نقش پلیس در پیشگیری از جرائم سایبری با تأکید بر قوانین موضوعه

هدیه سادات میرترابی[۱]
هادی شیرزاد[۲]
وهاب آقا کاشی[۳]

تاریخ دریافت: ۹۹/۵/۲۰
تاریخ پذیرش: ۹۹/۹/۱۴
نوع مقاله: پژوهشی

چکیده

زمینه و هدف: گسترش ابزارهای ارتباطی و امکان برقراری ارتباط با کمترین هزینه با سایر نقاط جهان، از یک‌سو فرصتی بی‌نظیر به شمار آمده و از سوی دیگر، تهدیدهایی را برای امنیت اقتصادی، فرهنگی، سیاسی انسان‌ها موجب شده است. یکی از مهم‌ترین این ته دیدها، تولد و گسترش قابل توجه پدیده‌ای به نام جرائم سایبری است؛ جرائمی که در مقایسه با جرائم سنتی، هر روز قربانیان بیش‌تری از بشریت گرفته و نیز روش‌های سنتی مبارزه با جرائم در خصوص آن‌ها کارگشا نیست. تحقیق حاضر به بررسی نقش نهاد پلیس در کنار سایر عوامل محدود کنندهٔ این جرائم از جمله اسناد، قوانین و کنوانسیون‌های بین‌المللی در پیشگیری از این جرائم می‌پردازد.

روش تحقیق: روش مورد استفاده در تحقیق حاضر، توصیفی و از نظر هدف، تحلیلی است (کتابخانه‌های مرکزی، سایت‌های علمی معتبر نظیر سایت جهاد دانشگاهی، ساینس دایرکت و غیره).

یافته‌ها و نتیجه‌گیری: در سال‌های اخیر، کشورهای پیشرو در امر مبارزه و پیشگیری از جرائم سایبری، اقدامات پیشگیرانه مؤثری در جهت مبارزه با این پدیده در بستر اینترنت داشته‌اند. نیروی انتظامی جمهوری اسلامی ایران نیز، با درک مسئله وجود بحران در فضای سایبر اقدامات مؤثری در جهت پیشگیری از وقوع جرائم رایانه‌ای داشته که بازتاب روانی و رسانه‌ای گسترده‌ای در پی داشته است. با این وجود به نظر می‌رسد لازم است نوعی تبادل اطلاعات، انتقال تجربیات و یکسان‌سازی اقدامات پیشگیرانه با توجه به شرایط اجتماعی و فرهنگی کشورهای پیشرو در امر مبارزه با جرائم سایبری صورت گیرد.

کلیدواژه‌ها: فضای سایبر، جرائم سایبری، پلیس، قوانین موضوعه.

---

۱. عضو هیئت‌علمی گروه حقوق دانشگاه آزاد اسلامی واحد تهران شرق، تهران، ایران (نویسندهٔ مسئول)
ut.ac.ir@mirtorabi۵۲
۲. استادیار پژوهشگاه علوم انتظامی و مطالعات اجتماعی ناجا، تهران، ایران.
۳. کارشناس ارشد حقوق خصوصی دانشگاه خوارزمی، تهران، ایران.

مقدمه

در عصر نوین شاید هیچ جرمی به‌مانند جرائم سایبری را نتوان سراغ داشت که بزهکاران آن بدین شکل، معادلات شناسایی را برای مأمورین تحقیق پیچیده ساخته باشند. بستر سایبر به واسطهٔ ویژگی‌های خاص خود، در وهلهٔ نخست، شناسایی بزهکار و در مراتب پسینی، کشف بزه را دشوار ساخته است. افزون بر ویژگی‌هایی که فضای سایبر به بزهکاری اعطاء کرده است، ابزارهای سنتی تحقیقاتی نیز در رویارویی با این جرائم به شدت ناکارآمد و فاقد اثربخشی لازم می‌باشند؛ زیرا مسلم است که با رایانه‌ای شدن صحنهٔ جرم، تجهیز کنشگران عرصهٔ بزهکاری به سلاح‌های نوین و بالطبع بهره‌برداری آن‌ها از روش‌های ارتکاب جرم متناسب با آن، نمی‌توان از ابزارهایی که هیچ سنخیتی با آن ندارند، بهره جست. لذا پی‌جوئی جرائم سایبر، مستلزم کاربست تدابیر روزآمد است.

بررسی و تجزیه و تحلیل جنبه‌های مختلف جرائم رایانه‌ای و اینترنتی مشخص خواهد ساخت که رایانه‌های مدرن و شبکه‌های ارتباطی، دارای صفات و خصوصیاتی است که فرصتی بسیار مناسب، برای مجرمان پدید می‌آورد و مشکلات زیادی را فرا روی بزه‌دیدگان و پلیس قرار می‌دهد؛ زیرا مخاطرات و صدمات این جرائم به مراتب بیشتر از حالت کلاسیک است و در بیشتر مواقع نیز کشف و ردیابی آن مشکل و دشوار است.

وقوع جرائم سایبری منجر به تخریب هویت ملی، دینی و افزایش آسیب‌های فرهنگی و سیاسی می‌باشند. در واقع، وقوع این جرائم را می‌توان ناشی از تأثیرات مدرنیته بر جوامع صنعتی دانست. در این میان، نقش محوری پلیس به عنوان یکی از متولیان امنیت بخشی در جامعه غیرقابل انکار است. وقوع این جرائم، وظیفهٔ خطیر این نهاد امنیتی را تحت‌الشعاع قرار داده و به چالش کشانده است. پلیس جمهوری اسلامی ایران تلاش می‌کند تا با بهره‌گیری از آخرین دستاوردهای فناوری اطلاعات و ارتباطات سیستم‌های پیشرفته انتظامی – امنیتی کشور، امنیت اجتماعی را بهبود بخشیده و محیطی امن، توأم با آسایش عمومی را برای کلیهٔ شهروندان، در پرتو ارزش‌های اسلامی فراهم کند (احمدوند و عطایی جعفری، ۱۳۸۳: ۲۲).

بدون تردید، سیستم کلان مبارزه با جرم که از سوی پلیس اتخاذ می‌شود، چه در محیط فیزیکی و چه در فضای مجازی یکسان است و پلیس در پیشگیری از وقوع جرائم سایبری

همان جایگاه را خواهد داشـــت. در واقع اقدامات پلیس برای پیشـــگیری از وقوع این جرائم، چیزی جز مبارزهٔ وضعی و سیاســـت عام این نهاد در مقابله با ســـایر جرائم نیست. اما آنچه باعث تفاوت در این حوزه می‌شود، ویژگی منحصر به فرد جرائم سایبری است که شیوه‌های اجرایی خاص خود را به منظور تحقق این سیاست عام طلب می‌کند (آیکاو و جی، ۱۳۸۵: ۱۵۱).

بیان مســـئله: نیمهٔ پایانی قرن بیســـتم و پس از جنگ جهانی دوم دورهٔ طلایی دانش و فناوری بشر و دورهٔ انتقال از عصر صنعت و ماشین به عصر فناوری اطلاعات است. توسعهٔ شبکه‌ها با کارکردهای نظامی، در ابتدا و توسعهٔ آن‌ها و تعریف کارکردهای جدید و ایجاد امکان اتصال مراکز دانشـــگاهی، پژوهشـــی علمی و تبادل اطلاعات با یکدیگر، در این نیمه اتفاق افتاده اســـت. امروزه این فناوری عظیم با میلیاردها رایانه، میلیون‌ها خدمات دهنده و صدها هزار شـــاهراه ارتباط اصلی در برابر بشـــر قرار دارد تا از مواهب و مزایای بی‌بدیل آن اســـتفاده کند یا خود را با پلیدی‌ها و آســـیب‌های آن به نابودی کشد. رایانه، اینترنت و تمامی ابزارهای مبتنی به فناوری اطلاعات و ارتباطات در ابتدا و در ذهن و تصمیم مبدعان و مخترعان آن، صرفاً با هدف خدمت به نوع بشـــر و ساده‌ســـازی و افزایش کیفیت زندگی انســـان، طراحی و تولید شـــدند. اما در عمل به شمشـــیر دو لبه تبدیل شده که سعادت و شـــقاوت را همزمان با هم به ارمغان می‌آورد. از ســـال ۱۹۶۰ تاکنون، ســـه نسل از جرائم رایانه‌ای برشـــماری شده‌اند. نسل اول مقارن سال‌های دههٔ هفتاد و هشتاد، اوایل دههٔ نود میلادی اســـت. چون استفاده از اینترنت در آن زمان شیوع نداشت، عمدهٔ جرائم مرتبط با رایانه‌ها بوده و از این‌رو، این دســـته از جرائم صرفاً به «جرائم رایانه‌ای» یاد می‌شـــوند. نسل دوم جرائم رایانه‌ای، از اوایل دههٔ هشتاد، تا اوایل دههٔ نود به وقوع پیوستند که به «جرائم علیه داده‌ها» تعبیر می‌شـــوند. در این نســـل، «داده‌ها» صرف نظر از اینکه در رایانه قرار داشته باشند، در ابزارهای انتقال مورد توجه قرار گرفت و دیگر تأکیدی بر رایانه نبود. نسل ســـوم جرائم رایانه‌ای نیز همزمان با فراگیرشدن اینترنت در سال ۱۹۹۰ میلادی به وجود آمد. این جرائم که با گسترش کاربرد شبکه و اینترنت به وجود آمدند، نام جرائم سایبری را به خود گرفتند. گســـترش جرائم سایبری در دنیا، خصوصاً در کشورهایی که بیش‌ترین

استفاده‌کنندگان رایانه و اینترنت در دنیا محسوب می‌شوند، باعث شد که حکومت‌ها به فکر ایجاد سازوکار قانونی و حقوقی پیشگیری، رسیدگی و مبارزه با اینگونه جرائم بیافتند. کنوانسیون‌های بین‌المللی نیز برای تشریک‌مساعی در روند شناسایی جرم و مجرمان، همکاری در پی‌جویی و تعقیب قضایی و پلیسی مجرمان و تبادل دانش و اطلاعات پلیس، در شناخت و کشف علمی جرائم سایبری نیز تشکیل شدند که از مهم‌ترین آن‌ها می‌توان به کنوانسیون بوداپست در سال ۲۰۰۱ اشاره کرد. از کشورهای فعال در پیشگیری و مبارزه با جرائم رایانه‌ای، می‌توان به ایالات‌متحده آمریکا، روسیه، چین، کره جنوبی، انگلستان، هند، فرانسه و آلمان اشاره کرد. در همین راستا، کشور ایران از این قاعده مستثنی نبوده و با کوشش‌های فراوان توانسته در زمینهٔ پیشگیری و مبارزه با جرائم مذکور قدم بردارد. پلیس به عنوان یکی از نهادهای امنیتی و انتظامی در جامعه، از زمان تأسیس آن تاکنون با اتخاذ سیاست‌های پیشگیرانه به این امر اهتمام ورزیده است. فلسفهٔ وجودی نهاد پلیس با در نظر گرفتن قانون و حقوق مردم، برقراری نظم و امنیت و پیشگیری از وقوع جرم است. کلیهٔ سیاست‌های اجرایی این نهاد، بر پایهٔ اصل معقول و قدیمی پیشگیری بهتر از درمان است استوار است؛ زیرا هزینه‌هایی که امر پیشگیری به دنبال دارد، خیلی کمتر از هزینه‌های گزاف مواجه با جرم است. حساس بودن وظیفهٔ خطیر پلیس، از آنجا ناشی می‌شود که می‌تواند از تهدیدهای جدی که بر فرهنگ، اجتماع، اقتصاد، امنیت جامعه و غیره تأثیر می‌گذارد، جلوگیری کند. این تحقیق به دنبال بیان سیاست‌های پیشگیرانهٔ وضعی پلیس در امر پیشگیری از وقوع جرم است که در واقع نفی مجازات به عنوان یکی از راه‌های پیشگیری از جرم مدنظر نیست، بلکه استفاده از شیوه‌های غیر قهرآمیز را ذاتاً و قبل از وقوع جرم، توسط پلیس توصیه می‌کند.

سؤال اصلی تحقیق: نقش پلیس در جهت پیشگیری از جرائم سایبری تا چه میزان موفقیت‌آمیز بوده است؟

فضای سایبر: به موجب یکی از تعاریف، محیط سایبر به اطلاعات الکترونیکی اطلاق می‌شود که از طریق اینترنت جا به جا می‌شوند. البته تعاریف دیگر سعی کرده‌اند تا به بیان موارد افتراق محیط سایبری از موضوعات مجازی و شبکه بپردازند و از دیدگاه آن‌ها محیط

مجازی، مجموعه اطلاعاتی است که در رایانه ذخیره‌سازی شده و از طریق اینترنت به یکدیگر متصل هستند (پلوگ[1]، ۲۰۰۹: ۷۰).

در یک معنای مختصر، فضای سایبری ناظر است به فضای برخط شبکه‌های رایانه‌ای به‌ویژه اینترنت یا فضایی مجازی و غیرواقعی است که در آن، داده‌های الکترونیکی بین رایانه‌ها مبادله می‌شود. همچنین، در تعاریف دیگر، فضای سایبر ناظر است به فضای مجازی که جامعهٔ کاربران اینترنت در آن بوده و منابع داده‌های الکترونیکی به واسطهٔ شبکه‌های رایانه‌ای قابل دسترس هستند یا مجموعه‌ای از سامانه‌های به هم پیوستهٔ داده‌ها و کاربران انسانی که با این سامانه‌ها در تعامل هستند[2]. با مداقه در تعاریف پیش‌گفته، می‌توان سه عنصر اساسی تشکیل دهندهٔ فضای سایبر را چنین گزیده آورد؛ نخست، سامانه‌ای رایانه‌ای؛ دوم، شبکهٔ اینترنت و سوم، کاربران. آنچه باید بدان توجه داشت، آن است که گرچه عنصر اول و سوم در فضای مادی موجود و ملموس است، اما عنصر دوم موجودیت مادی و ملموسی ندارد و از این روست که تمام کنش‌های انجام یافته در این فضایِ مجازی و غیرملموس، بعد مکانی مشخص و معینی ندارد.

از پدیده‌هایی که رایانه و پس از آن اینترنت همراه خود به ارمغان آورد، مخاطراتی بود که بر جای‌جای قلمرو گسترده‌اش، سایه انداخت. چنین مخاطراتی، چنانچه مورد بی‌توجهی جامعه و حکومت قرار گیرد، بسی بزرگ و گاه غیر قابل جبران خواهد بود؛ چراکه آسیب‌های روانی ناشی از کاربری نادرست و خلاف قانون، موجب اختلال در رفتار شهروندان شده، جامعه را در رسیدن به فواید بی‌شمار این فناوری نوین ناکام می‌گذارد. این اختلالات، شهروندان را فرسوده و ناتوان کرده، فعالیت‌های روزمرهٔ آن‌ها را مختل می‌کند. آسیب‌های اجتماعی و فرهنگی ناشی از آن، اعضای جامعه را در رفتار فردی با خانواده و رفتار اجتماعی با دیگر شهروندان و حکومت متزلزل و متأثر از فرهنگ‌های منحط بیگانه می‌کند. هنجارها و ارزش‌های متعالی جامعه رو به زوال رفته، احساس امنیت و آرامش از جامعه رخت برمی‌بندد. ضمن اینکه، آسیب‌های سیاسی آن، موجب تضعیف اقتدار و حاکمیت دولت شده، آن را

1. Ploug
2. NATO Cooperative Cyber Defence Centre of Excellence, Accessed 17 May 2017. https://ccdcoe.org/multimedia/cyberspace-definition-and-implications.html.

در ایجاد وحدت ملی و امنیت اجتماعی و امنیت اطلاعاتی دچار چالش‌های جدی می‌کند.

مشـــکلات حاکم بر فضای سایبر: پژوهشـــگران معتقدند که ورود فضای سایبر به فضای زندگی انســـان‌ها در کنار مزایا و محاســـن غیرقابل کتمان، باعث به وجود آمدن یکســـری دغدغه‌ها و نگرانی‌هایی از قبیل افزایش فاصله بین نسل‌ها و متزلزل شدن بنیاد خانواده شده که این موضوع روابط افراد را به شـــدت تحت تأثیر قرار داده اســـت که به اختصار به بعضی از آن‌ها اشاره می‌شود.

۱- افزایش فاصله بین نســـل‌ها: یکی از آثار فضای ســـایبر، ایجاد ناامنی در کشـــور است. گسســـت نســـلی فاصله‌ای است ژرف که ناشـــی از قطع پیوندها و روابط بین نسلی است. به عبارت دیگر، وقتی منابع هویتی نســـلی تقویت‌کنندهٔ یکدیگر نباشـــد و پیوستگی نسلی را به دنبال نداشـــته باشـــند، زمینه برای ظهور تعارض و گسست نسلی فراهم می‌شود؛ به گونه‌ای کـــه اعضای جامعـــه، وضعیت هویت خود را در نفی و تقابل با گذشـــتگان خود می‌بینند. این امـــر مـــا را در متن تحولات فرهنگی که وجود آن بـــرای پویایی جامعه در عرصه‌های مختلف حیاتی است قرار نمی‌دهد، بلکه ما را به حاشیه هدایت می‌کند. حاشیه‌ای که بسیار هزینه‌بر و مناقشه‌برانگیز است؛ به گونه‌ای که زمینه را برای فروپاشی اجتماعی و فرهنگی فراهم می‌کند (میری اشتیانی، ۱۳۸۲: ۲۲۴).

به دلیل اینکه فناوری‌های نوین، برای جوانان جذابیت بیشتری دارد، بنابراین آن‌ها یادگیری و پیشرفتشان در این زمینه بیش‌تر خواهد بود و افراد با سنین بالا، پیشرفت و گرایش چندانی نسبت به این فناوری جدید و حضور در فضای سایبر ندارند. این امر سبب می‌شود که فاصله بین نسل‌های قبل با نسل‌های بعدی بیشتر شود. این شکاف باعث می‌شود که هم‌زبانی بین نســـل‌ها از بین برود و نســـل جوان از ارزش‌های ملی و اسلامی و گذشتگان خویش دور شوند. همچنین، به دلیل تسلط بیش‌تر جوانان بر استفاده و بهره‌وری از فضای سایبر، بحران کنترل از ســـوی افراد بزرگ‌تر شـــکل می‌گیرد؛ چراکه کنترل جوانان و نوجوانان و سایر کاربران در فضای ســـایبر، ســـخت‌تر می‌شود و در نتیجه احتمال ارتکاب جرائم در این فضا بیش‌تر از هر زمانی احساس می‌شود.

۲- متزلزل شدن بنیاد خانواده: خانواده، پایهٔ بنیادین اجتماع و سلول سازندهٔ زندگی انسان

و خشـــت بنای جامعه و کانون اصلی حفظ ســـنن، هنجارها و ارزش اجتماعی است. بنابراین، خانواده‌ها و مسئولان باید بدانند، چه عواملی موجب پیدایش ارزش‌ها در یک جامعه می‌شود و چگونه می‌توان این ارزش‌ها را تغییر داد. به‌طوری که، زمانی که از ســـلامت و بهزیســـتی جامعه سخن به میان می‌آید، بی‌تردید می‌توان گفت که خانواده مهم‌ترین کانون جامعه است. از ســـوی دیگر، خانواده طیف وســـیعی از خدمات عاطفی، جسمی و مراقبتی را برای اعضای خود فراهم می‌آورد. ضعف و ناتوانی خانواده، منبع بســـیاری از مســـائل و مشکلات است که بهزیســـتی اجتماعی وظیفهٔ مقابله با آن‌ها را دارد. والدین در شـــکل‌گیری ساختار شخصیتی جوان و آگاهی و نگرش و عملکرد به مسائل مختلف، نقش بسیار کلیدی دارند.

امروزه، سرگرمی‌های موجود در فضای سایبر و افزایش مدت زمان استفاده از اینترنت، ملازم با انزواگرایی کاربر اســـت. او برای اینکه بتواند مدت بیشتری برای گشت‌وگذار در فضای سایبر صرف کند، باید سایر روابط خود را در زندگی روزمره‌اش به حداقل ممکن کاهش دهد. اینترنت، با داشتن شرایط دل‌انگیز و کاذب مجازی، به خصوص برای جوانان، می‌تواند باعث گسیختگی تمام ابعاد زندگی آن‌ها شده و آن‌ها را از خانواده دور کرده و به عمق انزواطلبی و تنهایی بکشاند. فریبندگی اینترنتی، در محیط خانواده می‌تواند باعث از هم گسیختگی ازدواج، روابط زناشویی و روابط والدین فرزندی شـــود. اینترنت، نقش گفت‌وگو و هم‌اندیشـــی در بین اعضای خانواده را کمرنگ‌تر کرده و زنگ خطر جدی را برای ارتباطات انسانی به صدا در آورده است. استفادهٔ زیاد از اینترنت با پیوند ضعیف اجتماعی، مرتبط است (میری اشتیانی، ۱۳۸۲: ۳۰).

جرم ســـایبر: در سال ۱۹۸۳، نخســـتین تعریف از جرم سایبری از سوی سازمان همکاری و توســـعهٔ اقتصادی اروپا منتشـــر شده است و به دنبال آن تعاریف متعددی از جرائم سایبری ارائه شـــده است. وجه مشـــترک تعاریف مختلف از جرائم سایبری، مربوط به ارتباط جرائم با سامانه، اینترنت یا شبکه است (کرد علیوند و میرزایی، ۱۳۹۷: ۱۹۲).

در قانون جرائم رایانه‌ای، موضوع جرائم رایانه‌ای و سایبری به صورت زیر تعریف شده است؛ جرائم رایانه‌ای، به آن دسته از جرائمی اطلاق می‌شود که موضوع و هدف جرم رایانه باشد یا جرم از طریق رایانه صورت بگیرد. اگر رایانه به شبکهٔ اینترنت هم وصل باشد، در این صورت، مصداق جرم اینترنتی پیدا می‌کند. جرم ســـایبری، مســـتلزم مجاورت فیزیکی میان قربانی

و مرتکب نیســـت. برعکس جهان واقعی، در جهان ســـایبر، جرم به صورت اتوماتیک از طریق فناوری واقع می‌شـــود. چون جرم در جهان واقعی اتفـــاق نمی‌افتد، از محدودیت‌های جهان فیزیک هم برخوردار نیست (جوان جعفری،۱۳۹۳: ۲۶).

در جرائم سایبری به دلیل واقع شدن در فضای مجازی و غیرواقعی، اثری ملموس و مادی از جرم و رد پای مجرم، آن‌گونه که در جرائم ســـنتی بر جای می‌ماند، دیده نمی‌شـــود و در بیشـــتر موارد، همان اندک آثار باقی مانده از جرم که قابلیت ردیابی مجرم را دارد به راحتی قابل امحاء و پاک‌ســـازی اســـت. به همین دلیل، می‌توان با اطمینان گفت که رقم ســـیاه در جرائم ســـایبری در مقایسه با جرائم سنتی، بسیار بالا است)طهماسبی و شاه‌مرادی، ۱۳۹۷: ۹۹). بنابراین، در محیط سایبر، به اقتضای ویژگی‌های خاص و از جمله سهولت ارتکاب جرم و فرمان رانی آزادی در این فضا، امکان رخ دادن پدیدۀ نامطلوب مجرمانه بیشـــتر می‌شـــود؛ چراکه یکی از ویژگی‌های به‌واقع متمایز و درعین حال ارزشمند فناوری اطلاعات و ارتباطات الکترونیکی نســـبت به دیگر فناوری‌ها مانند فناوری هسته‌ای، زیستی و ریز فناوری، حداقل در برهۀ کنونی، این است که اکثر افراد با حداقل مهارت فنی، می‌توانند از قابلیت‌های متنوع آن استفاده کنند (جلالی فراهانی، ۱۳۸۹: ۱۵).

جرم رایانه‌ای عبارت از جرائمی است که در فضای سایبر رخ می‌دهد و در تعریف گسترده، هر فعل یا ترک فعلی که از طریق یا به کمک رایانه یا از طریق اتصال به اینترنت، چه به‌طور مســـتقیم یا غیرمستقیم رخ می‌دهد و توســـط قانون ممنوع شده و برای آن مجازات در نظر گرفته شده است، جرم رایانه‌ای گفته می‌شود. با توجه به این تعریف، جرائم سایبری را می‌توان به سه دسته تقسیم کرد (حقیقی، ۱۳۹۵: ۳)؛ دستۀ اول، جرائمی هستند که در آن‌ها رایانه و تجهیزات جانبی آن موضوع جرم واقع می‌شـــود، مانند ســـرقت، تخریب و غیره. دستۀ دوم، جرائمی هستند که در آن‌ها رایانه به عنوان ابزار ارتکاب جرم به کار گرفته می‌شود که معمولاً از طریق شبکه‌های رایانه‌ای و اینترنت رخ می‌دهد، مثل کلاهبرداری، جعل و سرقت رایانه‌ای و غیره و دســـتۀ سوم، جرائمی هستند که می‌توان آن‌ها را جرائم سایبری نامید که در فضای مجازی به وقوع می‌پیوندد، اما آثار آن‌ها در دنیای واقعی ظاهر می‌شود، مانند نفوذ غیرمجاز، شنود غیرمجاز، انتشار ویروس، کرم‌های رایانه‌ای و غیره.

تقسیم‌بندی جرائم سایبری: برای روشن‌تر شدن ماهیت فضای سایبر و جرائم قابل ارتکاب در آن، معرفی انواع این جرائم ضروری است؛ جرائمی که می‌توان در یک دسته‌بندی کلی آن‌ها را به دو دستهٔ جرائم رایانه‌ای وسیله‌محور و جرائم رایانه‌ای موضوع‌محور تقسیم کرد. جرائم رایانه‌ای وسیله‌محور، شامل جرائم ضد اشخاص، ضد عفت و اخلاق عمومی و جرائم علیه اموال و جرائم موضوع‌محور، شامل جرائم ضد محرمانگی داده‌ها و سامانه‌های رایانه‌ای و مخابراتی، جرائم ضد صحت و تمامیت داده و سامانه‌های رایانه‌ای و مخابراتی و جرائم ضد قابلیت دسترسی می‌شود (جلالی و توسلی اردکانی، ۱۳۹۸: ۱۳).

جرائم سایبری از منظر قوانین

اسناد بین‌المللی: در حال حاضر، جرائم مجازی به عنوان یکی از دغدغه‌های بزرگ هزارهٔ سوم میلادی، آیندهٔ اجرای قوانین را در بسیاری از کشورهای جهان، به خطر انداخته است. کشورهای در حال توسعه، برای مبارزه با این جرائم، قوانینی تدوین کرده‌اند که بسیاری از آن‌ها از اسناد بین‌المللی سرچشمه می‌گیرند که این اسناد راهکاری مناسب را پیش‌روی قانون‌گذاران کشورها قرار داده است. ابعاد جرائم ارتکابی در فضای مجازی، نه تنها حاکمیت سرزمینی یک دولت را تحت تأثیر قرار می‌دهد، بلکه تمامی دولت‌های جهان را در بر می‌گیرد. ماهیت جرائم سایبری این‌گونه است که هیچ حد و مرز سرزمینی مشخصی را نمی‌شناسد (پرویزی، ۱۳۸۴: ۷۷).

- **کنوانسیون بوداپست:** به منظور مبارزه با جرائم مجازی و رفع چالش‌های موجود در این حوزه، برخی کنوانسیون‌های بین‌المللی به تصویب رسیده‌اند که کنوانسیون ۲۰۰۱ بوداپست با عنوان کنوانسیون جرائم رایانه‌ای یکی از آن‌هاست. در این کنوانسیون، هماهنگ‌سازی بین حقوق کیفری داخلی و مقررات یکپارچهٔ بین‌الملل، در خصوص عناصر تشکیل دهندهٔ جرائم فضای مجازی به چشم می‌خورد.

کنوانسیون بوداپست، به نام «پیمان جرائم اینترنتی بین‌المللی» نیز معروف است و اولین پیمان بین‌المللی ایجاد شده برای مقابله با جرائم اینترنتی است که حدود ۴۰ کشور مختلف در کنفرانس بین‌المللی بوداپست با موضوعیت جرائم اینترنتی در ۲۳ نوامبر ۲۰۰۱ در

مجارستان آن را امضاء کردند. این پیمان شامل تعاریف دقیق برای همه نوع از جرائم اینترنتی است و کیفر مربوط به هر کدام نیز مشخص شده است (دشتی و افشاری، ۱۳۹۸: ۹۸). همچنین، به منظور تعقیب متهمان این جرائم و بازجویی از آن‌ها، اختیارات خاصی برای مراجع قضایی و انتظامی مقرر شده است. این کنوانسیون نمی‌تواند به عنوان معاهده‌ای جامع تلقی شود؛ زیرا اولاً، تمام جرائم سایبری را در بر نمی‌گیرد و ثانیاً، این کنوانسیون، صرفاً برای کشورهای اروپایی لازم‌الاجراست. در هر صورت، معاهدات منطقه‌ای و دوجانبه، پاسخگوی حل مشکلات نبوده و معاهدهٔ اینترنتی در سطح بین‌المللی موردنیاز است (سولان گرناتی[1]، ۲۰۱۰: ۵).

هرچند ایران به این کنوانسیون نپیوسته و آن را امضاء نکرده است، اما با مطالعه و تحقیق در جرائم رایانه‌ای مصوب ۱۳۸۸، به راحتی ردپای مقررات کنوانسیون جرائم سایبر و تأثیراتش به وضوح دیده می‌شود.

سند بین‌المللی دیگری که در این زمینه وجود دارد، قواعدی تحت عنوان «نت اسمارت» است که برای حمایت از کودکان، نوجوانان و جوانانی وضع شده است که کاربر اینترنت می‌باشند. در این سند بین‌المللی، برای پیشگیری از وقوع جرائم سایبری بر ضد اشخاص یاد شده، توصیه‌هایی مقرر شده است. در کنار این اسناد بین‌المللی، سازمان ملل نیز با انتشار متون و نشریات مختلف، در راستای پیشگیری از جرائم سایبری و مبارزه با آن‌ها، اقدامات بسزایی را انجام داده که از جمله این نشریات، می‌توان به نشریهٔ سیاست جنایی سازمان ملل در زمینهٔ جرائم سایبری اشاره کرد. اگرچه، مطالب مندرج در این نشریه جنبهٔ الزام‌آور به خود نمی‌گیرد، اما در هر حال، در راستای اتخاذ سیاست‌های لازم برای زدودن این پدیدهٔ نوین بزهکاری، ایده‌های جدیدی به کشورها داده و مساعدت‌های شایسته‌ای به آن‌ها کرده است (رضوی، ۱۳۸۷: ۱۲۸).

اما شاید مهم‌ترین تلاش، اجلاس جهانی جامعهٔ اطلاعات در سال ۲۰۰۳ باشد که در آن تشکیل سازمان بین‌المللی اینترنت و انعقاد معاهده‌ای اینترنتی پیشنهاد شد. اتحادیهٔ بین‌المللی مخابرات در مه ۲۰۰۷، آژانس جهانی جرائم سایبری و متعاقباً گروه کارشناسان

1.. Solange Ghernaouti

ارشـــد را با هدف ارائه پیشـــنهادهایی برای جرم‌انگاری ســـایبری بنیان‌گذاری کرد. بالاخره، ســـند اصلاحـــی مقررات اتحادیهٔ بین‌المللی مخابرات با اعطـــای وجههٔ حقوقی بین‌المللی به قانون‌گذاری در فضای اینترنت با رأی اکثریت کشـــورها به تصویب رســـید (ضیایی، ۱۳۹۶: ۲۳۶).

- **دســـتورالعمل تالین:** پیمان آتلانتیک شمالی (ناتو) در سال ۲۰۱۳ به تهیهٔ پیش‌نویس ســـندی که بتواند آن را به الگویی قابل پیروی برای همهٔ کشـــورها بدل کند، مبادرت کرد. مجموعه دستورالعمل تالین ناتو، یک تحلیل مداوم از جنگ سایبری و کاربردی بودن قانون بین‌الملل در حوزهٔ ســـایبر اســـت. سندی که خود، به غیرالزام‌آور بودن قواعدش تصریح کرده است. دستورالعمل تالین توسل و تهدید به توسل به زور را در اقدامات سایبری تعریف کرده و هر دوی آن‌ها را ممنوع دانســـته اســـت. این دستورالعمل، به بررسی حقوق حاکم بر جنگ سایبری پرداخته و به‌طور کلی در برگیرندهٔ حقوق بر جنگ، حقوق بین‌الملل حاکم بر توسل به زور از ســـوی کشورها به عنوان ابزار سیاســـت ملی و حقوق بین‌الملل، تنظیم‌کنندهٔ رفتار درگیری‌های مسلحانه است (صلاحی، ۱۳۹۵: ۳۶).

- **اعلامیهٔ گروه ۷ در خصوص «رفتار مســـئولانهٔ دولت‌ها در فضای سایبری» در ایتالیا ۲۰۱۷:** این اعلامیه، با اشـــاره به گســـترش مخاطرات ناشـــی از تشـــدید منازعات و اقدامات تلافی‌جویانه در فضای ســـایبری و تهدیدات متوجه زیرساخت‌های حیاتی و مداخلهٔ سایبری در فرآیندهای انتخاباتی آمریکا و فرانســـه، بر ضرورت افزایش فوری همکاری‌های بین‌المللی برای ارتقای امنیت و ثبات در فضای سایبری و بر اعمال قوانین بین‌المللی بر رفتار دولت‌ها، در فضای ســـایبری تأکید کرده و بیان می‌کند که افراد لازم اســـت از حقوقی که در محیط آفلاین برخوردار هستند، در محیط آنلاین نیز برخوردار باشند.

قوانین داخلی: تصویب قانون حمایت از حقوق پدیدآورندگان نرم‌افزارهای رایانه‌ای ســـال ۱۳۷۹ (مادهٔ ۱۳ قانون مذکور، نقض حقوق پدیدآورندگان آن دسته از نرم‌افزارهای رایانه‌ای که مورد حمایت این قانون قرار گرفته‌اند، جرم تلقی و برای آن مجازاتی معادل ۹۱ روز تا ۶ ماه حبس و جزای نقدی تعیین کرده است)؛ سیاست‌های کلی شبکه‌های اطلاع‌رسانی رایانه‌ای از سوی مقام رهبری در سال ۱۳۸۰؛ تصویب قانون تجارت الکترونیک سال ۱۳۸۲ به خصوص

بـــاب چهارم آن در مورد جرائم و مجازات اقتباس شـــده از قانـــون نمونهٔ تجارت الکترونیکی آنسیترال است که به موجب مواد ۶۶، ۶۷،۶۸،۶۹، ۷۴، ۷۵، ۷۶ و ۷۷ این قانون، کلاهبرداری، جعل و دستیابی و افشای غیرمجاز اسرار تجاری، نقض حقوق مربوط به مالکیت معنوی (کپی رایت) و غیره که از طریق رایانه و در بستر تجارت الکترونیکی انجام شود، جرم تلقی و برای آن مجازات تعیین شده است (صبح خیز، ۱۳۹۴: ۱۲)؛ قانون وظایف و اختیارات وزارت ارتباطات و فنـــاوری اطلاعـــات مصوب ۱۳۸۲؛ قانون مجازات جرائم نیروهای مســـلح ۱۳۸۲/۱۰/۹(به موجب مادهٔ ۱۳۱ این قانون، جعل اطلاعات و داده‌های رایانه‌ای، تســـلیم و افشـــای غیرمجاز اطلاعات و داده‌ها و سوء استفادهٔ مالی از طریق رایانه (کلاهبرداری و اختلاس) توسط نظامیان جرم تلقی و مرتکب، حســـب مورد به مجازات جرم ارتکابی، محکوم می‌شـــود)؛ قانون نحوهٔ مجازات اشـــخاصی که در امور ســـمعی و بصری فعالیت‌های غیرمجاز می‌کنند، مصوب سال ۱۳۸۶؛ دستورالعمل رئیس قوهٔ قضاییه در مورد توسعهٔ کاربری فناوری اطلاعات و ارتباطات در دستگاه قضایی و استقرار نرم‌افزار مدیریت پرونده قضایی سال ۱۳۸۶؛ قانون جرائم رایانه‌ای ســـال ۱۳۸۸؛ قانون انتشار و دسترسی آزاد به اطلاعات سال ۱۳۸۸ مصوب مجمع تشخیص مصلح به خصوص مواد ۲۱ و ۲۲ آن در مورد مسئولیت مدنی و کیفری.

تشکیل شورای عالی مجازی در سال ۱۳۹۰ از مهم‌ترین موارد تلاش برای تطبیق قوانین و نهادهای داخلی با نظام جهانی فضای مجازی است. سند راهبردی پدافند سایبری کشور در مورخه ۹۴/۲/۲۹ تهیه شـــده و مطابق اساسنامه به تصویب مقام معظم رهبری رسیده است. براســـاس سند مذکور، هر لحظه ممکن است زیر ســـاخت‌های فناوری اطلاعات، شبکه‌های ارتباطی در ســـامانه‌های رایانه‌ای کشـــور که اصطلاحاً به عنوان ســـرمایهٔ ملی سایبری تلقی می‌شـــوند، از طریق تهدید ســـایبری، تخریب شده یا اطلاعات آن‌ها افشا یا به علت دسترسی غیرمجاز مختل شـــود. برای جلوگیری از خطرات ذکر شـــده، نظام جامع پدافند کشـــور باید طوری طراحی و ایجاد شـــود که از طریق رصد، پایش و مدیریت و کنترل به هنگام، تهدید و تهاجم ســـایبری دشـــمن را خنثی و از زیرساخت‌های فناوری اطلاعات کشور محافظت کند (کرم روان، ۱۳۹۸: ۱). مراحل دفاع ســـایبری که در ســـند راهبردی پدافند ســـایبری کشور ارائه شـــده اســـت، دارای مؤلفه‌های بازدارندگی، جلوگیری، هشداردهی، شناسایی، آمادگی

اضطراری و واکنش است. چرخهٔ پدافند سایبری، به صورت یک زنجیرهٔ متصل به هم بوده و با انجام این اقدامات صیانت فضای سایبر را ارتقاء می‌دهد.

– **قانون جرائم رایانه‌ای:** نخســـتین قانون جامع و متمرکز در ایران، قانون جرائم رایانه‌ای مصوب ۱۳۸۸ و قوانین اصلاحی آن، مندرج در قانون آیین دادرسی کیفری ۱۳۹۲ است. این قانون)قانون جرائم رایانه‌ای(مشتمل بر سه بخش و پنجاه و چهار ماده است و در بخش یکم این قانون، به جرائم و مجازات مقرر در قانون می‌پردازد و در هفت فصل، تقسیم‌بندی جرائم و در فصل هشـــتم، موارد تشـــدید مجازات را مطرح می‌کند. یکی از نوآوری‌های قانون جرائم رایانه‌ای نسبت به دیگر مصوبات قانونی، این است که حوزهٔ کشف جرائم و شناسایی مجرمان رایانه‌ای را قاعده‌مند کرده است.

باوجود تأکید قوانین داخلی ایران بر قانون‌گذاری ملی، مواضع بین‌المللی ایران در اتحادیهٔ بین‌المللی مخابرات، مبنی بر خروج زیرســـاخت‌های ســـایبری از انحصار قوانین کشورهای غربـــی، در کنار تأکید بر همکاری همه‌جانبهٔ بین‌المللی میان همه ذینفعان و پذیرش ســـند اصلاحی اتحادیه، گواه بر پذیرش روش مختلط در مدیریت فضای سایبر از سوی ایران است.

پیشگیری و نقش پلیس در پیشگیری از جرائم سایبری

پیش‌بینی، شناســـایی و ارزیابی خطر وقوع جرم از یک‌ســـو و اتخاذ تدابیر و اقدام‌های لازم برای از بین بردن یا کاهش جرم در قالب برنامهٔ ملی از ســـوی دیگر، از مؤثرترین روش‌های کاربردی پیشـــگیری از جرم به شـــمار می‌آیند. تدوین برنامهٔ ملی پیشگیری از جرم، مستلزم فرآیندی اســـت که با در نظر گرفتن آن، ســـازوکارهای مهار جرم در هر جامعه مشخص شده و ســـپس به اجرا در می‌آیند. در همین خصوص، شـــرکت‌های امنیت خصوصی نیز از طریق مراقبت و نگهبانی و ســـازوکارهای کنترل ورودی‌ها و هشـــاردهنده‌ها، در پیشگیری از جرم مشـــارکت می‌کنند. در واقع، پیشـــگیری از جرم، گاهی آگاهانه و گاهی به طور ناخودآگاه، توسط واحدهای تأمین امنیت ادارات و پلیس اعمال و اجرا می‌شود (توریول[1]، ۲۰۰۶: ۴۸).

جرم ســـایبر در واقع، در بســـتر دادوســـتدهای الکترونیکی و علیه داده ارتکاب یافته است

1.. TournYoL Du cLoS

و اطلاعـــات و به ندرت علیه ســـامانه‌های فیزیکی و ســـخت‌افزاری رخ می‌دهند. بنابراین، با پیشگیری این جرائم، می‌توان آثار منفی آن را در جامعه به حداقل رساند.

نگاهی گذرا به ادبیات حقوقی موجود، نشان می‌دهد که قانون‌گذار، در اکثر قریب به اتفاق موارد، از واژۀ پیشـــگیری استفاده کرده اســـت. جوهرۀ ذاتی جرم‌شناسی، به عنوان شاخه‌ای از علوم جنایی بر پیشـــگیری از جرائم اســـتوار بوده که به بررســـی علل، آثار و نتایج پدیدۀ بزهکاری می‌پردازد. معانی تازه برای پیشـــگیری از جرم با تأکید بر عوامل فردی و اجتماعی مختلف که بر وقوع جرم مؤثرند، راهکارهایی را پیش‌روی جرم‌شناســـان قرار داده اســـت. به تعبیر ســـاده، پیشـــگیری، هر اقدام سیاست جنایی بدون تأکید بر تهدید کیفری یا اجرای آن اســـت که با هدف تحدید امکان پیش‌آمد جنایی از راه‌های گوناگون انجام می‌شـــود. با این وصف، قلمرو جرم‌شناســـی امروزه بسیار گسترده شـــده و بزهکاری نیز تاکنون مورد مطالعه رشـــته‌های مختلفی قرار گرفته اســـت (اردبیلی، ۱۳۸۵: ۲۱). با توجه به ویژگی‌های عمدۀ پیشـــگیری که عبارت‌اند از: غیرقهرآمیز بودن تدابیر پیشگیرانه، اختصاصی بودن این تدابیر، کاســـتن آثار جرم و در نظر گرفتن عوامل خطر و محیط اجتماعی (جعفری، ۱۳۸۷: ۳۴)، دو نوع پیشـــگیری اجتماعی و پیشگیری وضعی توسط پلیس در میان انواع اقدامات پیشگیرانۀ این نهاد از مقبولیت بیشتری برخوردارند.

– **نقش پلیس در پیشـــگیری اجتماعی از جرائم ســـایبری:** پلیس به عنوان ضابط عام دادگســـتری، از کنشـــگران اصلی در برابر پدیدۀ مجرمانه و نهاد اصلی شناســـایی و بررسی جرم، در مقایسه با سایر نهادها، ارتباط نزدیک‌تری با بزه‌دیدگان دارد. از نظر رده‌بندی درون سازمانی، پلیس یکی از نهادهای پیشرو مبارزه با جرائم رایانه‌ای در کشور به شمار می‌آید. در ســـال ۱۳۷۸، با برگزاری نخســـتین همایش جرائم رایانه‌ای در کشور، این موضوع را به اثبات رساند و یکی از ادارات کل خود را البته همراه با جرائم خاص (نظیر کلاهبرداری و جعل) به رسیدگی جرائم رایانه‌ای اختصاص داد)جلالی فراهانی، ۱۳۸۴: ۲۴۹). نظارت همگانی پلیس در حوزۀ پیشـــگیری، به معنای مشـــارکت عموم مردم در اطلاع‌رسانی و همکاری با پلیس در جامعه به منظور کاهش جرائم و جرم است.

در ایالات‌متحده، وظیفۀ اطلاع‌رسانی برای پیشگیری از جرائم امنیتی به عهدۀ پلیس این کشور

نهاده شـــده است. در واقع، به منظور پیشگیری غیرکیفری از جرائم، دولت ایالت متحده آمریکا شماری از برنامه‌های آموزشی و آگاهی‌رسانی برای مقابله با جرائم سایبری، صرف‌نظر از هویت یا مقاصد مرتکبان، پشتیبانی می‌کند. برای مثال، وب‌سایت اف.بی.آی، اطلاعات و منابع مربوط به محفوظ داشتن رایانه‌ها از تأثیرات جرائم سایبری را ارائه می‌کند (پاکزاد، ۱۳۸۸: ۲۹۹).

پیشـــگیری اجتماعی شامل مجموعه اقدامات پیشگیرانه از جرائم است که به دنبال حذف یا خنثی کردن آن دسته از عواملی است که در تکوین جرم مؤثر است. این نوع پیشگیری، بر مبنای علت‌شناسی جرائم استوار است و با دخالت در محیط‌های اجتماعی، مانع از شکل‌گیری رفتار بزهکارانه و خنثی‌ســـازی عوامل جرم‌زا می‌شود. به عبارت دیگر، پیشگیری اجتماعی از جرم، راهبردی است که برخورد با علل ریشه‌ای اقدامات مجرمانه و بزه‌دیدگی را مدنظر قرار می‌دهد (گرنت[1]، ۲۰۱۵: ۵). به همین دلیل، در بررسی شیوه‌های پیشگیری از جرائم سایبری، از این نوع تقســـیم‌بندی استفاده می‌شـــود. پیش از پرداختن به جزییات این نوع پیشگیری، مناســـب است به قطعنامهٔ هشتمین کنگرهٔ سازمان ملل متحد در خصوص پیشگیری از جرم و اصلاح مجرمان که در سیزدهمین اجلاس سازمان ملل متحد توسط مجمع عمومی سازمان در قالب قطعنامهٔ شمارهٔ ۴۵/۱۲۱ تأیید شد، اشاره شود. در این قطعنامه، از کشورهای عضو خواســـته شده اســـت که در صورت لزوم با مدنظر قرار دادن این موارد، تلاش‌های خود را در مبارزه با جرائم رایانه‌ای شـــدت بخشـــند: مدرنیزه کردن قوانین و دادرســـی کیفری؛ ارتقای ضوابط پیشگیرانه و امنیتی رایانه؛ گزینش راه‌هایی برای حساس کردن عامهٔ مردم، قوهٔ قضاییه و پلیس به عنوان مجری قوانین نسبت به این مسئله و اهمیت پیشگیری از ارتکاب جرم‌های رایانه‌ای و دادن آموزش‌های کافی به مأموران و عوامل مسئول در زمینهٔ پیشگیری، تحقیقات، تعقیـــب و احقاق حق در جرائم رایانه‌ای. در میان اقدامات پیشـــگیری اجتماعی که می‌تواند به کاهش جرائم ســـایبری کمک کند، می‌توان به برنامه‌های خانواده‌مدار، تدابیر آموزشـــی-سایبری، بالا بردن سواد رسانه‌ای، تنظیم کدهای رفتاری، اطلاع‌رسانی و اطلاع‌گیری، توجه به حکمرانی خوب و شاخص‌های آن، مشارکت و اجماع‌گری، ارتقای پاسخگویی و شفافیت، فرهنگ‌سازی و تولید رسانه‌ای اشاره کرد (بهره‌مند و داودی، ۱۳۹۷: ۴۴).

1.. Grant

پیشـــگیری اجتماعی در دو شاخهٔ پیشـــگیری اجتماعی جامعه‌مدار و پیشگیری اجتماعی رشدمدار قرار می‌گیرد. تدابیر پیشگیری اجتماعی جامعه‌مدار توسط پلیس، سعی در بر طرف کـــردن زمینه‌هـــای اجتماعی بروز انگیزه‌های مجرمانه و منحرفانـــه را دارد (جلالی فراهانی، ۱۳۸۹: ۱۲۱-۱۵۵). تدابیر پیشـــگیرانهٔ اجتماعی رشدمدار توسط پلیس، دومین اقدام مهم برای خنثی‌ســـازی عوامل اجتماعی جرم‌زا و انحراف‌زا اســـت. منظور از پیشگیری رشدمدار، مجموعه اقداماتی اســـت که در دوران رشـــد و تکامل شـــخصیتی و جسمی اشخاصی به اجرا در می‌آید که در معرض ارتکاب این جرائم قرار دارند. با توجه به اینکه پیشـــگیری رشـــدمدار برخلاف پیشـــگیری جامعه‌مدار، با قشر جوان و نوجوان سروکار دارد، خط‌مشی‌ها و اقدامات پلیس، رویکردی تربیتی و آموزشی داشته و در این نوع پیشگیری، قدرت شناخت و تمیز آن‌ها تقویت می‌شـــود و مهارت‌های زندگی اجتماعی در فضای مجازی را می‌آموزند تا بتوانند در هنگام مواجهه با معضلات و انحرافاتی که در فضای سایبر با آن مواجه می‌شوند، واکنش‌های منطقی و صحیح از خود بروز دهند.

- **نقش پلیس در پیشـــگیری وضعی از جرائم سایبری:** اقدامات پیشگیرانهٔ وضعی پلیس، از جرائم ســـایبری را می‌توان در چهار گروه بررســـی کرد (حیدری نژاد، ۱۳۹۷: ۲۹)؛ تدابیر محدود کنندهٔ پلیس یا ســـلب‌کنندهٔ در دسترس، تدابیر نظارتی پلیس، تدابیر صدور مجوز و ابزارهای ناشـــناس کننده و رمزگذاری. بنابراین، پیشـــگیری وضعی توسط نهاد پلیس شامل تدابیری به منظور کاهش فرصت‌های مجرمانه است که اولاً به سوی اشکال خاصی از جرائم معطوف شـــده‌اند، ثانیاً شامل مدیریت، طراحی و دست‌کاری در محیط به صورت نظام‌مند و دائمی می‌باشـــند و در نهایت برای دشوارتر کردن و پرخطر کردن ارتکاب این جرائم نوظهور توسط پلیس پیشگیری، از آن استفاده می‌شود. بر این اساس، پلیس پنج راهبرد اصلی را برای پیشگیری وضعی از جرائم سایبری به کار می‌بندد: افزایش میزان تلاش به منظور جلوگیری از ارتکاب جرم رایانه‌ای، افزایش اطلاع‌رسانی خطرهای ناشی از ارتکاب جرم سایبری، کاهش دســـتاوردها، کاهش عوامل محرک و ســـلب توجیه‌ها (بهره‌مند و کوره‌پز و سلیمی، ۱۳۹۳: ۱۴۷-۱۷۶).

لازم بـــه ذکر اســـت، امروزه تدابیر پیشـــگیرانهٔ پلیس در جهت جلوگیـــری از وقوع جرائم

رایانه‌ای، توجیهی جهت ایجاد اخلال در امنیت و آزادی مردم محســـوب نمی‌شـــود. لذا این تدابیر، باید با حفظ حریم خصوصی اشـــخاص توسط پلیس و صرفاً جهت پیشگیری از جرائم سایبری، صورت گیرد و برابر مفاد مادۀ ۲۱، احدی در زندگی اعلامیۀ حقوق بشر همواره باید مدنظر قرار گیرد (وروایی و مؤمنی پور، ۱۳۹۳: ۵۵).

نقش پلیس جمهوری اسلامی ایران در پیشگیری از جرائم سایبری

اگرچه حقوق‌دانان به منظور حفظ نظم جامعه و پیشگیری از وقوع جرم، برای قوانین آیین دادرســـی کیفری، اهمیت بیش‌تری قائل شـــده‌اند (آخوندی، ۱۳۸۰: ۶۴) و پلیس را صرفاً مسئول کشف و تعقیب جرائم می‌پندارند، اما باید اذعان داشت که پلیس را می‌توان مهم‌ترین عامل پیشگیری از جرم، به شمار آورد؛ زیرا نقش حساس آن اقتضا می‌کند که گام‌هایی جلوتر از زمان برداشـــته و از پیش، آمادگی‌های لازم بـــرای مواجهه با ناامنی‌های احتمالی آینده را احراز کند (مظفری، ۱۳۸۴: ۵). پلیس جمهوری اسلامی ایران تلاش می‌کند تا با بهره‌گیری از آخرین دستاوردهای فناوری اطلاعات و ارتباطات و سیستم‌های پیشرفتۀ انتظامی- امنیتی کشـــور، امنیت اجتماعی را بهبود بخشـــیده و محیطی امن توأم با آسایش عمومی برای کلیۀ شهروندان فراهم آورد.

معاونت آگاهی ناجا اواخر ســـال ۱۳۷۸ شمســـی، به انحای گوناگون شـــروع به جمع‌آوری اطلاعاتی پیرامون جرائم ســـایبری کرد و در همین راســـتا، تحقیقی تحت عنوان «شـــناخت جرائم ســـایبری» توســـط جهاد دانشگاهی دانشـــگاه علم و صنعت صورت گرفت. همچنین، با بهره‌گیری از نظریه‌های کارشناســـان و متخصصان شـــورای انفورماتیک و تشکیل جلسات متعدد با صاحب‌نظران حقوقی و انفورماتیکی، به این نتیجه دست یافت که تشکیل واحدهای مبارزه با جرائم ســـایبری ضروری اســـت. تلاش‌های انجام شده سبب تصویب و ابلاغ تشکیل ادارۀ کل مبارزه با جرائم رایانه‌ای در زیر مجموعۀ معاونت آگاهی و همچنین تشـــکیل دایرۀ مبارزه با جرائم رایانه‌ای در ادارۀ آگاهی تهران بزرگ شد. بدین ترتیب، پلیس متخصص برای پیگیری پرونده‌های جرائم رایانه‌ای از ســـال ۱۳۸۱ شمســـی فعالیت خود را با قوت و اقتدار رسماً آغاز کرد (پرویزی، ۱۳۸۴: ۳۹-۴۱).

بدون تردید، سیســـتم کلان مبارزه با جرم که از ســـوی پلیس اتخاذ می‌شود، چه در محیط فیزیکی و چه در فضای مجازی یکســـان اســـت و پلیس در پیشگیری از وقوع جرائم سایبری، همان جایگاه خود را خواهد داشت. در واقع، اقدامات پلیس برای پیشگیری از وقوع این جرائم، چیزی جز مبارزهٔ وضعی و سیاست عام این نهاد در مقابله با سایر جرائم نیست. اما آنچه باعث تفاوت در این حوزه می‌شـــود، ویژگی‌های منحصر به فرد جرائم ســـایبری است که شیوه‌های اجرایی خاص خود را به منظور تحقق این سیاست عام طلب می‌کند (آیکاو، ۱۳۸۳: ۵۱).

در محیط فیزیکی، حضور پلیس در جامعه، عاملی در پیشگیری از جرم محسوب می‌شود. شکل و ترکیب خودروی پلیس و مأموران ملبس به لباس پلیس، تهدید برای مجرمان بالقوه به شـــمار می‌رود. به بیان دیگر، حضور پلیس در جامعه را می‌توان نوعی تهدید ضمنی برای مجرمان تلقی کرد. بدون تردید، حضور فیزیکی پلیس در مواردی که جرائم سایبری با ورود کاربران غیرمجاز به یک ســـایت رایانه‌ای صورت می‌پذیرد، نقش مؤثری در پیشگیری از این جرائم خواهد داشـــت (آیکاو، ۱۳۸۳: ۱۶۹). اما آیا به هنگامی که جرائم مزبور توســـط خطوط ارتباطی و از طریق شـــبکهٔ اینترنت و بدون نفوذ فیزیکی در ســـایت رایانه‌ای ارتکاب می‌یابد، می‌توان اقدامات پیشگیرانه را در این فضای مجازی تصور کرد و آن را محقق دانست؟

به نظر می‌رسد در چنین فضایی نیز می‌توان حضور داشت و با گشت‌زنی و مراقبت، مجرمان بالقـــوه را تهدیـــد کرد. به منظور انجام این امر، ابزارها و روش‌های خاصی موردنیاز اســـت که آشـــنایی با آن‌ها برای مأموران گشـــت شـــبکه‌های رایانه‌ای واحد مبارزه با جرائم ســـایبری ســـازمان‌های پلیس لازم و ضروری اســـت. گشت‌زنی و مراقبت یک مظنون در فضای مجازی کار چندان آســـانی نیست و هیچ ســـازمان پلیسی هرچند قدرتمند، به تنهایی نمی‌تواند این کار را انجام دهد، بلکه همکاری چندبخشی دولتی و غیردولتی لازمهٔ این اقدام است. در این مرحله از کار، وجود تعامل و همکاری مناسب میان شرکت‌های مخابراتی ارائه دهندهٔ خدمات و پلیس، اهمیت ویژهٔ خود را نشان می‌دهد.

امروزه، نرم‌افزارهای قدرتمندی در اختیار پلیس وجود دارد که شبیه سیستم‌های دزدگیر عمل کرده و پلیس یا مسئول امنیتی را از هرگونه تهدید قریب‌الوقوع به منظور انجام عملیات مجرمانه در فضای مجازی مطلع می‌سازد و امکان پیشگیری از این جرائم را به پلیس می‌دهد.

بـــه علاوه، ایـــن نرم‌افزارها آن دســـته از کاربران مجاز که با عدم رعایـــت مقررات مربوط به طبقه‌بندی، قصد دسترسی به اطلاعات غیرمجاز را دارند، شناسایی کرده و مشخصات لازم را در اختیار پلیس خواهد گذاشت. بسیاری از سیستم‌ها، اطلاعات مربوط به تلاش‌های موفق یا ناموفق افراد در ورود به سیستم را ثبت می‌کند. همچنین، سیستم‌های مزبور، امکان شناسایی افراد غیرمجاز که به‌طور مکرر، رمز عبور نادرســـت را توســـط صفحهٔ کلید تایپ می‌کنند نیز وجود دارد. البته چنانچه کاربر غیرمجاز، اطلاعات لازم برای ورود به سیستم را داشته باشد، با نفوذ در رایانه و دستیابی به فایل‌های حاوی رمز عبور، تمهیدات فوق را بی‌ثمر خواهد کرد.

یکی دیگر از شیوه‌های پیشگیری از جرم که سال‌هاست به‌طور معمول توسط نیروی انتظامی به کار گرفته می‌شود، آموزش همگانی و همچنین شناسایی و ارائه آموزش‌های خاص به اشخاص و سازمان‌هایی است که احتمال دارد در معرض جرائم سایبری قرار گیرند. در واقع، به‌کارگیری این شـــیوه، به همان اندازه که در پیشـــگیری از جرائم ارتکابی در محیط فیزیکی مؤثر است، در فضای مجازی نیز از تأثیر قابل‌توجهی برخوردار خواهد بود (آیکاو، ۱۳۸۳: ۱۸۴).

نقش پلیس بین‌الملل در مبارزه با جرائم سایبری

ســـال‌های متمادی اســـت که پلیس بین‌الملل فعالیت خود را در مبارزه با جرائم سایبری آغاز کرده اســـت. این سازمان با بهره‌گیری از متخصصان و کارشناسان کشورهای عضو، چند گروه کاری را در این زمینه تشـــکیل داده اســـت و روسای واحدهای مبارزه با جرائم سایبری کشـــورهای با تجربهٔ عضو ســـازمان را گرد هم آورده است. گروه‌های کاری منطقه‌ای در اروپا، آسیا، آمریکا و افریقا زیر نظر کمیتهٔ راهبردی جرائم فناوری اطلاعات مستقر در دبیرخانهٔ کل پلیس بین‌الملل فعالیت می‌کنند. گروه کاری اروپایی پلیس بین‌الملل، با حضور کارشناسانی از هلند، اسپانیا، بلژیک، آلمان، فرانسه، فنلاند، انگلیس، سوئد و ایتالیا در سال ۱۹۹۰ میلادی تشـــکیل شـــد و از آن به بعد، سه مرتبه در سال تشکیل جلسه می‌دهد. از جمله فعالیت‌های گروه کاری، می‌توان به تهیهٔ کتاب و لوح فشـــردهٔ راهنمای جرائم رایانه‌ای و پی‌جویی آن‌ها، تشکیل دوره‌های آموزشی برای نیروهای پلیس در طول پنج سال گذشته، سیستم اعلام‌خطر و پاسخگویی شبانه‌روزی اشاره کرد.

گروه کاری آمریکایی جرائم مرتبط با فناوری اطلاعات پلیس بین‌الملل، مرکب از کارشناسان و متخصصان کشـــورهای کانادا، آرژانتین، جامائیکا، ایالات‌متحده، کلمبیا و شـــیلی است که تاکنون چندین دوره آموزشی نیز برای نیروهای پلیس برگزار کرده است. گروه کاری جنوب اقیانوس آرام و آســـیایی پلیس بین‌الملل که در هند تشکیل‌شده و متخصصانی از کشورهای چین، هنگ‌کنگ، هند، استرالیا، ژاپن، نپال و سریلانکا عضو آن می‌باشند، فعالیت خود را از نوامبر سال ۲۰۰۰ میلادی آغاز کرده‌اند.

گروه کاری آفریقایی به منظور پیشـــگیری از جرائـــم مرتبط با فناوری اطلاعات، مرکب از کارشناســـان آفریقای جنوبی، نامیبیا، تانزانیا، اوگانـــدا و رواندا در ژوئن ۱۹۹۸ میلادی آغاز کرد. این گروه، دومین دورهٔ آموزش نیروهای پلیس را نیز با مساعدت مالی سفارت‌خانه‌های انگلیس و فرانسه برگزار کرده است (پرویزی ۱۳۸۴: ۸۷).

نتیجه‌گیری

تحقیـــق حاضر به بررســـی اقدامات پیشـــگیرانه برای جلوگیری از وقـــوع جرائم رایانه‌ای می‌پردازد. آنچه مســـلم اســـت پلیس از دیرباز به عنوان یک نهاد اجرایی، نقشـــی مؤثر در پیشگیری، مبارزه و کاستن وقوع بزه در جامعه ایفاء می‌کند. با عنایت به تعریف به عمل آمده از جرم سایبری، آنچه مسلم است وقوع این جرائم برخلاف جرائم سنتی پیشین در محیطی غیر فیزیکی واقع می‌شـــود و آنچه بیش از پیش وظایف نهادهای پیشـــگیرانه و کنترل کنندهٔ این نوع جرائم از جمله پلیس را خطیر می‌کند، این است که روش‌های سنتی، در پیشگیری و مبارزه با این جرائم پاسخگو نیست. ماهیت و ویژگی‌های خاص جرائم سایبری از جمله داشتن ابعاد جهانی و فراملی، فقدان توافق جهانی پیرامون تعریف قانونی واحد از جرائم ســـایبری، بالا بودن ســـرعت ارتکاب این جرائم، فقدان رویه‌های مشخص پیرامون همکاری‌های متقابل و بالا بودن هزینه‌های کشـــف این جرائم، مراجع قضایی و انتظامی را با چالش‌های جدیدی مواجه کرده است.

در حال حاضر، کشـــور ما به هیچ‌کدام از کنوانسیون‌های مبارزه با جرائم سایبری نپیوسته اســـت، اما خصوصیات ویژه جرائم ارتکابی در فضای مجازی، مبنی بر داشـــتن جنبهٔ فراملی و

بین‌المللی، لزوم حکومت قواعدی از این قبیل را به این دسته از جرائم، بیش از هر چیز دیگری روشن می‌سازد. امروزه پلیس لازم است با استفاده از نرم‌افزارهای قدرتمندی که در اختیار او قرار دارد، با گشت‌زنی و مراقبت در فضای مجازی، در پیشگیری از وقوع جرائم سایبری نقش مؤثری ایفا کند. تعامل و همکاری مناسب میان شرکت‌های مخابراتی ارائه‌کنندهٔ این‌گونه خدمات و پلیس می‌تواند در فرایند پیشگیری کمک زیادی داشته باشد. آموزش همگانی و همچنین شناسایی و ارائه آموزش‌های خاص به اشخاص و سازمان‌های که احتمال می‌رود در معرض جرائم سایبری قرار می‌گیرند، یکی دیگر از شیوه‌های پیشگیری از این جرائم است. از سویی به نظر می‌رسد می‌بایست نوعی تبادل اطلاعات، انتقال تجربیات و یکسان‌سازی اقدامات پیشگیرانه با توجه به شرایط اجتماعی و فرهنگی کشورهای پیشرو در امر مبارزه با جرائم سایبری صورت گیرد. همچنین، پلیس توانسته است با آموزش همگانی و همچنین شناسایی و ارائه آموزش‌های خاص به اشخاص و سازمان‌هایی که احتمال دارد در معرض جرائم سایبری قرار می‌گیرند، به همان اندازه که در پیشگیری از جرائم ارتکابی در محیط فیزیکی مؤثر واقع می‌شود، در فضای مجازی نیز از تأثیر قابل‌توجهی برخوردار باشد.

منابع

منابع فارسی

- احمدونـــد، علی‌محمـــد؛ عطایی جعفری، امیر مســـعود (۱۳۸۳). نقش و راهبرد فناوری اطلاعات در سیستم پلیس و فضاهای مجازی جرائم در ایران. *دوماهنامهٔ انسانی پلیس*. سال اول، شمارهٔ ۳.

- آخوندی، محمود (۱۳۸۰). *اندیشه‌هایی بر آیین دادرسی کیفری*. تهران: انتشارات وزارت فرهنگ و ارشاد اسلامی.

- اردبیلی، محمدعلی (۱۳۸۵). *حقوق جزای عمومی*. تهران: انتشارات میزان.

- آیکاو، دیوید جی (۱۳۸۵). *راهکارهای پیشگیری و مقابله با جرائم رایانه‌ای* (اکبر استرکی، محمدصـــادق روزبهانی، تورج ریحانی و راحله الیاســـی، مترجمان). تهران: معاونت پژوهش دانشگاه علوم انتظامی امین.

- بهره‌مند، حمید و داودی، ذوالفقار (بهار و تابستان ۱۳۹۷). پیشگیری اجتماعی از جرائم امنیتی – سایبری. *مطالعات حقوق کیفری و جرم‌شناسی*. دورهٔ ۴۸، شمارهٔ ۱.

- پاکزاد، بتول (۱۳۸۸). *تروریســـم ســـایبری*. رســـالهٔ دکتری حقوق جزا و جرم‌شناسی. دانشگاه شهید بهشتی.

- پرویزی، رضا (۱۳۸۴). *پی‌جویی جرائم رایانه‌ای*. تهران: انتشارات جام جم.

- جعفـــری، مجتبی (۱۳۸۴). خلاصه‌ای از مباحث درس جرم‌شناســـی دکتر نجفی ابرند آبادی.

- جلالی فراهانی (۱۳۸۴). *پیشگیری از جرائم رایانه‌ای*. پایان‌نامهٔ کارشناسی ارشد حقوق کیفری و جرم‌شناسی. دانشگاه امام صادق (ع).

- جلالی فراهانی، امیرحسین (۱۳۸۹). پیشگیری از جرائم رایانه‌ای، *مجلهٔ حقوقی دادگستر*. شمارهٔ ۴۷.

- جلالی، محمود و توسلی اردکانی، سعیده (زمستان ۱۳۹۸). ضرورت ایجاد نظام هماهنگ حقوقـــی بین‌المللی در مقابله با جرائم در فضـــای مجازی. *فصلنامهٔ مطالعات حقوق عمومی*. دورهٔ ۴۹، شمارهٔ ۴.

- جوان جعفری، محمد (۱۳۹۳). جرائم سایبر و چالش‌های نوین سیاست کیفری. مجموعه *مقالات همایش جهانی‌شدن حقوق و چالش‌های آن*.

- حقیقی، لیلا (۱۳۹۵). مروری بر جرائم سایبری؛ با تأکید بر قوانین مجازات رایانه‌ای. *دومین کنفرانس ملی راهکارهای توسعه و ترویج آموزش علوم در ایران*.

- حیدری نژاد، نصراله (۱۳۹۷). پیشگیری وضعی در جرائم سایبری از منظر حقوق کیفری ایران و جهان. *مجلهٔ حقوقی قانون یار*. دورهٔ ۲، شمارهٔ ۶.

- دشتی، بیتا و افشاری، مریم (بهار و تابستان ۱۳۹۸). مطالعهٔ تطبیقی جرائم سایبری در ایران و حقوق بین‌الملل. *پژوهشنامهٔ حقوق تطبیقی*. سال سوم، شمارهٔ ۴.

- رضوی، محمد (۱۳۸۷). جرائم سایبری و نقش پلیس در پیشگیری از این جرائم و کشف آن‌ها. *فصلنامهٔ دانش انتظامی*. سال نهم، شمارهٔ اول.

- صبح‌خیز، رضا (پاییز ۱۳۹۴). چالش‌های حقوقی جرائم سایبری در نظام حقوق بین‌الملل و نظام حقوقی ایران. *فصلنامهٔ پژوهش‌های اطلاعاتی و جنایی*. سال دهم، شمارهٔ سوم.

- صلاحی، سهراب و کشفی، سید مهدی (۱۳۹۵). جنگ سایبری از منظر حقوق بین‌الملل با نگاه به دستورالعمل تالین. *فصلنامهٔ مطالعات قدرت نرم*. شمارهٔ ۱۴.

- ضیایی، سید یاسر (زمستان ۱۳۹۵). قانون‌گذاری در فضای سایبر؛ رویکرد حقوق بین‌الملل و ایران. *مجلهٔ حقوقی بین‌المللی*. دورهٔ سی و چهارم، شمارهٔ ۵۷.

- طهماسبی، جواد و شاهمرادی، خیرالله (زمستان ۱۳۹۷). چالش‌ها و خلأهای موجود در فرآیند رسیدگی به جرائم سایبری. *مجلهٔ حقوقی دادگستری*. سال هشتاد و دوم، شمارهٔ یک‌صد و چهارم.

- کرد علیوند، روح الدین و میرزایی، محمد (تابستان ۱۳۹۷). گونه‌شناسی جرائم سایبری با نگاهی به قانون جرائم رایانه‌ای و آمار پلیس فتا. *مجلهٔ حقوقی دادگستری*. سال هشتاد و دوم، شمارهٔ یکصد و دوم.

- وروایی، اکبر و مؤمنی پور، حسین (۱۳۹۰). *از علت شناسی تا پیشگیری جرائم سایبری*.

- بهره‌مند، حمید؛ کوره‌پز، حسین و سلیمی، احسان (۱۳۹۳). راهبردهای وضعی پیشگیری از جرائم سایبری. *مجلهٔ آموزه‌های حقوق کیفری*.

منابع انگلیسی

- Grant, H. (2015). Social crime prevention in the developing world: exploring the role of police in crime prevention, Switzerland: springer.

- Solange Ghernaouti-Hélie (2010). We Need a Cyberspace Treaty: Regional and Bilateral Agreements Are Not Enough, Inter Media, vol. 38, Issue 3.

-Ploug, Thomas (May 2017). Ethics in Cyberspace: How Cyberspace May Influence Interpersonal Interaction, Ballerup28. Denmark, Springer pub: 2009, P 70(NATO Cooperative Cyber Defence Centre of Excellence, Accessed 17.

-TournYoL Du cLoS,Lorraine (2006). Evolutions de Loffer de securiteprivee en france RIcpT,n1.