مطالعات علوم سیاسی، حقوق و فقه

دوره ۲، شماره ۲/۱، تابستان ۱۳۹۵

صفحات ۱۴۰- ۱۴۸

ISSN: ۲۴۷۶-۴۴۶۹

www.irijournals.com

راهکارهای سیاست جنایی ایران در پیشگیری از جرایم سایبری

محمد ابوالفتحی[۱]*، مجتبی مهرورزی[۲]

[۱]استادیار گروه علوم سیاسی دانشگاه رازی کرمانشاه، کرمانشاه، ایران. (نویسنده مسئول)

[۲]دانشگاه آزاد اسلامی، واحد بروجرد، گروه حقوق، بروجرد، ایران.

چکیده

پیشگیری از جرم نخستین گام برای تحقق عدالت کیفری است. فضای سایبر به اقتضای ویژگیهای خاصی که دارد، بسیار مساعد برای پیشگیرهای مختلف می‌باشد. رهایی بستر، گمنامی کاربران، آسیب پذیری آماج، دشواریِ شناسایی بزهکاران، سهولت ارتکاب جرم، گستردگی خسارت، کثرت بزه‌دیدگان و کم سن بودن اغلب کاربران، ضرورت پیشگیری را از این جرایم را دو چندان ساخته است. لذا با اعمال شیوه های فنیِ پیشگیری از جرم می توان تا حد مطلوبی از این جرایم پیشگیری نمود.در این مقاله تلاش شده است تدابیر و توصیه های مختلف با تکیه بر راهکارهای پیشگیرانه در فضای سایبر تبیین و از این طریق راهکارهایی به منظور کاهش فرصتهای مجرمانه و افزایش خطر ارتکاب جرم ارائه شود.

کلمات کلیدی : فضای سایبر، جرایم سایبری، علت شناسی، پیشگیری اجتماعی، پیشگیری وضعی

۱. مقدمه

انسان عصر حاضر، افزون بر دنیای فیزیکی، که از زمان خلقت خود با آن مأنوس بوده و با شرایط و مقتضیات آن خو گرفته، به دنیای جدیدی به نام فضای سایبر پا گذاشته که از ویژگی‌های متمایز برخوردار است.

این فضا توانمندی‌هایی برای پیشبرد بهینه امور در اختیار دارد که بشر را ناگزیر از به کارگیری بدون تبعیض و فراگیر آن در تمامی عرصه‌های سیاسی، اقتصادی، اجتماعی، فرهنگی، صنعتی، بهداشت و درمان و حتی نظامی کرده است. انعطاف‌پذیری و سادگی بی‌نظیر در کاربری، حتی موانع سنی و میزان دانش و مهارت را نیز برداشته است. بی‌تردید، این وضعیت بیم و امیدهایی را برمی‌انگیزد. اما آنچه مسلم است اینکه بهره‌برداری صحیح و سودمند از این فضا مستلزم رعایت هنجارهایی است که تخطی از آن‌ها می‌تواند باعث آسیب‌هایی شود و برخی از آن‌ها حتی مستوجب جرم‌انگاری و مجازات گردند. با این حال، چنانچه به کاربران، که مانند کودکی نوپا در این دریای بی‌کران رها هستند، آموزش‌های صحیح داده نشود، هرگونه مقابله با هنجارشکنی های سایبری در جهت برقراری موازین اخلاقی سایبری، می‌تواند با ایرادات جدی حقوقی و اخلاقی مواجه گردد. با این تفاسیر ضرورت پیش بینی و اتخاذ سیاست‌ها و قواعد جدید متناسب با تحول سریع تکنولوژی در دیگر علوم و علم حقوق یک امر غیر قابل انکار و الزامی می‌باشد.

۲. گفتار نخست: تعاریف فضای سایبر

فضای سایبر اگرچه اصطلاحی نسبتاً جدید است اما مفهوم آن جدید نیست و پیدایش این مفهوم هم‌زمان با اختراع تلفن توسط الکساندر گراهام بل در سال ۱۸۷۶ بوده است. ولی واژه فضای سایبر اولین بار توسط ویلیام گیبسون در کتاب رمان نئورامانسر، که در آن فضای مذکور را عنوان موطن داده‌ها و اطلاعات موجود در یک آینده دور تاریک توصیف می‌کند، به کار برده شد. پس از آن واژه مذکور در فرهنگ‌های مختلف دنیا مورد استفاده قرار گرفت. همان‌طور که بسیاری از نویسندگان ایرانی معادل این کلمه واژه فضای مجازی را در نوشته‌های خود به کار برده‌اند. و واژه سایبر در فارسی به مجاز و مجازی ترجمه شده است. اما این ترجمه گویای دقیق این واژه نیست زیرا محیط سایبر محیطی است حقیقی و واقعی و نه دروغین و مجازی و فقط به شکل مادی و ملموس احساس شدنی نیست و در چنین فضایی آنچه تجربه می‌شود واقعی است. همانند صحبت کردن چهره به چهره شخصی با شخص دیگر یا تحقیق کتابخانه‌ای. همچنین از این طریق چنین فضایی می‌توان خرید و فروش کرد یا مدارک دانشگاهی گرفت.

برای فضای سایبر تعاریف متعددی شده است که در اینجا به برخی از آن‌ها، که حائز اهمیت بیشتری هستند، اشاره می‌شود:

-«فضای سایبر یک ناحیه واقعی است. فعالیت‌هایی که در این فضا اتفاق می‌افتد شامل تبادل اطلاعات و راه‌هایی برای تجمیع اطلاعات مثل گردهمایی خبری می‌باشد»

الف : ویژگی‌های فضای سایبر

با توجه به اینکه جزء اعظم فضای سایبر محیط شبکه رایانه‌ای به طور عام، که هم شامل شبکه‌های محلی و هم گستره جهانی می‌شود، می‌باشد بیان خصوصیات شبکه رایانه‌ای می‌تواند مبین خصوصیات فضای سایبر باشد.

۱ - سرعت و روزآمدی فضای سایبر ۲- سهولت تغییر هویت در فضای سایبر ۳- گسترده و فراگیر بودن فضای سایبر ۴- آزادی در فضای سایبر ۵- فرا مکانی و فرا زمانی بودن فضای سایبر ۶- نا متمرکز بودن فضای سایبر

ب : انواع جرایم سایبری

۱. تنوع انواع جرایم ارتکابی در فضای سایبری شامل جرایم نسل اول کامپیوتری و یک‌سری جرایم بسیار جدید و بی‌سابقه می‌باشد(باستانی، ۱۳۸۳).

۱- جرایم سنتی در محیط دیجیتال:

۲. ۱-۱- جاسوسی رایانه‌ای: افشای، انتقال و استفاده از اسرار است که این کار امنیت ملی را به مخاطره می‌اندازد(باستانی، ۱۳۸۳).

۳. ۱-۲ -ساپوتاژ رایانه‌ای: این جرم با جرم تخریب شباهت بسیاری دارد، هدف مجرم اخلال در نظام سیاسی و اقتصادی یک کشور است. در واقع اصلاح، موقوف‌سازی، پاره کردن غیرمجاز داده‌ها یا عملیات کامپیوتری به منظور مختل ساختن عملکرد عادی سیستم سابوتاژ رایانه‌ای گویند(باستانی، ۱۳۸۳).

۴. ۱-۳- جعل کامپیوتری: وارد کردن، تغییر، محو یا موقوف سازی داده‌های کامپیوتری یا برنامه‌های کامپیوتری به منظور و اهداف سیاسی و اقتصادی صورت می‌گیرد(باستانی، ۱۳۸۳).

۱-۴ - افترا و نشر اطلاعات از طریق پست الکترونیک

۱-۵ - تطهیر نامشروع پول

۱-۶- قاچاق مواد مخدر

۱-۷ -جرایم ناظر به کپی رایت و برنامه‌ها

۱-۸ - جرایم در تجارت الکترونیک

۱-۹ -کلاهبرداری

۱-۱۰- سرقت و سوءاستفاده از اطلاعات

۱-۱۱ - دسترسی غیرمجاز

۱-۱۲- پخش و انتقال ویروس

ج : مجرمین سایبر

۱- **هکر:** در دهه ۱۹۷۰ واژه هکر به شخصی اطلاق می‌شد که در برنامه‌نویسی بسیار ماهر و باهوش باشد. بعدها در دهه ۱۹۸۰ این واژه به معنی شخصی بود که در نفوذ به سیستم‌های جدید به صورت ناشناس تبحر داشته باشد. امروزه بیشتر با هدف ترساندن هکرها، رسانه‌ها و مقامات مسئول مانند آژانس‌های دولتی و ادارات پلیس، این واژه به هر شخصی که مرتکب یک جرم مرتبط با فناوری شود، اطلاق می‌کنند.

۲- **کرکرها:** از سوی دیگر کرکرها هکرهای بدخواهی هستند. آن‌ها به سیستم‌ها رخنه می‌کنند تا خراب‌کاری کنند، ویروس‌ها و کرم‌های رایانه‌ای را منتشر می‌کنند، فایل‌ها را پاک می‌کنند یا بعضی انواع دیگر ویرانی را به بار می‌آورند. اختلاس، کلاهبرداری یا جاسوسی صنعتی (سرقت اطلاعات محرمانه یک شرکت) تنها بخش کوچکی از اهداف احتمالی کرکرها می‌باشد.

۳. گفتار دوم : سیاست جنایی

سیاست جنایی، یکی از شاخه‌های بین رشته‌ای علوم جنایی است که مطالعه و تدبیر بحران پدیده جنایی و عوامل و تبعات و راهکارهای پیشگیری از آن را در گرانیگاه (مرکز ثقل) نظر و توجه خود دارد. در این مسیر، دانش سیاست جنایی ضمن بهره‌گیری از خطوط و مبادی فکری و اسالیب (روشها) متقن علومی چـون جامعه‌شناسی، روان‌شناسی، اقتصاد، تاریخ، سیاست و فلسفه، تا حد محسوسی سعی می‌کند از آورده‌ها و استنتاجات پسا گفتمانی شاخه‌های جنایی و تخصصی هم‌عرض خود از جمله جرم‌شناسی، حقوق کیفری و تاریخ حقوق بهره جست و رویکرد تأکیدی خود را در تبیین و مهارت بحران موصوف معرفی نماید.

پارادایم محوری دانش سیاست جنایی این است که در پدیدهٔ جنایی ماهیتی فردی و اجتماعی دارد به که در تعامل مستقیم با تمامی ساخت‌ها و نهادهای جامعه می‌باشد و لذا جدل با آن یک تعهد فردی نیست و متولی منحصر ندارد، بلکه تعهدی جامعوی است که ایفا و اجرای موفق آن مستلزم همکاری تمامی سازوکارهای نظام اجتماعی اعم از حقوقی، فرهنگی، سیاسی، اقتصادی و... است»

شش عنصر در بطن سیاست جنایی وجود دارد که عبارتند از: جرم و جرم‌انگاری، انحراف، دولت، جامعهٔ مدنی، نظام پاسخ‌گویی شناور و انعطاف‌پذیر در قبال جرم و انحراف و پیشگیری. این عناصر که تجلی بخش هویت حقیقی این دانش می‌باشند، به وضوح گستردگی حوزه نگرش و مداخله سیاست جنایی را در اکناف و فراسوهای نظام اجتماعی به تصویر می‌کشند. بر این اساس، طراحی یک سازه موفق برای سیاست جنایی، مستلزم تحصیل اشراف و فضیلت نهادهای اجتماعی مختلف و آسیب‌شناسی نقش و کارایی آن‌هاست که بدون مطالعات فراگیر در جامعه میسر نخواهد شد.

الف : اقسام سیاست جنایی

سیاست جنایی در مفهوم علمی آن اعتبار عاملان و نهادهای دخیل در آن به اقسام مختلفی دسته‌بندی شده است. در مشهورترین طبقه‌بندی، سیاست جنایی به چهار نوع یا قسم دسته‌بندی شده است که عبارتند از: سیاست جنایی تقنینی، سیاست جنایی قضایی، سیاست جنایی اجرایی و سیاست جنایی مشارکتی.

۱- سیاست جنایی تقنینی:

همان‌طور که صراحت خود اصلاح گویاست، به راهبرد یا تفکری جنایی اطلاق می‌گردد که از سوی مقنن اتخاذ شده و در چارچوب یک سری مقررات و انتظامات قانونی مشخص و آشکار تشریح می‌گردد. این قسم از سیاست جنایی عملاً نوع نگرش، قضاوت و برداشت قانون‌گذار را نمایش می‌دهد که اصولاً در قالب جعل و وضع نصوص قانونی عینیت می‌یابد. در این قسم از سیاست جنایی، اندیشه و منطق مقنن در قبال پدیده جنایی و نهادهای پیرامونی آن رخ می‌نمایاند که در آشکارترین بعد آن با نهاد جرم انگاری سروکار پیدا خواهیم کرد. در راستای روشن نمودن نوع نگرش مقنن به پدیده انحراف که گستره وسیعی از مفهوم پدیده جنایی را به خود اختصاص می‌دهد، التفات به این مسئله راهگشا خواهد بود که عموما" در هیچ نظامی مقنن در مرحله سیاست‌گذاری جنایی به خلاف عناوین مجرمانه، هرگز فهرستی از رفتارهای منحرفانه را معرفی و منتشر نمی‌کند. درواقع چندان متعارف نیست که مقنن دقیقاً در قانون حد و مرز رفتار انحرافی و غیر انحرافی را معرفی نماید، زیرا چنین امکانی نظر به نسبی بودن مفهوم انحراف، سخت منتفی جلوه می‌کند. مقنن در مرحله سیاست‌گذاری، در عرض نهاد جرم‌انگاری و تعیین نظام واکنش‌دهی در قبال اعمال مجرمانه، انحرافات و راهبردهای اجرایی مناسب در راستای واکنش نسبت بد آنها و نیز نقش جامعهٔ مدنی در این ابعاد موازی توجه دارد. و لذا در بعد قانونی سیاست جنایی، انحراف از موضوعیت آشکار برخوردارند.

۱-۱- بررسی و تحلیل سیاست تقنینی جرایم سایبری در ایران و راهکارهای پیشرو

۲-۱-۱- معتقدیم در شرایط حاضر و با توجه به مشکلات امنیتی موجود و محتمل، گلوگاه صنعتIT ، داشتن قانون جرایم رایانه‌ای نیست و وجود قانون تجارت الکترونیکی و سایر قوانین در حال حاضر کافی است. برعکس، تصویب این قانون به شکل فعلی ممکن است خود به یک گلوگاه جدی برای این صنعت تبدیل شود.

۳-۱-۱- تکنولوژی اطلاعات نه‌تنها به‌عنوان یک تکنولوژی که به عنوان یک شیوهٔ نوین زندگی، بازیگران تأثیرگذار متعددی دارد اعم از متخصصین، کاربران، گروه‌های صنفی ذی‌نفع، سرویس‌دهندگان ... تصویب هر نوع قانونی در این زمینه باید با توجه به منافع، اشتراک‌ها و تضادهای تمامی این گروه‌ها صورت گیرد.

۴-۱-۱- تصویب قانون جدید جرایم رایانه‌ای، با تمام ایرادات مبنایی و شکلی اش، می‌تواند گام مثبتی به سوی مقابله با مجرمین باشد. چنان که در ابتدا نیز ذکر شد، هدف این بود که پرسش‌هایی درباره قانون جرایم رایانه‌ای ICT و کمک به توسعه در ذهن جستجوگر خواننده ایجاد کنیم. نقدهای وارد شده را نیز می‌توان در بازنگری قانون مورد توجه قرار داد. به هر روی، باید یادآوری کرد که ممکن است به دلیل اینکه غالباً متون قانونی پیچیده و برای غیرحقوقی ها خسته کننده به نظر می‌رسند، و البته قانون جرایم رایانه‌ای نیز کم و بیش از این قاعده مستثنی نیست، رغبتی به مطالعه این قانون نداشته باشیم؛ اما فراموش نکنیم که اکنون با قانونی روبه‌رو هستیم که تمامی کاربران رایانه و اینترنت کشور را در بر گرفته، و مهم‌تر از

حق‌هایی که برایمان قایل شده، تکلیف‌هایی است که بر عهده‌مان گذارده است. برای آگاهی از حقوق و تکالیفی که این قانون برایمان تعیین کرده، ساده‌ترین راه می‌تواند مطالعه متن قانون و در صورت لزوم، مطالعه نقدهایی بر این قانون باشد.

۲- سیاست جنایی قضایی:

در واقع سیاست جنایی قضایی، برون داد سیاست جنایی تقنینی در جریان رسیدگی قضایی است و نیز تفسیری است که قضات دادگاه ها در حین اجرای قانون از آن به عمل می آورند و آن را به اجرا می گذارند.

۲-۱- بررسی و تحلیل سیاست جنایی قضایی در ایران و راهکارهای پیشرو

با بررسی قواعد سنتی حاکم بر شیوه تعیین مرجع قضایی کیفری صالح نسبت به جرایم ارتکابی در فضای جغرافیایی و امکان تسری آن قواعد نسبت به جرایم ارتکابی در فضای سایبر دیده شد که برخی کشورها در قوانین ناظر به جرائم سایبری خود به این موارد متوسل شده‌اند. در حالی که اجرای کامل این قواعد در فضای جدید سایبر امکان پذیر نیست، اگرچه برخی قواعد از قبیل قاعده «صلاحیت دولت متبوع اشخاص دخیل در ارتکاب جرم»، «صلاحیت دولت با منافع تهدید شده» و یا «صلاحیت دولت مقدم در تعقیب در جرایم با خطر جهانی» به لحاظ تأثیر کم ماهیت فضای محل ارتکاب جرم در اجرای آن‌ها، در این مورد قابلیت اجرا دارند. ولی از یک طرف در فضای سایبر مرزی وجود ندارد تا به روشنی بتوان به قاعده صلاحیت سرزمینی استناد کرد. البته این معضل بعد از حل معضل بزرگ‌تر تعیین محل ارتکاب جرم بروز پیدا می‌کند. از طرف دیگر امکان بهره‌مند شدن از هویت‌های چندگانه متفاوت در فضای سایبر، اعمال صلاحیت تابعیتی را در هاله‌ای از ابهام فرو می‌برد. وجود بزه دیدگان بی‌شمار و امکان آسیب رساندن به تأسیسات حیاتی چندین کشور در یک زمان، استناد به قواعد میان‌بری نظیر صلاحیت حمایتی را با مشکلات بسیاری مواجه ساخته است. در نهایت با اینکه معضل جرایم سایبری فراگیر شده، ولی هنوز اما و اگرهای بسیاری در خصوص آن مطرح است که این خود تمسک به صلاحیت جهانی را نیز مشکل می‌سازد. بنابراین طرح راهکارها و تئوری‌های جدید اجتناب‌ناپذیر می‌نماید و ناچار باید به فکر قواعد تازه‌ای بود که با ماهیت این فضا سازگاری داشته و قابل اجرا باشند. در همین راستا برخی دانشمندان و نویسندگان تئوری‌های جدیدی را از قبیل « تئوری فضای سایبر به عنوان یک فضای آزاد بین‌المللی» که هم‌عرض با سایر فضاهای بین‌المللی دیگر از قبیل دریاهای آزاد و ماورای جو و قطب ها باشد، «تئوری دادگاه دیجیتالی یا سایبری» که به صورت مجازی به تمام جرایم ارتکابی در فضای مذکور رسیدگی می‌کند و یا «تئوری حداقل ارتباط لازم» و یا به عبارتی داشتن ارتباط منطقی جرم با یک کشور، با ادعای سازگاری بودن آن‌ها با فضای سایبر، مطرح کرده‌اند که هر کدام از زاویه‌ای دارای ایراد و چالش می‌باشد. بدین توضیح که تئوری اول بیشتر ناظر به وب‌سایت‌هاست که فقط حدود یک پنجم از موضوع‌های فضای سایبر را تشکیل می‌دهند. در مورد تئوری دوم باید گفت اولاً تا زمان ایجاد دادگاه مذکور، این تئوری قابلیت اجرا ندارد. ثانیاً یک تئوری آرمان‌گرایانه و ایده‌آلی است و عملاً اجرای آن خیلی سخت است. ثالثاً: در صورت تشکیل هم نسبت به جرایم خیلی محدود و معدودی می‌تواند اجرا شود و قدرت پاسخ‌گویی به اکثر جرایم را ندارد. تئوری سوم می‌تواند با اقدامات تکمیلی دولت‌های مختلف راهکاری برای خروج از چالش باشد. برخی جرایم معدود دیگر، علیرغم وجود ابهام در اجرای صلاحیت‌های سنتی، بر اساس صلاحیت حمایتی یا جهانی قابل رسیدگی هستند. اگرچه در اجرای آن مسئله استرداد مجرمین می‌تواند به عنوان چالشی بر سرراه آن محسوب گردد ولی اشکال در اجرای صلاحیت منافاتی با قبول اصل آن ندارد. بنابراین صلاحیت واقعی و جهانی بدون در نظر گرفتن محل وقوع جرم می‌توانند نسبت به جرایم سایبری اجرا شوند.

در جایی که ملاک تعیین صلاحیت بر اساس قواعد سنتی مکان وقوع جرم باشد به لحاظ عدم قابلیت اجرایی صلاحیت سرزمینی به ناچار باید قاعده دیگری را جایگزین آن کرد که به نظر می‌رسد با عنایت به مشکل و یا غیرقابل تشخیص بودن محل وقوع جرم در فضای سایبر بهترین نوع صلاحیت، صلاحیت مبتنی بر تئوری ارتباط منطقی میان جرم و یک دولت (تئوری سوم مذکور در فوق) باشد. در این صورت باید تئوری مذکور را به عنوان اصل در راستای تشخیص صلاحیت مراجع قضایی دانست و سایر تئوری‌ها از قبیل محل بارگذاری و یا پیاده‌سازی، محل استقرار اشخاص دخیل، محل استقرار سیستم‌های

دخیل و یا محل تحقق اثر و نتیجه و...، که در راستای تعیین مکان وقوع جرم مطرح شده‌اند، می‌توانند در خدمت این تئوری جهت تعیین حداقل ارتباط لازم و منطقی میان یک مکان و جرم واقعه به کار گرفته شوند. با این توضیح که قواعد حاکم بر تعارض صلاحیت‌ها همچنان در خصوص تعارض صلاحیتی نسبت به جرایم سایبری باقی می‌باشد ولی در اینجا دیگر به عنوان ضابطه‌ای مستقل محسوب نمی‌شوند بلکه در راستای تشخیص ارتباط بیشتر جرم یا نتایج حاصل از آن با یک مکان (حوزه قضایی) خاص به کار می‌آیند و بدین ترتیب نظام قضایی و حوزه قضایی صالح را مشخص می‌کنند. این امر نیازمند همکاری بین‌المللی دولت‌ها به طور جدی و پیش‌بینی کنوانسیون‌های ناحیه‌ای و جهانی و تثبیت قواعدی مقبول می‌باشد. همان‌طور که در بند ۵ ماده ۲۲ کنوانسیون جرایم سایبری بوداپست مجارستان بر این مسئله، یعنی به شور نشستن کشورهای ذی‌نفع جهت تعیین مناسب‌ترین و شایسته‌ترین عضو سال به تعقیب و رسیدگی، تأکید شده است.

در کشور ما از لحاظ رویه عملی، تا قبل از تصویب قانون مجازات جرایم رایانه‌ای قضات سعی در اجرای قواعد سنتی صلاحیت با اتخاذ معیاری جدید و موافق با فضای جدید سایبر داشتند که در این خصوص رویه واحدی هم اتخاذ نشده بود. با تصویب قانون جرایم رایانه‌ای، این قانون مطالبی را در مواد ۳۰، ۲۹، ۲۸ و ۳۱ با تسری قلمروی حاکمیت کشور به سامانه‌های رایانه‌ای و مخابراتی یا حامل‌های داده موجود در قلمروی حاکمیت زمینی، دریایی و هوایی کشور و تارنماهای دارای دامنه مرتبه بالای کد کشور ایران، قاعده صلاحیت سرزمینی را به گونه‌ای دیگر نسبت به جرایم ارتکابی در فضای سایبر اعمال کرده است. در بند ج صلاحیت شخصی سنتی و در بند د، با قبول جرم هرزه نگاری اطفال با عنوان جرم موضوع صلاحیت جهانی، قاعده صلاحیت جهانی را برای رسیدگی به جرائم سایبری پیش‌بینی کرده است».

قانون تجارت الکترونیکی مصوب ۱۳۸۲ هم که در مورد محل انجام یک عمل تجاری در تجارت الکترونیکی در ماده ۲۹ قواعدی را بیان کرده است در فصل چهارم به بحث صلاحیت جزایی اشاره کرده و مقررات حاکم بر صلاحیت جزایی در خصوص جرایم تجارت الکترونیکی را به قانون احاله کرده هست، که در همین راستا با تصویب و تأیید قانون جرایم رایانه‌ای فوق‌الذکر قواعدی راجع به شیوهٔ اعمال صلاحیت در بخش دوم همین قانون پیش‌بینی شد.

در خصوص تعارض میان صلاحیت‌ها یا مسئله اعتبار امر مختومه به نظر می‌رسد یکی از مسائلی که کشورهای درگیر با جرایم سایبری باید مورد توجه قرار دهند تا با چالش مذکور مواجه نشوند، اتخاذ سیاست‌های کیفری متحدالشکل و هماهنگی در سراسر جهان است؛ چنانچه کشوری ملاحظه کند مجرم سایبری که به سیستم‌ها و داده‌های رایانه‌ای کشورش آسیب‌های بسیاری وارد کرده در کشور دیگر به طور عادلانه محاکمه و مجازات می‌شود، بعید است تصمیم بگیرد با تحمل مشقات بسیار خود را درگیر محاکمه مجدد مجرم مورد نظر نماید. در این صورت می‌توان انتظار داشت تعارض مثبت در صلاحیت و به تبع آن قاعده اعتبار امر مختومه کمتر مطرح شود.

در خصوص تعارض صلاحیت در حوزه‌های قضایی داخلی می‌توان با تأسیس یک هیئت یا شعبه مرکزی در پایتخت، در خصوص رسیدگی به جرائم سایبری در نقاط مختلف کشور، به همه مراجع قضایی داخلی تکلیف کرد تا در صورت دریافت هرگونه گزارش از مقام صلاحیت‌دار یا دریافت شکوائیه و یا مشاهده هر گونه جرمی از جرایم فضای سایبر بلافاصله شعبه مرکزی را در جریان امر قرار داده و منتظر تعیین تکلیف از آن باشند. همچنین شعبه پایتخت می‌تواند در برخی نقاط کشور شعبات فرعی داشته باشد. همان‌طور که ماده ۳۰ قانون جرایم رایانه‌ای در این زمینه مقرر می‌دارد: «قوه قضاییه موظف است به تناسب ضرورت شعبه یا شعبی از دادسراها، دادگاه‌های عمومی و انقلاب، نظامی و تجدید نظر را برای رسیدگی به جرایم رایانه‌ای اختصاص دهد». دادگاه فوق می‌تواند به صلاحدید خود و براساس قواعد پیش‌بینی‌شده در ماده ۲۹ قانون جرایم رایانه‌ای یا دیگر قواعد، نظیر ارتباط منطقی با یک حوزه، پرونده‌ها را به آن‌ها ارجاع یا احاله کند.

براساس ماده اخیر «چنانچه جرم رایانه‌ای در محلی کشف یا گزارش شود، ولی محل وقوع آن معلوم نباشد، دادسرای محل کشف مکلف است تحقیقات مقدماتی را انجام دهد. چنانچه محل وقوع جرم مشخص نشود، دادسرا پس از اتمام تحقیقات مبادرت به صدور قرار می‌کند و دادگاه مربوط نیز رأی مقتضی را صادر خواهد کرد». لذا دیده می‌شود که قانون مجازات جرایم رایانه‌ای ایران با در نظر گرفتن چالش‌های فضای سایبر و مشکل بودن تعیین محل ارتکاب جرم سایبری، محل گزارش جرم و

یا محل کشف جرم را، در جایی که محل وقوع قابل تأیید نباشد، جایگزین ضابطهٔ محل وقوع جرم نموده و همان مراجع را صالح به رسیدگی دانسته است. البته بهتر بود قانون‌گذار در این زمینه ضابطه‌ای را -از قبیل محل بارگذاری یا محل استقرار مرتکب و یا محل حصول نتیجه زیان‌بار و... تعیین می‌کرده است.

۳- سیاست جنایی اجرایی:

این قسم از سیاست جنایی به سیاست اطلاق می‌گردد که از سوی دولت یا قوه مجریه در راستای بسترسازی مناسب جهت اجرای اصول و استراتژی‌های سیاست جنایی تقنینی اتخاذ می‌گردد. در عرصه سیاست جنایی اجرایی که بخش وسیعی از آن مرتبط با مرحله کشف جرایم، تعقیب متهمین و اجرای احکام است، مداخله نهادهایی چون پلیس، سازمان زندان‌ها و... تحت عنوان ضابطان دستگاه قضایی مطرح می‌باشند. به‌عبارت‌دیگر، سیاست جنایی اجرایی سیاستی است که قوه مجریه و اعضای آن از جملهٔ پلیس برای سیاست جنایی تقنینی و به منظور پیشگیری از وقوع جرم یا گسترش آن در جامعه اتخاذ می‌کنند.

در عرصه سیاست جنایی اجرایی، از یک سو و نقش و عملکرد مجریان و ضابطان دادگستری در مرحله اولیه رویارویی با پدیدهٔ جنایی یعنی کشف جرایم و تعقیب متهمین مطرح است و از سوی دیگر، عملکرد این نهادها و به طور کلی عملکرد و نقش قوه مجریه در مرحله پاسخ‌گویی به جرایم و انحرافات، یعنی سطوح اجرای احکام و تصمیمات و بسترسازی در راستای پیشگیری از آن‌ها رخ می‌نمایاند. بر این اساس، سیاست جنایی اجرایی، قلمرو و اقتدار قوه مجریه را در امور کلان جنایی انعکاس می‌بخشد که همسو با دستگاه قضا از جمله ارکان اصلی و حقیقی تقویت مدیریت و انتظام اجتماع در مواجهه با پدیده کنایی می‌باشد. قوای اجرایی که اصولاً در جوامع مختلف نقش عمده‌ای در حوزه حفظ نظم و امنیت اجتماعی دارند، نمی‌توانند در مراحل مختلف سیاست‌گذاری‌های عمومی نظام از جمله سیاست جنایی، حضور و مدخلیتی نداشته باشند، چرا که شرط بنیادین و اولیه امکان برقراری و طنین مؤلفه‌هایی چون امنیت، اصول و بسترسازی علمی و تحریف حد و مرز و حریم قانونی برای مداخله این قوا در مراحل اجرایی سیاست‌های مذکور می‌باشد. و لذا مسلم می‌گردد که به زعم وجود و استقلال راهبردی سیاست جنایی اجرایی، کماکان قلمرویی اقتداری اولیه مقننه که نقش اصلی را در تألیف وظیفه و مسئولیت برای سایر اجزای نظام از جمله قوای اجرایی بر عهده دارد، رکن اساسی و گرانیگاه سیاست‌گذاری جنایی است.

۵. نتیجتاً این که سیاست جنایی اجرایی، تداعی گر نقش قوای اجرایی در اجرا و پیگیری استراتژی‌ها و راهبردهای کلان سیاست جنایی در پرتاب تبعیت از نظام نامه‌ها، موازین و نقشه نگاری‌های مقنن به عنوان طراح اصلی این سیاست می‌باشد و لذا در ارتباط با سطوح تعامل کنشگران و فعالان اصلی این قسم از سیاست جنایی و سایر اقسام آن، هرگز نمی‌توان از استقلال عملکردی مطلق به معنای استقلال در تدبیر مدل دخالت در عرصه سیاست جنایی حاکم بر جامعه و رژیم حقوقی، یاد نمود(کونانی و همکاران، ۱۳۹۱).

۳-۱. بررسی و تحلیل سیاست جنایی اجرایی در ایران و راهکارهای پیشرو

مطالعات جهانی نشان می‌دهد، درصورتی‌که بتوان رفتار مجرمان را در فضای سایبر شناسایی کرد، امکان پیشگیری از جرم و برخورد مناسب با مجرم باکیفیت دقیق‌تری انجام می‌شود. از آنجایی که، فضای سایبر شرایط را به وجود آورده است که حتی امکان شناسایی مجرمانی که جرم آن‌ها در فضای واقعی اتفاق افتاده از مسیر فضای مجازی قابل پیگیری است، رفتارشناسی مجرمان دنیای واقعی می‌تواند در فضای سایبر مورد توجه باشد. با این وجود، فضای سایبر به اندازه‌ای گسترده و پیچیده است که مجرمان می‌توانند در مکان‌هایی غیر از جاهایی که آثار و نتایج اعمال آن‌ها ظاهر می‌شود مرتکب جرم شده و به راحتی و با کمترین هزینه و اضطراب، بیشترین خسارات و صدمات را به بار آورده و درعین‌حال ناشناخته باقی بمانند. بنابراین، ارائه راهکارهای مناسب و توصیه‌های مؤثر برای پلیس و یا نهادهایی که به دنبال شناخت و درک رفتار مجرمان در فضای سایبر می‌باشند زمانی امکان پذیر است که آموزش و ابزار لازم را برای شناخت مجرمان در فضای سایبر را داشته باشند. در سطح ملی باید نهادهای مسئول از یک استراتژی ارتباطات مؤثر در مراحل مختلف بررسی رفتارشناسی مجرمان فضای سایبر استفاده‌کننده تا هماهنگی لازم وجود داشته باشد. ایجاد یک مرکز رفتارشناسی مجرمان ملی در فضای سایبر می‌تواند

هماهنگی لازم را بوجود آورده و انتقال تجربیات را در مراحل کشف جرم، پیشگیری از وقوع جرم مجرمان و ارتقای آموزش منابع انسانی را به دنبال داشته باشد. آموزش عمومی مردم در استفاده مناسب از شبکه‌های اجتماعی، استفاده از توانمندی‌های رسانه شهروندی و رسانه‌های جدید نیز می‌تواند در رفتارشناسی مجرمان نقش اساسی داشته باشد. لذا باید به شبکه‌های اجتماعی توجه بیشتری داشت و با فرصت دادن به کاربران، افراد مجرم و غیر مجرم را شناسایی کرد تا در مواقع اضطراری به راحتی مجرمان در دسترس باشند. نهایتاً باید پهنای باند دسترسی به شبکه‌های محلی و بین‌الملل را به اندازه‌ای تأمین شود که پلیس و عواملی که به دنبال مجرمان در فضای سایبر می‌باشند به راحتی بتوانند با رفتارشناسی افراد بزهکار، وظایف قانونی خود را انجام دهند تا اینترنت و فضای سایبر محلی امن برای اعمال جرم مجرمان نباشد و شهروندان بتوانند با رغبت بیشتر از کاربردهای فناوری اطلاعات در فضای سایبر بهره‌مند شوند(بهره‌مند و همکاران، ۱۳۹۳).

۴- سیاست جنایی مشارکتی:

مراد از سیاست جنایی مشارکتی، نوعی از سیاست جنایی است که به مداخله و مشارکت جامعه مدنی در کنار نهادهای دولتی و رسمی مرتبط با پاسخ‌دهی به پدیدهٔ جنایی و پیشگیری از آن اشاره داشت و بر مداخله توأمان این دو نهاد تأکید وافر می‌نماید. بنابراین، مداخله و مشارکت جامعه مدنی در سیاست جنایی، گرانیگاه و نقطه کانونی سیاست جنایی مشارکتی تفسیر و تعبیر می‌گردد. بدون شک، مشارکت عامه مردم در سیاست جنایی می‌تواند به ارتقای سطح کیفی اصول و استراتژی‌های اتخاذی در پهنای آن منتهی شود. مشارکت عامه مردم در سیاست جنایی می‌تواند به ارتقای سطح کیفی اصول و استراتژی‌های اتخاذی در پهنای آن منتهی شود(نژادسلطانی، ۱۳۸۹).

۴-۱. بررسی و تحلیل سیاست جنایی مشارکتی در ایران و راهکارهای پیشرو

آنچه مسلم است اینکه رفتارهای غیر اخلاقی و جرایم و انحراف‌ها آن‌قدر هم‌پوشانی و فصل مشترک با یکدیگر دارند که بتوان میان آن‌ها تعامل سازنده‌ای برقرار کرد و چون تاکنون در کشورمان هیچ گونه اقدامی انجام نشده، ایجاد هماهنگی میان این دو حوزه و پیشبرد هم‌زمان آن‌ها می‌تواند آثار راهبردهایی که می‌توانند برای حل این مسئله چند مجهولی، پیامدهای مثبت بسیاری به همراه داشته باشد نهادینه سازی اخلاق سایبری با کمک راهکارهای جرم شناخته پیشگیرانه اجتماعی سایبری، مثمرثمر واقع شوند: عبارتند از:

الف-پیش از هر چیز، باید با توجه به شرایط اجتماعی و فرهنگی جامعه، شناخت صحیح و واقع‌گرایانه‌ای از کاربران فضای سایبر در حوزه‌های مختلف حاصل گردد؛

ب- سپس باید هنجارهای اخلاقی مربوط، که بی‌تردید هدف اصلی آن‌ها بهره‌برداری مشروع و سودمند از این فضا و دوری جستن از هرگونه جرم، انحراف و در نهایت رفتارهای غیر اخلاقی است، وضع گردند؛

ج- در گام بعدی، با عنایت به راهکارهایی که به تفکیک در دو حوزه جامعه مدار و رشد مدار تبیین گردیدند، باید تلاش شود این هنجارها به نحوی مطلوب و مؤثر در میان اجتماع خاص مخاطبان حوزه‌های مختلف تبیین و تشریح گردند؛

د-در نهایت اینکه، به هنگام تدوین این هنجارها نباید از راهکارهای پیشگیرانه وضعی و همچنین ضمانت اجراهای کیفری و غیر کیفری غافل ماند. زیرا در واقع نه تنها قرارست و باید این تدابیر در آن هنجارها منعکس گردند و به اجرای صحیح آن‌ها کمک کنند که اجرای مؤثر، متناسب و بازدارنده آن‌ها نیز وابسته به انعکاس صحیح آن‌ها در تدابیر پیشگیرانه اجتماعی است.

۴. نتیجه گیری

در پایان، تنها به این نکته تأکید می‌گردد که چه خوبست در کنار حرکت پرشتاب و تا حدودی لگام گسیخته سایبری کردن امور خرد و کلان جامعه، به‌ویژه دسترس پذیر کردن هرچه بیشتر این فضا برای قشر جوان و نوجوان در محیط‌های مختلف که نمونه بارز آن را در عزم دولت برای متصل کردن تمامی واحدهای آموزشی عالی به شبکه جهانی اینترنت شاهد هستیم، قدری

به فکر سامان‌دهی آن بر اساس الگوهای خردگرایانه و واقع‌گرایانه باشیم. که پیدا است، پیش از این نسل جدیدبا چالش‌ها و مشکلات سایبری دست به گریبان نباشند.

منابع:

۱. باستانی، برومند(۱۳۸۳)، جرائم کامپیوتری و اینترنتی، انتشارات بهنامی، تهران.

۲. بهره‌مند، حمید، کوره پز، حسین، سلیمی، احسان(۱۳۹۳)، راهبرد های وضعی پیشگیری از جرایم سایبری، آموزه‌های حقوق کیفری شماره ۷.

۳. کونانی، سلمان، انصاری، جمال، مندنی، اسلام(۱۳۹۱)، سیاست جنایی، انتشارات مجد.

۴. نژادسلطانی، محمد ابراهیم(۱۳۸۹)، ترجمه مقدمه ای بر جنگ سایبری و تروریسم سایبر، ناشر بوستان حمید.