Journal iranian political sociology
Vol. 5, No. 2 , Ordibehesht 2022
https://dx.doi.org/10.30510/PSI.2022.277722.1616

Approaches to Reinforcing the Iranian Participatory Criminal policy on computer Crime based on EU Procedure

Navid Deilami Moezzi[1]
Mahdi Esmaeli[2]
Hasan Hajitabar Firouzjaei[3]

Received Date: 2 Jan 2022
Reception Date: 23 Apr 2022

Abstract

NGOs can help governments achieve development goals by attracting public participation and create activity opportunities for different individuals to utilize their capacities to prevent and tackle computer crimes. This study aimed to identify the existing contexts and challenges and propose solutions to reinforce the Iranian participatory criminal policy on computer crimes using the EU procedure. This study is applied research in terms of objectives and uses a descriptive-analytical approach. The findings of this research indicate that reciprocal interaction and participation between governments and NGOs can play an essential role in reinforcing security through prevention and awareness-raising, provided that individuals or groups understand the social need to deal with computer crimes for establishing specialized NGOs in this area. Moreover, developing comprehensive regulations regarding the systematization of these organizations and their computer crime-related activities is necessary. The Iranian civil society, relying on its religious teachings and rich participatory

[1] . Ph.D. student in Criminal Law and Criminology, Department of Law, Ayatollah Amoli Branch, Islamic Azad University (IAU), Amol, Iran
[2] . Assistant Professor, Department of Law, Tehran Central Branch, Islamic Azad University (IAU), Tehran, Iran(correspondling author), Dresmaeli@yahoo.com
[3] . Associate Professor, Department of Law, Qaemshahr Branch, Islamic Azad University (IAU), Qaemshahr, Iran.

culture, has a reasonable potential for crime prevention, which, thus far, has not been optimally fulfilled. The following actions can contribute to the preventative and confrontational efforts against computer crimes and help achieve the desired goals of a participatory criminal policy: modeling the specialized NGOs in the EU and their cooperation with the EU, utilizing the existing experiences, offering public education, and establishing transparent legal regulations for the active participation of Iranian NGOs, as well as trustbuilding activities.

Keywords: Criminal policy; Participatory, computer crimes, European Union, Nongovernmental organization (NGO)

ماهنامه علمی (مقاله علمی-پژوهشی) جامعه‌شناسی سیاسی ایران، سال پنجم، شماره ۲، اردیبهشت ۱٤۰۱ صص ۵۰۹-٤۷۵

https://dx.doi.org/10.30510/PSI.2022.277722.1616

راهکارهای تقویت سیاست جنایی مشارکتی ایران در جرایم رایانه‌ای در پرتو رویهٔ اتحادیهٔ اروپا[۱]

نوید دیلمی معزی[۲]
مهدی اسماعیلی[۳]
حسن حاجی‌تبار فیروزجائی[٤]

تاریخ دریافت: ۱٤۰۰/۱۱/۲
تاریخ پذیرش: ۱٤۰۰/۲/۳

چکیده

سازمان‌های مردم‌نهاد می‌توانند با جلب مشارکت‌های مردمی در رسیدن به اهداف توسعه، دولت را یاری داده و با ایجاد زمینه‌هایی برای فعالیت افراد مختلف از ظرفیت‌های آن‌ها در جهت پیشگیری و مقابله با جرایم رایانه‌ای بهره‌گیرند. پژوهش حاضر با هدف شناسایی بسترها و زمینه‌های موجود، چالش‌های پیش رو و ارائهٔ راهکارهایی در جهت تقویت سیاست جنایی مشارکتی در زمینهٔ جرایم رایانه‌ای در ایران با بهره‌گیری از رویهٔ اتحادیهٔ اروپا صورت گرفته

۱. پژوهش حاضر مستخرج از رساله دکتری اینجانب نوید دیلمی معزی در رشته حقوق کیفری و جرم‌شناسی دانشگاه آزاد اسلامی واحد آیت الله آملی (آمل) با عنوان ((سیاست جنایی جرایم رایانه‌ای در ایران با نگاهی به قوانین اتحادیهٔ اروپا)) با راهنمایی(نویسنده مسئول) آقای دکتر مهدی اسماعیلی و مشاوره آقای دکتر حسن حاجی‌تبار فیروزجائی می‌باشد.

۲. دانشجوی دکتری حقوق کیفری و جرم شناسی، گروه حقوق، واحد آیت ا.... آملی، دانشگاه آزاد اسلامی،آمل،ایران

۳. استادیار گروه حقوق، واحد تهران مرکزی، دانشگاه آزاد اسلامی، تهران، ایران(نویسنده مسئول)
Dresmaeli@yahoo.com

٤. دانشیارگروه حقوق، واحد قائمشهر، دانشگاه آزاد اسلامی، قائمشهر،ایران

است. این پژوهش از نظر هدف، کاربردی و بر اساس روش، تفسیری-کیفی است. یافته‌های پژوهش بیانگر آن است که تعامل دوجانبه و مشارکت میان دولت و سازمان‌های مردم‌نهاد می‌تواند نقش اساسی را در افزایش امنیت از طریق پیشگیری و اطلاع‌رسانی ایفا نماید؛ مشروط بر اینکه افراد یا گروه‌ها نیاز اجتماعی مقابله با این‌گونه جرایم را در جهت تشکیل سازمان‌های مردم نهاد تخصصی در این حوزه به‌طور صحیح درک نمایند. علاوه بر این، باید مقررات جامعی در زمینهٔ فعالیت و ساماندهی این سازمان‌ها در خصوص جرایم رایانه‌ای تدوین گردد. جامعهٔ مدنی ایران با تکیه بر آموزه‌های دینی و فرهنگ غنی مشارکتی خود، از بسترهای مناسبی برای پیشگیری از جرم برخوردار بوده ولی تاکنون از این مبانی و بسترها به نحو مطلوب استفاده نشده است. برای رسیدن به نتیجهٔ مطلوب در زمینهٔ سیاست مشارکتی می‌توان از سازمان‌های مردم‌نهاد تخصصی ایجاد شده و همکاری آن‌ها با اتحادیهٔ اروپا الگوبرداری نموده و با بهره‌گیری از تجربه‌های موجود، آموزش همگانی، تنظیم مقررات حقوقی شفاف جهت مشارکت فعال سازمان‌های مردم‌نهاد داخلی و ایجاد اعتمادسازی به مقابله و پیشگیری از جرایم رایانه‌ای پرداخت.

واژگان کلیدی: سیاست جنایی، مشارکتی، جرایم رایانه‌ای، اتحادیهٔ اروپا، سازمان مردم‌نهاد

مقدمه و بیان مسئله

جرایم رایانه‌ای از جمله جرایم نوظهوری است که مبارزهٔ مؤثّر با آن در پرتو راهبردهای مشارکت فعال جامعهٔ مدنی امکان‌پذیر می‌باشد. وقوع این جرایم منجر به آسیب‌های فرهنگی و سیاسی خواهد شد. در ایران و جوامع اروپایی طی بیست سال گذشته، به‌طور فزاینده‌ای شبکه‌های ارتباطی الکترونیکی و سیستم‌های اطلاعاتی و اینترنت گسترش یافته و تأثیر شگرفی بر تمام بخش‌های جامعه، از جمله حقوق بنیادی، تعاملات اجتماعی و اقتصادی داشته است. در پژوهش حاضر تکیه بر مقابله با جرایم رایانه‌ای بر پایهٔ یکی از شاخه‌های علوم جنایی تجربی یعنی علم سیاست جنایی است.

محور اصلی سیاست جنایی هر کشور، پیشگیری و مقابله با جرایم است (وطنی و اسدی، ۱۳۹۵: ۹۹). سیاست جنایی به انواع تقنینی، قضایی، اجرایی و مشارکتی تقسیم شده و محور این مقاله پیرامون سیاست جنایی مشارکتی می‌باشد. سیاست جنایی مشارکتی بر عملکرد مردم و سازمان‌های مردم نهاد[1] بر امر پیشگیری، کنترل جرم و کمک به دستگاه عدالت قضایی در فرایند دادرسی کیفری و اجرای حکم تأکید دارد.

تحقیق حاضر به این دلیل حائز اهمیت می‌باشد که جرایم رایانه‌ای از جمله مسائلی است که کلیهٔ آحاد جامعه، نهادهای قانون‌گذاری و مجریان قانون به نوعی درگیر آن هستند. این حوزه از جرایم از مسائل جدید در نظام حقوقی ملی و فراملی بوده و در آینده‌ای نه‌چندان دور با حجم انبوهی از جرایم داخلی و برون‌مرزی در این خصوص مواجه خواهیم شد. وقوع جرم در هر جامعه امری است گریزناپذیر و هر قدر که جامعه، قواعدی را برای مقابله با ممنوعیت‌ها وضع نماید و درصدد اعمال آن از طریق سازوکارهای نظارتی و پیشگیرانه باشد، باز هم امکان محو جرم از جامعه وجود ندارد؛ از این رو باید گفت سیاست‌هایی که امروزه در هر جامعه برای مقابله با پدیدهٔ مجرمانه در بخش‌های مختلف تقنینی، قضایی، اجرایی و مشارکتی در

---

۱. اصطلاح «سازمان‌های مردم‌نهاد» توسط فرهنگستان زبان فارسی به‌عنوان معادل اصطلاح لاتین «Non-Governmental Organizations» برگزیده شده و مخفف آن« سمن» است.

مقولهٔ پیشگیری از جرم تدوین و اعمال می‌شود، راهکاری برای مقابلهٔ مدرن با جرایم و اعمال مجازات‌ها است.

یکی از چالش‌های جدید حقوق کیفری مقابله با جرایم رایانه‌ای است. به بیان دیگر با توجه به گستردگی و شبکه‌ای بودن فضای‌سایبر، باید اذعان داشت مقابله با جرایم رایانه‌ای در فضای سایبر به جهت وسعت خسارت و تعدد بزه‌دیدگان، فرامرزی بودن و مشکلات کشف و تعقیب مجرم و بسیاری ویژگی‌های دیگر تنها با یک «راهبرد جنایی مشارکتی» می‌تواندبه گونه‌ای کارآمدو مؤثّرصورت گیرد. آنچه این نظرراتقویت‌می‌کند این است که جرایم سایبری در غیاب جرایم سنتی اتفاق نمی‌افتند و در واقع جایگزین جرایم سنتی نمی‌شوند، بلکه در کنارآن‌هاقرارمی‌گیرند. نتیجه این است که منابع، نیروها و امکانات موجود دستگاه عدالت کیفری دچار فرسایش‌و کمبودشده‌و امکان مواجهه با همهٔ این جرایم از آن‌ها سلب می‌شود.

برای مقابلهٔ همه جانبه و کارآمد با این جرایم، اتخاذ یک سیاست جنایی فراگیر با مشارکت گستردهٔ جامعهٔ مدنی، کاربران‌سایبرو سازمان‌های‌مردم‌نهاد ضروری است. در پرتو یک سیاست جنایی مشارکتی هر یک‌ازاین گروه‌ها باید در مراحل مختلف فرایند جنایی یعنی پیشگیری و مقابله با جرم، کشف جرم و تعقیب‌مجرم، مرحلهٔ‌رسیدگی به جرم و مجازات مجرم نقش‌آفرینی کنند تا ضمن کاستن از باردستگاه‌عدالت‌کیفری به مقابلهٔ هرچه گسترده‌تر و دقیق‌تر با جرم پرداخته شود.

متأسفانه امروزه شاهد هستیم که جرایم رایانه‌ای در فضای مجازی هر روز رو به افزایش است و با وجود قوانین کیفری موجود به نظر می‌رسد که دولت نتوانسته در زمینهٔ سیاست جنایی پیشگیرنده موفق عمل کند و لذا هر ساله شاهد ورود خسارت‌های هنگفت مالی و حیثیتی به اشخاص اعم از حقیقی و حقوقی هستیم. بنابراین اتخاذ یک سیاست جنایی مشارکتی مناسب در جهت کاهش آمار جرایم ارتکابی رایانه‌ای به‌ویژه مطالعهٔ قوانین و سیاست‌های اتحادیهٔ اروپا در این زمینه بسیار مفید به نظر می‌رسد.

هدف اصلی نگارندگان در این نوشتار شناسایی بسترها و جلوه‌های اعمال سیاست جنایی مشارکتی و ارائه راهکار در امر مبارزه با جرایم رایانه‌ای در ایران و بررسی چالش‌ها و موانع فراروی اجرای کارآمد و مؤثر تدابیر این نوع از سیاست جنایی با بهره‌گیری از قوانین و مقررات حاکم در اتحادیهٔ اروپا با پرداختن به دو سؤال اصلی ذیل می‌باشد: ۱- بسترها و زمینه‌های اعمال و اجرای برنامه‌های سیاست جنایی مشارکتی در زمینهٔ جرایم رایانه‌ای در ایران چگونه است؟ ۲- چالش‌های اساسی فراروی اعمال موفقیت‌آمیز برنامه‌های سیاست جنایی مشارکتی در این زمینه کدام است؟ بهره‌گیری از تجربیات و قوانین اتحادیهٔ اروپا در این زمینه چه کمکی می‌تواند به سیاست جنایی ایران نماید؟ در پایان نیز راهکار و راه‌حل‌های منطقی و سازنده جهت رفع و کاهش ایرادات و اشکالات قانونی و عملی و تقویت این نوع سیاست جنایی ارائه خواهد شد.

پژوهش حاضر از نظر هدف، کاربردی و از نظر روش، به صورت تفسیری-کیفی بر پایهٔ گردآوری اطلاعات به صورت کتابخانه‌ای، با استفاده از منابع به بررسی، توصیف و تحلیل ابعاد و زوایای گوناگون موضوع پژوهش پرداخته است. تجزیه و تحلیل اطلاعات جمع‌آوری شده به‌صورت کیفی و مبتنی بر استنتاج محقق از منابع و متون بوده است. در این تحقیق مقررات داخلی در خصوص سیاست جنایی مشارکتی و مقررات اتحادیهٔ اروپا مورد توجه قرار گرفته است. بنابراین، اطلاعات لازم با توجه به موضوع تحقیق به‌وسیلهٔ ابزارهای سنجش کتابخانه‌ای و اسنادی گردآوری شده است. برای بررسی تطبیقی پژوهش، قوانین و کنوانسیون جرائم سایبری به زبان فارسی ترجمه شده‌اند و همچنین مقالات و کتب موجود، مطالعه و اطلاعات گردآوری شده است.

یافته‌های تحقیق

پژوهش حاضر به دنبال ارائهٔ راهکارهای تقویت سیاست جنایی مشارکتی ایران در جرایم رایانه‌ای در پرتو رویهٔ اتحادیهٔ اروپا می‌باشد. یافته‌های پژوهش بیانگر آن است که تعامل دوجانبه و مشارکت میان‌دولت و سازمان‌های مردم نهاد می‌تواند نقش اساسی را در کاهش

جرایم و افزایش امنیت از طریق پیشگیری و اطلاع‌رسانی ایفا نماید؛ مشروط بر اینکه افراد یا گروه‌ها نیاز اجتماعی مقابله با این‌گونه جرایم را در جهت تشکیل سازمان‌های مردم نهاد تخصصی در زمینهٔ جرایم رایانه‌ای جهت مشارکت همگانی در این حوزه به طور صحیح درک و احساس نمایند. علاوه بر این، باید مقررات جامع و کاملی در زمینهٔ فعالیت و ساماندهی این سازمان‌ها در خصوص جرایم فضای مجازی به‌ویژه جرایم رایانه‌ای تدوین گردد.

سیاست جنایی حاکم بر جرایم حوزهٔ سایبر در ایران بیش‌تر متکی به پاسخ‌دهی از طریق دولت با محوریت قرار دادن امنیت ملی می‌باشد. لازم است که رویکردهای نوآورانه مشارکتی برای همکاری و همچنین ایجاد ظرفیت‌سازی در راه مبارزه با جرایم رایانه‌ای در نظر گرفته شود تا تأثیرگذاری آن بیشتر شود. مشارکت‌بخش‌های دولتی، غیردولتی و خصوصی، تنظیم موضوعات حقوقی و شفافیت پیرامون این همکاری نقش اساسی را در کاهش جرایم رایانه‌ای خواهد داشت. اما در مورد چهارچوب قانونی برای تسهیل این موضوع اجماع کمی وجود دارد؛ به‌گونه‌ای که ترس از مسئولیت ناشی از حفاظت از داده‌ها منجر به محدودیت‌های مشارکت و همکاری با بخش خصوصی می‌شود. موضوع دیگر مربوط به عدم تبادل اطلاعات، تخصص و روش‌های مناسب بین بخش دولتی و خصوصی است. اپراتورهای بخش خصوصی غالباً به منظور محافظت از مدل‌ها و اسرار تجاری، تمایل، تعهد قانونی و یا انگیزهٔ داوطلبانه‌ای ندارند که اطلاعات مربوط به وقوع جرم را به مقامات اجرای قانون گزارش داده یا به اشتراک بگذارند.

۱. مبانی نظری

۱-۱. تعریف جرایم رایانه‌ای

مهمترین چالش در خصوص جرایم رایانه‌ای، تعریف آن است. طیف گستردهٔ افعال مجرمانه‌ای که ذیل این مفهوم جا دارند و ماهیت متغیر آن که ناشی از پیشرفت لحظه به لحظهٔ فناوری اطلاعات و شیوه‌های سوءاستفاده از آن است، ارائهٔ تعریف جامع و مانع و خالی از مناقشه را مشکل و چه بسا غیرممکن می‌سازد؛ تا آنجا که در **کنوانسیون جرایم سایبری ۲۰۰۱**

در بوداپست نیز تعریفی از این جرایم به عمل نیامده است. حتی سازمان ملل متحد نیز در نشریهٔ بین‌المللی سیاست جنایی خود بر عدم وجود توافق در **تعریف جرایم رایانه‌ای** تأکید نموده است. در نتیجه می‌توان گفت تعریفی رسمی و بین‌المللی در خصوص جرم رایانه‌ای وجود ندارد (میکولون، ١٣٨٦: ١٨٣).

سازمان ملل متحد در سال ١٩٩٤ در شمارهٔ ٤٤ «نشریهٔ بین‌المللی سیاست جنایی» با اذعان بر اینکه در زمینهٔ جرایم رایانه‌ای تعریف مورد توافق و مشترکی وجود ندارد، جرایم رایانه‌ای را از یک سو شامل فعالیت‌های مجرمانه با ماهیت سنتی مثل سرقت و جعل دانسته که همگی معمولاً در همه جا مشمول ضمانت اجراهای کیفری می‌شوند و از سوی دیگر شامل فعالیت‌های مجرمانهٔ نوینی که در آن‌ها رایانه امکان این‌گونه سوءاستفاده‌ها را مهیا ساخته و پیش از این امکان‌پذیر نبوده است می‌داند (تقی‌زاد و همکاران، ١٣٩٦). در حقیقت سازمان ملل به نوعی از طبقه‌بندی جرایم رایانه‌ای اشاره دارد و نه تعریف جرم رایانه‌ای (باستانی، ١٣٨٣: ٢٢).

در کنگرهٔ دهم سازمان ملل متحد در مورد پیشگیری از جرم نیز جرایم رایانه‌ای در قالب دو تعریف طبقه‌بندی شده‌اند. نخستین تعریف در مفهوم جزایی ارائه شده که شامل هرگونه رفتار مستقیم غیرقانونی به وسیلهٔ عملیات الکترونیکی می‌باشد که امنیت سامانه‌های رایانه‌ای و داده‌های پردازش شده به‌وسیلهٔ آن‌ها را هدف قرار می‌دهد؛ و تعریف دوم در مفهوم کلی یعنی جرم مرتبط را در بر می‌گیرد (بیگی و خوشیاری، ١٣٩٠: ٦). حتی در قانون تجارت الکترونیک نیز اشاره‌ای به جرایم رایانه‌ای نشده و تنها در بند (و) از ماده (٢) به تعریفی از سیستم رایانه‌ای بدین صورت اشاره شده است: «سیستم رایانه‌ای هر نوع دستگاه یا مجموعه‌ای از دستگاه‌های متصل سخت افزاری و نرم افزاری است که از طریق اجرای برنامهٔ پردازش خودکار داده پیام عمل می‌کند». در قانون جرایم رایانه‌ای مصوب خرداد ١٣٨٨ مجلس شورای اسلامی نیز می‌توان جرایم رایانه‌ای را چنین تعریف نمود: هرگونه عمل خلاف قانون که با سوءنیت، از طرف شخص یا اشخاص با بکارگیری از رایانه صورت پذیرد جرایم رایانه‌ای نامیده می‌شود.

۱-۲. تعریف سیاست جنایی مشارکتی[1]

دیر زمانی نیست که گرایش جدید از سیاست جنایی بر پایهٔ مشارکت هرچه وسیع‌تر و فعال ارکان جامعهٔ مدنی به‌ویژه مردم در اجرای سیاست جنایی شکل گرفته است که عبارت از «سیاست جنایی مشارکتی» می‌باشد. این راهبرد سیاست جنایی، بیانگر مشارکت مردم و نهادهای غیررسمی و غیردولتی چه در امر پیشگیری از جرم و چه در واکنش نسبت به جرایم و انحرافات اجتماعی است و هدف مهم آن، تضمین حق امنیت جامعه با ترکیب هوشمندانهٔ پیشگیری و پاسخ‌دهی و بازپروری اجتماعی بزهکاران است. در واقع تأمین امنیت به‌عنوان نتیجهٔ مبارزه با پدیدهٔ مجرمانه، خود هدف عمده‌ای است که با مشارکت مردم تحقق می‌یابد (جمشیدی، ۱۳۹۰: ٢٤). به عبارت دیگر در نظر گرفتن آثار ضرورت حیاتی ایجاد ابزارها و اهرم‌های تقویتی دیگری به غیر از پلیس یا قوهٔ قضاییه به منظور اعتبار بخشیدن به طرح سیاست جنایی است، که به‌وسیلهٔ قوهٔ مجریه و مقننه تهیه و تدوین می‌گردد (عظیم زاده و حسابی، ۱۳۹۰: ۱۲۱). سیاست جنایی مشارکتی خود به دو نوع کنشی یا پیشگیرانه و واکنشی یا پاسخ‌گو تقسیم می‌شود. در نوع اول آن، قبل از اینکه جرمی اتفاق بیفتد دخالت مردم و نهادهای جامعوی قابل مشاهده است و از ظرفیت‌های آن برای جلوگیری از ارتکاب جرم استفاده می‌شود. در جرم‌شناسی به آن پیشگیری اجتماعی گفته می‌شود که بهترین و پایدارترین نوع پیشگیری از جرم می‌باشد. در نوع دوم آن بعد از ارتکاب جرم در حد ممکن، از قابلیت‌ها و توانایی‌های جامعهٔ مدنی برای حل اختلاف استمداد می‌شود و اختلافی که برخاسته از بطن جامعه است، برای رسیدگی نیز همانجا ارجاع داده می‌شود (شیعه علی، زارع و زارع، ۱۳۹۵: ۲۹۳). انجام خدمات عام‌المنفعه به جای مجازات، یکی از جلوه‌های نوین عدالت ترمیمی است. عدالت ترمیمی که به آن، عدالت احیا کننده نیز گفته می‌شود، تفکر جدیدی است که بر ترمیم و مقابله با آثار جرم در جامعه و به‌ویژه از طریق مشارکت ارکان مختلف جامعهٔ مدنی (بزه‌دیده، بزهکار و مردم) تکیه می‌کند (رستمی، ١٣٨٦: ١٥٢). کار عام‌المنفعه در عین حال یکی از مصادیق مهم مشارکت مردم در فرایند اصلاح و درمان بزهکاران می‌باشد که این راهبرد

1. Participatory criminal policy

در خصوص مجرمان رایانه‌ای به جهت برخورداری از تخصص کافی کار با رایانه، بسیار هموار و مساعد است (جمشیدی، ۱۳۹۰: ۲٤۱).

اهمیت سیاست جنایی مشارکتی بدین لحاظ است که قوانین و تدابیری که دولت برای سرکوبی و یا پیشگیری از جرم اتخاذ می‌کند، در صورتی که از سوی مردم حمایت نشود، در معرض خطر عدم اجرا و عدم استقرار قرار می‌گیرد. بکاریا در اهمیت سیاست جنایی مشارکتی این امر را توصیه می‌نماید که برای پیشگیری از وقوع جرم، باید قوانین روشن و ساده‌ای وضع گردد و تمام قدرت ملت برای دفاع از آن بسیج شود و هیچ قدرتی برای نابودی آن به‌کار گرفته نشود (بکاریا، ۱۳۸۵: ۱۳۲).

۳-۱. سازمان‌های مردم نهاد

سازمان‌های مردم نهاد یا سمن به سازمانی اشاره می‌کند که مستقیماً بخشی از ساختار دولت محسوب نمی‌شود اما نقش مهمی به عنوان واسط بین جامعه مدنی و حاکمیت ایفا می‌کند و در نقش ناظری هوشیار از قانون و عدالت پشتیبانی می‌نماید. برطبق آیین‌نامه تشکل‌های مردم نهاد مصوب هیئت وزیران، تشکل‌های مردم نهاد به تشکل‌هایی اطلاق می‌شود که توسط اشخاص حقیقی غیردولتی به‌صورت داوطلبانه با رعایت مقررات تأسیس شده و غیرانتفاعی، غیرسیاسی و عضو پذیر می‌باشد. همچنین می‌توان بیان داشت این تشکل‌ها توسط مردم و برای رفع مشکل اجتماع شکل می‌گیرند. اداره اطلاعات عمومی سازمان ملل نیز این عنوان را به هر سازمان غیردولتی و داوطلبانه‌ای که در سطح محلی، ملی یا بین‌المللی فعالیت داشته و افرادی با علایق مشترک آن را اداره می‌کنند اطلاق می‌نماید (کاملی و رضایی، ۱۳۹۰: ٦٤). از دستاوردهای این سازمان‌ها می‌توان به تقویت سرمایه اجتماعی، تشویق به مشارکت و آموزش عمومی دربارهٔ گستره وسیعی از موضوعات مورد علاقهٔ مردم و حل معضلات اجتماعی، مشارکت گرفتن از نخبگان جهت افزایش آگاهی در جامعه و افزایش همبستگی و تعهدات شهروندان اشاره نمود. نتیجه جذب سرمایه اجتماعی نوعی اطاعت آگاهانه شهروندان نسبت به نظام سیاست مشارکتی مطلوب دولت‌ها در زمینه‌های مختلف خواهد بود (صالحی و همکاران، ۱۳۹٤: ۳۷-۳٦).

۲. جلوه‌های اعمال سیاست جنایی مشارکتی در قبال جرایم رایانه‌ای در حقوق ایران و اتحادیهٔ اروپا

۱-۲. جلوه‌های اعمال سیاست جنایی مشارکتی ایران در جرایم رایانه‌ای

در این سیاست جنایی، برای پیشگیری از جرم و مبارزه با آن از اسباب و وسایل مختلف دولتی و غیردولتی کمک گرفته می‌شود که می‌توان برای اعمال آن، از طرق مختلف مانند فرهنگ‌سازی، آموزش، مفهوم دینی امر به‌معروف و نهی از منکر بهره برد. باید بگوییم سیاست جنایی مشارکتی در میان دستورات اسلام و دستورات قرآن در سورهٔ آل عمران، آیه ۱۰٤ نیز یافت می‌شود (رشادتی، ۱۳۹۰:۳٤٤). امر به‌معروف و نهی از منکر به‌عنوان ابزاری برای نظارت عمومی در راه پیشگیری و بازداشتن مردم از گناه و جرم است. در واقع احکام امر به‌معروف و نهی از منکر با هدف پیشگیری از انحرافات اخلاقی، جرم و گناه در جامعه اسلامی تبیین و در اصل هشتم قانون اساسی به این امر اشاره شده است (چاله چاله، ۱۳۸۷: ٥٤). یکی از طرق نظارت بر این‌گونه جرایم، توسط نهادهای مدنی، اشخاص و با مشارکت مردم که می‌تواند مصداقی از امر به‌معروف و نهی از منکر بوده و موجب پیشگیری از جرایم رایانه‌ای در فضای مجازی شود، مربوط به نظارت بر ورودی‌ها است که سعی بر جلوگیری از دسترسی اشخاص نفوذگر به اطلاعات مالی دارد (اسدی، ۱۳۸٤: ۱٥). مادهٔ ٦٦ قانون آیین دادرسی کیفری مصوب ۱۳۹۲ دربارهٔ سیاست جنایی مشارکتی مواردی را بیان داشته است که تا به‌حال در نظام قضایی ایران توجهی شایسته به آن نشده است و در واقع شاید برای نخستین بار در مرحلهٔ اعلام جرم و بعد از شروع به تعقیب جرم جایگاه ویژه‌ای برای نهادهای اجتماعی حتی غیردولتی تعریف و تعیین نموده است. باید خاطر نشان نمود که این ماده در سال ۱۳۹٤ با اصلاحاتی روبرو گردید. مادهٔ مذکور پس از اصلاحات سال ۱۳۹٤ مقرر داشته است: «سازمان‌های مردم نهادی که اساسنامهٔ آن‌ها در زمینهٔ حمایت از اطفال و نوجوانان، زنان، اشخاص بیمار و دارای ناتوانی جسمی یا ذهنی، محیط‌زیست، منابع طبیعی، میراث فرهنگی، بهداشت عمومی و حمایت از حقوق شهروندی است، می‌توانند نسبت به جرایم ارتکابی در زمینه‌های فوق اعلام جرم کنند و در تمام مراحل دادرسی شرکت نمایند.». براساس مادهٔ ٦٦، نقش متمایز و متفاوتی برای

مشارکت سازمان‌های غیردولتی تهیه و تدارک دیده شده است. در تبصرهٔ ۲ مادهٔ فوق‌الذکر نیز چنین آمده است: «ضابطان دادگستری و مقامات قضایی مکلفند بزه‌دیدگان جرایم موضوع این ماده را از کمک سازمان‌های مردم نهاد مربوطه، آگاه کنند.» از این تبصره نیز چنین بر می‌آید که نقش این نهادهای اجتماعی و غیردولتی و البته غیرقضایی در زمینهٔ اعلام جرم و حتی تعقیب جرم تا بدان حد اساسی و تعیین‌کننده در نظر گرفته شده است که حتی اگر جرمی از جرایم موضوع این ماده که همگی جزو جرایم با آثار اجتماعی (به‌ویژه نسبت به بخش آسیب‌پذیر جامعه) به شمار می‌روند، بدون اطلاع نهادها و سازمان‌های مذکور در مادهٔ فوق صورت بگیرند و توسط حتی نهادهای قضایی (از جمله ضابطان دادگستری) کشف گردند، باز هم باید بدین نهادها در این زمینه اطلاع‌رسانی صورت گرفته و آن‌ها را نیز در تعقیب و تحقیق کیفری عاملان ارتکاب این جرایم سهیم و شریک کرد (شیعه علی، زارع و زارع، ۱۳۹٤: ۲۹٦-۲۹٤). یکی از نمودهای سیاست جنایی مشارکتی در زمینهٔ جرایم رایانه‌ای در فضای مجازی، کاستن از اختیارات نهادهای دولتی و نظارتی در امر فیلترینگ و تفویض حداقل قسمتی از این امر به برخی از شهروندان و کاربران شریف فضای مجازی، که رویکردی سنجیده و ملایم‌تر نسبت به مسئله فیلترینگ دارند، می‌باشد. این امر موجب افزایش دقت و هوشمندی سامانه‌های فیلترکننده برای اجتناب از اشتباه در فیلترینگ نیز می‌شود. نمونهٔ دیگری از سیاست جنایی مشارکتی در جرایم رایانه‌ای رعایت ادب و نزاکت در اتاق گپ و گفت‌وگو است که در صورت عدم پایبندی به آن، کاربران دیگر، شخص هنجارشکن را از ادامهٔ حضور در اتاق گپ محروم می‌کنند (حاجی ده‌آبادی، سلیمی، ۱۳۹۳: ۸۳-۸۲) سیاست جنایی حاکم بر جرایم این حوزه در ایران بیش‌تر متکی به پاسخ‌دهی از طریق دولت با محوریت قرار دادن امنیت ملی بوده هر چند با اعمال تدابیری در خصوص تفتیش و توقیف داده‌های رایانه‌ای و مخابراتی حساسیت‌هایی را به‌منظور حفظ حریم خصوصی شهروندان ابراز نموده است اما طی دهه‌های اخیر کانون حوزهٔ مطالعاتی امنیت حول «امنیت انسانی» با محوریت حفظ امنیت بهداشت و سلامت، اقتصادی و حقوق سیاسی و مدنی شهروندان بوده لذا بازتاب رویکردهای امنیت‌مدار در عصر حاضر سبب می‌شود تا سیاست جنایی در چالش با قواعد حقوق بشر قرار گیرد. این

در حالی است که دولت می‌توانست در حوزهٔ فضای مجازی با واگذاری بخشی از اختیارات خود به کاربران و نهادهای غیردولتی بهتر و مطلوب‌تر این حوزه را مدیریت نماید. و از این رهگذر عدالت و نظم اجتماعی در جامعه به نحوه شایسته‌تری تأمین گردد (بابایی، صدیق‌نژاد، ١٣٩٦).

در برنامه‌های پیشگیری با توجه به تنوع علل ایجاد جرم، مشارکت تمامی افراد و نهادهایی که در زمینهٔ پیشگیری از جرم دارای مهارت و مسئولیت هستند امری اجتناب‌ناپذیر است. به همین دلیل برنامهٔ پیشگیری را نمی‌توان در یک وزارتخانه، سازمان یا نهاد خاصی محدود ساخت. وزارتخانه‌های مختلف، مقامات، نهادهای محلی، سازمان‌های غیردولتی، تجار و شهروندان، همه و همه باید با همکاری یکدیگر برنامه‌های پیشگیری را به اجرا درآورند (جوان جعفری و سیدزاده‌ثانی، ١٣٩١: ٢٨٦). در راستای پیشگیری از جرایم فضای مجازی در ایران مرکز ماهر (مرکز مدیریت امداد و هماهنگی عملیات رخداد) و مرکز آپا (مرکز آگاهی رسانه، پشتیبانی و امداد رایانه‌ای) تأسیس شده‌اند. مرکز ماهر در سال ١٣٨٥با هدف اصلی تأمین امنیت اطلاعات ایجاد شد، با این حال تاکنون اقدامی فنی از سوی این مرکز جهت حفاظت مطلق از اطلاعات صورت نگرفته است. عمدهٔ اقدامات این مرکز تدابیر پیشگیرانه از جمله هشداردهی و آگاه سازی عمومی جهت حفاظت از اطلاعات مربوط به حریم خصوصی شهروندان است[1]. مرکز آپا نیز مرکزی دانشگاهی است که از سال ١٣٨٦ فعالیت خود را زیر نظر دانشگاه امیر کبیر با هدف ارتقا آگاهی و درک مسائل مرتبط با امنیت اطلاعات در میان کاربران و سرویس دهندگان فضای مجازی آغاز نمود[2]. این مراکز می‌توانند در راستای سیاست جنایی مشارکتی با اقداماتی همچون آگاهی رسانی و تشویق جامعه در جهت ایجاد تشکل‌های مردم نهاد فعال در حوزه جرایم رایانه‌ای در فضای مجازی، انتقال دانش از طریق برگزاری دوره‌های آموزشی و همچنین برگزاری نشست، سمینار و همایش در راستای پیشگیری و مقابله با حوادث فضای مجازی نقش مؤثرتری را در زمینه ایفا نمایند.

---

1. https://cert.ir/about
2. https://apa.aut.ac.ir

با بررسی ابعاد مختلف این موضوع، متأسفانه به‌طور رسمی اسامی سازمان‌های مردم‌نهاد فعال در زمینهٔ پیشگیری از جرایم رایانه‌ای و مقابله با آن در دسترس نیست ولی می‌توان به منظور بهبود کارکردهای سیاست جنایی مشارکتی در ایران موارد ذیل را بیان نمود:

دانشگاه علاوه بر بعد آموزشی، می‌تواند در زمینه‌های دیگر و به شیوه‌ای متفاوت در این راستا ایفای نقش نماید. به‌عنوان مثال، واحد جرایم سایبری پلیس می‌تواند به‌ازای همکاری و در اختیار داشتن فضای دانشگاه و نیروی متخصص آن‌ها، مجرمان سایبری را مدتی در اختیار گروه علوم کامپیوتر یا دیگر گروه‌های مرتبط دانشگاه قرار دهد تا دانشجویان آن‌ها ضمن تحقیق و بررسی مجرمان مذکور به کسب تجربه و دانش در خصوص جرایم سایبری بپردازند (Wexler, 2014:27). مورد دیگر، همکاری با شرکت‌های خصوصی است که گامی بزرگ در راستای بهره‌برداری از منابع بالقوهٔ محلی به‌منظور کشف، مقابله و پیشگیری از جرایم سایبری به حساب می‌آیند. آموزش خانواده ها و عموم مردم، از دیگر موارد مهم در این زمینه است. برای استفاده از اینترنت و حضور در فضای سایبر، آموزش ضروری است (Forbs, 2013). بخشی از تأمین امنیت فضای سایبر برعهدهٔ خود کاربران بوده و بخش دیگر آن بر عهده پلیس. کاربران اینترنتی باید به‌منظور پیشگیری از قربانی شدن در دام جرایم سایبری، آموزش‌های لازم در زمینهٔ استفاده ایمن از اینترنت را دریافت و سپس اقدام به ایمن‌سازی رایانهٔ خود نمایند. پلیس فتا نیز می‌تواند از طریق آموزش مردم به‌طور عمومی و به همهٔ اقشار و رده‌های سنی جامعه دربارهٔ چگونگی استفاده ایمن از اینترنت و خطرات فضای سایبر، وظیفهٔ خود را در زمینهٔ پیشگیری ایفا نماید. در این راستا می‌توان از طرح‌های پیشنهادی زیر استفاده نمود:

الف- طرح انجمن آموزش ایمنی سایبری

انجمنی که می‌تواند صرفاً از نیروهای متخصص پلیس به‌منظور آموزش بهره ببرد و یا اینکه با سایر ارگان‌ها و سازمان‌ها در این زمینه همکاری کند که قطعاً گزینهٔ بهتر و مناسب‌تری می‌باشد. چنین انجمنی می‌تواند به برگزاری کلاس‌های آموزشی برای عموم مردم و آگاه‌سازی آن‌ها در دو حوزهٔ خطرات فضای سایبر و چگونگی ایمن کردن این محیط اقدام نماید و نیز

می‌تواند با نشر اطلاعات و برگزاری سخنرانی‌هایی در تمامی سازمان‌ها، ارگان‌ها و شرکت‌های بخش خصوصی و دولتی مانند بانک‌ها، شرکت‌های تجاری و ... زمینهٔ آموزش‌های لازم را فراهم نماید.

ب- مصاحبه با قربانیان سایبر

پلیس می‌تواند با استفاده از این استراتژی و قرار دادن این مصاحبه‌ها در اختیار مردم، انواع جرایم سایبری، چگونگی گرفتاری در دام آن‌ها و عواقب و خطرات ناشی از آن را برای عموم جامعه ملموس نموده و در نتیجه انگیزهٔ آموزش و ایمن‌سازی این محیط را در آن‌ها ایجاد نماید (Wexler, 2014:34).

ج- طرح آموزش بزرگسالان و سالمندان

باید خاطر نشان ساخت که آموزش و آگاه‌سازی افراد بزرگسال از خطرات و آسیب‌پذیری‌های این دنیای جدید امری ضروری است. چرا که بخش بزرگی از بزه‌دیدگی جرایم رایانه‌ای بخاطر ناآشنایی یا کمی آگاهی از فضای تبادل اطلاعات می‌باشد (جلالی فراهانی، ۱۳۸۳: ۱۰۳). به‌عنوان مثال در آمریکا اخیراً افراد مسن و بزرگسالان هدف جرایم سایبری قرار گرفته‌اند به این دلیل که آن‌ها تمایلی به مهارت‌آموزی و کسب اطلاعات دربارهٔ کامپیوتر ندارند. شاید شما هم در خیابان با افراد مسنی که تقاضای برداشت یا انتقال پول از دستگاه‌های خودپرداز را دارند، برخورد کرده باشید، چیزی که به راحتی زمینهٔ ارتکاب جرایم سایبری را فراهم نموده و البته به‌همان سادگی و با فرا گرفتن اطلاعات اندکی به‌راحتی قابل پیشگیری می‌باشد.

د- آموزش دانش‌آموزان و دانشجویان

چنین آموزش‌هایی می‌تواند در سطوح مختلف و در سراسر کشور توسط پلیس و با هماهنگی مدارس و دانشگاه‌ها در قالب برنامه‌های درسی، برگزاری سخنرانی‌ها برای مدیران، معلمان مدارس، کارکنان، اساتید و دانشجویان دانشگاه‌ها، کارگاه‌های آموزشی، چاپ و نشر مواد فرهنگی از طریق بروشور، برچسب و پوستر انجام شود (فهیمی، ۱۳۸۰: ۱۰۵). نباید

فراموش کرد که ما در حال پرورش نسلی دیجیتال هستیم و نوجوانان و جوانان ما در خط مقدم حملهٔ مجرمان سایبری قرار گرفته‌اند (Wexler, 2014:35).

ه- آموزش والدین

کارشناسان پلیس فتا بیان نموده‌اند که در همهٔ کشورهای پیشرفته سالیان سال است که والدین به کمک نرم‌افزارهای ویژه فعالیت فرزندان خود را در اینترنت کنترل می‌کنند، اما در کشور ما نظارت چندانی بر این موضوع وجود ندارد؛ زیرا بسیاری از والدین ایرانی در سطح پایین‌تری از اطلاعات نسبت به فرزندانشان قرار دارند؛ به‌عبارتی والدین ما دچار فقر یا کم‌سوادی سایبری می‌باشند و کارشناسان با تأکید بر اهمیت یادگیری علوم کامپیوتری از سوی والدین اظهار کردند: احتیاجی نیست که والدین تبدیل به یک نفوذگر رایانه‌ای شوند، فقط کافی است در زمینهٔ علوم کامپیوتری اطلاعاتی مفید و ضروری داشته باشند، تا آن حد که شکاف اطلاعاتی میان آن‌ها و فرزندانشان کاهش یافته و محدودتر شود. در زمینهٔ آموزش والدین نیز پلیس فتا می‌تواند با هماهنگی مدارس اقدام به برگزاری دوره‌های آموزشی، سخنرانی‌ها ، چاپ و نشر کتب و بروشور، دسترسی به نرم‌افزارهای کنترل و آموزش کار با آن‌ها و ... نماید (پلیس فتا، ۱۳۹۳).

۲-۲. جلوه‌های اعمال سیاست جنایی مشارکتی جرایم در اتحادیهٔ اروپا

امنیت سایبری در اتحادیهٔ اروپا یک بعد آموزشی قوی دارد؛ رویهٔ آن‌ها بدین گونه است که این آموزش تنها منحصر به متخصصان فناوری اطلاعات نباشد بلکه بر اساس راهنمایی‌های مرکز تحقیقات و صلاحیت امنیت سایبری و آژانس امنیت شبکه و اطلاعات اروپا، باید در برنامه‌های درسی سایر حوزه‌ها از جمله مهندسی، مدیریت بازرگانی، حقوق و... بخش اصلی باشد. علاوه بر این توجه و مشارکت ویژهٔ معلمان و دانش آموزان در دوره‌های ابتدایی و متوسطه نسبت به امنیت سایبری مورد تأکید قرار گرفته است (کمیسیون اروپا، ۲۰۱۷). اتحادیهٔ اروپا باید از محیط آنلاین که بالاترین آزادی و امنیت را برای منافع همه فراهم می‌کند، محافظت نماید. این استراتژی ضمن اذعان به اینکه عمدتاً مقابله با چالش‌های امنیتی وظیفهٔ کشورهای عضو است، اقدامات خاصی را پیشنهاد می‌دهد که می‌تواند عملکرد کلی اتحادیهٔ

اروپا را ارتقا بخشد. این اقدامات کوتاه مدت و بلند مدت بوده، شامل ابزارهای متنوعی برای سیاست‌گذاری هستند و انواع مختلفی از بازیگران را شامل می‌شوند، خواه مؤسسات، صنعت یا کشورهای عضو باشند. چشم انداز اتحادیهٔ اروپا در این پنج راهبرد اساسی بیان شده است: دستیابی به تاب‌آوری سایبری، کاهش شدید جرایم اینترنتی، توسعهٔ سیاست دفاع سایبری و توانایی‌های مربوط به سیاست مشترک امنیتی و دفاعی، توسعه منابع صنعتی و فناوری برای امنیت سایبری، ایجاد سیاست منسجم بین‌المللی فضای مجازی و ارتقا ارزش‌های اصلی اتحادیهٔ اروپا. برای ارتقا تاب‌آوری سایبری در اتحادیهٔ اروپا، هم مقامات دولتی و هم بخش‌خصوصی باید توانایی‌های خود را توسعه دهند و به‌طور مؤثر همکاری کنند. اروپا بدون تلاش قابل توجهی برای ارتقا ظرفیت‌ها، منابع و فرایندهای عمومی و خصوصی برای جلوگیری، کشف و رسیدگی به حوادث امنیتی در فضای مجازی، آسیب‌پذیر خواهد ماند. به همین دلیل کمیسیونی را در زمینهٔ امنیت شبکه و اطلاعات تدوین کرده است. آژانس امنیت شبکه و اطلاعات اروپا[1] در سال ۲۰۰٤ تأسیس شد. این آژانس به عنوان نقطه کانونی برای کسب اطلاعات و دانش در جامعه امنیت سایبری عمل کرده و برای تقویت و مدرن‌سازی در رابطه با امنیت شبکه و اطلاعات، مقررات جدیدی را برای دستیابی به انعطاف‌پذیری و کاهش جرایم در فضای مجازی پیشنهاد نمود. اساس این مقررات بر پایهٔ افزایش آگاهی و ترویج فرهنگ امنیت شبکه و اطلاعات به نفع شهروندان، مصرف کنندگان، شرکت‌ها و سازمان‌های بخش عمومی در اتحادیهٔ اروپا بود. این برنامه در راستای توسعهٔ سیاست مشارکتی اتحادیهٔ اروپا با ایجاد همکاری داوطلبانه بین نهادهای عمومی و ذی‌نفعان اجرا می‌شود. همچنین همکاری با سایر نهادهای اتحادیه در سطح بین‌المللی که به نحوی با این موضوع سر و کار دارند را مدنظر قرار می‌دهند. آژانس امنیت و اطلاعات و شبکه اروپا از سال ۲۰۱۳ کمپینی را که هر ساله در ماه اکتبر به منظور حمایت از اتحادیهٔ اروپا در جهت آگاهی از امنیت فضای مجازی و احساس مسئولیت مشترک در قبال شهروندان برای رفتار ایمن و آگاهانه در فضای مجازی با همکاری شرکای مختلف در کشورهای عضو اتحادیه، کمیسیون اروپا و مرکز مبارزه

1. European Union Agency for Cybersecurity (ENISA)

با جرایم رایانه‌ای اروپا برگزار می‌شود را هماهنگ می‌کند (شبکه پیشگیری از جرم اروپا، ۲۰۱۸ و Vogel, 2007: 8). علاوه بر این، دستورالعملی برای ارائه‌دهندگان ارتباطات الکترونیکی تدوین شد که آنها را به همکاری و مدیریت مناسب خطرات شبکه‌های خود و گزارش تخلفات امنیتی ملزم می‌کند. همچنین، قانون حفاظت از داده‌های اتحادیهٔ اروپا برای اطمینان از الزامات حفاظتی داده‌ها در زمینهٔ خدمات الکترونیکی، کنترل کننده‌های داده را ملزم می‌نماید حوادث مربوط به نقض اطلاعات شخصی را به مقامات صالح اطلاع دهند. البته علیرغم پیشرفت مبتنی بر تعهدات داوطلبانه در اتحادیهٔ اروپا هنوز شکاف‌هایی از نظر توانایی‌های ملی، هماهنگی در موارد حوادث فرامرزی و همچنین مشارکت و آمادگی بخش خصوصی وجود دارد. با این وجود، تهمیداتی جهت آمادگی برای مبارزه با این جرایم همانند تمرینات عملیاتی مشارکتی مربوط به حوادث سایبری در سطح اتحادیهٔ اروپا برای شبیه‌سازی همکاری بین کشورهای عضو و بخش خصوصی در دستورکار اتحادیهٔ اروپا قرار دارد. افزایش آگاهی یکی از زمینه‌هایی است که اتحادیهٔ اروپا به‌منظور مشارکت کاربران در بالابردن امنیت سایبری و کاهش جرایم اینترنتی از طریق انتشار گزارش‌ها، تشکیل کارگاه‌های تخصصی و توسعه مشارکت‌های عمومی و خصوصی در پیش دارد و شایان ذکر است یوروپل و یوروجاست و مقامات ملی حفاظت از داده‌ها نیز در زمینه افزایش آگاهی فعال هستند. اتحادیه اروپا اقدامات عملی دیگری نیز در این خصوص انجام داده است. از جمله بین سال‌های ۱۹۹۹ تا ۲۰۰۲ در قالب برنامه اجرایی اینترنت امن‌تر، ۲۵ میلیون یورو برای کمک به اداره بهتر اینترنت توسط کاربران معمولی برای حفاظت از فرزندانشان در محیط مجازی اختصاص داد. نسخه‌های بعدی این برنامه نیز موفق بوده و آخرین نسخه تا پایان سال ۲۰۰۸ اجرایی شد. در نسخه‌های جدیدتر، این برنامه بر ارتقا شبکه‌سازی به منظور تشویق مردم به مشارکت در تالارهای گفتگوی مجازی در مورد اینترنت امن‌تر، ارتقای سامانه‌های مسدودسازی و آگاهی دادن به والدین، معلمان و کودکان در مورد قابلیت‌ها و خطرات بالقوه اینترنت و تبادل تجربیات همه جانبه با آن‌ها تأکید شده است (عاملی و حسنی، ۱۳۹۱: ١٤-١٣). علاوه بر این سازمان‌های مردم نهادی نیز در زمینهٔ امنیت فضای مجازی فعالیت می‌نمایند که عبارتند از:

الف- کارگروه ضد فیشینگ[1]

این کارگروه، یک اتحادیهٔ صنعت بین‌المللی است که از طریق مبارزه با فعالیت‌های متقلبانه در فضای مجازی و جعل ایمیل از طریق ارائه، گسترش و توسعهٔ داده‌های استاندارد و مدلی از سیستم‌های پاسخ و پروتکل‌ها اقدام می‌کند.

ب- اسپم هاوس[2]

این سازمان بین‌المللی غیرانتفاعی، مستقر در لندن و ژنو، تهدیدهای سایبری (اسپم، فیشینگ، نرم‌افزارهای مخرب و بات‌نت‌ها) را ردیابی نموده و به‌صورت واقعی، اطلاعات تهدیدی عملی را برای اپراتورهای شبکه، شرکت‌ها و فروشندگان امنیتی فراهم می‌کند. همچنین با سازمان‌های اجرای قانون در سراسر جهان برای شناسایی منابع اسپم و بدافزار همکاری می‌نماید.

ج- اتحادیهٔ سازمان‌های غیردولتی اروپا برای ایمنی کودک آنلاین[3]

این اتحادیه توسط کمیسیون اروپا، تأمین مالی شده، بازوی اجرایی اتحادیهٔ اروپا بوده و بستری برای محافظت از کودکان در سرتاسر اروپا فراهم می‌کند تا تخصص و بهترین روش‌ها را در زمینهٔ سیاست‌های مربوط به ایمنی کودکان به‌صورت آنلاین به اشتراک بگذارد.

د- انجمن بین‌المللی خطوط ویژهٔ تلفن اینترنت[4]

یک شبکه جهانی مشارکتی از سازمان‌های غیرانتفاعی است که برای مقابله با توزیع آنلاین تصاویر مستهجن کودکان از طریق ایجاد خطوط ویژه برای گزارش محتوای غیرقانونی تلاش می‌کنند.

ه- مرکز تماشای اینترنت[5]

1. APWG
2. Spamhaus
3. European NGO Alliance for Child Safety Online (eNACSO)
4. International Association of Internet Hotlines (INHOPE)
5. Internet Watch Foundation (IWF)

یک شرکت غیرانتفاعی با تأسیس بریتانیا و مستقر در انگلیس است که برای شناسایی، یافتن و حذف تصاویر و فیلم‌های آنلاین سوءاستفادهٔ جنسی از کودکان با همکاری آژانس‌های اجرای قانون در سراسر جهان کار می‌کند.

و- شرکت رند[1]

این اتاق فکر مستقل، که به کیفیت و استحکام محصول کار خود مشهور است، منبع خوبی برای تحقیقات معتبر و تفسیر آگاهانه است (قانون جورج تاون، ۲۰۲۰).

ز- سازمان امنیت سایبری اروپا[2]

سازمانی کاملاً شخصی و غیرانتفاعی که در ژوئن ۲۰۱٦ طبق قانون بلژیک تأسیس شد. این سازمان نمایندهٔ قراردادی کمیسیون اروپا برای اجرای مشارکت قراردادی عمومی و خصوصی امنیت فضای مجازی است. اعضای این سازمان شامل طیف گسترده‌ای از سهامداران مانند شرکت‌های بزرگ، شرکت‌های نوپا، مراکز تحقیقاتی، دانشگاه‌ها، کاربران نهایی، اپراتورها، انجمن‌ها و همچنین دولت‌های محلی، منطقه‌ای و ملی کشورهای عضو اتحادیهٔ اروپا، کشورهای عضو منطقهٔ اقتصادی اروپا و اتحادیهٔ تجارت آزاد اروپا و دیگر کشورهای مرتبط است. هدف این سازمان ارتقا تحقیقات و نوآوری در امنیت فضای مجازی با پیشنهاد یک برنامه استراتژیک و ارائه نقشه راه چند ساله با بروزرسانی‌های منظم در جهت افزایش و تقویت امنیت فضای مجازی در اروپا است[3].

مقامات دولتی اروپا همچنین معتقدند که تقویت بخش مالی نیز در همکاری بخش دولتی با بخش خصوصی، از جمله صنعت و جامعه مدنی جهت مقابله مؤثر با جرایم سایبری دارای اهمیت ویژه‌ای است. برخی از کشورهای عضو اتحادیه اروپا در همین زمینه گام‌هایی اساسی برداشته‌اند. به عنوان نمونه در هلند، مؤسسات مالی و مقامات اجرای قانون در کنار هم برای رفع کلاهبرداری آنلاین و جرایم اینترنتی در گروه ویژهٔ جرایم الکترونیکی کار می‌کنند (کمیسیون اروپا، ۲۰۱۷: ١٦).

1. The Rand Corporation
2. European Cyber Security Organisation (ECSO)
3. https://www.ecs-org.eu/about

۳. چالش‌های فراروی سیاست جنایی مشارکتی ایران در قبال جرایم رایانه‌ای و راهکارهای مقابله با آن در پرتو اتحادیهٔ اروپا

سازمان‌های مردم نهاد در راستای عملکرد خود با مشکلات و موانعی روبرو هستند. نا آگاهی جامعه نسبت به کارکردهای سازمان‌های مردم نهاد، ویژگی‌هایی چون داوطلبانه بودن، استقلال از دولت و مشکلات مالی روند کند فعالیت‌های این سازمان‌ها را تشدید می‌نماید. نداشتن سازمان‌دهی، نبود عملکرد حرفه‌ای، ساختار سازمانی نامناسب و کلاً فقدان نظم و ترتیب در این نهادها، عدم ارتباط سازمان‌های مردم نهاد با یکدیگر جهت استفاده از تجارب، باور ضعیف دولت از نقش سمن‌ها، همچنین دشواری کسب مجوز توسط سازمان‌های غیردولتی در کشور ما از جمله موانع پیش‌روی سازمان‌های مردم نهاد در رسیدن به اهداف سیاست جنایی مشارکتی ایران در مبارزه با جرایم رایانه‌ای در فضای مجازی محسوب می‌شوند.

یکی از چالش‌های جدید حقوق کیفری، مقابله با جرایم رایانه‌ای در فضای مجازی است. مشکلات کشف و تعقیب مجرم و بسیاری ویژگی‌های دیگر تنها می‌تواند با یک «راهبرد جنایی مشارکتی» به‌صورت کارآمد و مؤثر انجام گیرد (جوان جعفری، ۱۳۸۵: ٢٦). برای مقابلهٔ همه‌جانبه و کارآمد با این جرایم، اتخاذ یک سیاست جنایی فراگیر با مشارکت گستردهٔ جامعهٔ مدنی، کاربران سایبر، سازمان‌های مردم‌نهاد و به ویژه دولت ضروری است. در پرتو یک سیاست جنایی مشارکتی هریک از این گروه‌ها باید در مراحل مختلف فرایند جنایی یعنی پیشگیری و مقابله با جرم، کشف جرم و تعقیب مجرم، مرحلهٔ رسیدگی به جرم و مجازات مجرم نقش‌آفرینی کنند تا ضمن کاستن از بار دستگاه عدالت کیفری به مقابلهٔ هرچه گسترده‌تر و دقیق‌تر با جرم پرداخته شود. یکی از نمودهای سیاست جنایی مشارکتی در زمینهٔ جرایم رایانه‌ای در فضای تبادل اطلاعات، کاستن از اختیار نهادهای دولتی و نظارتی در امر فیلترینگ و تفویض حداقل قسمتی از این امر به برخی شهروندان و کاربران شریف فضای سایبر می‌باشد. قانون‌گذار کیفری باید با به رسمیت شناختن عرف‌های مطلوب موجود در عرصهٔ مجازی، زمینهٔ مشارکت اجتماعی شهروندان اینترنت را در ساماندهی این فضا فراهم آورد. باید

بپذیریم که هیچ سیاستی در قبال جرایم رایانه‌ای بدون مشارکت تمام بخش‌های درگیر یعنی حکومت، بخش خصوصی، جامعه و به‌طور کلی، تمام کسانی که به‌نحوی از فضای سایبر ذی‌نفع و متأثر می‌باشند، قابلیت اجرا و تداوم نخواهد داشت. بنابراین قانون‌گذار در فضای سایبر با اتخاذ راهبرد «سیاست جنایی مشارکتی» در کلیهٔ مراحل و حتی بازپروری مجرم بسیار مؤثر می‌باشد. لذا مقنن باید به گونه‌ای قانون‌گذاری نماید که در هر یک از این مراحل امکان بهره‌گیری از مشارکت مردم و سازمان‌های مردم‌نهاد وجود داشته باشد و از بار دستگاه عدالت کیفری تا حد امکان بکاهد (حاجی ده‌آبادی و سلیمی، ۱۳۹۳: ۸۳).

با نگاهی به قوانین و مقررات، می‌توان به این نتیجه رسید که در قوانین فراتقنینی ایران رویکرد مثبتی نسبت به مشارکت مردم، با قالب‌های مختلف و در عرصه‌های متنوع اجتماعی، وجود دارد و حتی می‌توان گفت که یکی از دلایل وقوع انقلاب اسلامی در ایران، همان‌طور که مقدمهٔ قانون اساسی نیز بر آن تأکید دارد، ضرورت مشارکت مردم در کلیهٔ عرصه‌های اجتماعی و تعیین سرنوشت خویش است.

با این حال با وجود چنین بستر مناسبی تا به حال قوانین و مقررات تقنینی و فروتقنینی جامع و کاملی جهت پیاده کردن اصول قانون اساسی در زمینهٔ مشارکت مردم و سمن‌ها در زمینهٔ پیشگیری از جرم به خصوص در موضوع جرایم رایانه‌ای وضع نشده است. شاید بتوان دلیل این امر را از یک‌سو، نبود سیستم جامع و هماهنگ مدیریت پیشگیری از جرم و از سوی دیگر در روابط شکنندهٔ دولت‌ها با سمن‌ها جستجو کرد (بابایی و صفائی آتشگاه، ۱۳۹۳: ۱۰۱).

چالش‌های مهم در سیاست جنایی مشارکتی جرایم رایانه‌ای را می‌توان به شرح ذیل بیان نمود:

۱-۳. چالش‌های اجتماعی و فرهنگی

در خصوص چالش‌های اجتماعی و فرهنگی، دو عامل مهم را می‌توان برشمرد که عبارتند از سطح پایین دانش عمومی در زمینهٔ فناوری اطلاعات و ارتباطات و عدم اعتماد عمومی در مورد امنیت اطلاعات (حسن بیگی، ۱۳۸٤: ۸)، عدم آموزش به کودکان و نوجوانان در زمینهٔ

شیوهٔ استفادهٔ درست از رایانه و اینترنت و آشنا نمودن آن‌ها با خطرات فنی (هک) و عدم توجه به پیشگیری رشدمدار یک چالش بزرگ است.

امنیت اطلاعات و ایمن‌سازی شبکه‌های کامپیوتری را نمی‌توان مختص یک فرد یا سازمان در نظر گرفت. پرداختن به مقولهٔ امنیت اطلاعات و ایمن‌سازی شبکه‌های کامپیوتری در هر کشور، مستلزم توجه تمامی کاربران و نهادها صرف‌نظر از موقعیت شغلی و سنی به جایگاه امنیت اطلاعات و ایمن‌سازی شبکه‌های کامپیوتری بوده و می‌بایست به این مقوله در سطح کلان و از بعد منافع ملی و فراملی نگاه کرد. وجود ضعف امنیتی در شبکه‌های کامپیوتری و اطلاعاتی، عدم آموزش و توجیه صحیح تمامی کاربران، عدم وجود دستورالعمل‌های لازم برای پیشگیری از نقایص امنیتی، عدم وجود سیاست‌های مشخص و مدون به‌منظور برخورد مناسب و به‌موقع با اشکالات امنیتی، مسائلی را به‌دنبال خواهد داشت که ضرر آن متوجهٔ تمامی کاربران کامپیوتر در یک کشور شده و عملاً زیرساخت اطلاعاتی یک کشور را در معرض آسیب و تهدید جدی قرار می‌دهد (پورتال امنیت و فضای مجازی، ۱۳۹۷). راهکار برون رفت از این چالش را می‌توان در توجه به پیشگیری رشدمدار و جایگاه و نقش سازمان‌های مردم‌نهاد در حوزهٔ آموزش جست و جو نمود.

۲-۳. عدم توجه به جلوه‌های پیش‌بینی شده در دین اسلام

بارزترین جلوهٔ دستورات قرآن در این زمینه که از فروع دین اسلام نیز به شمار می‌رود، دستور امر به‌معروف و نهی از منکر است (رشادتی، ۱۳۹۰: ٣٤٤). امر به‌معروف و نهی از منکر به‌عنوان ابزاری برای نظارت عمومی در راه پیشگیری و بازداشتن مردم از گناه و جرم است. در واقع احکام امر به‌معروف و نهی از منکر با هدف پیشگیری از انحرافات اخلاقی، جرم و گناه در جامعهٔ اسلامی تبیین شده است. به‌همین مناسبت در اصل هشتم قانون اساسی به این امر مهم اشاره شده و امر به‌معروف و نهی از منکر، به‌عنوان وظیفه‌ای همگانی و متقابل از جانب مردم نسبت به یکدیگر، دولت نسبت به مردم و مردم نسبت به دولت شناخته شده است (چاله چاله، ۱۳۸۷: ٥٤). عدم توجه به این مهم، یکی از چالش‌های فراروی سیاست

جنایی مشارکتی ایران در قبال جرایم رایانه‌ای محسوب شده و توجه به این مهم را ضروری می‌نماید.

۳-۳. عدم بکارگیری راهکارهای نظارتی

یکی از طرق نظارت بر جرایم رایانه‌ای در فضای مجازی که موجب پیشگیری از این جرایم می‌شود، مربوط به نظارت بر ورودی‌ها است که سعی می‌شود از دسترسی اشخاص نفوذگر به اطلاعات مالی جلوگیری شود. این نظارت اهمیت فراوانی در حفاظت از اطلاعات مالی داشته و حفاظت دقیقی از این اطلاعات به عمل می‌آورد؛ به‌گونه‌ای که حتی بسیاری از سامانه‌های نظارتی اطلاعات مربوط به تلاش‌های موفق یا ناموفق افراد در ورود به بخش‌هایی که در آن اطلاعات مالی ذخیره شده است را ثبت می‌کنند (اسدی، ١٣٨٤: ١٥). راه‌های گوناگونی برای کنترل ورودی‌ها وجود دارد که ساده‌ترین آن استفاده از رمز عبور در رایانه است (عباسی، ۱۳۸۹: ۲۲). بدیهی است که بالا بردن ضریب کنترل می‌تواند در برابر مجرمان با انگیزه عمل نموده و آن‌ها را در دستیابی به آماج جرم ناکام بگذارد. از دیگر راهکارهایی که می‌تواند به‌عنوان کنترل ورودی عمل کند، استفاده از شبکه‌های مجازی کاوشگر الکترونیک است. این کاوشگرها که از آن‌ها به پلیس مجازی تعبیر می‌شود، وظیفهٔ کنترل دسترسی به اطلاعات مالی را بر عهده دارند. علاوه بر نظارت ورودی نظارت بر خروجی نیز اهمیت شایانی داشته و مکمل کنترل ورودی است. در این نوع نظارت علاوه بر اینکه تمامی راه‌های خروج اطلاعات مدنظر قرار می‌گیرد، به احتمال نشت اطلاعات مالی در فضای سایبر نیز توجه می‌شود. در این سیستم کنترلی تمام اطلاعات مالی که منشأ خود را ترک می‌کنند مورد بررسی و نظارت کامل قرار می‌گیرند.

٤. راهکارهای رفع چالش سیاست جنایی مشارکتی در پرتو سیاست‌های اتحادیهٔ اروپا

همکاری با بخش خصوصی در مبارزه با جرایم رایانه‌ای بسیار مهم است. بخش خصوصی بسیاری از شواهد مربوط به جرایم سایبری و زیرساخت‌های لازم را در اختیار دارد که می‌تواند با حذف و گزارش محتوای غیرقانونی به مجریان قانون در این امر تأثیرگذار باشد. مشارکت بخش‌های دولتی و خصوصی، تنظیم موضوعات حقوقی و شفافیت پیرامون این همکاری نقش

اساسی را در کاهش جرایم سایبری و افزایش امنیت از طریق پیشگیری و اطلاع‌رسانی خواهد داشت. (پلیس اتحادیهٔ اروپا و دادگستری اروپا، ۲۰۱۹: ۱۷). برای ارتقاء مقاومت در برابر سایبر در اتحادیهٔ اروپا، هم مقامات دولتی و هم بخش خصوصی توانایی‌های خود را توسعه داده و به‌طور مؤثر همکاری می‌نمایند. در این راستا، کمیسیونی در مورد امنیت شبکه و اطلاعات نیز تدوین شده است.

رویکرد اتحادیهٔ اروپا در قبال جرایم فضای مجازی به موازات جامعهٔ اطلاعاتی خود توسعه یافته است. این رویکرد توسط اسناد امنیتی داخلی اتحادیهٔ اروپا (کمیسیون اروپا، ۲۰۱۵) و چهارچوب مشترک مقابله با تهدیدات ترکیبی، که راهنمای استراتژیک در مورد امنیت سایبری و جرایم سایبری می‌باشد، ارائه شده است (کمیسیون اروپا و سرویس اقدام خارجی اتحادیهٔ اروپا، ۲۰۱۶). کشورهای اتحادیهٔ اروپا علاوه بر این، همکاری با کشورهای ثالث و تأکید ویژه‌بر یادگیری مداوم از طریق بیان نیازهای آموزشی در رابطه با مسائل مربوط به جرایم سایبری برای مقامات اجرایی و قضایی را به‌طور جدی پیگیری می‌نمایند. با توجه به نقش مهم بخش خصوصی در زمینهٔ ارائهٔ راه حل جهت بهبود وجههٔ عمومی این نوع از سیاست، مبارزه با جرایم سایبری از طریق مکانیسم‌های پیشرفتهٔ گفت‌وگو مورد تأکید قرار گرفته است. برای اجرای قانون، مشارکت‌های مختلف از جمله همکاری بین آژانس‌ها و شرکت‌های کارت اعتباری که امکان ردیابی مؤثر افراد را فراهم می‌نماید، صورت می‌پذیرد (پارلمان اروپا، ۲۰۱۵: ۲۸). رویهٔ مشارکتی اتحادیهٔ اروپا در زمینهٔ جرایم سایبری بیشتر بر پایهٔ همکاری بازیگران بخش دولتی و خصوصی متمرکز شده است و ادعا می‌شود ذی‌نفعان باید برای ایجاد اختلال در شبکهٔ مجرمان سایبری همکاری نمایند. به‌طور مثال مشارکت بین مرکز جرایم سایبری اتحادیهٔ اروپا و مایکروسافت در این مورد از اهمیت ویژه‌ای برخوردار است (کارگروه مشترک در زمینهٔ جرایم سایبری، ۲۰۱۷: ۱۳). «جی کت»[1] نیز به‌عنوان یک سازمان شبکه‌ای سیال و یک کارگروه این امکان را دارد تا با کشورهای غیرعضو به‌طور مؤثر همکاری نماید. به دلیل بین‌المللی بودن جرایم سایبری، اغلب مجرمان در کشورهای خارج از اتحادیهٔ اروپا قرار دارند.

1. J-CAT

این کارگروه می‌تواند از طریق توافق‌نامهٔ موقت همکاری کند (Reitano *et al.*, 2015:145). «جی کت» به‌عنوان یک شکل عملیاتی در حال ظهور و در حال تکامل می‌باشد که نشان‌دهندهٔ عملکرد غیررسمی و انعطاف پذیرتر نسبت به یوروپل و مرکز مبارزه با جرایم سایبری به‌منظور جلوگیری از موانع موجود و اقدامات سنتی و کند می‌باشد. سرانجام، اگرچه این کارگروه به عنوان الگویی عملیاتی منجر به نتایج بهتری می‌شود، اما موضوعات گسترده‌تری برای مبارزهٔ مؤثر با جرایم سایبری باقی می‌ماند. همچنین طبق مادهٔ ۲۳ کنوانسیون جرایم سایبری، اعضای کنوانسیون از طریق اعمال ابزارهای بین‌المللی مربوط به همکاری در حوزهٔ توافق‌هایی دوجانبه مبنی بر انجام تحقیقات یا دادرسی مرتبط با سامانه‌ها و داده‌های رایانه‌ای یا جمع‌آوری ادله و آثار الکترونیکی جرایم کیفری با یکدیگر همکاری می‌نمایند.

در خاتمه باید اذعان نمود با در نظر گرفتن چالش‌های ذکر شدهٔ سیاست جنایی مشارکتی در قبال جرایم رایانه‌ای در ایران و بسترسازی‌های انجام شده در کشور برای برون رفت از این چالش‌ها، الگوبرداری از برخی سیاست‌های اتخاذ شده در اتحادیهٔ اروپا مفید و راهگشا خواهد بود. با توجه به رویهٔ اتحادیهٔ اروپا در جهت ارتقا عملکرد سیاست جنایی مشارکتی خود که بهره‌گیری از ابزارهای متنوع و بازیگران مختلف از جمله مؤسسات، صنعت، شرکت‌های بزرگ، شرکت‌های نوپا، مراکز تحقیقاتی، دانشگاه‌ها، آموزش و پرورش، کاربران نهایی، اپراتورها و انجمن‌ها می‌باشد، همچنین افزایش آگاهی و ترویج فرهنگ امنیت شبکه و اطلاعات به نفع شهروندان، مصرف کنندگان، شرکت‌ها و سازمان‌های بخش عمومی، ایجاد کمپین سالانه به‌منظور آگاهی از امنیت فضای مجازی و احساس مسئولیت مشترک در قبال شهروندان برای رفتار ایمن و آگاهانه در این فضا، در نظر گرفتن تهمیداتی جهت آمادگی برای مبارزه با جرایم فضای مجازی همانند تمرینات عملیاتی مشارکتی مربوط به حوادث سایبری در سطح اتحادیهٔ اروپا برای شبیه‌سازی همکاری بین کشورهای عضو و بخش خصوصی، همکاری با کشورهای ثالث و تأکید ویژه‌بر یادگیری مداوم از طریق بیان نیازهای آموزشی و مهم‌تر از همه ایجاد سازمان‌های مردم نهاد تخصصی که هریک به‌طور ویژه و خاص در زمینهٔ پیشگیری و مبارزه با جرایم فعالیت می‌نمایند و همچنین تقویت بخش مالی در همکاری بخش

دولتی با بخش خصوصی، از جمله صنعت و جامعه مدنی جهت مقابله مؤثر با جرایم سایبری، کشور ما نیز می‌تواند از تجربیات کسب شده توسط اتحادیهٔ اروپا در جهت توانمندسازی سازمان‌های مردم نهاد با اتخاذ راهبردی عملیاتی و تخصصی در حوزه مقابله با جرایم رایانه‌ای و جذب منابع مالی از بخش‌های مختلف برای خوداتکایی مالی و حتی با کسب درآمد از طریق ارائه خدمات به دولت و بخش خصوصی کمک شایانی به تقویت تشکل خود در راستای رسیدن به اهداف و حل مشکل اجتماع مطابق با اساسنامه نمایند و نقشی اساسی جهت کاهش چالش‌های فراروی این حوزه داشته باشند.

تأکید می‌شود سازمان‌های مردم نهادی که می‌خواهند در حوزه جرایم رایانه‌ای فعالیت مؤثر نمایند باید با بهره گرفتن از دانش و تجربه‌های بین‌المللی و ظرفیت فنی، یادگیری فرهنگ همکاری و مبادلهٔ اطلاعات، آگاهی دربارهٔ عملکرد سمن‌های مدرن بین‌المللی از نظر فنون، ظرفیت و مهارت‌های علمی و تخصصی پویا عمل نمایند (فرامرز قراملکی و سالاری، ۱۳۸۸: ٦٦).

نتیجه‌گیری:

با توجه به مباحث یاد شده در مقالهٔ حاضر، به‌نظر می‌رسد، ایران با الهام از مبانی دینی، ضوابط و مقررات قابل توجهی برای مشارکت جامعهٔ مدنی در این زمینه فراهم نموده است. ضمن اینکه جامعهٔ مدنی ایران با تکیه بر تکالیف و آموزه‌های دینی و پشتوانهٔ فرهنگ غنی مشارکتی خود، از قابلیت‌ها و بسترهای مناسبی در این راستا برخوردار می‌باشد. اگرچه تاکنون از این مبانی و بسترها به نحو مطلوب و کامل استفاده نشده است. علاوه بر این، قانون اساسی زمینهٔ چنین مشارکتی را در تمام مراحل تصمیم‌گیری‌های سیاسی برای همهٔ افراد اجتماع فراهم نموده است هرچند در هیچ‌یک از اصول قانون اساسی، به‌صراحت اشاره‌ای به مشارکت جامعهٔ مدنی و به‌ویژه سمن‌ها در زمینهٔ پیشگیری از جرم نشده است اما در این زمینه قول مخالفی نیز وارد نیست، بنابراین می‌توان به این نتیجه رسید که مشارکت تمامی عناصر جامعهٔ مدنی از جمله سمن‌ها در زمینهٔ پیشگیری از جرم مغایر با قانون اساسی جمهوری اسلامی ایران نیست. سیاست‌گذاران جنایی باید تدابیر لازم را برای آموزش و کسب مهارت افراد جامعه جهت مداخله مؤثر به‌کار گرفته و با تکیه بر اصول اخلاقی، جامعه را برای مشارکت فعال در پیشگیری از رفتارهای مجرمانه ترغیب نمایند. در وضع کنونی، سیاست جنایی مشارکتی نه تنها در ایران، بلکه در بسیاری از کشورها کارایی مؤثری را برای پیشگیری از جرایم سایبری دارا نیست. چارهٔ خروج از این بحران و بن‌بست ناشی از آن در کشورهای غربی مطرح شده و کم‌کم با پذیرش و اجرای مشارکت جامعهٔ مدنی در زمینهٔ واکنش به پدیدهٔ مجرمانه، ابعاد و جلوه‌های مختلفی از آن در این کشورها به منصهٔ ظهور و اجرا رسید. راهبردهای سیاست جنایی مشارکتی در دستور کار نهادهای عمدهٔ حقوقی اتحادیهٔ اروپا قرار گرفته است. این امر می‌تواند افق روشنی را برای دست اندرکاران سیاست جنایی سایر کشورها از جمله ایران بگشاید تا با استفاده از این راهکارهای تجربه شده در جهت تدوین و اجرای سیاست جنایی مشارکتی مطلوب گام بردارند. ارتقا سطح آگاهی‌های جامعه، مخصوصاً قشر جوان که بیشترین استفاده را از فضای سایبر دارند، می‌تواند مکمل سیاست‌های مورد بررسی باشد. رفع انگیزه‌های مجرمانه و منحرفانه که توسط پیشگیری اجتماعی صورت می‌گیرد به تنهایی از

عهدهٔ نهادهای رسمی دولتی بر نمی‌آید، بلکه نیازمند مشارکت همه جانبه در سطوح گوناگون جامعه می‌باشد. پس آنچه اهمیت دارد چگونگی مشارکت مردم است. این ضعف را می‌توان با توانمندسازی و آموزش و همچنین از طریق تشویق جامعهٔ مدنی به تشکیل سازمان‌های مردم‌نهاد تخصصی در خصوص مبارزه با انواع گوناگون جرایم رایانه‌ای و حتی پیش‌بینی جرایم نوظهور در آینده با توجه به پیشرفت فناوری‌های مدرن و الهام گرفتن از نهادهای مشارکتی اتحادیهٔ اروپا، همکاری‌های منطقه‌ای و بین‌المللی و تبادل دستاوردها در کاهش جرایم و توسعهٔ نظم اجتماعی تا حد قابل قبولی کاهش داد. با این حال تاکنون قوانین و مقررات جامع و کاملی در زمینهٔ سازمان‌های مردم نهاد برای مبارزه و پیشگیری از جرایم رایانه‌ای وضع نشده است. کنوانسیون جرایم رایانه‌ای به دولت‌های طرف قرارداد پیشنهاد می‌کند که در رابطه با هماهنگ‌سازی بین حقوق کیفری داخلی و مقررات بین‌المللی، تعقیب متهمان این جرایم و بازجویی از آن‌ها در امور مربوط به ارائهٔ دلایل جرم و اعلام دقیق محل وقوع آن، به یکدیگر یاری رسانند. همچنین امور دیگری از قبیل اصول کلی مربوط به همکاری بین‌المللی، استرداد مجرمان، همکاری‌های دوجانبه، نقش مراکز غیردولتی در مبارزه با جرایم در فضای مجازی، ضمانت اجراها و ... در زمرهٔ مباحث مهم مطروحه در کنوانسیون مزبور است. در حال حاضر، کشور ما به هیچ کدام از کنوانسیون‌های بین‌المللی تصویب شده در این حوزه نپیوسته است. اما ویژگی فراملی بودن جرایم ارتکابی، ضرورت پیوستن به کنوانسیون‌ها و مشارکت فعال در عرصهٔ جهانی را جهت رسیدن به اهداف سیاست مشارکتی کشور به‌منظور برون رفت از چالش‌های پیش‌رو در این زمینه روشن می‌سازد. سیاست جنایی ایران بیش‌تر متکی به پاسخ‌دهی از طریق نهادهای دولتی بوده و کمتر به کارایی نهادهای مردمی غیردولتی در جرایم رایانه‌ای توجه نموده است. در حالی که می‌توان همچون اتحادیهٔ اروپا به‌منظور اثربخشی بیشتر با واگذاری بخشی از اختیارات خود به کاربران و نهادهای غیردولتی بهای بیشتری به مردم به‌عنوان عضوی مؤثر در این نوع سیاست جنایی داد و نتیجهٔ مطلوب‌تری را کسب نمود.

پیشنهادها:

با توجه به یافته‌های این مطالعه، می‌توان موارد زیر را به‌عنوان پیشنهاد ارائه نمود:

۱- توجه و تکیه بر توانایی و کارکرد رسانه‌ها در خصوص فرهنگ‌سازی،آموزش و افزایش سطح نظارت طبیعی شهروندان؛

۲- در راستای سیاست جنایی مشارکتی تشویق مؤسسه‌های مالی و شرکت‌ها برای به‌کارگیری تدابیر امنیتی مناسب قبل از اینکه دولت برای آن فکری بکند؛

۳- پژوهش در نحوهٔ شکل‌گیری و پیش‌بینی جرایم نوین در آینده با توجه به پیشرفت فناوری‌ها و آمادگی کامل برای مواجهه با آن و همکاری سازمان‌های مردم نهاد داخلی در عرصهٔ بین‌المللی؛

٤- برگزاری کنفرانس‌های بین‌المللی و بررسی آخرین دستاوردها در این حوزه؛

۵- ارتقای سطح فرهنگ فردی، اجتماعی و آموزش مفهوم دینی امر به‌معروف و نهی از منکر، مشارکت سازمان‌های مردم نهاد تخصصی و الگوبرداری از نهادهای مشابه در اتحادیهٔ اروپا، تنظیم مقررات شفاف حقوقی و اعتمادسازی در این خصوص و آموزش و آگاه‌سازی والدین شاید بتواند از تهدیدات و آسیب‌های جرایم رایانه‌ای بکاهد.

٦- برگزاری تمرینات شبیه‌سازی سایبری به منظور آمادگی و هماهنگی نهادهای اجرایی و مشارکتی و همچنین تبادل اطلاعات و دستاوردها با آژانس‌های بین‌المللی که به انعطاف‌پذیری سیاست جنایی مشارکتی ایران کمک خواهد کرد.

کتابنامه

فارسی

الف. کتاب

۱. باستانی، برومند ؛ آشوری، محمد: جرایم رایانه‌ای و اینترنتی جلوه‌ای نوین از بزهکاری، چاپ اول، انتشارات بهنامی، تهران، ۱۳۸۳.

۲. بکاریا، سزار: جرائم و مجازات‌ها: ترجمه محمد علی اردبیلی، چاپ پنجم، نشر میزان، تهران، ۱۳۸۵.

۳. جمشیدی، علیرضا: سیاست جنایی مشارکتی، چاپ اول، انتشارات میزان، تهران، ۱۳۹۰.

٤. جوان جعفری، عبدالرضا ؛ سیدزاده ثانی، سید مهدی: *رهنمودهای علمی پیشگیری از جرم*، چاپ اول، نشر میزان، تهران، ۱۳۹۱.

۵. رشادتی، جعفر: پیشگیری از جرم در قرآن کریم، چاپ اول، انتشارات پیام راشده، تهران، ۱۳۹۰.

٦. فرامرز قراملکی، احد؛ سکندری، مرضیه: اخلاق در سازمان‌های مردم نهاد؛ چاپ اول، نهاد ریاست جمهوری، مرکز امور زنان و خانواده، تهران، ۱۳۸۸.

ب. مقالات

۱. اسدی، مریم: «فناوری‌های امنیت اطلاعات: با یک دیدگاه طبقه بندی»، مجله بین‌المللی علوم اطلاع رسانی و مدیریت اطلاعات، دوره ۲۰، شماره ۳ و ٤، ۱۳۸٤.

۲. بابایی، جابر؛ صفائی‌آتشگاه، حامد: «جایگاه قانونی مشارکت سازمان‌های مردم‌نهاد در پیشگیری از جرم در ایران»، فصلنامهٔ علمی مطالعات پیشگیری از جرم، شماره ۳۳، ۱۳۹۳.

۳. بابایی، داریوش؛ صدیق‌نژاد، حمیدرضا: «سیاست جنایی ایران در فضای سایبر». چهارمین کنفرانس جهانی و اولین کنفرانس ملی پژوهش‌های نوین ایران و جهان در روان‌شناسی و علوم تربیتی، حقوق و علوم اجتماعی، ۱۳۹٦.

٤. بیگی، جمال؛ خوشیاری، رزاق: «جرایم رایانه‌ای و مقابله با آن در اسناد بین‌المللی». همایش منطقه‌ای چالش‌های جرایم رایانه‌ای در عصر امروز، مراغه، دانشگاه آزاد اسلامی مراغه، ٦ آذر، ۱۳۹۰.

۵. پلیس فتا : والدین به جای نظارت، همراه کودکان در فضای سایبری باشند، ۱۳۹۳. بازیابی از: https://www.cyberpolice.ir/news/41461/. (تاریخ بازدید از سایت: ۱۳۹۹/۰٦/۰۱)

٦. پورتال امنیت و فضای مجازی، مبانی امنیت اطلاعات، ۱۳۹۷. بازیابی از:
(تاریخ بازدید از سایت: ۱۳۹۹/۰٦/۱۰) https://www.sis-eg.com/fa/article/42773-

۷. جلالی فراهانی، امیرحسین: «پیشگیری از جرایم رایانه‌ای»، مجلهٔ حقوقی دادگستر، شماره ٤۷، ۱۳۸۳.

۸. جوان جعفری، عبدالرضا: «جرایم سایبر و چالش‌های نوین سیاست کیفری»، مجموعه مقالات همایش جهانی شدن حقوق و چالش‌های آن، دانشگاه فردوسی مشهد، ۱۳۸۵.

۹. چاله چاله، فرشید: «اصول و مبانی پیشگیری از جرم»، مجله دادرسی، شماره ٦۷، ۱۳۸۷.

۱۰. حاجی ده‌آبادی، احمد؛ سلیمی، احسان: «اصول جرم انگاری در فضای سایبر (با رویکردی انتقادی به قانون جرایم رایانه‌ای»، فصلنامهٔ مجلس و راهبرد، شماره ۸۰، ۱۳۹۳.

۱۱. حسن بیگی، ابراهیم: «توسعهٔ شبکهٔ ملی دیتا، چالش‌های فراروی و تهدیدهای متوجهٔ امنیت ملّی»، فصلنامهٔ مطالعات مدیریت، شماره ٤۸، ۱۳۸٤.

۱۲. رستمی، ولی: «مشارکت مردم در فرایند کیفری (بررسی سیاست جنایی کشورهای غربی)»، فصلنامهٔ حقوق دانشگاه تهران، شماره ۲، ۱۳۸٦.

۱۳. شیعه علی، علی؛ زارع، وحید ؛ زارع، مجتبی: «جایگاه سیاست جنایی مشارکتی واکنشی در مرحلهٔ تعقیب کیفری در حقوق ایران»، نشریهٔ مطالعات حقوق کیفری و جرم شناسی، دوره ۲، شماره ٤و۵، ۱۳۹٤.

۱٤. صالحی، سید حسین؛ خلجی، عباس؛ باصری، احمد: «تأثیر سازمان‌های مردم نهاد بر مؤلفه‌های امنیت»، فصلنامه مدیریت بحران، شماره ۲٦، ۱۳۹٤.

۱۵. عاملی، سعیدرضا؛ حسنی، حسین: «دوفضایی شدن آسیب‌ها و ناهنجاری‌های فضای مجازی: مطالعه تطبیقی سیاست‌گذاری‌های بین‌المللی»، فصلنامه تحقیقات فرهنگی، دورهٔ پنجم، شماره ۱، ۱۳۹۱.

۱٦. عباسی، مراد: «حریم خصوصی، فضای مجازی و چالش‌های پیشگیرانهٔ فراروی ناجا»، فصلنامهٔ علمی ترویجی مطالعات پیشگیری از جرم، شماره ۱۷، ۱۳۸۹.

۱۷. عظیم‌زاده اردبیلی، فائزه ؛ حسابی، ساره: «سیاست جنایی و تطور مفهومی آن»، فصلنامه تعالی حقوق، شماره ۱۵، ۱۳۹۰.

۱۸. فهیمی، مهدی: «جرایم رایانه‌ای و روش‌های مقابله و پیشگیری از آن»، فصلنامهٔ دیدگاه‌های حقوقی، شماره ۲۳و ۲٤، ۱۳۸۰.

۱۹. کاملی، محمدجواد؛ رضائی، علی: «عوامل مؤثر بر اشراف اطلاعاتی بر سازمان‌های مردم نهاد شهر همدان در سال ۱۳۸۷»، فصلنامه مطالعات مدیریت انتظامی، شماره ۱، ۱۳۹۰.

۲۰. میکولون میریام اف:«کنوانسیون جرم‌های سایبری: اجرای هماهنگ حقوق کیفری بین‌المللی چشم انداز فرآیند دادرسی عادلانه چیست؟» (ترجمه امیر حسین جوانبخت)، مجله حقوقی دادگستری، شماره ۵۹، ۱۳۸٦.

۲۱. وطنی، امیر؛ اسدی، حمید: «سیاست جنایی جمهوری اسلامی ایران در جرائم سایبری با تأکید بر ویژگی‌های خاص این جرائم»، پژوهشنامهٔ حقوق اسلامی، شماره ۱ (پیاپی ٤۳)، ۱۳۹۵.

ب. منابع انگلیسی

1. European Commission: Communication from the commission to the council and the European Parliament, The Council, The European Economic and Social Committee and The Committee of the Regions, The Agenda on European Security, Strasbourg, 2015.

2. European Commission: Joint Communication to the European Parliament and the Council, Resilience, Deterrence and Defence: Building strong cybersecurity for the Eu, Brussels, 2017.

3. European Commission and European External Action Service (EEAS): Joint communication to the European Parliament and the Council, Joint Framework on Countering Hybrid Threats: A European Union response, 2016.

4. European court of Auditors: Challenges to effective EU cybersecurity policy, Briefing Paper, 2019.

5. European Crime Prevention Network: EUCPN Toolbox Series No.12 Cybersecurity and Safety. Policies and practices. Brussels, 2018.

6. European Cyber Security Organisation: About ECSO. Retrieved from: https://www.ecs-org.eu/about, 2020. (Last visited on 2020/09/25).

7. European Union Law: Cybersecurity Strategy of the European Union. Retrieved from: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=celex:52013JC0001, 2013. (Last visited on 2020/09/15).

8. European Parliament:The law enforcement challenges of cybercrime: Are we really playing catch-up? Technical Report, Directorate- General for Internal Policies, Policy Department C: Citizens Rights and Constitutional Affairs, Study for the LIBE Committee, 2015.

9. Forbes: How to Prevent Cybercrime. Retrieved from: http://www.forbes.com/sites/thesba/2013/08/28/how_to_prevent_cybercrime/, 2013. (Last visited on 2020/09/16).

10. Georgetown Law: International and Foreign Cyberspace Law Research Guide. Retrieved from: https://guides.ll.georgetown.edu/c.php?g=363530&p=4821480, 2020. (Last visited on 2020/09/10).

11. Reitano, Troels Oerting and Hunter, Marcena: Innovations in international cooperation to counter cybercrime: The joint Cybercrime Action Taskforce (J-CAT). The European Review of Organised Crime, 2015.

12. SOCTA: EU serious and organised crime threat assessment report. The Hague, Netherlands: Europol. Retrieved from https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and -organised-crime-threat-assessment-2017, 2017 (Last visited on 2020/09/10).

13. Vogel Joachim: Towards a global convention against cybercrime, First Word Conference of Penal Law. Penal Law in the XXlst Century, Guadalajara (Mexico), 2017.

14. Wexler Chuck: The role of local law enforcement agencies in preventing and investigating cybercrime, Critical Issues in Policing Series, Police Executive Research Forum, Washington, D. C, 2014 .