reveals that the possibility of applying preventive measures in the form of intervening in situations that cause crime in the deep web is ruled out and that the use of defensive strategies to minimize cyber threats and focus on social preventive and early preventive measures instead of situational prevention is what that needs to be considered.

امکان‌سنجی پیشگیری از جرم در تارنمای تاریک

زهرا ره‌پیک*

دانش آموخته کارشناسی ارشد حقوق جزا و جرم‌شناسی، پردیس فارابی دانشگاه تهران، قم، ایران.

حسن عالی‌پور

استادیار و عضو هیأت علمی گروه حقوق جزا و جرم‌شناسی دانشگاه تهران پردیس فارابی، استاد مدعو، واحد تهران شمال، دانشگاه آزاد اسلامی، تهران، ایران.

zrah002@gmail.com

تاریخ دریافت:۳۱فروردین ۱۴۰۲ تاریخ پذیرش: ۱۵ مرداد ۱۴۰۲

چکیده

تارنمای تاریک یا تارنمای عمیق بخشی ناپیدا از فضای سایبر و در مقام تمثیل کوه یخی شناور در اقیانوس است که تنها نوک آن هویدا است ولی بخش اصلی و تهدیدکننده آن در برابر دیدگان متصدیان امر قرار ندارد. نخستین چالش تارنمای تاریک، عدم امکان شناسایی آن برای اعمال تدابیر پیشگیرانه است؛ به‌گونه‌ای که موضوع پیشگیری یعنی تهدید سایبری در پس پرده ابهام قرار دارد. سپس کنترل ناپذیری و فقدان مرز محیطی چالش دیگری برای پیشگیری از جرم است و نهایتاً چینش راهکارهای متناسب برای این محیط به‌عنوان ضلع سوم چالش‌های پیشگیری از جرم مطرح می‌شود. مقاله حاضر با استفاده از منابع کتابخانه‌ای و اینترنتی با روش توصیف و تحلیل می‌کوشد تا به چالش‌های پیشگیری از جرم در تارنمای تاریک از منظر وضعیت بستر پیشگیری، موضوع پیشگیری و راهکارهای پیشگیرانه بپردازد. نتیجه تحقیق بیانگر این است که امکان اعمال تدابیر پیشگیرانه به‌منزله مداخله در موقعیت‌ها و وضعیت‌های ایجادکننده جرم در تارنمای عمیق منتفی است و آنچه باید در این فضا مدنظر قرار بگیرد استفاده از راهکارهای تدافعی برای کاهش حداقلی تهدیدات سایبری و تمرکز بر تدابیر پیشگیرانه اجتماعی و زودرس به‌جای هزینه کردن درباره تدابیر پیشگیرانه وضعی است.

.

کلید واژگان: امکان پیشگیری از جرم، پیشگیری اجتماعی، پیشگیری وضعی، تارنمای تاریک، تهدید سایبری.

فصلنامه علمی
مطالعات حقوقی فضای مجازی
سال دوم | شماره سوم | پاییز ۱۴۰۲

مقدمه

بزهکاری سایبری پیش از آنکه با تدابیر مؤثر و کارآمد پیشگیری شود، در محیط‌های متفاوت باقابلیت‌های نو رخ نموده است که بیش از قبل، تدابیر پیشگیرانه را به چالش کشیده است. یکی از این قابلیت‌ها، وجود صفحاتی در بخشی از فضای اینترنت موسوم به تارنمای تاریک است که برای عموم مردم در دسترس نیست. به‌عبارت‌دیگر، این‌گونه صفحات رمزنگاری‌شده‌اند و توسط موتورهای جستجوگر، مانند گوگل، قابل‌شناسایی نیستند. مسأله‌ای که در این مقاله درصدد پرداختن به آن هستیم این است که آیا امکان در نظر گرفتن تدابیر پیشگیرانه در تارنمای تاریک وجود دارد یا خیر؟ باید توجه نمود که از طرفی، اصل پیشگیری دارای یک سری ویژگی‌ها و ملزومات هست و از طرف دیگر، فضای تارنمای تاریک واجد مشخصات ویژه‌ای است. مسأله اصلی این نوشتار در پرداختن این دوگانگی و تعارض است. از یک‌سو تدابیر پیشگیری از وقوع جرم اعم از وضعی و اجتماعی متکی به پیش‌بینی جرم، احتمال وقوع و ارزیابی موقعیت‌های جرم و سپس ارائه راهکارهای مرتبط است ولی در محیط تارنمای تاریک[1]، فضایی کنترل ناپذیر و بدون امکان ردیابی شکل‌گرفته که نه می‌توان به‌درستی ویژگی‌های بروز جرم را تخمین زد و نه می‌توان از راهبردهای پیشگیرانه موجود بهره گرفت. از سوی دیگر، تارنمای تاریک نهایتاً متکی به اعمال انسانی از طریق داده‌ها و تارنماها است و چنانچه تدابیر پیشگیرانه موجود دست‌کم از منظر اجتماعی یا تدابیری که اقتضای توجه به خصوصیات انسانی دارند، در قبال جرائم قابل ارتکاب در این فضا مدنظر قرار بگیرند، می‌توان همچنان سخن از تدابیر پیشگیری از بزهکاری در دارک نت گفت؛ بنابراین بررسی نوع و ماهیت این تدابیر پیشگیرانه اولین مسأله است که باید به آن پرداخته شود؛ این‌که آیا تدابیر پیشگیرانه از نوع نظارت افراد در تارنمای تاریک قابل تحقق است یا خیر؟ آیا این تدابیر باید چهره فنی داشته باشند یا از طرقی غیر از طرق فنی نیز قابل‌پیگیری است؟ به‌عبارت‌دیگر، انواع پیشگیری از جرم در تارنمای تاریک و مصادیق آن کدام است؟ در این نوشتار با معرفی تارنمای تاریک به راهبردها و چالش‌های پیشگیری از بزهکاری سایبری در این محیط پرداخته می‌شود:

۱. بستری دور از دسترس تدابیر پیشگیرانه: تارنمای تاریک

اینترنت شبکه یکپارچه‌ای نیست؛ به این معنا که از سطوح و لایه‌های مختلفی تشکیل‌شده است و هرکدام دارای ویژگی‌هایی هستند. یکی از اقسام تارنما، «تارنمای سطحی[2]» است یا تارنمای سطحی همان اینترنت نمایه شده، عمومی و قابل‌دسترس برای همه است که به‌راحتی قابل‌ردیابی می‌باشد (Braga & Luna, 2018: 273). موتورهای جستجوگر تنها بخش اندکی از کل محتوای بارگذاری شده در اینترنت را برای کاربران تارنمای سطحی نمایش می‌دهند و دست یافتن به برخی از اطلاعات، نیازمند ورود به قسم دیگری از اینترنت، به نام «تارنمای تاریک» می‌باشد. «تارنمای عمیق[3]» شامل محتوایی است که توسط موتورهای جستجوی سنتی مانند گوگل فهرست نشده است (Finklea, 2017: 2). یا به دلیل اینکه متعلق به شبکه‌های خصوصی (مانند ایمیل شخصی) هستند یا به این دلیل که فقط برای کاربران نوع خاصی از محتوا قابل‌دسترسی است (Braga & Luna, 2018: 275).

«تارنمای تاریک[4]» زیرشاخه‌ای از تارنمای عمیق است و تمرکز ما در این مقاله بر این بخش می‌باشد. دارک وب محیطی است که بر اساس پروتکل‌هایی با امنیت بالا و ناشناس ایجادشده است و داده‌ها در آن با پیچیدگی زیادی رمزگذاری شده‌اند (Braga & Luna, 2018: 275). تارنمای تاریک حاوی اطلاعاتی است که می‌تواند در راه دستیابی به اهداف نامشروع و یا غیرقانونی به کار گرفته شود؛ البته «همان‌طور که مجرمان می‌توانند به ناشناس بودن وب تاریک اعتماد کنند، مجریان قانون، ارتش و نهادهای اطلاعاتی نیز می‌توانند به آن

[1] Dark net
[2] Surface web
[3] Deep web
[4] Dark web

اعتماد کنند. همچنین ناشناس بودن در وب تاریک می‌تواند برای محافظت از مقامات در برابر شناسایی و هک توسط دشمنان استفاده شود» (Finklea, 2017: 1).

بااین‌حال، بدیهی است گمنامی در این فضا این امکان را به مجرم می‌دهد تا با دسترسی به اینترنت در هر زمان و هر مکان بدون ترس از شناسایی و تعقیب قضایی قربانیان بالقوه را موضوع رفتارهای مجرمانه خود قرار دهند (جایشانکار، ۱۳۹۴: ۱۸۸). به‌بیان‌دیگر، ویژگی مخفیانه بودن و محیط رمزنگاری‌شده تارنمای تاریک، بستر مناسبی را برای ارتکاب اعمال مجرمانه (از جذب تروریست گرفته تا تجارت مواد مخدر، پورنوگرافی کودکان، اطلاعات سرقت شده و خدمات پول‌شویی) و یا هر عملی که به‌صورت علنی در محیط خارجی یا محیط آزاد تارنمای سطحی به‌راحتی قابل انجام نیست را فراهم می‌کند. «این دامنه‌های پنهان با ارزهای رمزنگاری‌شده یا بیت کوین، دارک کوین، پیر کوین و لایت کوین معامله می‌کنند تا ناشناس ماندن را به حداکثر برسانند. اکثر وب‌سایت‌های تاریک از نرم‌افزار ناشناس کننده[5] استفاده می‌کنند که هویت کاربر را با پوشش داده‌های دریافتی رمزگذاری می‌کند. درواقع، این امر از شناسایی مبدأ کاربر توسط دیگران جلوگیری می‌کند» (Vogt, 2017: 109). استفاده از نرم‌افزار (TOR) افراد را از شکل رایج نظارت اینترنتی موسوم به «تحلیل ترافیک» مصون می‌دارد. تحلیل ترافیک داده‌هایی از قبیل مبدأ و مقصد ارتباط را در اختیار قرار می‌دهد. بر اساس این اطلاعات تحلیلگران می‌توانند به سلایق و علایق افراد پی برده (Braga & Luna, 2018: 276). و برای آن برنامه‌ریزی نمایند.

نهایتاً، اگر بخواهیم به تصویر ذهنی صحیح‌تری نسبت به اقسام مختلف تارنما برسیم، باید فضای اینترنت را به کوه یخی تشبیه کنیم که تنها بخش اندکی از آن بیرون از سطح آب و قابل‌رؤیت برای ما می‌باشد که این همان بخشی است که از آن به «تارنمای سطحی» تعبیر می‌شود؛ اما بخش بسیار بزرگ‌تری از این کوه یخ، در زیر آب و پنهان از انظار است که در مقام تشبیه، مانند «تارنمای عمیق و تاریک» می‌باشد. گفته می‌شود در وب تاریک، بیش از ۸۰ درصد از محتوایی که اینترنت سطحی می‌تواند ارائه دهد، وجود دارد (Al-Suwaidi, Nobanee & Jabeen, 2018: 394). بنابراین درصد زیادی از اطلاعات موجود در اینترنت در تارنمای عمیق و تاریک قرار دارد و در این فضا حجم قابل‌توجهی از اطلاعات با تعدد موضوعی مختلف (اعم از موضوعات مجرمانه یا غیر مجرمانه) وجود دارد. به همین علت، نمی‌توان تارنمای تاریک را منحصراً به‌عنوان فضای ارتکاب جرم در نظر گرفت و با این استدلال محدودیت‌های قانونی را علیه آن اعمال نمود. حقیقت این است که مسأله تارنمای تاریک و چالش‌های آن موضوعی جدید، نه‌فقط در ایران، بلکه در سطح جهانی می‌باشد. در مقالات متعددی از جای‌جای جهان، پژوهشگران اذعان می‌کنند که رویکرد مشخصی، به‌عنوان قاعده، در مواجهه با تارنمای تاریک وجود ندارد.

دولت‌ها به‌عنوان متولیان تنظیم سیاست‌های عمومی، مهم‌ترین کنشگر حوزه پیشگیری در سطح داخلی به شمار می‌روند و از طرف دیگر در سطوح جهانی، نهادهای بین‌المللی مانند سازمان ملل متحد و زیرمجموعه‌های آن می‌توانند در قالب سازوکارها، دستورالعمل‌ها و معاهدات، کشورهای عضو را در امر پیشگیری ترغیب و در این راه تسهیلگری کنند (جندلی، ۱۳۹۳: ۴۸). دراین‌باره «دفتر مبارزه با مواد مخدر و جرائم سازمان ملل متحد (UNODC[6]) در گزارش سالانه خود اعلام کرد که فقدان یک توافق بین‌المللی در مورد جرائم سایبری و تروریسم (به‌عنوان یکی از مهم‌ترین جرائم ارتکابی در تارنمای تاریک)، تلاش‌ها برای محاکمه تروریست‌ها را خنثی می‌کند و به این نتیجه رسید که کشورها باید یک توافق جهانی را در نظر بگیرند که آن‌ها را ملزم می‌کند تا در طول تحقیقات جرائم سایبری و تروریسم سایبری با یکدیگر همکاری کنند» (Vilic, 2017: 18). علل مختلفی وجود دارد که قانون‌گذاری درباره این فضا را با دشواری و چالش مواجه می‌کند برای مثال، «یکی از این موانع، محدودیت‌های عملکرد پلیسی در قبال تغییرات فنّاورانه است. در چارچوب یک محیط اینترنتی درحال‌توسعه سریع، پایبندی به شناسایی و پیشگیری از فعالیت‌های غیرقانونی از طریق یک الگوی نظارتی سنتی سایبری و

[5] TOR (The Onion Router)
[6] United Nations Office on Drugs and Crime

فصلنامه علمی
مطالعات حقوقی فضای مجازی
سال دوم | شماره سوم | پاییز ۱۴۰۲

پدرسالارانه این پتانسیل را دارد که ایجاد مقررات مؤثر در برخی از محیط‌های جدید را در بهترین حالت بسیار دشوار و در بدترین حالت غیرممکن کند» (O'Brien, 2014: 254). چالش‌های دیگری نیز در این راه وجود دارد که در ادامه به‌تفصیل به آن‌ها می‌پردازیم.

۲. چالش‌های پیشگیری از جرم در تارنمای تاریک

با عنایت به مطالب گذشته، اصل لزوم پیشگیری از وقوع جرم در فضای مجازی و خصوصاً تارنمای تاریک به‌حکم قاعده لا ضرر و بنای عقلا بیش‌ازپیش روشن می‌گردد؛ اما مسأله اصلی در این نقطه وجود چالش‌هایی در مسیر پیشگیری از جرم در تارنمای تاریک است که فرایند پیشگیری را با دشواری‌هایی مواجه کرده است. در ادامه به برخی از مهم‌ترین این چالش‌ها اشاره می‌کنیم:

۲، ۱. چالش فقدان اطلاعات و عدم آگاهی

اولین مشکلی که در آغاز فرایند پیشگیری در تارنمای تاریک با آن مواجه می‌شویم، مسأله در دسترس نبودن و فقدان منابع اطلاعاتی و آماری رسمی از جامعه هدف مدنظر است. منون جندلی معتقد است جهت پیشبرد یک طرح پیشگیرانه بایستی ارزیابی همه جانبه‌ای از اوضاع‌واحوال و شرایط حاکم بر موضوع پیشگیری صورت پذیرد که یکی از مهم‌ترین جنبه‌های آن کسب اطلاعات کمی و کیفی راجع به بزهکاری، مرتکبان و بزه دیدگان آن است (جندلی، ۱۳۹۳: ۱۰۴-۱۰۵). تارنمای تاریک به‌موجب ویژگی‌های خاص خود از قبیل رمزآلود بودن داده‌ها و ناشناس بودن کاربران آن، متولیان پیشگیری را با محدودیت‌های جدی در مسیر پیش‌بینی تدابیر مربوط مواجه می‌کند. مرورگرهای وب معمولی آدرس IP منحصربه‌فرد خود را نشان می‌دهند و آن‌ها را برای مجریان قانون قابل‌ردیابی می‌کنند؛ اما یک مرورگر تارنمای تاریک یک آدرس IP نادرست را برای پنهان کردن هویت کاربر صادر می‌کند. همان‌طور که پیشتر بیان شد، لازمه پیشبرد اصولی و اجرای موفقیت‌آمیز یک طرح پیشگیرانه، مواجهه آگاهانه و مبتنی بر آمار دقیق از هر آنچه در امر مجرمانه دخیل و مؤثر می‌باشد است. «ناشناس بودن وب تاریک نه‌تنها فعالیت‌های غیرقانونی را تشویق می‌کند، بلکه بسیاری از سازمان‌های مجری قانون را تا حد زیادی از وجود آن بی‌اطلاع نگه می‌دارد، حتی درحالی‌که حوزه قضایی آن‌ها تحت تأثیر جرائم معاملاتی آنلاین قرار دارد.» همین بی‌اطلاعی باعث بروز خطا در هدف‌گذاری و نهایتاً عدم دستیابی به نتیجه موردنظر و یا حتی فاصله گرفتن از چشم‌انداز مطلوب و عقب‌گردی جبران‌ناپذیر می‌گردد؛ بنابراین فقدان منابع آماری و عدم امکان شناسایی جرائم واقع در تارنمای تاریک، نه‌تنها واجد تأثیر سوء پیشینی بر اقدام پیشگیرانه است، بلکه تأثیرات پسینی آن در مرحله ارزیابی طرح نیز به چشم می‌خورد. علاوه بر این، عدم آگاهی مجریان قانون از ساختار، امکانات و چگونگی عملکرد مجرمان در تارنمای تاریک مانع دیگری در راه شناسایی عامل مجرمانه و تدبیر کنش‌های پیشگیرانه در این فضا می‌باشد (Goodison, 2020).

۲،۲. چالش نظارت دولت‌ها

دومین چالشی که در راه پیشگیری از جرائم در تارنمای تاریک با آن روبرو می‌شویم، چالشی در ارتباط با نظارت دولت‌ها بر این فضاست که در دو سطح قابل‌بررسی است: اول، مسأله اصل مشروعیت نظارت دولت‌ها بر فضای شبکه بین‌المللی اینترنت است. با این توضیح که اینترنت بستری جهانی است و به‌صورت رسمی تحت نظارت یا کنترل هیچ دولتی قرار ندارد. به همین دلیل به نظر می‌رسد نظارت دولت بر فضای آزاد اینترنت خالی از اشکال نباشد یا حداقل نیازمند مبانی متقن قانونی و عقلانی باشد. به گفته راسل جی اسمیت در مقاله نقض حقوق بشر در عصر دیجیتال «تکنولوژی اطلاعات نوعی توانمندی را در اختیار دول مستبد گذاشته تا بر اتباع خود نظارت داشته باشند و در صورت لزوم آنان را مجازات کنند» (جایشانکار، ۱۳۹۴: ۲۹۱). درصورتی‌که پاسخ به چالش نظارت یا عدم نظارت دولت منفی باشد، یعنی دولت را واجد حق نظارت بر تارنمای تاریک ندانیم، در مقابل رشد روزافزون اقدامات مجرمانه فردی و شبکه‌ای در وب تاریک باید سکوت پیشه کنیم و شاهد مخدوش شدن نظم عمومی در سطحی بسیار فراتر از دنیای واقعی باشیم؛ درحالی‌که برای اقدامات مجرمانه

دانشگاه آزاد اسلامی واحد مراغه

مشابه در دنیای واقعی بعضاً ضمانت اجراهای سنگینی وضع کرده‌ایم. اما درصورتی‌که دولت را محق در نظارت در تارنمای تاریک و بلکه بالاتر، آن را موظف به این‌گونه رصدها بدانیم، با چالش دیگری تحت عنوان «نقض حریم خصوصی کاربران» مواجه می‌شویم.

پس مسأله دوم، نظارت دولت به‌مثابه مقدمه‌ای بر نقض حریم خصوصی است. در تحلیل جرم‌شناختی برای اتخاذ تدابیر پیشگیرانه مؤثر باید اطلاعاتی مثل جرائم ارتکابی در محل موردنظر، بزهکاران، بزه دیدگان، علل بزهکاری، وضعیت‌های پیش جنایی و... از قبل موردبررسی روشمند قرار بگیرد (خانعلی‌پور واجارگاه، ۱۳۹۰: ۲۷). بنابراین دولت باید امکانات دسترسی به این قبیل اطلاعات و آمارها را داشته باشد و این جز از طریق داشتن تسلط اطلاعاتی بر کاربران محقق نمی‌گردد؛ اما این تسلط و دسترسی می‌تواند در تعارض با برخی حقوق مسلم شهروندان، مانند حق برخورداری از حریم خصوصی قرار گیرد. در قانون اساسی جمهوری اسلامی ایران مانند بسیاری از کشورها، به حق داشتن حریم خصوصی به‌عنوان حقی مسلم اشاره و در دو اصل بیست و سوم و بیست و پنجم متبلور شده است.

در حقوق بین‌الملل نیز در چندین کنوانسیون و اعلامیه جهانی و منطقه‌ای مسأله حریم خصوصی در چارچوب حقوق بشر توسعه‌یافته است. برای مثال، در سال ۱۹۴۸، مجمع عمومی سازمان ملل متحد اعلامیه جهانی حقوق بشر را تصویب کرد و در ماده ۱۲ آن صراحتاً مداخله خودسرانه در حریم خصوصی افراد را ممنوع اعلام داشت. در سال ۱۹۵۰، شورای اروپا کنوانسیون اروپایی برای حمایت از حقوق بشر و آزادی‌های اساسی را معرفی کرد که در پی آن بود تا اهداف اعلامیه جهانی حقوق بشر را با حاکمیت قانون رسمیت بخشد (Vogt, 2017: 107).

حال، شایسته است در اطلاق حریم خصوصی به فضای تارنمای تاریک اندکی تأمل کرد. پرواضح است مواردی مثل مکالمات تلفنی، ایمیل‌ها و پیامک‌ها، مخصوصاً درصورتی‌که به‌وسیله تدابیر امنیتی محافظت‌شده باشند، در حیطه حریم خصوصی فرد و مشمول حمایت قانون قرار می‌گیرند. چه در موارد نام‌برده، تلقی هر یک از افراد نیز یک ارتباط حفاظت‌شده و محرمانه بین خود و مخاطب خود می‌باشد؛ اما آیا تارنمای تاریک هم به همین نحو، بستری حفاظت‌شده و امن برای کاربران است؟ آیا تصور ذهنی کاربران، اقدامات خود در تارنمای تاریک را به همان میزان جزئی از حریم خصوصی خود می‌داند که صفحه پیامک تلفن همراه خود را می‌داند؟ در نگاه اول، پاسخ مثبت به نظر می‌رسد. طراحی (TOR) به نحوی است که یک فعالیت را چندین بار رمزگذاری می‌کند و واضح است که با توجه به چنین شرایطی انتظار ذهنی کاربران این است که فعالیت آن‌ها ناشناس باقی می‌ماند.

در مرحله بعد، با نگاهی عمیق‌تر باید تعیین کنیم که آیا این انتظار ذهنی از جهت عینی هم انتظار معقولی است یا خیر. به نظر می‌رسد برای بشر قرن بیست و یکم، این انتظار تا حد زیادی غیرمنطقی است که فعالیت آنلاین او در سایه حریم خصوصی و دور از دسترس دیگران (هر شخصی غیر از مخاطب مستقیم خود) قرارگرفته باشد؛ صرف‌نظر از این‌که فعالیت او در تارنمای سطحی باشد یا تارنمای عمیق و تاریک (Vogt, 2017: 107). با استدلال اخیر، کاربران اینترنت عملاً از در اختیار داشتن یک فضای خصوصی در فضای اینترنت و حتی دستگاهی که با آن به اینترنت متصل می‌شوند، محروم می‌گردند و به‌عبارت‌دیگر، تخصیص گسترده‌ای به عموم حق حریم خصوصی آن‌ها وارد می‌شود.

نهایتاً با لحاظ تمام جوانب چالش نظارتی به نظر می‌رسد پیروی از رویکرد میانه‌ای که هم حریم خصوصی افراد را تا حد مورد قبولی رعایت نماید و هم از امنیت اجتماعی حراست کند، ما را به نتایج بهتری برساند که البته رسیدن به این رویکرد نیازمند بهره‌گیری از دانش فنی و نظرات صاحب‌نظران حوزه فناوری اطلاعات (IT)، اینترنت، وب، امنیت و شبکه و نهایتاً سیاست‌گذاری در عرصه‌های جهانی و داخلی می‌باشد. به‌عبارت‌دیگر، «حفاظت از حقوق بشر با تعامل میان خلاقیت تکنولوژیکی و اصلاح سیاستی محقق می‌شود» (جایشانکار، ۱۳۹۴: ۳۰۴).

فصلنامه علمی
مطالعات حقوقی فضای مجازی
سال دوم | شماره سوم | پاییز ۱۴۰۲

۳،۲. چالش فقدان مقررات حاکم

چالش سوم، چالش فقدان مقررات ناظر بر تارنمای تاریک است. تاکنون، نه‌تنها در ایران، بلکه در سایر کشورهای جهان نیز قوانین و مقررات مدونی با این موضوع تنظیم‌نشده است و آنچه در عمل بعضاً از طرف دولت‌ها انجام می‌پذیرد، اعمالی خودسرانه (بدون پشتوانه قانونی مشخص) یا با استناد به قواعد کلی حقوقی است. برای برون‌رفت از این چالش ابتدا بایستی اولین مانع، یعنی ناشناخته بودن فضای تارنمای تاریک، اعمال ارتکابی در آن و کاربران آن را موردتحقیق قرار داد. در گزارشی که توسط مؤسسه ملی دادگستری[7] منتشر شد، یکی از مهم‌ترین پیش‌نیازهای پیشگیری از جرم در تارنمای تاریک را آموزش و یادگیری می‌داند و در ذیل آن به دو حوزه آموزشی اولویت‌دار اشاره می‌کند: «۱- برگزاری دوره‌هایی برای بازپرسان و ضابطان، برای ایجاد آشنایی اولیه با شواهد دیجیتالی که درصحنه پیدا می‌شود. ۲- آموزش هدفمند برای واحدهای تخصصی، در مورد حفظ شواهد و همچنین آموزش پیشرفته در مورد روش‌هایی که توسط مجرمان در تارنمای تاریک استفاده می‌شود» (Goodison, 2020).

ازآنجایی‌که رشد فعالیت‌های مجرمانه در تارنمای تاریک، مسأله‌ای جهانی است و اختصاصی به جغرافیای ایران ندارد، شایسته است، معاهداتی با موضوع پیشگیری از جرم در تارنمای تاریک تنظیم و به امضا و تصویب کشورها برسد. با تصویب اصول کلی ناظر بر پیشگیری از جرم در تارنمای تاریک، هر یک از کشورها می‌توانند جزییات مقررات آن را در قوانین داخلی خود منعکس نمایند و گامی در جهت محدودسازی فعالیت‌های مجرمانه بردارند. باید توجه داشت که انتظارات غیرمعقول دراین‌باره، مانند یکسان‌سازی جهانی سیاست‌های جزایی و به‌طور خاص، سیاست پیشگیری از جرم در تارنمای تاریک، مانع رسیدن به نتایج مطلوب خواهد شد. هر کشور دارای نظام حقوقی و سیاسی مختص خود است؛ علاوه بر این، هر نظام از مبانی خاصی پیروی می‌کند و درصورتی‌که حقیقتاً به نظام‌مند بودن خود پایبند باشد، نمود مبانی و پایه‌های فلسفی آن در پدیده‌های جزئی، مانند قانون، پدیدار می‌شود؛ بنابراین، انتظار دستیابی به قانون و یا سیاست واحد جهانی دراین‌باره نامعقول و به‌دوراز واقعیت به نظر می‌رسد؛ اما باوجود اختلاف‌نظرهای نام‌برده، می‌توان به تدوین تعدادی قاعده که از ارزش‌های مشترک بین اکثر کشورها حمایت می‌کنند، امیدوار بود و حتی آن را لازم دانست؛ زیرا سیاست‌گذاری در عرصه بکر و نوظهور تارنمای تاریک پروژه سنگینی است که با همکاری‌های بین‌المللی آسان‌تر می‌شود.

۴،۲. چالش ماهیت رفتار مجرمانه

مجرم بر اساس مقتضیات حاکم، رفتار مجرمانه خود را سامان می‌دهد. برای مثال، نحوه استتار و مخفیانه عمل کردن برای سرقت در شب با سرقت در روز یا سرقت در مکان شلوغ با خلوت متفاوت است. به همین ترتیب ارتکاب جرم در فضای واقعی و فضای مجازی تفاوت دارد؛ چراکه مقتضیات و شرایط حاکم بر این دو فضا با یکدیگر فرق دارد. برای مثال، این نوع از جرائم به دلیل واقع‌شدن در فضای مجازی و غیرواقعی، اثری ملموس و مادی از جرم و رد پای مجرم، آن‌گونه که در جرائم سنتی بر جای می‌ماند، دیده نمی‌شود و در بیشتر موارد همان اندک آثار باقی‌مانده از جرم که قابلیت ردیابی مجرم را دارد به‌راحتی قابل امحاء و پاک‌سازی است (طهماسبی و شاهمرادی، ۱۳۹۷: ۹۹). همچنین رمزآلود بودن تارنمای تاریک، ابعاد گوناگونی ناظر به کاربر و اطلاعات او دارد. برای مثال، مجرمان با استفاده از سرویس‌هایی مانند (TOR) می‌توانند مکان خود را پنهان کنند تا از ردیابی توسط مجریان قانون در امان بمانند. هم‌چنین این سرویس‌ها با رمزگذاری کردن اطلاعاتی که ردوبدل می‌شود، راه دستیابی به آن‌ها را ناهموار یا ناممکن می‌سازند.

همین ویژگی‌ها موجب شده است که تشخیص و احراز ارکان جرم با چالش‌هایی روبرو شود. زمان، مکان، نوع و نحوه رفتار ازجمله مؤلفه‌هایی است که باید برای تشخیص مجرمانه بودن یا نبودن در وهله اول و تشخیص عنوان جرم ارتکابی در وهله بعدی ذیل عنصر مادی جرم بررسی شود. همچنین احراز عنصر روانی کاربر تارنمای تاریک رکن مهم دیگری در نوع و میزان مسئولیت کیفری است که

[7] NIJ (National Institute of Justic)

در نظر گرفتن هرگونه ضمانت اجرا مستلزم تعیین تکلیف درباره این رکن و رکن مادی جرم می‌باشد. درحالی‌که مطالب پیشین نشان داد این تشخیص‌ها در فضای تارنمای تاریک با پیچیدگی‌های اساسی روبروست.

یکی از مسائلی که در پی مشخص نبودن ماهیت اعمال مجرمانه در تارنمای تاریک به وجود می‌آید، صلاحیت قضایی مراجع رسیدگی به جرائم واقع در این فضاست. «با توجه به ماهیت جرائم سایبری، تعیین محل ارتکاب جرم یا محل حصول نتیجه همیشه به‌آسانی امکان‌پذیر نیست» (طهماسبی و شاهمرادی، ۱۳۹۷: ۱۰۱). «هم‌چنین ماهیت اینترنت امکان ارتباط بین چند حوزه قضایی را به وجود آورده است و عناصر یک جرم ممکن است نه‌تنها در مکان و حوزه‌ای با حضور فیزیکی مجرم شروع‌شده و یا به نتیجه رسیده باشند، بلکه این امکان نیز هست که در تمام حوزه‌های دیگری که در اثر عملکرد کاربر به‌صورت الکترونیکی درگیر شده‌اند نیز بحث وقوع جرم مطرح باش» (زلقی و مالمیر، ۱۳۹۹: ۹۲).

حال، چنانچه جرم ارتکابی از جرائم بین‌المللی باشد و چند کشور را درگیر کرده باشد، پیچیدگی مسأله دوچندان می‌شود. در این صورت باید به این پرسش‌ها پاسخ داد که کدام کشور صلاحیت رسیدگی به این جرم را دارد؟ در کشور منتخب، کدام حوزه قضایی صالح به رسیدگی است؟ (زلقی و مالمیر، ۱۳۹۹: ۹۲). بنابراین با عبور فعالیت کاربران تارنمای تاریک از مرزهای محلی و ملی و به دلیل ماهیت متقابل صلاحیتی، همکاری‌های میان صلاحیتی و بین سازمانی محققین ضروری می‌نماید (Goodison, 2020). مطالعه چالش‌های پیش روی پیشگیری از جرم در تارنمای تاریک نشان می‌دهد این کار پیچیدگی‌های مضاعفی نسبت به پیشگیری در فضای واقعی دارد و نیازمند همکاری گسترده گروه‌های علمی متخصص در حوزه‌های مختلف در عین توجه به مؤلفه سرعت پیشرفت تکنولوژی و یافتن راه‌های ارتکاب جرم در تارنمای تاریک می‌باشد.

۳. راهکارهای پیشگیری از جرم در تارنمای تاریک

به‌طورکلی می‌توان برای کاهش جرم از طریق به کار بستن تدابیر پیشگیرانه چهار مرحله در نظر گرفت: مرحله اول، تبیین وضعیت؛ در این مرحله بایستی به نحو نظام‌مند، ابعاد مختلف جرمی را که می‌خواهیم از آن پیشگیری کنیم، بررسی نماییم (که این مداقه در بخش پیشین گذشت). مرحله دوم، برنامه‌ریزی؛ مدون کردن راهکارهای عملی پیشگیری و پاسخ به این پرسش که با اعمال اقدامات پیشگیرانه به دنبال رسیدن به چه هدفی هستیم؟ مرحله سوم، اجرا و مرحله آخر نیز ارزیابی می‌باشد (جندلی، ۱۳۹۳: ۱۰۲-۱۰۳). در این بخش بر آنیم تا به بررسی مرحله دوم پیشگیری یعنی انواع و مصادیق پیشگیری در تارنمای تاریک بپردازیم.

۱،۳. پیشگیری وضعی

این نوع از پیشگیری با دنبال کردن دو هدف «کاهش فرصت‌های مجرمانه» و «افزایش خطر ارتکاب جرم»، درواقع «بازدارندگی» را در نوع خاصی از جرائم که اقدامات پیشگیرانه ناظر به آن تنظیم‌شده است، افزایش می‌دهد. به‌عبارت‌دیگر، پیشگیری وضعی اقداماتی غیر کیفری است که از بالفعل شدن اندیشه مجرمانه جلوگیری می‌کند و جلوی ارتکاب جرائم مشابهی که ممکن است در یک وضعیت و موقعیت خاص به وقوع بپیوندد را می‌گیرد (گسن، ۱۳۷۶: ۶۱۰). کُرنیش و کلارک، پنج راهبرد اصلی را برای پیشگیری وضعی از جرائم پیشنهاد می‌کنند که هر یک از این راهبردها، پنج راهکار (راهکارهای ۲۵ گانه پیشگیری وضعی) را در برمی‌گیرند که ما در این مقاله به موارد مرتبط و قابل‌اجرا در ساحت تارنمای تاریک اشاره می‌کنیم. این پنج راهبرد، عبارت‌اند از: افزایش میزان تلاش به‌منظور ارتکاب جرم، افزایش خطرهای ارتکاب جرم، کاهش دستاوردها، کاهش عوامل محرک و سلب توجیه‌ها (بهره‌مند، کوره‌پز و سلیمی، ۱۳۹۳: ۱۵۴). افزایش میزان تلاش به‌منظور ارتکاب جرم در تارنمای تاریک را می‌توان از طریق محدودسازی دسترسی به سرویس‌هایی مانند (Tor). که مهم‌ترین ابزار برای ناشناس ماندن کاربر و رمزگذاری داده‌ها و اطلاعات است، محقق نمود. همچنین «پالایش نظام‌مند می‌تواند تا حد زیادی از ارتکاب جرائم رایانه‌ای از پیش تعیین نشده به‌وسیله مجرمان اتفاقی جلوگیری کن» (بهره‌مند، کوره‌پز و سلیمی، ۱۳۹۳: ۱۵۴). تدابیر

فصلنامه علمی
مطالعات حقوقی فضای مجازی
سال دوم | شماره سوم | پاییز ۱۴۰۲

محدودکننده یا سلب‌کننده دسترسی در دو قالب دیواره‌های آتش و فیلترینگ قابل‌بررسی هستند درواقع این دو فرآیند مکمل یکدیگر به شمار می‌روند؛ از طرفی دیواره‌های آتش از ورودی‌های غیرمجاز در صورت معتبر نبودن مشخصات عبور کننده جلوگیری می‌کند و از طرف دیگر فیلترینگ مانع دسترسی کاربران شبکه داخلی به اطلاعات غیرمجاز می‌شود (خانعلی‌پور واجارگاه، ۱۳۹۰: ۱۲۵).

یکی از راهکارهای وضعی ناظر به افزایش خطر ارتکاب جرم، نظارت دولتی است که کلارک آن را تحت عنوان «ارتقای نظارت رسمی[8]» مطرح می‌کند. نظارت دولتی همان‌طور که از عنوانش پیداست، نوعی از نظارت و زیر نظر داشتن کاربران توسط دستگاه‌های رسمی کشور است که می‌تواند که به دو گونه سنتی (به‌وسیله ابزار فیزیکی) و سایبری (به‌وسیله ابزار و فناوری‌های الکترونیکی) انجام شود. به‌طوری‌که «کلیه فعالیت‌های شبکه‌ای اشخاص، حتی ضرباتی که بر روی صفحه‌کلیدشان زده‌اند یا نقاطی را که به‌وسیله ماوس بر روی آن‌ها کلیک کرده‌اند ضبط می‌گردد. سپس مأمور موردنظر می‌تواند با بررسی این سوابق، موارد غیرقانونی را تحت پیگرد قرار دهد» (حیدری نژاد، ۱۳۹۷: ۳۴). البته این نظارت الکترونیکی، زمانی بر پیشگیری از وقوع جرم اثر خواهد داشت که کاربران از این نظارت مطلع باشند وگرنه کاربرد آن به دستیابی به ادله ارتکاب جرم کاهش خواهد یافت (بهره‌مند، کوره‌پز و سلیمی، ۱۳۹۳: ۱۶۳). همچنین به‌کارگیری تکنیک‌هایی[9] و نرم‌افزارهای ردیابی[10] که قادر به کشف رمز از داده‌های رمزنگاری‌شده تارنمای تاریک هستند، مفید به نظر می‌رسد. «این تکنیک یکی از ابزارهای توسعه‌یافته توسط دارک وب است که به‌طور خودکار هزاران ویژگی چندزبانه، ساختاری و معنایی را استخراج می‌کند تا مشخص شود چه کسی محتوای ناشناس آنلاین ایجاد می‌کند» (Vilic, 2017: 20). به‌عبارت‌دیگر در این روش، با در کنار هم قرار دادن و بررسی مجموع ویژگی‌ها و سبک نوشتاری تلاش می‌شود تا هویت شخص نویسنده کشف گردد.

یکی از راهکارهای ذیل کاهش دستاوردهای جرم، «پنهان کردن آماج[11]» است. پنهان کردن آماج جرم یا بزه دیدگان احتمالی از تیررس مجرمان به‌وسیله ناشناس کننده‌ها و رمزنگارها امکان‌پذیر است. بدین‌صورت که ناشناس کننده‌ها، هویت افراد مبدأ و مقصد مبادله اطلاعات را پنهان می‌کنند و رمزنگارها محتوای ارتباطات را نامفهوم می‌سازند (بهره‌مند، کوره‌پز و سلیمی، ۱۳۹۳: ۱۶۵). بهره‌گیری از ناشناس کننده‌ها به‌خصوص برای زنان و کودکان مفید است؛ زیرا بدون آن‌که فرصت شناسایی و سوءاستفاده به مجرمان سایبری بدهند، می‌توانند از فضای مجازی استفاده نمایند (خانعلی‌پور واجارگاه، ۱۳۹۰: ۱۳۰). انتقادی که به این پیشنهاد وارد است، عبارت است از این‌که همان‌گونه که عموم مردم قادر به پنهان کردن هویت و اطلاعات خود می‌شوند، مجرمین نیز به همین وسیله هویت خود را ناشناس می‌کنند و با آرامش خاطر بیشتری به ارتکاب جرم می‌پردازند! مضاف بر این‌که تجویز این راهکار، باعث همه‌گیری استفاده از روش‌های رمزنگاری و نهایتاً موجب اختلاط مجرم و غیرمجرم می‌گردد و کار برای متصدیان پیشگیری از جرم و مجریان قانون بیش‌ازپیش سخت می‌شود.

آخرین راهبرد کلارک، به سلب توجیه‌ها اشاره دارد. این راهبرد بیان می‌دارد که با استفاده از اقدامات وضعی باید تا حد امکان این توجیه‌ها را از بزهکاران گرفت تا اعمال مجرمانه آن‌ها فاقد پشتوانه وجدانی شود و از این طریق قصد مجرمانه او متزلزل گردد.

وضع کدهای رفتاری[12] را می‌توان راهکاری عملی ذیل راهبرد سلب توجیه به شمار آورد. کدهای رفتاری مجموعه قواعدی است که اصول و تبعات نقض آن را به مسئولین هر حوزه گوشزد می‌کند. ثمره عملی تدوین و ارائه کد رفتاری، آگاهی فرد مسئول نسبت به وظایف و حیطه مسئولیت و اختیارات وی است. دسته‌ای از کدهای رفتاری، کدهای رفتاری خاص هستند که برای افراد دارای مسئولیت خاص و مرتبط با اطلاعات حساس، مثلاً اطلاعات محرمانه مملکتی، پیشنهاد می‌شود. نداشتن دانش و اطلاعات کافی در این افراد، راه را

[8] Strengthen formal surveillance
[9] Writeprint
[10] Web spiders
[11] Conceal targets
[12] Codes of Conduct

برای سوءاستفاده بزهکاران حرفه‌ای باز می‌کند و موجب ورود آسیب‌های هنگفت به حوزه تحت مسئولیت آنان می‌شود (بهره‌مند و داوودی، ۱۳۹۷: ۴۱).

در پایان لازم است به ذکر چند نکته در ارتباط با مطالب بیان‌شده بپردازیم: نکته اول این‌که بسیاری از راهکارهای پیشگیری وضعی برای مجرمین حرفه‌ای قابل پیش‌بینی نیست و اگر هم قابل پیش‌بینی باشد، اثر موقتی بر رفتار مجرمانه آن‌ها دارد؛ زیرا راهکارهای پیشگیری وضعی اساساً از سنخ راهکارهای سطحی و ناظر به فضا و موقعیت موجود در حال حاضر هستند؛ بنابراین مجرمین می‌توانند با تغییر وضعیت، تدابیر پیشگیرانه وضعی را بی‌اثر یا کم اثر کنند و به نظر بسیاری از جرم‌شناسان با جابجایی محل ارتکاب پدیده مجرمانه، جرم را به مکان دیگری منتقل کنند. به همین دلیل می‌توان گفت نقطه اثر اقدامات پیشگیرانه وضعی بر افعال مجرمین تازه‌کار، اتفاقی و یا کسانی است که به هر دلیلی به ارتکاب جرم در فضای تارنمای تاریک تحریک می‌شوند اما با مشاهده خطرات و دشواری‌های مسیر، از ارتکاب جرم تام منصرف می‌شوند؛ اما از طرف دیگر برخی معتقدند «تدابیر پیشگیری موقعیت مدار باوجود پدیده جابجایی هنوز می‌تواند خوش‌بینانه باشد؛ زیرا هرچند احتمال رخداد این پدیده وجود دارد ولی نباید آن را پیامد گریزناپذیر پیشگیری از جرم دانست و وانگهی در صورت رخداد اندازه و پهنه آن گسترده نیست» (رایجیان اصلی، ۱۴۰۱: ۱۸۸). اما این نظر وقتی به چالش کشیده می‌شود که پیشگیری وضعی را در ارتباط با تکنولوژی‌های نوین موردبحث قرار دهیم. در این صورت سرعت تغییرات فنی و نیز روزآمد شدن عملکرد مجرمانه بزهکاران، به‌طور مضاعف از گستره و عمق اثرگذاری مطلوب راهکارهای وضعی می‌کاهد.

نکته دوم مسأله هتک حریم خصوصی است. شاید بتوان این‌گونه ادعا کرد که چالش حریم خصوصی و به‌طور عام، چالش‌های حقوق بشری، قابل‌اعتناترین و اصلی‌ترین انتقادات وارد به پیشگیری وضعی هستند؛ چراکه راهکاری مانند نظارت که از مهم‌ترین راهکارهای پیشگیری وضعی است، همیشه در مظان اتهام تعدی به حریم خصوصی افراد و به عبارت بهتر، در دوگانه هتک حریم خصوصی و برقراری امنیت از طریق پیشگیری از جرم قرار داشته است. در کشاکش حفظ حقوق فرد و حقوق اجتماع، برخی با استناد به اصول و معاهدات حقوق بشری، اصالت را به حق داشتن حریم خصوصی و نتیجتاً عدم مشروعیت نظارت رسمی بر رفتار کاربران می‌دهند. بعضی دیگر، با توجه به گستردگی خطرات ناشی از جرائم سایبری و با استناد به وظیفه دولت مبنی بر حمایت از نظم و امنیت عمومی، پیشگیری وضعی را به‌عنوان یکی از راهکارهای جلوگیری از وقوع جرم تجویز می‌کنند.

بنابراین پیشگیری وضعی در مورد جرائم سایبری و به‌ویژه تارنمای تاریک، به‌وضوح دارای محدودیت‌های جدی می‌باشد. رمون گسن به‌خوبی در مقاله پیشگیری وضعی و کنترل بزهکاری، به عدم قابلیت اجرای راهکارهای پیشگیری وضعی در مورد تمام جرائم اشاره و آن را مستلزم وجود دو خصیصه می‌داند: اول، مادی بودن آماج و دوم، عمدی بودن جرائم (گسن، ۱۳۷۶: ۶۱۶). به همین دلیل است که معتقدیم قابلیت تحقق اقدامات پیشگیرانه وضعی در جرائم واقع در تارنمای تاریک بسیار ناچیز و در حد صفر است؛ چراکه ازیک‌طرف، بزه دیده جرائم واقع در تارنمای تاریک فاقد فیزیک (جسم مادی) است و از طرف دیگر ممکن است به‌صورت غیر عامدانه موضوع اعمال مجرمانه قرارگرفته باشد. به‌عنوان جمع‌بندی، ازجمله محدودیت‌های تارنمای تاریک که ما را در اعتقاد به کارآمد نبودن پیشگیری وضعی مصمم نموده است، می‌توان به دودسته اشاره کرد: دسته اول، محدودیت‌های فنی است. پیشرفت روزافزون تکنولوژی و فناوری‌های دیجیتال، عمر اقدامات پیشگیرانه وضعی را به‌شدت کوتاه کرده است. مدت زیادی به طول نمی‌انجامد که یک راهکار پیشگیری وضعی که با صرف زمان زیاد و هزینه‌های هنگفت به ساحت اجرا درآمده است، توسط مجرمین سایبری خنثی و دور زده می‌شود. دسته دوم، محدودیت‌ها و چالش‌های قانونی ناظر به این نوع پیشگیری است؛ مانند حق حریم خصوصی و اصل آزادی جریان اطلاعات و حق بهره‌برداری مشروع از اطلاعات (جلالی فراهانی، ۱۳۸۳: ۱۱۲). به نظر نگارنده، به کار بستن راهکارهای پیشگیری وضعی، به‌مثابه شر ضروری و مسکن موقتی، در مواقعی که راهکار جایگزین بهتر و مؤثرتری در دست نباشد، لازم است؛ اما خطر سوءاستفاده از اختیار نظارتی همواره وجود دارد و امر قابل‌انکاری نیست. به همین دلیل به نظر می‌رسد ضمن تحدید اختیار نظارتی و تصریح روشن قانون به موارد مجاز،

فصلنامه علمی
مطالعات حقوقی فضای مجازی
سال دوم | شماره سوم | پاییز ۱۴۰۲

بایستی درباره اقدامات پیشگیرانه جدیدتر، مؤثرتر و موافق‌تر با فضای تارنمای تاریک تأمل کرد و پیشگیری وضعی را با عنایت به محدودیت‌های فنی و قانونی، به‌عنوان جایگزین موقت و اولویت چندم مدنظر قرار داد.

۲،۳. پیشگیری اجتماعی

برخلاف پیشگیری وضعی که کاربرد آن به‌مثابه مسکنی موقتی جهت بهبود سریع اما ناپایای وضع موجود است، پیشگیری اجتماعی به رفع عوامل ایجاد جرم می‌پردازد و سعی دارد تا با از بین بردن علت جرم، معلول (جرم) را کاهش دهد. «در پیشگیری اجتماعی تلاش می‌شود که با انجام برنامه‌های اجتماعی، فرهنگی، اقتصادی، رفاهی و نظایر آن‌ها و درمان نارسایی‌های اجتماعی و بالا بردن ارزش‌های اجتماعی و اخلاقی شرایط یک منطقه و نیز وضعیت مجرمان بالقوه اعتلا یافته و این روند به کاهش میزان جرم بینجامد» (صبح دل، ۱۳۹۶: ۹۵). در این بخش به مصادیق پیشگیری اجتماعی در تارنمای تاریک در قالب پیشگیری قضایی، اجرایی و هماهنگ اشاره می‌کنیم:

پیشگیری قضایی: قانون‌گذار در بند پنجم اصل یکصد و پنجاه و ششم قانون اساسی در مقام بیان وظایف قوه قضاییه به «اقدام مناسب برای پیشگیری از وقوع جرم و اصلاح مجرمین» اشاره می‌کند. به همین جهت، دستگاه قضایی نهادهایی را باهدف پرداختن به امر پیشگیری از جرم تأسیس نمود؛ ازجمله: معاونت پیشگیری از وقوع جرم، «ستاد مردمی پیشگیری و حفاظت اجتماعی، بنیاد صیانت از نهاد خانواده و مؤسسه خادمان علم و اخلاق (امید)» (صبح دل، ۱۳۹۶: ۱۰۳). به نظر نگارنده پیشگیری از جرم نه به‌صورت مستقیم، بلکه به‌صورت غیرمستقیم و به‌عنوان تابعی از عملکرد قوه قضاییه نسبت به متهمان و محکومان موردتوجه قرار می‌گیرد. به‌موجب این رویکرد، مراکز رسانه‌ای و اطلاع‌رسانی قوه قضاییه بایستی در بازتاب اخبار، وقایع و عملکرد این قوه اصل پیشگیری از جرم را مدنظر داشته و خط‌مشی آن‌ها مبتنی بر اثرگذاری ایجابی (فرهنگ‌سازی مثبت) و سلبی (هشدار دهی و منع از انجام اعمال و ایجاد موقعیت‌های مخاطره‌آمیز در تارنمای تاریک) باشد. پیشگیری از وقوع دوباره جرم (تکرار جرم توسط مجرم) و اصلاح مجرم نیز می‌تواند از طریق برنامه‌های تربیتی تدارک دیده‌شده توسط نهاد قضایی محقق گردد.

پیشگیری اجرایی: بزهکاری در جامعه بیش از هر چیز ناشی از شرایط اجتماعی، فرهنگی و اقتصادی می‌باشد. به‌نحوی‌که نابسامانی در هر یک از این حوزه‌ها پیامدهای منفی را متعاقباً به بار خواهد آورد. این پیامدها در شکل خفیف خود به‌صورت «مشکل» و «آسیب» و در شکل حاد و خطرناک خود به‌صورت «جرم» بروز می‌یابد.

بدیهی است عدم ثبات در شرایط اقتصادی، فقر و بیکاری مهم‌ترین عامل در ارتکاب جرائم مالی می‌باشد. «قوه مجریه به‌عنوان نهاد مسئول در این زمینه وظیفه دارد تا برای بهینه‌سازی وضعیت اقتصادی جامعه، فقرزدایی و حل معضل بیکاری و مسکن افراد جامعه تلاش نماید. در همین راستا نیز قانون اساسی جمهوری اسلامی ایران، رفع نیازهای مادی و معنوی افراد را بر دوش دولت (قوه مجریه) قرار داده و دولت را به رفع تبعیض‌های ناروا و ایجاد امکانات عادلانه برای همه شهروندان موظف نموده است. (اصل بیست و هشتم تا سی و یکم قانون اساسی)» (ساریخانی و سلطانی بهلولی، ۱۳۹۵: ۱۵۳). یکی از راهکارهای پیشنهادی برای پیشگیری از وقوع جرم در تارنمای تاریک که ذیل وظایف دولت قابل‌طرح می‌باشد، حکمرانی خوب در فضای سایبر است. «این اصطلاح اولین بار توسط بانک جهانی به کار رفت و اشاره به تصمیماتی داشت که واجد قابلیت تأثیرگذاری بر عملکرد اقتصادی کشورها بود. گرچه این تعریف در ابتدا تنها دارای بعد اقتصادی بود اما بعدها بعد سیاسی نیز به آن افزوده شد و مواردی مثل مشروعیت، شفافیت، پاسخگویی، تحقق حقوق بشر از طریق حاکمیت قانون و شایستگی دولت‌ها را نیز دربرگرفت» ازآنجایی‌که بسیاری از جرائم ارتکابی در تارنمای تاریک در رسته جرائم امنیتی هستند و ازآنجایی‌که این نوع از جرائم ارتباط مستقیمی با وضعیت سیاسی، اجتماعی، اقتصادی و فرهنگی کشور دارند، بدون پرداختن به مسائل مورداشاره در حکمرانی خوب نمی‌توان در پیشگیری از آن‌ها موفق بود (بهره‌مند و داوودی، ۱۳۹۷: ۴۱).

دانشگاه آزاد اسلامی واحد مراغه

پیشگیری هماهنگ: بعضی دیگر از راهکارهای پیشگیری، نهاد متولی واحدی ندارد یا قانون‌گذار صرفاً به بیان یک سری بایدها و نبایدها پرداخته و مسئول اجرای آن‌ها را مجمل گذاشته است. از همین روی، دستگاه‌های مختلفی بایستی به پیاده‌سازی آن همت بگمارند. بدیهی است یک سیاست پیشگیری جامعه‌مدار جامع، بایستی با تشریک‌مساعی و هماهنگی تمام نهادهای دخیل در حوزه فرهنگ، سیاست، اقتصاد و جامعه صورت بگیرد. ازجمله این راهکارها می‌توان به موارد زیر اشاره کرد:

الف) همکاری بین‌المللی: همکاری‌های دوجانبه و چندجانبه بین کشورها و همچنین همفکری و چاره‌اندیشی جهانی در قالب نهادهای بین‌المللی یکی از مهم‌ترین راه‌های دستیابی و به‌کارگیری الگوی مناسب پیشگیری از جرم در تارنمای تاریک می‌باشد. وجه تمایز این راهکار و نکته مثبت آن، بهره‌گیری از دانش نظری و تجربی سایر کشورها و هم‌افزایی علمی در این حوزه می‌باشد. برای مثال اینترپل در سپتامبر ۲۰۰۲ یک بخش ویژه علیه تروریسم ایجاد کرد و سازمان همکاری و توسعه اقتصادی[13] در همین سال دستورالعمل‌هایی را برای امنیت سیستم‌ها و شبکه‌های اطلاعاتی با پیشنهاد دولت‌های کشورهای عضو به‌منظور جلوگیری از تروریسم سایبری، ویروس‌های رایانه ای و هک سیستم‌ها منتشر کرد تا امنیت اطلاعات و امنیت شبکه‌های رایانه‌ای را ارتقا دهند و حریم خصوصی افراد و آزادی شخصی آن‌ها ایمن باشد. از نمونه همکاری‌های منطقه‌ای نیز می‌توان به فعالیت‌های اتحادیه اروپا علیه تروریسم به‌طورکلی و شورای اروپا، با ایجاد کمیته کارشناسان در مورد تروریسم سایبری[14] و تصویب کنوانسیون جرائم سایبری (CETS) شماره ۱۸۵ (۲۰۰۱) و کنوانسیون در مورد پیشگیری از تروریسم (CETS) اشاره کرد (Vilic, 2017: 19).

ب) همکاری با ارائه دهنگان خدمات اینترنتی (ISP): درراه پیشگیری از وقوع جرم در تارنمای تاریک نباید از نقش شرکت‌های خدمات اینترنتی غافل شد. سازمان‌های مجری قانون باید با ارائه‌دهندگان خدمات اینترنتی برای جمع‌آوری «شواهد کلیدی» در پرونده‌های تروریسم سایبری [و سایر جرائم واقع در تارنمای تاریک] همکاری کنند. هم‌چنین اپراتورهای شبکه‌های بی‌سیم[15] باید از کاربران خود بخواهند که ثبت‌نام و هویت خود را شناسایی نمایند (Vilic, 2017: 19).

ج) اطلاع‌رسانی: در سال‌های اخیر فضای مجازی و دنیای دیجیتال نقش پررنگ‌تری در زندگی همه پیداکرده است، اما هنوز در میان برخی اقشار ناشناخته است. علاوه بر این، قشر جوان و نوجوان که بیشترین هم‌زیستی را با این فضا دارند اکثراً با قسمت تارنمای سطحی آشنا هستند و دانش و مهارت آن‌ها محدود به همین بخش است. این در حالی است که بیشترین جذابیت‌ها در تارنمای عمیق و تاریک برای همین رده سنی وجود دارد. همین موضوع می‌تواند باعث شود که نوجوان برای پاسخ به کنجکاوی خود دست به اقدامات به‌ظاهر بی‌خطر اما ناشیانه‌ای بزند که نتایج نامطلوبی را به بار آورد. تحقیقات بسیاری نشان می‌دهد «طیف وسیعی از مجرمان و بزه دیدگان این جرائم را افراد کم‌سال و جوان تشکیل می‌دهند» (جلالی فراهانی، ۱۳۸۳: ۱۰۳)؛ بنابراین با توجه به ناشناخته بودن خصوصیات، مخاطرات و چگونگی تدابیر امنیتی در تارنمای تاریک هشداردهی نسبت به آن، لازم است. بدیهی است باید توجه شود که این اطلاع‌رسانی باعث ترغیب بیشتر مردم به تجربه کردن این فضا نگردد و بیشتر جنبه هشداردهی و انذار داشته باشد. «به‌منظور پیشگیری باید افرادی که در معرض بزه دیدگی هستند از موقعیت یا خصوصیت بزه دیدگی‌شان مطلع شوند؛ زیرا نرخ جرم بیش از آن‌که تحت تأثیر انگیزه بزهکاران باشد، می‌تواند ناشی از آسیب‌پذیری خاص بزه دیدگان یا دسته‌های خاصی از آنان باشد که به دلایل متعددی خود را در معرض یک خطر جدی قرار می‌دهند» (خانعلی‌پور واجارگاه، ۱۳۹۰: ۴۶). از طرف دیگر، این اطلاع‌رسانی نباید در تشویق جوانان به عدم استفاده از این محیط نمود پیدا کند؛ بلکه باید طوری آموزش ببینند که مشارکت خود را در فعالیت‌های آنلاین مخاطره‌آمیز به‌صورت آگاهانه کاهش دهند. به‌عبارت‌دیگر، هدف اصلی بایستی رشد فکری و سرعت بخشیدن به فرایند تفکر آگاهانه باشد و نه ایجاد سوءظن نسبت به عوامل خطر (جایشانکار، ۱۳۹۴: ۱۸۵). «در راستای وظیفه اطلاع‌رسانی، برخی دولت‌ها با تأسیس مراکز اطلاع‌رسانی آنلاین اقدام به ارائه مشاوره و

[13] OECD
[14] CODEXTER
[15] Wi-Fi

فصلنامه علمی
مطالعات حقوقی فضای مجازی
سال دوم | شماره سوم | پاییز ۱۴۰۲

توصیه‌های عملی به سیاست‌گذاران، متصدیان و پژوهشگران شاغل در ارکان مختلف دولت می‌کند» (بهره‌مند و داوودی، ۱۳۹۷: ۳۹). این اقدام نشان‌دهنده این است که در کنار آموزش همگانی نباید از آموزش خواص غافل شد. هم‌پای سرعت پیشرفت تکنولوژی، مجرمین سایبری نیز راه‌های بهتر و سریع‌تر ارتکاب جرم را پیدا می‌کنند و لازم است مجریان قانون نیز همیشه به روز کردن دانش خود را در دستور کار داشته باشند؛ بنابراین باید توجه نمود که تطبیق مستمر اقدامات فناوری، سازمانی و نظارتی از مهم‌ترین اصول حاکم بر الگوهای پیشگیری در تارنمای تاریک می‌باشد.

۳،۳. پیشگیری رشد مدار

«منظور از پیشگیری رشد مدار، مجموعه اقداماتی است که در دوران رشد و تکامل شخصیتی و جسمی کودکانی به اجرا درمی‌آید که در معرض ارتکاب این اعمال قرار دارند. با توجه به این‌که پیشگیری رشد مدار با قشر کم سن و سال سروکار دارد، خط‌مشی‌ها و اقدامات آن، رویکردی تربیتی و آموزشی داشته و در این نوع پیشگیری قدرت شناخت و تمیز آن‌ها تقویت می‌شود» (جلالی فراهانی و باقری اصل، ۱۳۸۷: ۱۳۴). ازآنجایی‌که در شکل‌گیری شخصیت کودکان و مراحل تکامل اجتماعی و جامعه‌پذیری آنان دو نهاد خانواده و مدرسه نقش پررنگی دارند، در ادامه به مهم‌ترین راهکارهای پیشگیری رشد مدار در قالب نقش این دو نهاد مؤثر پرداخته می‌شود:

۱) آموزش و توجیه خانواده‌ها: خانواده به‌عنوان مهم‌ترین نهاد دخیل در شکل‌گیری مؤلفه‌های شخصیتی کودک، نقش به سزایی در پیشگیری از جرم دارد. جهت‌گیری‌های تربیتی والدین به نحو آشکاری بر رفتار و کنش‌های دوره بزرگ‌سالی فرزندان تأثیر می‌گذارد. به همین دلیل ضرورت دارد والدین نسبت به چگونگی عملکرد خود در مواجهه با فعالیت‌های سایبری فرزندان، به‌ویژه در سنین کودکی و نوجوانی، آموزش‌های لازم را دریافت کنند. «برای مثال، برنامه آموزشی والدینی که فرزندانشان با اینترنت سروکار دارند، می‌تواند حاوی نکات زیر باشد: ایجاد حس مسئولیت‌پذیری و توانایی انتخاب گزینه‌های سالم هنگام استفاده از اینترنت، تصمیم‌گیری به‌جا و مناسب درباره محتوایی که قرار است مشاهده کنند، آموزش نحوه رویارویی با محتوای نامناسبی که ممکن است مشاهده کنند و کاهش عواقب آن. در حقیقت باید ابتدا به والدین چگونگی اتخاذ این رهیافت‌ها را نسبت به کودکانشان آموزش داد» (جلالی فراهانی و باقری اصل، ۱۳۸۷: ۱۴۱).

در پیشگیری رشد مدار، چون با کودکان و نوجوانانی مواجه هستیم که نظام شخصیتی آن‌ها در حال شکل‌گیری است و کوچک‌ترین اعمال و رفتارها، خصوصاً از سوی والدین، بر ساختمان این نهال ظریف تأثیرگذار است، باید به جزییات روان‌شناختی آنان نیز توجه بسیاری داشت. برای مثال، اکثر نوجوانان در سنین خاصی دوست دارند با آنان مانند یک فرد بزرگ‌سال رفتار شود و اطرافیان روی آن‌ها حساب باز کنند. به همین دلیل دست به اقدامات بزرگ سالانه می‌زنند و بدین‌وسیله سعی در فاصله گرفتن از دنیای کودکی و ثابت کردن این موضوع به دیگران دارند. بدیهی است اقدامات تربیتی از قبیل نظارت مستقیم و امرونهی‌های از بالا به پایین و قهرآمیز نه‌تنها ثمره مثبتی در زمان حال ندارد، بلکه ممکن است نتایج معکوسی را در آینده به ارمغان آورد.

۲) آموزش از طریق مدارس: آموزش‌وپرورش نقش مهمی در تربیت و رشد فکری کودکان و نوجوانان دارد؛ بنابراین تدارک برنامه‌های آموزشی و مهارت‌هایی از قبیل تفکر نقادانه و مهارت نه گفتن برای پیشگیری از ایجاد زمینه‌های مجرمانه از کودکی در افراد مؤثر می‌باشد (جایشانکار، ۱۳۹۴: ۲۸۸). اگر اعمال مجرمانه را صرفاً ناشی از فرصت‌های بزهکاری بدانیم، طبعاً به‌سوی حذف یا کم کردن اوضاع‌واحوال یا موقعیت‌های ارتکاب جرم حرکت می‌کنیم؛ درحالی‌که اگر انگیزه مرتکب در انتخاب راه‌های گذار به عمل مجرمانه را بدانیم می‌توانیم او را در فرایند گذار اندیشه به عمل مجرمانه متوقف نماییم (گسن، ۱۳۷۶، ۶۱۰). به همین دلیل است که بر پیشگیری رشد مدار بیش از پیشگیری‌های موقعیت مدار تأکید می‌گردد.

دانشگاه آزاد اسلامی واحد مراغه

از دیگر موضوعات اولویت‌دار در حوزه آموزش‌وپرورش، «سواد رسانه‌ای» است. فراگیری این دانش، در مواجهه با فضای تارنمای تاریک اهمیت دوچندانی پیداکرده است؛ تا جایی که می‌توان گفت وارد شدن به این فضا بدون داشتن اطلاعات و مهارت‌های لازم، مانند وارد شدن به رینگ بازی بوکس است بدون این‌که آشنا با اصول، قواعد و نحوه این بازی باشیم.

«سواد رسانه‌ای عمری کوتاه در مطالعات رسانه‌ها و ارتباطات اجتماعی دارد. در تعاریف و برداشت‌های ارائه‌شده از سواد رسانه‌ای، چهارعنصر کلی مورد تأکید بوده‌اند که عبارت‌اند از: مهارت‌ها، دانش، رفتارها و تأثیرات» (علوی‌پور، عسگری، خسروی و سروی زرگر، ۱۳۹۹: ۱۷۱). به‌عبارت‌دیگر، «سواد رسانه‌ای، شامل مهارت و توانایی شایسته و به‌کارگیری ماهرانه پیام‌ها و مبادلات رسانه‌ای – سایبری است. سواد رسانه‌ای به مخاطب می‌آموزد در برخورد با پیام‌های گوناگون برخورد نقادانه و مدیریت اطلاعات داشته باشد و تسلیم ابزارهای چندرسانه‌ای قدرتمند فرهنگ رسانه نشود و به‌طورکلی، استفاده‌کننده‌ای متفکر در برخورد با رسانه باشد» (بهره‌مند و داودی، ۱۳۹۷: ۳۴-۳۵). آموزش سواد رسانه‌ای به کودکان و نوجوانان از اهمیت به سزایی برخوردار است؛ زیرا از طرفی آموزش در سنین پایین، آموزش مؤثرتری است و از طرف دیگر، این گروه سنی ارتباط بیشتری با فضای مجازی دارند و نتیجتاً بیشتر امکان مواجه‌شدن با مخاطرات تارنمای تاریک را نیز دارا هستند.

در حوزه آموزش سواد رسانه‌ای باید کودکان را تشویق کنیم تا در فضایی پرسش‌گرانه توانایی خود را درباره موضوع به چالش کشیده شده، عمیق‌تر کنند. در این برنامه به‌جای تطابق با یک الگوی خطی و از پیش تعیین‌شده، بر کندوکاو و اشتراک‌گذاری تجربیات در فرآیند ساخت دانش تأکید می‌گردد. در این صورت نقش مربی آماده کردن دانش برای بلعیده شدن توسط مخاطبان نیست؛ بلکه روش‌هایی همچون طرح سؤال‌های باز پاسخ و تفکر برانگیز، بحث در مورد سؤال‌ها، هدایت و مدل‌سازی توسط مربی برای مخاطبان، حالت میزگرد داشتن کلاس و تشویق بیشتر مخاطبان به صحبت کردن و ارزیابی توسط مربی به‌ویژه برای سؤال‌هایی که پیچیده و دشوار هستند و تشویق کودکان به دفاع از نظرات و ایده‌های خود توصیه می‌شود. برخی معتقدند محتوای مشخصی را نمی‌توان برای واحد سواد رسانه‌ای در نظر گرفت؛ بلکه مربی باید با توجه به موقعیت اجتماعی کودکان، شرایط فرهنگی و بافتاری که دانش‌آموزان از آن برآمده‌اند، محتوا را انتخاب کند (انصاری، سراجی و یوسف‌زاده، ۱۴۰۰: ۱۴۵). به نظر می‌رسد این شیوه کارآمدی بیشتری داشته باشد؛ زیرا بسیار محتمل است که محتوای از پیش تعیین‌شده یکسان برای تمامی دانش‌آموزان باوجود تفاوت‌های اجتماعی و فرهنگی و...، موجب صرف زمان و انرژی زیاد در مبحثی شود که مبتلابه مخاطب نیست و از طرف دیگر، مباحث مهم و مطالبی که مناسبت بیشتری دارند، مغفول انگاشته شوند.

نتیجه‌گیری

نگارنده در این مقاله در پی فهم امکان پیشگیری از جرم در تارنمای تاریک یا عدم امکان آن، در وهله اول و در مرحله دوم، چگونگی این پیشگیری در صورت ممکن بودن اصل آن بود. نظر به اینکه جرائم ارتکابی در دارک نت ازلحاظ گستره تأثیر بسیار وسیع‌تر از فضای واقعی و به لحاظ خطرناکی درجه بالایی از خطر را دارا هستند و با توجه به خصوصیات ویژه فضای تارنمای تاریک از قبیل رمزی بودن داده‌ها و ویژگی‌های خاص مجرمین دارک نت که اغلب آنان را مجرمین حرفه‌ای تشکیل می‌دهند، لزوم پیشگیری از جرم در این فضا روشن می‌گردد؛ اما با عنایت به همین دلایل، این پیشگیری به‌سادگی امکان‌پذیر نیست و چالش‌های جدی‌ای پیش روی دست‌اندرکاران این حوزه قرار دارد؛ چالش‌هایی که اهم آن عبارت‌اند از: فقدان اطلاعات کافی از تارنمای تاریک، مشروعیت یا عدم مشروعیت نظارت دولت‌ها، چالش نقض حریم خصوصی، فقدان مقررات حاکم و چالش ماهیت رفتار مجرمانه. موارد مذکور چالش‌های مبتلابه جهانی است و حل آن‌ها منوط به آموزش و افزایش سطح آگاهی و انجام پژوهش‌ها و هم‌افزایی‌های ملی و بین‌المللی مربوط به تارنمای تاریک است. در ادامه به بررسی پاره‌ای از راهکارهای پیشگیری از جرم در دارک نت، با عنایت به امکانات موجود پرداخته شد. ذیل پیشگیری وضعی، با الهام از راهبردهای کلان پنج‌گانه کلارک به بیان راهکارهایی جزئی از قبیل مدیریت مکان، افزایش نظارت‌های دولتی (رسمی)،

فصلنامه علمی
مطالعات حقوقی فضای مجازی
سال دوم | شماره سوم | پاییز ۱۴۰۲

به‌کارگیری نظارت سایبری و سلب توجیه از طریق هشدار دهی و وضع کدهای رفتاری پرداخته شد. نتیجه به‌دست‌آمده از بررسی راهکارهای پیشگیری وضعی این است که این نوع از پیشگیری، نه به‌عنوان الگوی پیشگیری ثابت و دائمی، بلکه به‌عنوان پیشگیری موقت و با خاصیت مسکن، مورد تجویز قرار می‌گیرد و آنچه پیشگیری اصلی است و باید موردعنایت مسئولان باشد، پیشگیری اجتماعی می‌باشد. چراکه به‌کارگیری پیشگیری وضعی در تارنمای تاریک به جهت محدودیت‌های اساسی (فنی و قانونی) و چالش‌های مهمی که در پی دارد (مسائل حقوق بشری) و همچنین دوام کم آن، در بلندمدت قابل‌اتکا نیست و اثر مطلوبی از خود بر جای نمی‌گذارد.

راهکارهای پیشگیری اجتماعی با بررسی نقش قوه قضاییه، قوه مجریه و سایر نهادها بیان گردید. در مورد پیشگیری قضایی، پیشنهاد می‌شود مراکز رسانه‌ای و اطلاع‌رسانی قوه قضاییه در بازتاب اخبار، وقایع و عملکرد این قوه اصل پیشگیری از جرم را مدنظر داشته و خط‌مشی آن‌ها مبتنی بر اثرگذاری ایجابی (فرهنگ‌سازی مثبت) و سلبی (هشدار دهی و منع از انجام اعمال و ایجاد موقعیت‌های مخاطره‌آمیز) باشد. پیشگیری از وقوع دوباره جرم (تکرار جرم توسط مجرم) و اصلاح مجرم نیز می‌تواند از طریق برنامه‌های تربیتی تدارک دیده‌شده توسط نهاد قضایی محقق گردد. در همین راستا، قوه مجریه موظف است مطابق اصل بیست و هشتم تا سی‌ام قانون اساسی، به بهبود و سامان‌بخشی اوضاع اقتصادی، فرهنگی و اجتماعی جامعه بپردازد. با توجه به این‌که وضعیت نابسامان اقتصادی، اجتماعی، سیاسی و فرهنگی از مهم‌ترین عوامل وقوع جرم می‌باشد، تلاش در جهت بهبود آن‌ها به کاهش آمار جرائم کمک و به طریقی از وقوع آن‌ها پیشگیری می‌کند. در کنار قوای حاکمیتی، سایر نهادها نیز می‌توانند از طریق اطلاع‌رسانی و فرهنگ‌سازی راجع به فضای سایبری و تارنمای تاریک، نقش مؤثری در پیشگیری از جرم ایفا کنند. همکاری‌ها و هم‌افزایی‌های دوجانبه و چندجانبه بین کشورها، همکاری‌های منطقه‌ای و جهانی از طریق نهادهای بین‌المللی نیز امری است که نباید از آن غافل شد. توجه به این موضوع، از طرفی باعث ارتقای سطح دانش کشورها و از طرف دیگر سرعت بخشیدن به روند تنظیم تدابیر پیشگیرانه خواهد شد. راهکار دیگر، استفاده از اطلاعات موجود نزد ارائه‌دهندگان خدمات اینترنتی است. همکاری با این اپراتورها می‌تواند در دستیابی به هویت اشخاص ناشناس در تارنمای تاریک و شواهدی کلیدی دراین‌باره مؤثر باشد. در پیشگیری رشد مدار ازآنجایی‌که جامعه هدف ما کودکان و افراد کم سن و سال هستند، بیشتر اقداماتی با رویکرد آموزشی و تربیتی مدنظر قرار می‌گیرد. یکی از این راهکارها، آموزش و توجیه خانواده‌ها در ارتباط با چیستی و چگونگی اتخاذ رویکرد مناسب در مواجهه با فرزندانی است که با فضای سایبری سروکار دارند. از دیگر راهکارهای پیشگیری رشد مدار، آموزش و کمک به کسب مهارت‌های لازم در مدارس به کودکان و نوجوانان است. ازجمله این موضوعات آموزشی می‌توان به تفکر نقادانه و سواد رسانه‌ای اشاره نمود. درنهایت، به نظر می‌رسد پیشگیری از جرم در تارنمای تاریک، ممکن اما نیازمند کار حقوقی و فنی دقیق می‌باشد و لازم است متخصصان این حوزه هم‌پای پیشرفت فناوری اطلاعات و بلکه سریع‌تر و در ضمن تلاش برای بالا بردن اطلاعات و آگاهی خود در زمینه تارنمای تاریک، به ترمیم خلأهای قانونی موجود پرداخته و راهکارهای نوین‌تر و متناسب با فضای تارنمای تاریک را ارائه دهند و از روزآمد کردن آن‌ها غافل نشوند.

فهرست منابع

- انصاری، سعید، سراجی، فرهاد، یوسف‌زاده، محمدرضا. (۱۴۰۰). «چیستی، چرایی و چگونگی آموزش سواد رسانه ای در دوره ی ابتدایی»، فناوری اطلاعات و ارتباطات در علوم تربیتی، تابستان، شماره ۴۴.
- بهره‌مند، حمید، داوودی، ذوالفقار. (۱۳۹۷). «پیشگیری اجتماعی از جرائم امنیتی سایبری»، مطالعات حقوق کیفری و جرم‌شناسی، بهار و تابستان، دوره ۴۸، شماره ۱.
- بهره‌مند، حمید، کوره‌پز، حسین محمد، سلیمی، احسان. (۱۳۹۳). «راهبردهای وضعی پیشگیری از جرائم سایبری» آموزه‌های حقوق کیفری، بهار و تابستان، شماره ۷.
- جایشانکار، کی. (۱۳۹۴). جرم‌شناسی سایبری (بررسی جرم‌شناختی جرائم سایبری)، مهدی مقیمی، چاپ اول، تهران، دانشگاه علوم انتظامی امین.
- جلالی فراهانی، امیرحسین. (۱۳۸۳). «پیشگیری از جرائم رایانه‌ای» حقوقی دادگستری، تابستان، شماره ۴۷.

دانشگاه آزاد اسلامی واحد مراغه

- جلالی فراهانی، امیرحسین، باقری اصل، رضا. (۱۳۸۷). «پیشگیری اجتماعی از جرائم و انحرافات سایبری» مجلس و پژوهش، بهار، شماره ۵۵.
- جندلی، منون. (۱۳۹۳). درآمدی بر پیشگیری از جرم (تعاریف، تاریخچه، رویکردها و دورنما)، شهرام ابراهیمی، چاپ اول، تهران، نشر میزان.
- حیدری نژاد، نصراله. (۱۳۹۷). «پیشگیری وضعی در جرائم سایبری از منظر حقوق کیفری ایران و جهان»، قانون یار، تابستان، دوره ۲، شماره ۶.
- خانعلی‌پور واجارگاه، سکینه. (۱۳۹۰). پیشگیری فنی از جرم، چاپ اول، تهران، نشر میزان.
- رایجیان اصلی، مهرداد. (۱۴۰۱). کلیات جرم‌شناسی: محتوا و تحول؛ از دیروز تا امروز، چاپ اول، تهران، نگاه معاصر.
- زلقی، علی، مالمیر، محمود. (۱۳۹۹). «خلأهای قانونی و اجرایی و راهکارهای پیشگیری از ارتکاب جرائم سایبری»، کارآگاه، پاییز، شماره ۵۲.
- ساریخانی، عادل، سلطانی بهلولی، مریم. (۱۳۹۵). «نقش قوه مجریه در پیشگیری اجتماعی از جرم» حقوقی دادگستری، تابستان، شماره ۹۴.
- صبح دل، محمد. (۱۳۹۶). «جایگاه حقوقی قوه قضاییه در پیشگیری اجتماعی»، قانون یار، زمستان، شماره ۴.
- طهماسبی، جواد، شاهمرادی، خیرالله. (۱۳۹۷). «چالش‌ها و خلأهای موجود در فرایند رسیدگی به جرائم سایبری»، حقوقی دادگستری، زمستان، شماره ۱۰۴.
- علوی‌پور، سید محسن، عسگری، سید احمد، خسروی، علیرضا، سروی زرگر، محمد. (۱۳۹۹). «سیاست‌گذاری سواد رسانه‌ای در ایران: چالش‌ها و ظرفیت‌ها» مطالعات میان‌رشته‌ای در رسانه و فرهنگ، بهار و تابستان، شماره ۱۹.
- Finklea, Kristin. (2017).Dark Web. Congressional Research Service, 10 March, 7-5700.
- Al-Suwaidi, Noura, Nobanee, Haitham, Jabeen, Fauzia. (2018). Estimating Causes of Cyber Crime: Evidence from Panel Data FGLS Estimator. International Journal of Cyber Criminology, Vol 12, No 2.
- Vogt, Sophia Dastagir. (2017). the Digital Underworld: Combating Crime on the Dark Web in the Modern Era. Santa Clara Journal of International Law, Vol 15.
- VILIĆ, Vida M. (2017). Dark Web, Cyber Terrorism and Cyber Warfare: Dark Side of the Cyberspace. Balkan Social Science Review, Vol 10.
- Braga, Romulo Rhemo Palitot, & Luna, Arthur Augusto Barbosa. (2018). Dark web and bitcoin: an analysis of the impact of Digital anonymate and cryptocurrencies in the practice of money laundering crime. Direito Desenvolvimento, Vol 9, No 2.
- O'Brien, M. (2014). The internet, child pornography and cloud computing: the dark side of the web. Information & Communications Technology Law, Vol 23, No 3.
- Goodison, Sean E, Woods, Dulani, Barnum, Jeremy D, Kemerer, Adam R, & Jackson, Brian A. (2020). National Institute of Justice (NIJ), "Taking on the Dark Web: Law Enforcement Experts ID Investigative Needs", 15 June available at https://nij.ojp.gov/topics/articles/taking-dark-web-law-enforcement-experts-id-investigative-needs