فصلنامه علمی تخصصی فقه و حقوق معاصر

سال هشتم- شماره ۲۵- پاییز۱۴۰۲- ص۳۴۰-۳۶۵

موانع و محدودیت های پلیس فتا در کشف جرایم سایبری درفضای مجازی

سجاد رجبی نژاد[۱]

چکیده

پلیس فتا به عنوان متولی امنیت در فضای مجازی ایران، نقشی کلیدی در کشف و پیشگیری از جرایم سایبری ایفا می‌کند. با این حال، این نهاد با موانع و محدودیت‌های متعددی در انجام وظایف خود روبرو است که بر کارایی آن در کشف جرایم سایبری تاثیر می‌گذارد. این مقاله به بررسی این موانع و محدودیت‌ها و ارائه راهکارهایی برای رفع آنها می‌پردازد.پلیس فتا با کمبود نیروی متخصص، تجهیزات و نرم‌افزارهای لازم برای کشف جرایم سایبری پیچیده مواجه است.قوانین و مقررات مربوط به جرایم سایبری در ایران کامل و به‌روز نیستند و این امر کار پلیس فتا را در پیگرد قانونی مجرمان سایبری دشوار می‌کند.همکاری بین‌المللی در زمینه مبارزه با جرایم سایبری ضعیف است و این امر به مجرمان سایبری اجازه می‌دهد تا به راحتی از مرزها عبور کرده و از عدالت فرار کنند.سطح آگاهی عمومی از جرایم سایبری و راه‌های پیشگیری از آنها پایین است و این امر زمینه را برای سوء استفاده مجرمان سایبری فراهم می‌کند.

واژگان کلیدی: پلیس فتا ، جرایم سایبری ، فضای سایبری

---

[۱] کارشناسارشد حقوق جزا و جرم شناسی.

مقدمه

با گسترش روزافزون اینترنت و استفاده فزاینده از فضای مجازی، جرایم سایبری نیز به طور قابل توجهی افزایش یافته است. این جرایم که شامل هک، کلاهبرداری اینترنتی، سرقت اطلاعات و انتشار محتوای مجرمانه می‌شوند، می‌توانند ضررهای مالی و معنوی زیادی به افراد، سازمان‌ها و دولت‌ها وارد کنند.در ایران، پلیس فتا به عنوان متولی امنیت در فضای مجازی، وظیفه کشف و پیشگیری از جرایم سایبری را بر عهده دارد. این نهاد در سال ۱۳۸۹ تأسیس شد و از آن زمان تاکنون اقدامات موثری در جهت مقابله با جرایم سایبری انجام داده است. با این حال، پلیس فتا با موانع و محدودیت‌های متعددی در انجام وظایف خود روبرو است که بر کارایی آن در کشف جرایم سایبری تاثیر می‌گذارد.پلیس فتا نقش مهمی در حفظ امنیت فضای مجازی ایران ایفا می‌کند. با این حال، این نهاد با موانع و محدودیت‌های متعددی در انجام وظایف خود روبرو است که بر کارایی آن در کشف جرایم سایبری تاثیر می‌گذارد. رفع این موانع و محدودیت‌ها نیازمند اقدامات اساسی از جمله افزایش بودجه و امکانات پلیس فتا، اصلاح و به‌روزرسانی قوانین و مقررات مربوط به جرایم سایبری، تقویت همکاری بین‌المللی در زمینه مبارزه با جرایم سایبری و افزایش آگاهی عمومی از جرایم سایبری و راه‌های پیشگیری از آنها است.

با رفع این موانع و محدودیت‌ها، پلیس فتا می‌تواند به طور موثرتری با جرایم سایبری مقابله کند و امنیت فضای مجازی را برای همه کاربران افزایش دهد.علاوه بر موارد فوق، در مقدمه و نتیجه‌گیری می‌توانید به موارد زیر نیز اشاره کنید: اهمیت فضای مجازی در دنیای امروز، آثار و پیامدهای جرایم سایبری ، نقش پلیس فتا در پیشگیری از جرایم سایبری ، مسئولیت‌های فردی و اجتماعی در قبال جرایم سایبری ،همچنین می‌توانید از آمار و ارقام مربوط به جرایم سایبری در ایران و جهان برای تقویت مطالب خود استفاده کنید.

تعریف پیشگیری

پیشگیری از جرم و نابهنجاریهای اجتماعی برای نخستین بار توسط آنریکوفری پرچم دار مکتب تحققی مطرح شده است و امروزه شاخه ای از جرم شناسی به نام جرم شناسی پیشگیری ظهور یافته که بسیار شایان توجه محققان و دانشمندان بخصوص سازمانهای پلیس و دادگستری است. (شهری، ۱۳۹۵ ، ۶۰) برخی جرم شناسان واژه پیشگیری را به معنای پیش دستی کردن و یا آگاه کردن و هشدار دادن آورده اند. (ابراهیمی ،۱۳۹۸ ، ۴۳) پیشگیری از وقوع جرم یعنی « پیش بینی شناخت ارزیابی خط جرم و انجام اقدامهای برای رفع یا تقلیل آن که این اقدام می تواند سرکوب گر یا غیر سرکوب گر باشد. (ابرند آبادی ،۱۳۹۷، ۵۵)

تعاریف زیادی از پیشگیری بعمل آمده است که برخی از تعاریف اشاره می گردد .

رمون گس: «پیشگیری را هرگونه تدبیر یا اقدامی که هدف نهایی آن محدود کردن دامنه ارتکاب جرم از راه غیر ممکن ساختن ، دشوار کردن ، یا کاهش احتمال وقوع آن بوده و بدون استفاده از تهدید کیفر یا اجرای آن باشد»

موریس کوسن : پیشگیری از مجموعه اقدامات و تدابیر غیر قهر آمیز می داند که با هدف خاص مهار بزهکاری کاهش احتمال جرم و کاهش وخامت جرم در خصوص علل جرائم اتخاذ شود .

هر چیزی که به مقابله با جرم پرداخته و از بروز آن جلوگیری کند یا موجبات کاهش آن را فراهم سازد پیشگیری از جرم تلقی می شود این رویکرد در تفکرات سیاست جنایی آنریکوفری بروز پیدا کرد و تدابیر دفاع فردی که برای پیشگیری از تکرار جرم بیان شده است و نیز پیشگیری عمومی که براساس تدابیر جمعی حاصل می شود نشان از برداشت موسع فردی از پیشگیری است.(میر محمد صادقی، ۱۳۹۳، ۱۰۲)

طبق نظر شرمن « هر رویدادی که اعمال شود و نتیجه آن نشان بدهد که از نرخ بزهکاری کاسته شده است آن رویه را می توان پیشگرانه دانست.

در جرم شناسی پیشگیری از وقوع جرم را می توان در هر وضعیتی که از وقوع جرم جلوگیری شود بحث کرد و جرم شناسان پذیرفته اند که پیشگیری باید دارای سه ویژگی باشد .

۱- هدف اصلی آن تأثیر گذاری بر علل و عوامل موثر بر پیدایش بزهکاری .

۲- جنبه جمعی داشته باشد چرا که اقدامات فردی در بحث اصلاح و درمان است .

۳- اقدامات باید غیر قهر آمیز و غیر کیفری باشد. (ابراهیمی ، ۱۳۹۸، ۶۶)

پیشگیری از نظر لغوی به معنای « جلوگیری کردن ، مانع شدن ، جلو بستن و نیز اقدامات احتیاطی برای جلوگیری از رخدادهای بد و ناخواسته ». (معین ، ۱۳۹۹، ۴۳)

در مقررات ایران اصطلاح پیشگیری از جرم تعریف نشده و تنها نویسندگان لایحه پیشگیری از وقوع جرم آن را از رهگذر ماده ۱ « پیشبینی ، شناسایی و ارزیابی خطر وقوع جرم و اتخاذ تدابیر و اقدامات لازم برای از بین بردن یا کاهش آنها » تعریف کرده اند .

مصادیق و انواع جرایم سایبری

با پیشرفت تکنولوژی و استفاده از رایانه در تمام امور اقتصادی، نظامی و اجتماعی جرایم مختلفی میتواند در حوزه رایانه رخ دهد. لذا قانونگذار برای مبارزه و پیشگیری از این جرایم در سال ۱۳۸۸ اقدام به تصویب قانون جرایم رایانه ای در ۵۶ ماده نمود. در حقوق ایران، نه در قانون تجارت الکترونیک و نه در قانون جرایم رایانه‌ای هیچ تعریفی از این مفهوم ارایه نشده است .شاید دلیل آن اختلافات مبنایی است که میان حقوقدانان از تعریف جرایم رایانه‌ای وجود دارد. اما می‌توان به عنوان نمونه تعریف زیر را ارایه کرد:آن دسته از جرایمی‌که با سوءاستفاده از یک سیستم رایانه‌ای برخلاف قانون ارتکاب می‌یابد جرایم رایانه‌ای نام دارد. البته این دسته از جرایم را می‌توان شامل جرایم سنتی که به واسطه رایانه صورت می‌گیرد از قبیل کلاهبرداری و سرقت و نیز جرایم نو ظهوری که با

تولد رایانه پا به عرصه حیات گذاشته اند دانست، مانند جرایم علیه صحت و تمامیت داده‌ها. در واقع در حقوق ایران تعریف جرایم رایانه ای به سکوت واگذار شده و در بیشتر موارد تقریباً همان تعریف ارایه شده از طرف سازمان همکاری و توسعه اقتصادی را پذیرفته اند. قانون جرایم رایانه ای مصوب ۱۳۸۸/۱۱/۱۱ یکی از کاملترین قوانین در زمینه جرایم مربوط به فضای مجازی و رایانه ای می باشد. در این قانون در فصل اول: جرائم علیه محرمانگی داده ها و سیستم های رایانه ای و مخابراتی، شامل؛ دسترسی غیرمجاز، شنود غیرمجاز، جاسوسی رایانه ای، در فصل دوم: جرائم علیه صحت و تمامیت داده ها و سیستم های رایانه ای و مخابراتی، شامل؛ جعل رایانه ای، تخریب و اخلال در داده ها یا سیستم های رایانه ای و مخابراتی در فصل سوم سرقت و کلاهبرداری مرتبط با رایانه، در فصل چهارم: جرایم علیه عفت و اخلاق عمومی، در فصل پنجم: هتک حیثیت و نشر اکاذیب و در فصل هفتم سایر جرایم جرم انگاری شده اند.در این مبحث از پایان نامه بر آنیم تا مصادیق وانواع جرایم رایانه ای را که در قانون جرایم رایانه ای مصوب ۱۳۸۸ ذکر شده است بیان داریم.

مصادیق جرایم سایبری

بر اساس ماده۲۱ قانون جرایم رایانه ای مصادیق جرایم رایانه ای عبارتند از :

الف) محتوا علیه عفت و اخلاق عمومی

اشاعه فحشاء و منکرات. (بند۲ ماده۶ قانون مطبوعات)

تحریک ، تشویق ، ترغیب ، تهدید یا دعوت به فساد و فحشاء و ارتکاب جرایم منافی عفت یا انحرافات جنسی . (بند ب ماده ۱۵ قانون جرائم رایانه ای و ماده ۶۳۹ قانون مجازات اسلامی) انتشار ، توزیع ومعامله محتوای خلاف عفت عمومی. (مبتذل و مستهجن) (بند ۲ ماده ۶ قانون مطبوعات و ماده ۱۴ قانون جرائم رایانه ای) تحریک تشویق ، ترغیب ، تهدید یا تطمیع افراد به دستیابی به محتویات مستهجن و مبتذل. (ماده ۱۵ قانون جرایم رایانه ای)

استفاده ابزاری از افراد (اعم از زن و مرد) در تصاویر و محتوا ، تحقیر و توهین به جنس زن ، تبلیغ تشریفات و تجملات نامشروع و غیرقانونی (بند ۱۰ ماده۶ قانون مطبوعات)

ب) محتوا علیه مقدسات اسلامی

محتوای الحادی و مخالف موازین اسلامی (بند۱ماده۶ قانون مطبوعات)

اهانت به دین مبین اسلام و مقدسات آن (بند ۷ ماده ۶ قانون مطبوعات و ماده ۵۱۳ قانون مجازات اسلامی) اهانت به هر یک از انبیاء عظام یا ائمه طاهرین (ع) یا حضرت صدیقه طاهره (س) (ماده ۵۱۳ قانون مجازات اسلامی)

تبلیغ به نفع حزب گروه یا فرقه منحرف و مخالف اسلام (بند ۹ ماده ۶ قانون مطبوعات)

نقل مطالب از نشریات و رسانه ها و احزاب و گروه های داخلی و خارجی منحرف و مخالف اسلام به نحوی که تبلیغ از آنها باشد. (بند ۹ ماده ۶ قانون مطبوعات)

اهانت به امام خمینی (ره) و تحریف آثار ایشان (ماده ۵۱۴ قانون مجازات اسلامی)

اهانت به مقام معظم رهبری و سایر مراجع مسلم تقلید (بند ۷ ماده ۶ قانون مطبوعات)

ج) محتوا علیه امنیت و آسایش عمومی

تشکیل جمعیت ، دسته ، گروه در فضای مجازی (سایبر) با هدف برهم زدن امنیت کشور. (ماده ۴۹۸ قانون مجازات اسلامی)

هر گونه تهدید به بمب گذاری. (ماده ۵۱۱ قانون مجازات اسلامی)

محتوایی که به اساس جمهوری اسلامی ایران لطمه وارد کند. (بند ۱ ماده ۶ قانون مطبوعات)

انتشار محتوا علیه اصول قانون اساسی. (بند ۱۲ ماده ۶ قانون مطبوعات)

تبلیغ علیه نظام جمهوری اسلامی ایران. (ماده ۵۰۰ قانون مجازات اسلامی)

اخلال در وحدت ملی و ایجاد اختلاف مابین اقشار جامعه به ویژه از طریق طرح مسائل نژادی و قومی. (بند ۴ ماده ۶ قانون مطبوعات)

تحریک یا اغوای مردم به جنگ و کشتار یکدیگر. (ماده ۵۱۲ قانون مجازات اسلامی)

تحریک نیروهای رزمنده یا اشخاصی که به نحوی از انحا در خدمت نیروهای مسلح هستند به عصیان ، فرار، تسلم یا عدم اجرای وظایف نظامی. (ماده ۵۰۴ قانون مجازات اسلامی)

تحریص و تشویق افراد و گروه ها به ارتکاب اعمالی علیه امنیت ، حیثیت و منافع جمهوری اسلامی ایران در داخل یا خارج از کشور. (بند ۵ ماده ۶ قانون مطبوعات)

تبلیغ به نفع گروه ها و سازمانهای مخالف نظام جمهوری اسلامی ایران (ماده ۵۰۰ ق م.ا)

فاش نمودن و انتشار غیرمجاز اسناد و دستورها و مسایل محرمانه و سری دولتی و عمومی. (بند ۶ ماده ۶ قانون مطبوعات و مواد ۲و۳ قانون مجازات انتشار و افشای اسناد محرمانه و سری دولتی و ماده ۳ قانون جرائم رایانه ای)

فاش نمودن و انتشار غیرمجاز اسرار نیروهای مسلح. (بند ۶ ماده ۶ قانون مطبوعات)

فاش نمودن و انتشار غیرمجاز نقشه و استحکامات نظامی. (بند ۶ ماده ۶ قانون مطبوعات)

انتشار غیرمجاز مذاکرات غیرعلنی مجلس شورای اسلامی. (بند ۶ ماده ۶ قانون مطبوعات)

انتشار بدون مجوز مذاکرات محاکم غیرعلنی دادگستری و تحقیقات مراجع قضایی. (بند ۶ ماده ۶ قانون مطبوعات)

انتشار محتوای که از سوی شورای عالی امنیت ملی منع شده باشد

د) محتوا علیه مقامات و نهادهای دولتی و عمومی

اهانت و هجو نسبت به مقامات ، نهادها و سازمان های حکومتی و عمومی (بند ۸ ماده ۶ قانون مطبوعات و مواد ۶۰۹ و ۷۰۰ قانون مجازات اسلامی)

افترا به مقامات ، نهادها و سازمان های حکومتی و عمومی. (بند ۸ ماده ۶ قانون مطبوعات و ۶۹۷ قانون مجازات اسلامی)

نشراکاذیب و تشویش اذهان عمومی علیه مقامات ، نهادها و سازمانهای حکومتی. (بند ۱۱ ماده۶ قانون مطبوعات و ۶۹۸ قانون مجازات اسلامی)

جعل پایگاه های اینترنتی بانک ها ، سازمان ها و نهادهای دولتی و عمومی (مواد ۶ و ۷ قانون جرایم رایانه ای مصوب سال۱۳۸۸)

ه) محتوای که برای ارتکاب جرایم رایانه ای به کار می رود (محتوا مرتبط با جرایم رایانه ای)

انتشار یا توزیع و در دسترس قرار دادن یا معامله داده ها یا نرم افزارهایی که صرفاً برای ارتکاب جرایم رایانه ای به کار می رود. (ماده ۲۵ قانون جرائم رایانه ای)

فروش انتشار یا در دسترس قرار دادن غیرمجاز گذرواژه ها و داده هایی که امکان دسترسی غیرمجاز به داده ها یا سامانه های رایانه ای یا مخابراتی دولتی یا عمومی را فراهم می کند. (ماده ۲۵ قانون جرائم رایانه ای) انتشار یا در دسترس قرار دادن محتویات آموزش دسترسی غیرمجاز ، شنود غیرمجاز ، جاسوسی رایانه ای ، تحریف و اخلال در داده ها یا سیستم های رایانه ای و مخابراتی. (ماده ۲۵ قانون جرائم رایانه ای) آموزش و تسهیل سایر جرایم رایانه ای. (ماده ۲۱ قانون جرائم رایانه ای)

انتشار فیلترشکن ها و آموزش روشهای عبور از سامانه های فیلترینگ. (بند ج ماده ۲۵ قانون جرائم رایانه ای)

انجام هرگونه فعالیت تجاری و اقتصادی رایانه ای مجرمانه مانند شرکت های هرمی، فعالیت های غیرمجاز مرتبط با بازار اوراق بهادار (قانون اخلال در نظام اقتصادی کشور و بند الف ماده ۴۹ قانون بازار و اوراق بهادار ج.ا.ا. و سایر قوانین مرتبط)

ایجاد مراکز قمار در فضای مجازی (مواد ۷۰۵، ۷۰۸ و ۷۱۰ قانون مجازات اسلامی

و) محتوای که تحریک ، ترغیب ، یا دعوت به ارتکاب جرم می کند (محتوای مرتبط با سایر جرایم(انتشار محتوای حاوی تحریک ، ترغیب ، یا دعوت به اعمال خشونت آمیز و خودکشی. (ماده ۱۵ قانون جرائم رایانه ای)

تبلیغ و ترویج مصرف مواد مخدر ، مواد روان گردان و سیگار. (ماده ۳ قانون جامع کنترل و مبارزه ملی با دخانیات۱۳۸۵)

درج پیوند (لینک) یا تبلیغ تارنماهای فیلتر شده یا باز انتشار محتوای مجرمانه نشریات توقیف شده و رسانه های وابسته به گروه‌ها و جریانات منحرف و غیر قانونی

تشویق تحریک و تسهیل ارتکاب جرائمی که دارای جنبه عمومی هستند از قبیل اخلال در نظم ، تخریب اموال عمومی ، ارتشاء ، اختلاس ،کلاهبرداری ، قاچاق مواد مخدر، قاچاق مشروبات الکلی و غیره.(ماده ۱۲۶ قانون مجازات اسلامی)

تبلیغ و ترویج اسراف و تبذیر. (بند ۳ ماده ۶ قانون مطبوعات)

فروش، تبلیغ، توزیع و آموزش استفاده از تجهیزات دریافت از ماهواره(ماده ۱ قانون ممنوعیت بکارگیری تجهیزات دریافت ماهواره مصوب ۱۳۷۳/۱۱/۲۵)

ز) محتوا مجرمانه مربوط به امور سمعی و بصری و مالکیت معنوی تحلیل شود

انتشار و سرویس دهی بازی های رایانه ای دارای محتوای مجرمانه یا فاقد مجوز از وزارت فرهنگ و ارشاد اسلامی (بنیاد ملی بازی های رایانه ای مواد مختلف قانون مجازات اسلامی و قانون جرائم رایانه ای) معرفی آثار سمعی و بصری غیرمجاز به جای آثار مجاز.(ماده ۱ قانون نحوه مجازات اشخاصی که درامورسمعی و بصری فعالیت غیرمجاز دارند)

عرضه تجاری آثار سمعی و بصری بدون مجوز وزارت فرهنگ و ارشاد اسلامی (ماده ۲ قانون نحوه مجازات اشخاصی که در امور سمعی و بصری فعالیت غیر مجاز دارند)

تشویق و ترغیب به نقض حقوق مالکیت معنوی (ماده ۱ قانون حمایت از حقوق پدید آورندگان نرم افزار های رایانه ای و ماده ۷۴ قانون تجارت الکترونیکی)

ح) محتوای مجرمانه مرتبط با انتخابات مجلس شورای اسلامی

انتشار هرگونه محتوا با هدف ترغیب و تشویق مردم به تحریم و یا کاهش مشارکت در انتخابات (بند ۳ و ۸ ماده ۶۶ قانون انتخابات مجلس شورای اسلامی و ماده ۴۶ آیین نامه اجرایی آن)

انتشار هرگونه ادعای غیرواقع مبنی بر توقف انتخابات و یا دعوت به تجمع اعتراض‌آمیز، اعتصاب، تحصن و هر اقدامی که به نحوی موجب اخلال در امر انتخابات گردد (بند ۸ ماده ۶۶ قانون انتخابات مجلس شورای اسلامی)

انتشار و تبلیغ علائم تحریم انتخابات گروه‌های ضدانقلاب و معاند (ماده ۵۰۰ قانون مجازات اسلامی) انتشار هجو یا هجویه و یا هرگونه محتوای توهین‌آمیز در فضای مجازی علیه انتخابات (ماده ۷۰۰ قانون مجازات اسلامی و بند ۸ ماده ۶۶ قانون انتخابات مجلس شورای اسلامی)

انتشار هرگونه مطلب خلاف واقع مبنی بر انصراف گروه‌های قانونی از انتخابات (ماده ۶۴ قانون انتخابات مجلس شورای اسلامی)

استفاده از سایت‌ها و وبلاگ‌های رسمی نهادها و دستگاه‌های دولتی جهت بهره‌برداری در تبلیغات نامزدهای انتخاباتی)

شایان ذکر است تمامی شرکت‌ها، موسسات، شهرداری‌ها، سازمان‌ها و نهادهایی که قسمتی از دارایی آنها جزء بودجه و اموال عمومی است مشمول این ماده می‌شوند. (ماده ۵۹ قانون انتخابات مجلس شورای اسلامی)

درج محتوای تبلیغاتی نامزدهای انتخاباتی خارج از مدت زمان مقرر شده برای فعالیت انتخاباتی. (ماده ۵۶ قانون قانون انتخابات مجلس شورای اسلامی و ماده ۴۵ آیین‌نامه اجرایی آن)

انتشار هرگونه محتوا در جهت تحریک، ترغیب، تطمیع و یا تهدید افراد به خرید و فروش آراء، رای دادن با شناسنامه جعلی و شناسنامه دیگری، جعل اوراق تعرفه، رای دادن بیش از یک‌بار و سایر روش‌های تقلب در رای‌گیری و شمارش آراء. (ماده ۶۶ قانون انتخابات مجلس شورای اسلامی و ماده ۱۲۶ قانون مجازات اسلامی)

انتشار هرگونه محتوا جهت ایجاد رعب و وحشت برای رای‌دهندگان یا اعضاء شعب. (بند ۱۶ ماده ۶۶ قانون انتخابات مجلس شورای اسلامی)

استفاده ابزاری از تصاویر زنان برای تبلیغات انتخاباتی و یا عدم رعایت شئونات اسلامی در انتشار تصاویر مربوط به زنانی که نامزد انتخاباتی می‌باشند. (بند ۱۰ ماده ۶ قانون مطبوعات)

انتشار هرگونه محتوا در جهت توهین، افترا و نشر اکاذیب با هدف تخریب نظام، قوای سه‌گانه، سازمان‌های حکومتی و نهادهای اجرایی و نظارتی انتخابات به منظور بهره‌برداری انتخاباتی. (مواد ۵۰۰ ، ۶۹۸ ، ۶۰۹ قانون مجازات اسلامی و بند ۸ ماده ۶ قانون مطبوعات و ماده ۱۸ قانون جرایم رایانه‌ای) انتشار هرگونه محتوا و مکاتبات دارای طبقه‌بندی (محرمانه و سری) مرتبط با انتخابات.(ماده ۳ قانون مجازات انتشار و افشای اسناد محرمانه و سری دولتی و ماده ۳ قانون جرایم رایانه‌ای و بند ۶ ماده ۶ قانون مطبوعات)

انتشار اخبار کذب از نتایج بررسی صلاحیت‌ها، شمارش آراء، ادعاهای بی‌اساس پیرامون تقلب در انتخابات یا مخدوش بودن انتخابات بدون دلیل و مدرک. (مواد ۶۹۷ و ۶۹۸ قانون مجازات اسلامی و بند ۸ ماده ۶۶ قانون انتخابات مجلس شورای اسلامی)

ط) محتوای مجرمانه مرتبط با انتخابات ریاست جمهوری

انتشار هرگونه محتوا به منظور ترغیب و تشویق مردم به تحریم و یا کاهش مشارکت در انتخابات ، تجمع اعتراض آمیز بدون مجوز ، اعتصاب ، تحصن ، ادعای غیرواقع مبنی بر توقف انتخابات و یا هر اقدامی که به نحوی موجب اخلال در امر انتخابات ریاست جمهوری گردد.(بند ۷ ماده ۳۳ قانون انتخابات ریاست جمهوری و بند۵ ماده ۶ و ۲۵ قانون مطبوعات)

تشویش اذهان عمومی ، سیاه نمایی و بیان مطالب خلاف واقع علیه کشور ، ایجاد اختلافات مابین اقشار جامعه بویژه از طریق طرح مسائل قومی و نژادی ، انتشارهرگونه نتایج نظرسازی و نظرسنجی کاذب در خصوص انتخابات و نامزدهای انتخابات ریاست جمهوری(بند۷ مادۀ ۳۳ قانون انتخابات ریاست جمهوری- مواد۵۰۰ و ۶۹۸ قانون مجازات اسلامی – بند ۴ مادۀ ۶ قانون مطبوعات- مصوبه شورایعالی امنیت ملی)

انتشار و تبلیغ علائم تحریم انتخابات (ماده ۵۰۰ قانون مجازات اسلامی) انتشار هجو یا هجویه و یا هر گونه محتوای توهین آمیز یا تخریب در فضای مجازی علیه انتخابات و نامزدهای انتخابات ریاست جمهوری (ماده ۷۰۰ قانون مجازات اسلامی)

انتشار هرگونه مطلب ،علیه نامزدهای انتخاباتی و یا انتشارمطالبی خلاف واقع دال بر انصراف گروه یا نامزدهای انتخابات ریاست جمهوری (مواد ۷۴ و ۹۱ قانون انتخابات ریاست جمهوری اسلامی)

استفاده غیرمجاز از سایت ها و وبلاگ های متعلق به دستگاه های دولتی و مؤسسات و نهادهایی که تمام یا بخشی از دارایی و بودجه آنها از اموال عمومی است ، به منظور تبلیغ له یا علیه نامزدهای انتخابات ریاست جمهوری (مواد۶۲ ،۶۸)

انتشار محتوای تبلیغاتی نامزدهای ریاست جمهوری در فضای مجازی خارج از مدت زمان مقرر برای فعالیت انتخاباتی (مواد ۶۶ و ۶۷ قانون انتخابات ریاست جمهوری)

انتشار هرگونه محتوا در جهت تحریک ، ترغیب ، تطمیع و یا تهدید افراد به خرید و فروش آراء، رأی دادن با شناسنامه جعلی و شناسنامه دیگری ، جعل اوراق تعرفه ، رأی دادن بیش از یک بار ، تقلب در رأی گیری و شمارش آراء(ماده ۳۳ قانون انتخابات ریاست جمهوری و ماده ۱۲۶ قانون مجازات اسلامی)

انتشار هرگونه محتوا به منظور ایجاد رعب و وحشت برای رأی دهندگان یا اعضاء شعب (بند ۱۶ ماده ۳۳ قانون انتخابات ریاست جمهوری و آئین نامه اجرایی آن)

استفاده ابزاری از تصاویر اشخاص برای تبلیغات انتخابات ریاست جمهوری (بند ۱۰ ماده ۶ قانون مطبوعات)

انتشار هرگونه محتوا مشتمل بر توهین، افترا و نشر اکاذیب علیه نظام ، قوای سه گانه ، سازمان های حکومتی و نهادهای اجرایی و نظارتی انتخابات ریاست جمهوری (مواد ۵۰۰ ، ۶۱۸ و ۶۰۹ قانون مجازات اسلامی و بند ۸ ماده ۶ قانون مطبوعات و ماده ۱۸ قانون جرایم رایانه ای)

انتشار هرگونه محتوای دارای طبقه بندی (محرمانه و سری) مرتبط با انتخابات ریاست جمهوری (تبصره ۴ ماده ۸۰ قانون انتخابات ریاست جمهوری، ماده ۳ قانون مجازات انتشار و افشای اسناد محرمانه و سری دولتی و ماده ۳ قانون جرایم رایانه ای و بند ۶ ماده ۶ قانون مطبوعات)

انتشار محتوای خلاف واقع در ارتباط با نتایج بررسی صلاحیت ها ، شمارش آراء ، نتایج انتخابات (مواد ۶۹۷ و ۶۹۸ قانون مجازات اسلامی و بند ۷ماده ۳۳ و ۸۰ و ۸۵ قانون انتخابات ریاست جمهوری) انتشار محتوا با هدف دخالت در امر انتخابات با سمت یا سند مجعول یا به هر نحو غیر قانونی در فضای مجازی(بند ۱۵ و ۱۷ ماده ۳۳ و ۸۵ قانون انتخابات ریاست جمهوری)

انتشار و توزیع هرگونه محتوای تبلیغاتی از سوی کارکنان ادارات ، سازمان ها ، ارگان های دولتی و نهادها با ذکر سمت خود، له یا علیه هر یک از نامزدهای انتخابات ریاست جمهوری درفضای مجازی (مواد ۶۸و ۸۸ قانون انتخابات ریاست جمهوری)

انتشار و توزیع هرگونه محتوای تبلیغاتی از سوی مقامات اجرایی و نظارتی انتخابات له یا علیه هر یک از نامزدهای انتخابات ریاست جمهوری درفضای مجازی ماده ۷۳ قانون انتخابات ریاست جمهوری)

انواع جرایم سایبری

الف : جرایم سنتی درمحیط دیجیتال :

جاسوسی رایانه‌ای :جاسوسی رایانه‌ای همانند جاسوسی کلاسیک ناظر به کسب اسرار حرفه‌ای، تجاری، اقتصادی، سیاسی، نظامی و نیز افشا و انتقال و استفاده از اسرار است، فرد مرتکب جرم با دستیابی وفاش کردن این اسرار، ضرر سیاسی، نظامی، مالی، تجاری می‌کند. این جرم امنیت ملی را با مخاطره مواجه می‌کند.(شیرزاد،۱۳۹۸ ،۲۲)

سابوتاژ رایانه‌ای :این جرم با جرم تخریب شباهت بسیاری دارد، هدف مجرم اخلال در نظام سیاسی واقتصادی یک کشور و بالطبع اخلال در امر حکومت است. درواقع اصلاح، موقوف سازی، پاک کردن غیرمجاز داده‌ها یا عملیات کامپیوتر به منظور مختل ساختن عملکرد عادی سیستم سابوتاژ رایانه‌ای گویند.(انصاری ، ۱۳۹۰ ، ۴۳)

جعل کامپیوتری: واردکردن، تغییر، محو یا موقوف سازی داده‌های کامپیوتری یا برنامه‌های کامپیوتری به منظور و اهداف سیاسی واقتصادی صورت میگرد. جعل کامپیوتری جعل داده هاست. در جعل کامپیوتر ی عمل ارتکابی بر داده‌ها اثر می‌گذارد، با این تفاوت که داده، ماهیت اسناد عادی را ندارد.(ذبیح اله نژاد،۱۳۹۶ ،۴۳)

افترا و نشر اطلاعات از طریق پست الکترونیک: پست الکترونیک مرسوم‌ترین و گسترده‌ترین سرویس شبکه‌های کامپیوتری و بین المللی است، هر کاربر می‌تواند در شبکه‌های بین‌المللی از طریق یک آدرس مشخص الکترونیک شناخته شود که با دسترسی به رمز آن می‌توان به آسانی درآن تقلب کرد. این قالبیت پست الکترونیک می‌تواند ابزاری جالب برای نشر اطلاعات مجرمانه یا نشر اکاذیب و افترا به اشخاص باشد و احتمال کنترل اطلاعات برای تهیه‌کننده کاملاً مشکل است ودر عمل به خاطر تعداد بسیار زیاد پست الکترونیک ارسالی، اتخاذ تدابیر کلی و گسترده امنیتی مشکل بوده وتنها برای بخش کوچکی از داده‌ها میسر می‌باشد. (باستانی، ۱۳۹۳، ۳۲)

تطهیر نامشروع پول: بدست آوردن پول از طریق غیرقانونی یا پول کثیف، به نحوی که قانونی یا پاک به نظر برسد، از جرایم کلاسیک بوده که در محیط سایبر به کمک اینترنت، پست الکترونیک و شبکه‌های بین‌المللی ارتباطی صورت می‌پذیرد، نحوه ارتکاب بدین نحو است که باندهای بزرگ نامشروع توسط پست الکترونیک یا اینترنت بدون هیچ کونه اثر و نشانی درخواست ارسال مبالغی پول به حساب شخص معینی را می‌نمایند و در تقاضای خود نحوه ارسال پول و دستمزد و مدت استرداد را بیان ودر صورت قبول طرف نوع و نحوه تنظیمات لازم را اعلام می‌دارند و اصولاً درزمان استرداد پول یک عنوان مشروع در تجارت الکترونیک را با منشأ تجاری انتخاب وبا هدف خود هماهنگ می‌نمایند لازم است ذکر شود غالب این درخواستها از افراد کشورهایی که از لحاظ تکنولوژی اطلاعاتی و ارتباطی و هماهنگی پلیسی در سطح بین‌المللی در درجه پایین‌تری قراردارند انتخاب می‌شود. (حسن بیگی، ۱۳۹۴، ۷۶)

قاچاق موادمخدر: باتوجه به گسترش ارتباطات شبکه‌ای و در محیط سایبر و دسترسی آسان افراد به هم از طریق پست الکترونیک و اینترنت هرگونه قاچاق مواد مخدر اعم از خرید، فروش، پخش، توزیع یافتن واسطه‌ها و مصرف‌کنندگان از طریق شبکه‌های کامپیوتری انجام می‌شود. از ویژگیهای آن حذف و کمتر نمودن واسطه‌ها وتوزیع کنندگان، گسترش دامنه فعالیت قاچاق چیان تا سطح بین‌المللی، اقدامات پلیس در خصوص کشف فروشندگان و خریداران موادمخدر به سختی و در مواردی غیرممکن می‌باشد و ضریب اطمینان قاچاق موادمخدر از طریق ارتباطات کامپیوتری و شبکه‌ای بالاتر از نوع سنتی آن می‌باشد.(بیات،۱۳۹۷ ، ۵۲)

جرایم ناظر به کپی رایت وبرنامه‌ها: هرگونه تکثیر، ارسال، انتقال، در اختیار عامه گذاشتن، پخش گسترده، توزیع، فروش واستفاده غیرمجاز از برنامه‌های کامپیوتری سرقت نرم‌افزار گویند.

جرایم در تجارت الکترونیک: شامل کلاهبرداری در تجارت، تعریف کلی و کلاسیک کلاهبرداری عبارتست از"تحصیل مال دیگری بااستفاده از وسایل متقلبانه"شخصی در نقطه‌ای نامعلوم با واردشدن به شبکه بین‌المللی (مثل اینترنت)و معرفی خود به عنوان تاجر و صاحب یک شرکت معتبر در یک سایت تجاری و ارائه "نهادی مشابه اداره ثبت اسناد که این نهاد عهده دار ثبت داده‌های تجاری وتجاراست تا بدین ترتیب تاجر مجوز ورود به عرصه تبادلات

الکترونیک را کسب نماید "وهم چنین نهادی که در تجارت الکترونیک به معنای زیرساخت کلید عمومی است. (شاه محمدی، ۱۳۹۳، ۹۸)

اساس تجارت الکترونیک واز محورهای عمده و مهم آن داشتن این نهاد برای تجار می‌باشد "(تماماً غیرواقع و کذب)، اظهار می‌دارد که کالایی را با قیمت معین، نوع و تعداد مشخص در اختیار داشته و قابل عرضه به مشتریان می‌باشد از طرفی خریدارانی که در فضای شبکه‌ها مشغول تجارت الکترونیک (خریدوفروش) می‌باشند پس از دریافت پیام، نسبت به برقراری ارتباط شبکه‌ای که غالباً به صورت پست الکترونیک یا ارسال درخواست هز طریق شبکه می‌باشد قبول (خرید) خودرا اعلام و مقداری از کالای موردنظر را درخواست می کنند .شخص فروشنده پس از جلب اعتماد طرف مقابل، نسبت به اعلام شماره حساب یا شماره کارت اعتباری خود برای دریافت وجه اقدام می‌نماید. خریدار نیز پس از پرداخت وجه (غالباً به صورت پرداختهای الکترونیکی)منتظر دریافت کالا می‌باشد در صورتیکه شخص فروشنده قبلاً با عملیات‌های متقلبانه و نفوذ توانسته بوده که نهادهای نامبرده را به صورت غیرواقع برای خود اختیار نماید و بدین وسیله مبلغی را من غیرحق کسب نماید .(حسن بیگی، ۱۳۹۴، ۷۸)

جرم آینده، تروریسم سایبر: والتر لاکور یک متخصص تروریسم در مرکز مطالعات استراتژیک و بین‌المللی اشاره می کند که یک مقام رسمی سیا ادعا کرده است که می‌تواند "با یک میلیارد دلار و ۲۰ هکر قابل، ایالت متحده را فلج کند."لاکور یادآوری می کند که اگرچه هدف تروریست‌ها معمولاً قتل سران سیاسی، گروگان گیری یا بعضاً حمله ناگهانی به تسهیلات دولتی یا عمومی است، اما صدمه‌ای که ممکن است به وسیله حمله الکترونیکی به شبکه‌های رایانه‌ای وارد آید می‌تواند"بسیار غم انگیزتر باشد و اثرات آن تا مدت‌ها باقی بماند."لاکور معتقد است که تروریسم رایانه‌ای ممکن است برای تعداد کثیری از مردم بسیار ویران کننده تر از جنگ‌های بیولوژیک یا شیمیایی باشد. از اقدامات سایبر ترور ارتباط بین تروریست‌ها از طریق شبکه‌های بین‌المللی و تبادل افکار و اعمال مجرمانه در سطح بسیار پیچیده است که از ویژگیهای این نوع ارتباط عدم توانایی پلیس در کنترل و شنود این ارتباطات می‌باشد. اما آیا واقعاً تروریسم سایبر امکان‌پذیر است؟ درسال ۱۹۹۱ حین جنگ خلیج فارس که میان عراق و ائتلافی از چند کشور به رهبری ایالت متحده درگرفت، یک جوان ۱۸ ساله فلسطینی، متهم به نفوذ به رایانه‌های پنتاگون شد. این مرد جوان ظاهراً به اطلاعات سری مربوط به موشک پیتریوت دسترسی پیدا کرده بود که یک سلاح کلیدی آمریکا برای دفاع در مقابل حمله موشکهای اسکاد عراق محسوب می‌شد.(الهی منش ،۱۳۹۷ ، ۳۲) در نفوذ دیگری در همان جنگ چندین نوجوان هلندی به رایانه‌های نظامی، زمینی، هوایی و دریایی ایالت متحده در۳۴ سایت مختلف نفوذ کردند، نفوذکنندگان در یکی از حملات خود به داده‌های بسیار حساسی درباره پرسنل نظامی، نوع و میزان تجهیزات نظامی فرستاده شده به خلیج فارس، اهداف موشکها و توسعه سیستم‌های تسلیحاتی دست یافتند، در واقع این نوجوانان کرکرهایی بودند که تنها به خواندن این فایلها اکتفا نکردند بلکه اطلاعات مربوط به تحرکات ارتش و توانایی موشک‌ها را سرقت کردند ودر اختیار عراقی‌ها قراردادند. (باستانی ، ۱۳۹۳ ، ۵۴)

بزه کار و بزه دیده در فضای سایبری

بزهکاری سایبری

در عصر نوین شاید هیچ جرمی به مانند جرایم سایبری را نتوان سراغ داشت کـه بزهکـاران آن بدین شکل معادلات شناسایی را بـرای مـأمورین تحقیـق پیچیـده سـاخته باشـند. بسـتر سـایبر به واسطه ویژگیهای خاص خود، در وهله نخست شناساییِ بزهکار و در مراتـبِ پسـینی، کشـف بزه را دشوار ساخته است. افزون بر ویژگی هایی که فضای سایبر به بزهکاری اعطاء کرده اسـت، ابزارهای سنتیِ تحقیقاتی نیز در رویارویی با این جرایم به شدت ناکارآمـد و فاقـد اثربخشـیِ لازم می باشند؛ زیرا مسلم است که با رایانهای شدن صحنه جرم ،تجهیـز کنشـگران عرصـهٔ بزهکـاری به سلاح های نوین و بالطبع بهره برداری آنان از روشهای ارتکاب جرمِ متناسب با آن، نمیتـوان از ابزارهایی که هیچ سنخیتی با آن ندارند، بهره جسـت. لـذا پـی جـوئیِ جـرایم سـایبری مسـتلزم کاربست تدابیرِ روزآمد است. در این راستا، در چند سال اخیر فن ترسیم نیمرخ جنایی بـه واسـطهٔ امتیازات خاصی که دارد، ذهن پژوهشگران عرصهٔ جرمشناسیِ فضای سـایبر و مـأمورین تحقیـقِ واحدپلیسِ سایبری را به خود معطوف ساخته است و آنان را متقاعد ساخته که این شـیوه، یکـی از مؤثرترین و کم هزینه ترین روشهای مبارزه با جرایم سایبری است. البته باید اشاره داشـت کـه به جهت نوظهور بودن استفاده از این فـن در جـرایم سـایبری ضـروری اسـت تـا جـرایم پرخطـر سـایبری و آن دسـته از جرایمـی سـایبری کـه هزینـه هـای سـنگین سیاسـی- اقتصـادی را بـه بـار می آورند، در اولویت قرار گیرند. (کوزه پز ، ۱۳۹۳ ، ۱۳۱)

ضرورت به کارگیری فناوری اطلاعات در پلیس فتا

گسترش شبکه‌های ارتباطی و اهمیت اطلاعات در حیات اجتماعی، منشأ تحولات نوینی در زندگی انسان شده است . پدیده انفجار اطلاعات و ظهور انقلاب نامیده شود. یکی از اساسی‌ترین عوامل» عصر اطلاعات «، اطلاعاتی باعث شده است عصر حاضر بروز و گسترش این پدیده، توسعه روزافزون فناوری اطلاعات است. فناوری اطلاعات امروزه تمام حوزه‌های زندگی بشری را تحت تأثیر خود قرار داده است و گستره این تأثیر و عمق آن در آینده نیز افزایش خواهد یافت. فناوری اطلاعات از دو واژه‌ی اطلاعات و فناوری تشکیل شده است.(عالی پور، ۱۳۹۰، ۷۲)

جرایم رایانه‌ای، مبتنی بر فناوری اطلاعات است و در جهان شبکه‌ای امروز، دیگر هیچ جزیره‌ای منزوی محسوب نمی‌شود. از این رو، جرایم رایانه‌ای طبع جهانی دارد و مقابله با آن‌ها اقدامات یکسان بین‌المللی را می‌طلبد و چنانچه این جرایم در سیستم‌های قضایی کشورهای مختلف به صورت یکسان تعریف نشوند، تلاش‌های ضابطان اجرایی برای برخورد هماهنگ با این جرایم، غامض و پیچیده خواهد شد.

پلیس بین‌الملل، کنوانسیون اروپایی جرایم مجازی و همگی در این زمینه به دنبال ادبیات واحدی هستند. به نظر می‌رسد که قواعدی نیز باید وضع گردد تا مسئولیت رسیدگی به جرایم در سطح بین‌المللی را مشخص نماید

موانع و محدودیت های جرم‌شناسی سایبری

اگر قرار باشد جرم‌شناسی سایبری به عنوان یک شاخه مجزا معرفی شود، چالش‌های متعددی پیش روی جرم شناسان سایبری امروزی قرار خواهد گرفت. این چالش‌ها عبارت‌اند از: ۱- مشکلات آموزشی، ۲- تحقیق در زمینه جرم‌شناسی سایبری، ۳- حرفه‌ای سازی این رشته.

بسیاری از دانشگاه‌های ایالات متحده و انگلستان برنامه‌های درسی مربوط به جرم‌شناسی را همراه با دروس مربوط به جرایم سایبری ارائه می‌کنند. اخیرا برخی از دانشگاه‌های انگلستان نظیر «دانشگاه کلیسای مسیح کانتربوری»، «دانشگاه دوبلین» و «دانشگاه بِدفورد شایر» برگزاری کلاس‌های کارشناسی ارشد پزشکی قانونی سایبری و محاسبه پزشکی قانونی را آغاز کرده‌اند. برگزاری کلاس‌های بیشتر در مورد پزشکی قانونی سایبری حاکی از آن است که دانشگاه‌ها بیشتر به بخش تحقیق در خصوص جرایم سایبری علاقمند هستند تا علل آن‌ها. اگرچه جنبه عملی تحقیقات نیز حائز اهمیت است، اما چشم‌پوشی از مسائل نظری تولید کننده جرایم سایبری نمی‌تواند مکمل درکی کل نگرانه از جرایم سایبری باشد(گوردون هیوز،۱۳۹۰، ۲۸) . در مقطع کارشناسی ارشد باید کلاس‌هایی در خصوص جرم‌شناسی سایبری و پزشکی قانونی سایبری برگزار شود. بدین ترتیب، امکان ترکیب جنبه‌های نظری و عملی جرایم سایبری فراهم می‌شود. استفاده از مدرسان متخصص برای تدریس جرایم سایبری و نیز انجام تحقیقات یکی از چالش‌های مرتبط با ایجاد برنامه‌های درسی مربوط به جرم‌شناسی سایبری است. رشد علم اینترنت، علوم کامپیوتر و فناوری اطلاعات تأثیر بسزایی بر توسعه رشته جرم‌شناسی سایبری دارد. به نظر نمی‌رسد که جرم شناسان سنتی در حال منطبق ساختن خود با نیازهای روبه رشد شاخه (درحال توسعه) جرم‌شناسی باشند. آن‌ها به یادگیری رشته‌های دیگر نظیر فناوری اطلاعات و علم اینترنت (که هر دو آن‌ها حوزه جرم‌شناسی سایبری را در بر می‌گیرند) تمایلی ندارند. جرم شناسان سنتی بدون برخورداری از دانش فنی نمی‌توانند از آموزش جنبه‌های نظری جرایم سایبری فراتر روند. از طرفی، اگر قرار باشد تکنوکرات ها (حامیان تکنوکراسی) نیز در آموزش جرم‌شناسی سایبری سهیم شوند از تمرکز آن‌ها بر اصول جرم‌شناسی سایبری کاسته خواهد شد و احتمالاً این افراد بیشتر به سخن گفتن در مورد فناوری و نه مسائلی که منجر به ارتکاب جرایم سایبری می‌شوند تمایل خواهند داشت. از سوی دیگر، چنانچه قرار باشد وکلا به تدریس دروس جرم‌شناسی سایبری بپردازند تمرکز آن‌ها باید تنها بر قوانین سایبری باشد و سایر مؤلفه - های مهم جرایم سایبری را نادیده بگیرند. این قبیل آموزش‌های ذره گرایانه که توسط جرم شناسان، تکنوکرات ها و یا وکلا ارائه می‌شوند در به ثمر نشاندن تلاش‌های انجام شده در جهت توسعه شاخه رسمی جرم‌شناسی سایبری مؤثر نخواهند بود. نیاز شدیدی به متخصصین دارد. متخصصینی که می‌توانند جرم‌شناسی سایبری را وارد مرحله دیگری از تکامل کنند. واحدهای جرم‌شناسی سنتی می‌توانند یک

برنامه چند رشته‌ای مرکب از جرم‌شناسی سایبری و پزشکی قانونی سایبری را با کمک گرفتن از سایر واحدها مانند دانشکده علوم کامپیوتر، حقوق فناوری اطلاعات ارائه دهند. آن دسته از متخصصینی که موفق به کسب مدرک جرم‌شناسی سایبری می‌شوند می‌توانند به عنوان دستیار برای انجام تحقیقات و اقدامات آموزشی و توسعه این شاخه، بکار گرفته شوند. بدین ترتیب مجموعه‌ای متشکل از متخصصینی که به نوعی گنجینه‌ای را در اختیار می‌گذارند تشکیل می‌شود و ترکیبی از دانش نظری و عملی در خصوص جرایم سایبری، تحقیقات و قوانین به وجود می‌آید. این افراد متخصص برای پیشبرد این حرفه و یاری رساندن به اداره دادگستری کیفری در انجام تحقیقات در مورد جرایم سایبری ارزشمند خواهند بود. (گاتن،۱۳۹۳ ، ۶۵)

نقش پلیس درکشف جرایم سایبری

از زمانی که بشر پا به عرصهٔ جود گذاشت، احساس امنیت همواره از نیازهای اولیه او بوده است امروزه می توان امنیت را بالاترین ارزش دانست و ان را مهم ترین کارکرد حکومت ها یا نظام های سیاسی تلقی کرد امنیت اجتماعی یا عمومی یکی از انواع امنیت و زیر مجموعه یکی از انواع امنیت ملی هر کشور به شمار میآید .سازمان پلیس یکی از نهادهای موثری است که در عصر جدید به منظور برقراری و حفظ نظم و امنیت و نیز پیشگیری ازبروز جرایم در جامعه از سوی نظام سیاسی ایجاد می گردد و نیز بر اساس این رسالت به طور مستقیم با اجتماع و مردم تعامل دارد .

فناوری اطلاعات با سرعت شگفت انگیزی تمامی ارکان حیات بشری از جمله مقوله نظم امنیت و آرامش عمومی را دستخوش تحولات و دگرگونی های اساسی قرار داده است . همزمان با ظهور رایانه و اینترنت و فرایند جهانی شدن در عصر حاضر فناوری اطلاعات و ارتباطات امکان ظهور جامعه شبکه ای را فراهم اورده است که تعاریف جدیدی از هویت ها و جوامع انسانی عرضه می کند و بافت اصلی ان را اطلاعات و نظام ارتباطات الکترونیک تشکیل می دهد . در نتیجه پیدایش این جامعه شبکه ای ، مراودات اجتماعی از شکل سنتی خود به صورت جوامع مجازی ، ماشرت های دیجیتالی از طریق متون الکترونیک وسیستم های چند رسانه ای تغییر ماهیت داده اند که این امر باعث پیدایش نوعی ناامنی اجتماعی و ظهورجرایم و بزه کاری نویندر فضای مجازی شده است و فرایند فاصله رو به رشد این نوع جرایم را می توان عامل ایجاد آسیب به امنیت اجتماعی و تحت الشعاع قرار دادن امنیت اخلاقی دانست .

در اینجاست که نقش پلیس به عنوان نهاد برقرار کننده نظم و امنیت اجتماعی و مسئول پیشگیری و کشف جرایم در جامعه مطرح می شود .از آنجا که میان محیط فیزیکی و فضای مجازی تفاوتهای بسیار وجود دارد باید دیدکه آیا هنوز سیستم های پلیسی می توانند در چنین فضایی کارایی داشته باشند و کارآمد بمانند .

پلیس جمهوری اسلامی ایران تلاش می کند تا با بهره گیری از آخرین دستاوردهای فناوری اطلاعات و ارتباطات سیستم های پیشرفته انتظامی امنیتی کشور امنیت اجتماعی را بهبود بخشد و محیطی امن توام با آسایش عمومی را برای کلیه شهروندان در پرتو ارزش های اسلامی فراهم کند .

باتوجه به اهمیت روزافزون سیاست پیشگیری از جرم در کشورهای درحال توسعه و تأثیر آن در پایش (کنترل) نرخ جرم کشورها در سال های اخیر، به بسط قانونی و اجرایی این سیاست در درون دستگاه قضایی و انتظامی روی آورده اند. باوجود این، برای رسیدن به تأثیرات ثمربخش برنامه های پیش گیرانه باید گام های بسیار مهمی برداشته شود و سرمایه اجتماعی دستگاه های متولی عدالت کیفری تقویت شود و مشارکت فعال تری با نهادهای مدنی ایجاد شود. به موجب ماده ۱۲۸از فصل دوم قانون آیین دادرسی کیفری مصوب ۱۳۹۲/۱۲/۰۴،ضابطان دادگستری مأمورانی هستند که تحت نظارت و تعلیمات دادستان در کشف جرم، حفظ آثار و علائم و جمع آوری ادله وقوع جرم، شناسایی، یافتن و جلوگیری از فرار و مخفی شدن متهم، تحقیقات مقدماتی، ابلاغ اوراق اجرای تصمیمات قضایی، به موجب قانون اقدام می کنند. از آنجا که پلیس باید همواره جلوتر از زمان، حرکت کند و آمادگی های لازم را برای رویارویی با ناامنی های احتمالی آینده را داشته باشد، از اینرو باتوجه به این نقش حساس، می توان پلیس را مهمترین عامل پیشگیری از جرم به شمار آورد. تعامل و همکاری مؤثر میان پلیس و سازمان های مختلف می تواند در جهت نیل به اجرایی ساختن فرآیند پیشگیری از جرایم به ویژه جرایم سایبری کمک کند. مع الوصف، وجود پلیس در جامعه هم پیش رویدادی است هم پس رویدادی؛ به نحوی که صرف احساس این موضوع که در فضای مجازی، پلیس تخصصی به نام پلیس فتا وجود دارد که باعث می شود هزینه ارتکاب جرم برای مجرمان بیشتر و عملاً جذابیت و تمایل ارتکاب جرم و انگیزه ارتکاب جرم کاهش یابد.از آنجا که دلایل ارتکاب جرم در این فضا، عمدتاً ادلۀ الکترونیک می باشند، پلیس به منظور بررسی و کشف جرایم سایبری با مسائلی مواجه می شود که در سایر جرایم مطرح نیست. ماهیت خاص دلایل الکترونیکی به گونه ای است که پذیرش آنها را در مراجع قضایی با چالش های ویژهای مواجه کرده است به منظور مقابله با این چالش ها، مأموران پلیس باید روش های خاص جمع آوری دلایل مذکور را که مرکب از چهار مرحلۀ جمع آوری مدرک، بررسی، تجزیه وتحلیل و ارائه گزارش می باشد، به نحو صحیحی اجرا کند، مرحلۀ جمع آوری شامل جست وجو برای شناسایی، جمع آوری و مستندسازی مدارک الکترونیکی است .

دستیابی به هدف اصلی حقوق کیفری که مبارزه علیه بزهکاری و حفظ نظم و امنیت و آسایش افراد جامعه است، بدون شناسایی و کشف جرم، دستگیری مجرم، صدر حکم و اجرای مجازات ممکن نیست. به موجب بند ۱ ماده ۱۵ قانون آیین دادرسی کیفری، نیروی انتظامی جمهوری اسلامی ایران، در مقام ضابط دادگستری، تحت نظارت و تعلیمات مقام قضایی، در کشف جرم و بازجویی مقدماتی، حفظ آثار و دلایل جرم و جلوگیری از فرار

و مخفی شدن متهم، به موجب قانون اقدام می‌کند و چرخ‌های عدالت کیفری را به حرکت درآورده مبارزه عملی با جرم و مجرمان را تحقق می‌بخشد.

از این دیدگاه پلیس در سیستم کلان مبارزه با جرم، تهدید بالفعل مجرمان، بازدارندگی و ارعاب مجرمان بالقوه و همچنین تسریع در اجرای مجازات، دارای نقش مهم و ارزنده‌ای خواهد بود که برای ایفای این نقش، باید به کشف جرایم، اعم از سنتی و پیشرفته بپردازد (پرویزی، ۱۳۹۴ ، ۵۵). در اینجا نیز، علی‌رغم سیاست‌های عام و مشترک موجود در کشف تمام جرایم، به دلیل وجود تفاوت‌های ماهوی میان محیط فیزیکی و فضای مجازی، روش‌های کشف جرایم سایبری نیز متفاوت خواهد بود؛ برای مثال صحنه جرایم ارتکابی در محیط فیزیکی، به طور معمول، متمرکز بوده و پراکندگی جغرافیایی نخواهد داشت، اما در جرایم سایبری، پراکندگی جغرافیایی صحنه جرم بسیار زیاد و معمولا دور از هم و در محدوده مرزی کشورهای مختلف است. ابزارهای بررسی صحنه جرایم سایبری، عمدتا نرم‌افزارهای تخصصی می‌باشند که براساس استانداردهای بین‌المللی تولید شده از سوی ماموران پلیس مورد استفاده قرار می‌گیرند. بنابراین با ابزارهای بررسی صحنه سایر جرایم تفاوت اساسی دارند. دلایل ارتکاب جرایم سایبری، غالبا ادله الکترونیک است که با سرعت قابل ملاحظه‌ای، امکان تغییر و از بین بردن آنها وجود دارد .بنابراین سرعت عمل در شناسایی و جمع‌آوری این دلایل، بسیار ضروری خواهد بود.

بدون تردید، در راستای تحقق نقش موثر پلیس در کشف جرایم سایبری، استفاده از نیروهای متخصص پلیسدر این حوزه و شیوه‌های تحقیق و بررسی توسط این نیروها، از اهمیت فوق‌العاده‌ای برخوردار است و ضرورت مطالعه آن در تحقیق مزبور بیش از هر امر دیگری احساس می‌شود.

الف) ویژگی‌های ماموران کشف جرایم سایبری

سیاست‌های کلی نیروی انتظامی جمهوری اسلامی ایران مبتنی بر این اصل است که در راستای تربیت پلیس مقتدر، با در نظر گرفتن معیارهای متنوع، ویژگی‌های مختلفی از جمله: تقوا، قاطعیت، قانون‌مندی، مردمی بودن و توانایی‌های علمی و تخصصی را در ماموران خود به وجود آورد.اما پرسشی که در اینجا باید به آن پاسخ داده شود، این است که آیا همان خصوصیات شخصیتی، مهارت‌ها و آگاهی‌های ماموران پلیس کشف و تعقیب جرایم ارتکابی در محیط فیزیکی، برای ماموران کشف جرایم سایبری نیز کافی است یا ماموران اخیر، نیازمند آموزش‌های خاصی هستند؟

چنانچه واضح است، علاوه بر خصوصیاتی که در میان همه ماموران پلیس مشترک است، مامور کشف جرایم سایبری باید ویژگی‌های دیگری نیز داشته باشد، برای مثال شناخت علم رایانه، چگونگی عملکرد و اصطلاحات مورد کاربرد در آن و نیز آگاهی از مسائل امنیتی رایانه و شبکه به منظور کشف جرایمی از قبیل هک کردن سایت‌ها یا تهاجم به شبکه، برای آن دسته از ماموران پلیس که در این حوزه فعالیت دارند، ضروری است. بنابراین،

ماموران کشف جرایم سایبری، به منظور برخورداری از عملکرد موثر در این حوزه ویژه، نیازمند آموزش‌های وسیع و جامعی هستند. به طور معمول، سازمان‌های بزرگ پلیس، که در آن متخصصان فناوری اطلاعات و علوم رایانه، به منظور کشف جرایم سایبری، اقدام به تشکیل گروه ویژه‌ای می‌کنند و به نیروهای پلیس اطلاعات لازم را می‌دهند، این نیاز به راحتی مرتفع سازند، اما اگر جرایم مزبور در جایی ارتکاب یابند که اداره پلیس آن محل فاقد امکانات یاد شده باشد، ضرورت آموزش تخصصی برای ماموران پلیس آشکارتر می‌شود.

کشف جرایم، فرایندی خلاق و نیازمند مهارت‌های خاصی است که می‌توان آنها را آموخت و توسعه داد. اگرچه داشتن استعداد ذاتی برای تبدیل شدن به یک مامور پلیس زبردست در حوزه جرایم سایبری لازم است، اما این امر کافی نیست و برای توسعه و کامل کردن مهارت‌ها، آموزش نیز لازم است. آموزش پیشرفته در زمینه جرایم سایبری باید در دسترس کسانی که کشف جرم را عملا اداره می‌کنند، قرار بگیرد. فناوری‌های نوین مدام در حال ظهور هستند و ماموران پلیس باید در جریان آخرین اطلاعات روز داشته باشند .

درحال حاضر، علی‌رغم تشکیل دایره مبارزه با جرایم رایانه‌ای در اداره آگاهی نیروی انتظامی جمهوری اسلامی ایران، مقامی تحت عنوان «مامور کشف جرایم سایبری» که وظیفه او منحصرا بررسی جرایم ارتکابی در حوزه باشد، وجود ندارد. شاید یکی از دلایل این امر، فقدان قانون لازم‌الاجرا درخصوص جرایم ارتکابی در فضای مجازی می‌باشد؛ زیرا در صورتی که قانون خاصی در این حوزه تصویب شود، نیروی انتظامی به عنوان ضابط دادگستری، باید تمام تلاش خود را در جهت کشف این جرایم در کشور به کار گیرد.

ب) شیوه کشف جرایم سایبری

پلیس به‌عنوان ضابط دادگستری، بلافاصله پس از اطلاع از وقوع جرم، باید اقداماتی را که برای حفظ آثار و دلایل جرم و جلوگیری از فرار یا اختفای متهم ضروری است، انجام دهد و مراتب را به مقام قضایی اعلام کند. از آنجا که دلایل ارتکاب جرم در فضای مجازی، عمدتا ادله الکترونیک می‌باشند، پلیس به منظور بررسی و کشف جرایم سایبری با مسائلی مواجه می‌شود که در سایر جرایم مطرح نیست. ادله دلایل الکترونیک، ویژگی‌هایی دارند که آنها را از دلایل سنتی متمایز می‌سازد. این گونه دلایل نسبت به اسناد و مدارک دیگر، آسیب‌پذیرتر هستند؛ زیرا به آسانی می‌توان آنها را دستکاری یا جعل کرد و یا با استفاده از دانش فنی مناسب پنهان کرد .

ماهیت خاص دلایل الکترونیکی به گونه‌ای است که پذیرش آنها را در مراجع قضایی با چالش‌های ویژه‌ای مواجه کرده است. به منظور مقابله با این چالش‌ها، ماموران پلیس باید روش‌های خاص جمع‌آوری دلایل مذکور را که مرکب از چهار مرحله جمع‌آوری مدرک، بررسی، تجزیه و تحلیل و ارائه گزارش می‌باشد، به نحو صحیحی اجرا کند.

مرحله جمع‌آوری شامل جستوجو برای شناسایی، جمع آوری و مستندسازی مدارک الکترونیکی است .برای اینکه پلیس بتواند داده‌ها یا سیستم‌های رایانه‌ای را تفتیش و توقیف نماید، به دستور مقام قضایی نیاز دارد؛ مگر کسی که داده‌ها یا سیستم‌های مذکور را در اختیار دارد، رضایت کتبی به منظور تفتیش آن بدهد. در عین حال، در صورت وجود ظن منطقی مبنی بر وجود ادله و فوریت امر، پلیس می‌تواند بدون دستور قضایی اقدام به تفتیش یا توقیف داده‌ها نماید. در حقیقت، هنگام بررسی دلایل وقوع جرم، پلیس باید اطمینان یابد که حقوق شخصی افراد را کاملا رعایت کرده است.

فرایند بررسی، مدارک را قابل رویت کرده و اصل و مفهوم آن را مشخص می‌سازد. این کار باید به طریقی صورت گیرد که دلایل موردنظر، از هرگونه تغییر، تحریف یا آسیب مصون بماند. در مرحله تجزیه و تحلیل، به ارزشی اثباتی و اهمیت دلیل پرداخته می‌شود و در نهایت در مرحله ارائه گزارش، پلیس باید گزارش مکتوبی که کلیات مربوط به فرایند بررسی و اطلاعات مربوطه به دست آمده را دارا باشد، به مقام قضایی ارائه دهد. دلایل ارائه شده تنها در صورتی قابلیت استناد خواهند داشت که ابزارها و روش‌های استاندارد در مراحل شناسایی، کشف، جمع آوری، مستندسازی، تجزیه و تحلیل، حفظ و مراقبت از دلایل الکترونیکی و ارائه آنها به دادگاه، به نحو صحیحی به کار گرفته شده باشد.

پلیس فتا و فناوری اطلاعات و ارتباطات در فضای مجازی

واژه پلیس در افکار عمومی همواره به عنوان ضابط قضایی نقش بسته و با مأموریت کشف جرم همراه بوده در واقع، پلیس تنها به عنوان ابزار سیاست‌های کیفری- واکنشی- مورد استفاده قرار می‌گرفته است؛ به بیان دیگر نقش پلیس به طور سنتی فقط در چارچوب نظام کیفری تعریف می‌شود. این در حالی است که اصولاً پیدایش نهاد پلیس در جوام انسانی تنها جهت کشف و سرکوبی جرایم نبوده است، بلکه مأموریت نخستین پلیس همانا حفظ نظم و انضباط و پیشگیری از جرم در سطح جوام می‌باشد. (ذبیح اله نژاد، ۱۳۹۶ ، ۶۷)

با شکل‌گیری فضای مجازی، مرزها کم‌رنگ‌تر شده است و جهانی‌شدن در کلیه‌ی امور اجتماعی به وضوح دیده می‌شود. سرعت، ارزانی، بالا بودن کیفیت، نزدیکی و در دسترس بودن، شفافیت و تنوع از ویژگی‌های فضای مجازی است. همین ویژگی‌ها زمینه مناسبی را برای مجرمین فراهم کرده است. لذا پلیس با درک این موضوع وارد فضای مجازی شده است.

در گذر زمان، با افزایش شناخت، آگاهی و دانش انسان در خصوص پدیده‌ها، نیازها و شیوه‌های پاسخگویی به آن‌ها، رفته رفته علم و فناوری به وجود آمد و مدام در حلقه‌ی پیشرفت قرار گرفت. تا جایی که امروزه این فناوری است که بسیاری از جنبه‌های زندگی انسان را باز تعریف می‌کند و اگرچه مزایای فراوانی نیز برای او فراهم آورده

است، گاه انسان را در پی خود کشیده تا جایی که ساخته‌ها و پرداخته‌های دست بشر، انسان سرگشته‌ی عصر انفجار اطلاعات را اسیر خود ساخته و به هر سو که اراده کند، می‌کشد. (شاه محمدی، ۱۳۹۳، ۹۹)

نیمه‌ی پایانی قرن بیستم و پس از جنگ جهانی دوم، دوره‌ی طلایی دانش و فناوری بشر و دوره‌ی انتقال از عصر صنعت و ماشین به عصر فناوری اطلاعات است. توسعه‌ی شبکه‌ها با کارکردهای نظامی در ابتدا و توسعه‌ی آن‌ها و تعریف کارکردهای جدید و ایجاد امکان اتصال مراکز دانشگاهی، پژوهشی، علمی و تبادل اطلاعات با یکدیگر در این نیمه اتفاق افتاده است. تجاری سازی فناوری اطلاعات و ارتباطات و به تب آن کاهش هزینه‌های رایج و امکان استفاده‌ی عموم از این فناوری، اینترنت را به معنای امروز آن در دهه‌ی پایانی قرن بیستم به مردم معرفی نمود و امروزه این فناوری عظیم با میلیاردها رایانه، میلیون‌ها خدمات دهنده و صدها هزار شاه راه ارتباطی اصلی در برابر بشر قرار دارد تا از مواهب و مزایای بی بدیل آن استفاده کند یا خود را با پلیدی‌ها و آسیب‌های آن به نابودی کشد. رایانه، اینترنت و تمامی ابزارهای مبتنی بر فناوری اطلاعات و ارتباطات، در ابتدا و در ذهن و تصمیم مخترعان آن، صرفاً با هدف خدمت به بشر و ساده‌سازی و افزایش کیفیت زندگی انسان، طراحی و تولید شده‌اند. اما در عمل تبدیل به چاقوی دو لبه‌ای گشته‌اند که سعادت و شقاوت را هم زمان با هم به ارمغان می‌آورند و شهروند امروز دهکده‌ی دیجیتالی جهانی را برابر یک انتخاب و یک سؤال بزرگ قرار داده است که)) آیا انسان نیازمند باز تعریف نیازها، خواسته‌ها، مناف و. خود در فضای به اصطلاح مجازی است؟فناوری اطلاعات و ارتباطات ضمن تأثیرگذاری بر تمامی جنبه‌های زندگی اجتماعی بشر، بر جرایم، تهدیدها و آسیب‌ها نیز تأثیر گذاشته است. بسیاری از جرایم قدیمی با استفاده از ابزارهای رایانه‌ای با سهولت، اثرگذاری و مناف بیشتر برای مجرمین از سوی آنان صورت می‌گیرند و حتی دسته‌ی دیگری از جرایم که کاملاً جدید بوده و صرفاً اختصاص به فضای مجازی دارند نیز شکل گرفته و در قاموس مجرمین از منظر ارتکاب و در قاموس پلیس از منظر پی جویی و مقابله وارد شده‌اند ((عالی پور،۱۳۹۰، ۵۴)

نسل سوم جرایم رایانه‌ای نیز هم زمان با فراگیر شدن اینترنت از اوایل دهه‌ی ۱۹۹۰ میلادی به وجود آمدند. این جرایم که با گسترش کاربرد شبکه و اینترنت به وجود آمدند نام)) جرایم سایبری را به خود گرفتند. (رضـــوی،۱۳۹۶، ۱۴۰) گسترش جرایم رایانه‌ای در دنیا باعث شد تا حکومت‌ها در جهت ایجاد ساز و کار قانونی و حقوقی رسیدگی و مبارزه با این‌گونه جرایم قدم بردارند. کنوانسیون‌های بین‌المللی نیز برای تشریک مساعی در روند شناسایی جرم و مجرم، همکاری در پی جویی و تعقیب قضایی و پلیسی مجرمان و تبادل دانش و اطلاعات پلیسی در شناخت و کشف علمی جرایم سایبری نیز تشکیل شدند که از مهم‌ترین آن‌ها می‌توان به کنوانسیون بوداپست در سال ۲۰۰۱ میلادی اشاره کرد. از کشورهای فعال پیش رو در پی جویی و مبارزه با جرایم رایانه‌ای می‌توان به ایالات متحده آمریکا، روسیه، چین، کره جنوبی، انگلستان، هند و فرانسه اشاره کرد. (زیبر، ۱۳۹۰، ۷۴)

توسعه‌ی روزافزون زیر ساخت‌های فناوری اطلاعات و ارتباطات در کشور و افزایش کاربران از اینترنت و سایر فناوری‌های اطلاعاتی، ارتباطی و مخابراتی نظیر خطوط تلفن‌های ثابت و همراه، شبکه‌های دیتای کشوری و محلی، ارتباطات ماهواره‌ای از جمله دلایلی است که لزوم ایجاد و توسعه‌ی ساز و کار برای برقراری امنیت در فضای تولید و تبادل اطلاعات جمهوری اسلامی ایران را توجیه می‌کند. همچنین توسعه‌ی خدمات الکترونیک، بانکداری الکترونیک، تجارت الکترونیک، آموزش الکترونیک و سایر خدمات از این دست، نیز لزوم ایجاد پلیسی تخصصی در مجموعه‌ی نیروی انتظامی جمهوری اسلامی ایران را برای تأمین امنیت و مقابله با جرایمی که در این فضا به وقوع می‌پیوندند را آشکار می‌کند(گلستانی،۱۳۹۱، ۹۳) از سوی دیگری رشد قارچ گونه‌ی جرایم در حوزه‌ی فضای تولید و تبادل اطلاعات کشور) فتا(مثل کلاهبرداری اینترنتی، جعل داده‌ها و عناوین، سرقت اطلاعات، تجاوز به حریم خصوصی اشخاص و گروه‌ها، هک و نفوذ به سامانه‌های رایانه‌ای و اینترنتی، هرزه نگاری و جرایم اخلاقی و برخی جرایم سازمان‌یافته‌ی اقتصادی، اجتماعی و فرهنگی ایجاب می‌کند که پلیس تخصصی که توان پی جویی و رسیدگی به جرایم سطح بالای فناورانه داشته باشد، به وجود آید. از سوی دیگر با توجه به تصویب قانون جرایم رایانه‌ای در مجلس شورای اسلامی و لزوم تعیین ضابط قضایی برای این قانون و نیز مصوبات دولت جمهوری اسلامی ایران مبنی بر تشکیل پلیس فضای تولید و تبادل اطلاعات، در بهمن ماه ۱۳۸۹ به دستور فرماندهی محترم نیروی انتظامی جمهوری اسلامی ایران پلیس فتا تشکیل گردید. (جوان جعفری، ۱۳۹۹، ۸۳)

هدف از تشکیل پلیس فضای تولید و تبادل اطلاعات می‌توان تأمین امنیت فضای مجازی، صیانت از هویت دینی، ملی و ارزش‌های انسانی جامعه در فتا، حفظ حریم خصوصی و آزادی‌های مشروع، صیانت از مناف، اسرار و اقتدار ملی در فضای تولید و تبادل اطلاعات، حفظ زیر ساخت‌های حیاتی کشور در مقابل حملات الکترونیک، اعتماد و آسودگی خاطر آحاد شهروندان جامعه برای انجام تمامی امور قانونی از جمله فعالیت‌های اقتصادی، اجتماعی و فرهنگی به منظور صیانت از حاکمیت و اقتدار ملی دانست.

ماهیت اصلی پلیس فتا، عملیاتی است به این معنا که به صورت کاملاً تخصصی و از طریق تجهیز به مسائل ارزشمند نیروی انسانی، دانشی و تجهیزاتی، نسبت به تأمین امنیت فضای تولید و تبادل اطلاعات با رویکرد مقابله با جرایم از طریق پیش‌بینی، پیش‌گیری و کشف جرم اقدام می‌نماید. از جمله وظایف و مأموریت‌هایی که این پلیس در فضای مجازی به عهده دارد می‌توان ایجاد امنیت و کاهش مخاطرات برای فعالیت‌های علمی، اقتصادی، اجتماعی در جامعه‌ی اطلاعاتی، حفاظت و صیانت از هویت دینی و ملی، مراقبت و پایش از فضای تولید و تبادل اطلاعات برای پیش‌گیری از تبدیل شدن این فضا به بستری برای انجام عملیات‌هایی برای تحقق فعالیت‌های غیر قانونی و ممانعت از تعرض به ارزش‌ها و هنجارهای جامعه در فتا از جمله‌ی وظایف و مأموریت‌های پلیس فضای تولید و تبادل اطلاعات ناجا می‌باشد بین امنیت فضای تولید و تبادل اطلاعات کشور با سازمانی فعال یا نوآورانه و به سوی

پیشرفت، کارآمد، پویا، پاسخ‌گو و قانونمند در راستای فراهم نمودن اعتماد و آسودگی خاطر آحاد شهروندان جامعه و صیانت از حاکمیت و اقتدار ملی و ارزش‌های اسلامی در افق ایران ۱۴۰۴ چشم‌انداز پلیس فضای تولید و تبادل اطلاعات ناجا است. (گوردون هیوز، ۱۳۹۰ ، ۳۴)

تاثیر فناوری اطلاعات و ارتباطات در فضای مجازی

فناوری اطلاعات با سرعت شگفت‌انگیزی تمامی ارکان حیات بشری از جمله مقوله‌ی نظم و امنیت و آرامش عمومی را دستخوش تحولات و دگرگونی‌های اساسی نموده است. همزمان با تحولات قرن بیستم و فرایند جهانی شدن، در عصر حاضر، تکنولوژی ارتباطات و اطلاعات، امکان ظهور جامعه شبکه‌ای را فراهم آورده است که تعاریف جدیدی از هویت‌ها و جرائم انسانی عرضه می‌کند. جهان جدید به صورت شبکه‌ای در آمده که بافت اصلی آن را اطلاعات و نظام ارتباطات الکترونیک تشکیل می‌دهد. در پس این جامعه شبکه‌ای، تغییر ماهیت مراودات اجتماعی به شکل جوام مجازی و معاشرت‌های الکترونیکی از طریق متون الکترونیک و سیستم چندرسانه‌ای به عنوان محیط نمادین پدید آمده است که باعث پیدایش نوعی ناامنی اجتماعی و جرایم و بزهکاری‌های در سیستم (IT) جدید در فضاهای مجازی شده است.

نتیجه گیری :

در ایران هم با تشکیل و راه اندازی پلیس فتا، اقدام های جدی به منظوررفع آسـ یب های مجازی و جرائم فضای مجازی صـورت پذیرفته اند و وجود نیروهای متخصـص و آگاه به فناوری در این مجموعه، نه تنها موجب تأمین سـلامت و امنیت فضای مجازی می شوند، بلکه با آگاهی و اطلاع رسانی عمومی در مخاطرات و معضل های اجتماعی و امنیتی موجود در دنیای مجازی به عنوان حافظ نظم و امنیت در این حوزه، نقش مؤثر ایفاءمی نمایند. همچنین علاوه بر ضـرورت ملاحظه دقیق ویژگی های خاص و منحصـربه فرد فضای مجازی، می تواند به دلیل انعطاف پذیری و جامعیت لازم، از الگوهای پیشگیری وضعی و اجتماعی از وقوع جرائم مرسوم نیز استفاده کرد.با تشکیل و راه‌اندازی پلیس فتا، اقداماتی جدی در جهت رفع آسیب‌های سایبری و جرایم فضای مجازی صورت پذیرفته است. با توجه به نو پا بودن این پلیس، راهی بس طولانی و دشوار در پیش است تا این نهاد تازه تأسیس بتواند با توانمندی‌های اکتسابی، خود را آماده‌ی مبارزه و تقابل با هرگونه از جرایم سایبری کند. برای جلوگیری از بروز هرگونه جرایم سایبری، پلیس فتا باید راه کارهای پیشگیرانه را مدنظر قرار دهد. به همین منظور برخی از اسناد بین‌المللی از جمله"کنوانسیون مبارزه با جرایم سایبری ۲۰۰۱ بوداپست"به تصویب رسیده است. افزون بر این، سازمان ملل و سازمان‌های منطقه‌ای نیز با انتشار متون و نشریات مختلف در راستای پیشگیری از جرایم سایبری و مبارزه با آن، اقدامات خوبی را انجام داده‌اند.پلیس برای دستیابی به یک الگوی مناسب پیشگیری از وقوع جرایم سایبری، علاوه بر ضرورت ملاحظه دقیق ویژگی‌های خاص و منحصر به فرد فضای سایبر، می‌تواند

به الگوهای پیشگیری از وقوع جرایم مرسوم نیز اعتنا کند. از میان الگوهای گوناگون، پیشگیری وضعی و اجتماعی از جرایم، به دلیل انعطاف‌پذیری و جامعیت لازم می‌تواند مورد توجه قرار گیرند؛ به ویژه تدابیر پیشگیرانه وضعی که اساسا صبغه فنی دارند و به خوبی می‌توانند با تدابیر فنی قابل اتخاذ توسط پلیس در این فضا، سازگاری یابند. پیشگیری وضعی از جرایم سایبری عمدتا عمل گرا و غیر نظری است. در این بخش می‌توان از طریق دشوار ساختن ارتکاب جرم، افزایش خطر دستگیری و کاهش جاذبه آماج‌های جرم از وقوع آن پیشگیری نمود. در خصوص مفهوم و شکل‌های بکارگیری تدابیر پیشگیرانه وضعی توسط پلیس در فضای سایبر، به طور کلی می‌توان از طریق به کارگیری تدابیر نظارتی، تدابیر صدور مجوز.، ناشناس کننده‌ها و رمزنگارها و تدابیر محدودکننده دسترسی (فیلترینگ) به پیشگیری از جرایم سایبری پرداخت. همین‌طور با عملیاتی شدن نهاد حاکمیتی CERT ملی (گروه‌های واکنش سریع) که پلیس در آن نقش پررنگی دارد، می‌تواند به ساماندهی اقدامات حوزه و به ویژه نظارت بر اقدامات سایر فعالان مسئول، ارائه دهندگان خدمات و حتی کاربران نهایی کمک کند. در عین حال پلیس و نهادهای حاکمیتی در این حوزه بهتر می‌توانند به وظایف خویش عمل کنند و از نقض حقوق و آزادی‌های مشروع شهروندان جلوگیری کرده و با آن برخورد کنند.رفع انگیزه‌های مجرمانه و منحرفانه از دیگر روش‌های پیشگیرانه‌ای است که توسط پیشگیری اجتماعی صورت می‌گیرد. البته باید توجه داشت، فرآیند پیشگیری اجتماعی از جرایم سایبری به تنهایی از عهده پلیس بر نمی‌آید، بلکه نیازمند سیاست‌گذاری و همکاری همه جانبه در سطح کلان می‌باشد.ارتقاء سطح آگاهی‌های جامعه، مخصوصا نوجوانان و جوانان که بیشترین استفاده را از فضای سایبر دارند، می‌تواند در پیشگیری از جرایم سایبری بسیار مؤثر باشد. پلیس باید با بهره‌گیری از آموزه‌های مکتب بزه دیده شناسی در تهیه طرح‌های پیشگیری عمومی و جامع و آموزش‌های همگانی حداکثر استفاده را در این خصوص بنماید.فضای مجازی تعارض قوانین داخلی کشورها یکی از موانع مهم در پی جویی فراملی جرایم سایبری است. همچنین چالش‌های مهم دیگر مانند وب عمیق و تاریک، اینترنت اشیا، پول‌های مجازی، محیط ابری وجود دارد که باید به آن‌ها پرداخته شود. باید یک نظام حقوقی منسجم جهانی توسط سازمان ملل با تأیید کشورها برای مقابله با جرایم سایبری تدوین و تحت اراده جهانی اجرا شود. با رفع این موانع و محدودیت‌ها، پلیس فتا می‌تواند به طور موثرتری با جرایم سایبری مقابله کند و امنیت فضای مجازی را برای همه کاربران افزایش دهد.علاوه بر موارد فوق، در مقدمه و نتیجه‌گیری می‌توانید به موارد زیر نیز اشاره کنید: اهمیت فضای مجازی در دنیای امروز، آثار و پیامدهای جرایم سایبری ، نقش پلیس فتا در پیشگیری از جرایم سایبری ، مسئولیت‌های فردی و اجتماعی در قبال جرایم سایبری ،همچنین می‌توانید از آمار و ارقام مربوط به جرایم سایبری در ایران و جهان برای تقویت مطالب خود استفاده کنید.

منابع و ماخذ

الف : کتب

۱. انصاری، ولی الله، ۱۳۹۰،کشف علمی جرائم، چاپ اول، انتشارات سمت.

۲. باستانی، برومند ، ۱۳۹۳ ، «جرائم کامپیوتری و اینترنتی» انتشارات بهنامی، تهران.

۳. پرویزی، رضا، ۱۳۹۴، پیجویی جرایم رایانهای، چاپ اول، تهران: انتشارات جهان جا م جم.

۴. حسن بیگی، ابراهیم ،۱۳۹۴، «حقوق و امنیت در فضای سایبر» مؤسسه فرهنگی مطالعات و تحقیقات بین‌المللی ابرار، تهران.

۵. زیبر، اولریش، ۱۳۹۰ ،جرائم رایانه ای،ترجمه ی نوری، محمدعلی و نخجوانی، رضا و بختیاروند، مصطفی و رحیمی، احمد، تهران، انتشارات گنج دانش، چاپ دوم.

۶. شیرزاد، کامران، ۱۳۹۸ ،جرایم رایانه ای از دیدگاه حقوق جزای ایران و حقوق بین الملل، چاپ اول، تهران: انتشارات بهینه فراگیر.

۷. عالی پور، حسن، ۱۳۹۰ ،حقوق فناوری اطلاعات و ارتباطات (جرائم رایانه ای)، تهران: انتشارات خرسندی

۸. گوردون هیوز، ۱۳۹۰،پیشگیری از جرم، ترجمه ی کلامی، علیرضا و جغتایی، محمدتقی تهران، انتشارات سازمان بهزیستی کشور و دانشگاه علوم بهزیستی و توانبخشی، چاپ اول.

۹. گاتن، آلن، ۱۳۹۳،کشف ادله الکترونیکی، ترجمه مصیب رمضانی، چاپ اول، دبیرخانه شورای عالی اطلاع رسانی، تهران: انتشارات طوس.

۱۰. میر محمد صادقی، حسین ، ۱۳۹۳ ،ملاحظاتی در موضوع پیشگیری از وقوع جرم.

۱۱. معین ، محمد ، ۱۳۹۹ فرهنگ فارسی، روزنه، موسسه چاپ و انتشارات دانشگاه تهران

مقالات

۱۲. الهی منش ، محمد رضا ، تبریزی ، صادق ، ۱۳۹۷ ، کشف علمی جرایم با توسل به ادله نوین و مدارک الکترونیکی (دیجیتال)، کاراگاه ، سال ۱۱، شماره ۴۴.

۱۳. ابرند آبادی ، علی حسین، ۱۳۹۷ ، پیشگیری عادلانه از جرم، منبع: پژوهشنامه حقوق کیفری سال سیزدهم بهار و تابستان ۱۴۰۱ شماره ۱.

۱۴.

۱۵. ابراهیمی ، شهرام (۱۳۹۸)، رویکردهای موسع و مضیق پیشگیری و آثار آن ، مجله آموزه های حقوقی دانشگاه علوم رضوی ، شماره ۲۱ .

۱۶. بیات، بهرام، شرافتیپور، جعفر و عبدی، نرگس ۱۳۹۷. پیشگیری از جرم با تکیه بر رویکرد اجتماع محور، تهران: معاونت اجتماعی نیروی انتظامی.

۱۷. رضـــوی، محمد ۱۳۸۶. جرایم ســـایبری و نقش پلیس در پیشـــگیری از این جرایم و کشـــف آنها، فصلنامه دانش انتظامی، شماره ۳۳، سال نهم، بهار.
۱۸. ذبیح اله نژاد، وحید ۱۳۹۶نقش پلیس فتا در پیشـــگیری وضـــعی و پیشـــگیری اجتماعی از جرائم سایبری، فصلنامه دانش انتظامی البرز، سال پنجم، شمارۀ اول، بهار .
۱۹. شاه محمدی، غلامرضا و تاهو، منصور ۱۳۹۳بررسی شیوه های پیشگیری از جرائم سایبری؛ مبتنی بر فناوری اطلاعات، فصلنامۀ پژوهش های اطلاعاتی و جنایی، دورۀ نهم، شمارۀ۳۵.
۲۰. شهری ،غلامرضا، ۱۳۹۵نقش پلیس در کنترل و پیشگیری از نابهنجاریهای اجتماعی ، فصلنامه مطالعات پیشگیری از جرم ، سال اول ، شماره اول .
۲۱. کوزه پز ، محمد حسین ، و همکاران ،۱۳۹۳، تبیین جرم شناختی بزه کاران سایبری ، پژوهش حقوق کیفری ، سال سوم ، شماره نهم .
۲۲. گلستانی، محمود؛ پهلوانی، محمدتقی و عبدالله‌پور، مهدی ۱۳۹۱ چالش ها و فرصت های پیشروی جرم شناسی سایبری، فصلنامۀ دانش انتظامی سمنان، سال دوم، شمارۀ ششم.