اصول جرم‌انگاری در فضای سایبر
(با رویکردی انتقادی به قانون جرائم رایانه‌ای)

احمد حاجی‌ده‌آبادی،* احسان سلیمی**

تاریخ دریافت ۱۳۹۲/۶/۱	تاریخ پذیرش ۱۳۹۳/۸/۲۱

جرم‌انگاری بی‌ضابطه و گسترده در قوانین کیفری علاوه‌بر اینکه موجبات بروز آثار و تبعات سوء تورم کیفری را فراهم می‌کند با اهداف حقوق جزا نیز مغایرت دارد. وجود ضمانت اجراهایی خاص در حقوق جزا همچون سلب حیات، محدود کردن آزادی، تنبیه بدنی و ... ضرورت جرم‌انگاری مضیّق و برمبنای اصول را روشن می‌سازد. جرائم سایبری به اقتضای ویژگی‌هایی از قبیل سهولت ارتکاب جرم، کثرت بزه‌دیدگان و کم‌سن بودن اغلب مجرمان آن، در کنار اصول عمومی، اصول جرم‌انگاری خاصی را می‌طلبد. یافته‌های این پژوهش گویای این مطلب است که جرم‌انگاری در جرائم سایبری هنگامی صحیح و قابل پذیرش است که برمبنای اصولی چون «ضرورت» و «مشروعیت» انجام شود و ضمن احترام به حریم خصوصی و حقوق شهروندی، تناسب دقیقی بین رفتار مجرمانه و نوع و مقدار مجازات داشته باشد و درعین‌حال به ابزار و وسایل موجود دستگاه عدالت کیفری و اقشار آسیب‌پذیر توجه داشته باشد. همچنین توجه جدی به راهبردها و رویکردهای بین‌المللی، توجه ویژه به اقشار آسیب‌پذیر، اتخاذ راهبردهای علمی و فنی دقیق و دانش بین‌رشته‌ای و شناسایی مسئولیت کیفری اشخاص حقوقی برای مقابله همه‌جانبه با جرم ضروری است. در نهایت، قانونگذار می‌بایست تا حد امکان بستر یک سیاست جنایی مشارکتی و فراگیر را برای مقابله با جرم فراهم نماید.

کلیدواژه‌ها: جرائم سایبری؛ اصول جرم‌انگاری؛ ویژگی‌های جرائم رایانه‌ای؛ معیارهای جرم‌انگاری

---

* عضو هیئت علمی گروه حقوق جزا و جرم‌شناسی، دانشکده حقوق، پردیس فارابی دانشگاه تهران؛
Email: adehabadi@ut.ac.ir

** کارشناسی ارشد حقوق جزا و جرم‌شناسی، دانشکده حقوق، پردیس فارابی دانشگاه تهران (نویسنده مسئول)؛
Email: ehsansalimi1367@yahoo.com

مقدمه

پیشرفت شتابان فناوری اطلاعات در سال‌های اخیر دستاوردها و دگرگونی‌های بی‌شماری را در ابعاد گوناگون زندگی بشر به‌وجود آورده است. بیشتر فعالیت‌های روزمره زندگی به نوعی وابسته به رایانه‌هاست و روزبه‌روز بر این وابستگی افزوده می‌شود. این فناوری بزرگ که در ابتدا برای آسایش و رفاه هرچه بیشتر انسان‌ها مورد بهره‌برداری قرار می‌گرفت به‌تدریج به ابزاری برای مجرمان، جهت نیل به آمال مجرمانه نیز تبدیل شد. امروزه فعالیت بزهکارانه عمومی، دیگر منحصر به دنیای حقیقی نیست. به‌موازات گسترش فعالیت‌ها و ارتباطات در فضای سایبر،[1] بخشی از بزهکاران نیز فعالیت مجرمانه خود را به فضای سایبر منتقل کرده‌اند یا از رهگذر چنین فضایی، مرتکب جرم یا جرائمی می‌شوند (پیکا، ۱۳۹۰: ۱۱). این فضای جدید به‌گونه‌ای حقوق جزای سنتی را دستخوش تحولات بنیادی کرده که تعریف از جرائم در محیط‌های مجازی انطباق چندانی با تعاریف کلاسیک نداشته و در بسیاری موارد متفاوت است (حسن‌بیگی، ۱۳۸۴: ۳۵). همچنین جرائم سایبری به اقتضای ویژگی‌های منحصربه‌فرد خود همچون سهولت ارتکاب جرم، فرامرزی بودن جرم، کم‌سن بودن مجرمان، گستردگی خسارت و کثرت بزه‌دیدگان، ضرورت دقت در فرایند جرم‌انگاری را افزایش داده‌اند. به بیانی دیگر می‌توان ادعا کرد جرم‌انگاری از یک فعل یا ترک فعل در فضای سایبر، اقدامی خطیر است که توجه به ویژگی‌ها و عوامل مختلفی را می‌طلبد، در غیر این صورت نه‌تنها اهداف جرم‌انگاری محقق نمی‌شود، بلکه اقتدار حقوق کیفری نیز دچار صدمات جبران‌ناپذیر خواهد شد.

جرم‌انگاری کارآمد و مؤثر یکی از دغدغه‌های جدی نظام قانونگذاری در هر کشوری است. درصورتی‌که جرم‌انگاری به‌صورت غیرکارشناسی و بدون رعایت اصول و قواعد صورت بگیرد در عمل شاهد خواهیم بود که یا قوانین ناعادلانه فرصت‌ها را برای افراد جامعه محدود می‌کنند و یا قوانین با وجود آنکه پشتوانه کیفری دارند اعتباری نزد افراد ملت ندارند و توسط افراد آنها اجرا نمی‌شوند و بدین‌ترتیب علاوه‌بر اینکه بر شمار قوانین متروک افزوده می‌شود، اقتدار و صلابت حقوق کیفری نیز درهم می‌شکند. اصول جرم‌انگاری برای جرائم سایبری را می‌توان به دو دسته عام و خاص تقسیم نمود. اصولِ عام جرم‌انگاری که

---

۱. فرهنگستان زبان و ادب فارسی واژه «رایا سپهر» را به‌جای «فضای سایبر» (Cyber Space) در نظر گرفته است.

بیشتر بیانگر قواعد بنیادین جرم‌انگاری مانند اصل مشروعیت، اصل ضرورت، رعایت حریم خصوصی، تناسب جرم و مجازات و توجه کامل به امکانات موجودِ دستگاه عدالت کیفری است در مورد همه مواردی که نیاز به جرم شمردن یک عمل هست باید رعایت شوند. در کنار این اصول به جهت ویژگی‌های منحصربه‌فرد و بی‌نظیر فضای سایبر باید از اصولی سخن گفت که خاص جرائم سایبری است. در ادامه در دو بخش، ابتدا به برشمردن «اصول عام» جرم‌انگاری درخصوص جرائم سایبری و سپس به بیان «اصول خاص» جرم‌انگاری در جرائم سایبری پرداخته خواهد شد.

۱. مبانی نظری

قانون اساسی جمهوری اسلامی ایران در فصل سوم به تفصیل حقوق و آزادی‌های ملت را برشمرده است که به‌خوبی نشانگر موضع‌گیری قاطع نظام جمهوری اسلامی در برابر هرگونه خودکامگی قانونگذار در امر جرم‌انگاری است. جرم‌انگاری نیز به حکم بداهت عقل و به‌عنوان شرط لازم برای مشروعیت جرم‌انگاری و تعیین مجازات، تنها از طریق قانون موضوعه امکان‌پذیر می‌باشد. اصل (۳۶) قانون اساسی بر این مهم تأکید ورزیده است. مطابق این اصل «حکم به مجازات و اجرای آن باید تنها از طریق دادگاه صالحه و به‌موجب قانون باشد». سؤال بنیادی در مورد فرایند جرم‌انگاری این است که آیا قانونگذاران مجازند با اتکا به قدرت و سلطه رسمی بر افراد جامعه، به‌طور مطلق یک رفتار را جرم محسوب کنند و برای مرتکب رفتار، مجازات در نظر گیرند؟ بی‌شک اگر این فرض پذیرفته شود نفس موقعیت و مقام قانونگذار به‌عنوان عامل مشروعیت‌بخش در امر جرم‌انگاری کفایت خواهد کرد. برخی دیدگاه‌های پوزیتیویستی چنین شائبه‌ای را ایجاد می‌کنند، اما مشروعیت قانونگذار با مشروعیت جرم‌انگاری توسط قانونگذار دو مقوله مستقل است. شکی نیست که قانونگذار باید از طریق قانونی به قدرت رسیده باشد، بااین‌حال رسمیت قانونگذار برای مشروعیت‌بخشی به جرم‌انگاری تنها شرطی لازم است ولی شرطی کافی نیست. اصل (۳۷) قانون اساسی مقرر می‌دارد: «اصل، برائت است و هیچ‌کس از نظر قانون مجرم شناخته نمی‌شود مگر اینکه جرم او در دادگاه صالحه ثابت گردد». بنابراین در مقام جمع بین حقوق افراد و جامعه ابتدا باید در راستای اصول آزادی، اباحه و برائت، از جرم‌انگاری خودسرانه امتناع ورزید و در آخرین

مرحله و در راستای صیانت از نظم و هنجارهای جامعه در برابر صدمه‌زنندگانِ قابل سرزنش، از شیوه قهرآمیز جرم‌انگاری و مجازات سود جست.

درواقع جرم‌انگاری اساساً امری خلاف اصل (خلاف اصول اباحه و برائت) بوده و تنها در موارد خاص یعنی در مواردی که یک رفتار به‌قدر کافی زیانبار و سرزنش‌آمیز باشد مشروعیت خواهد داشت. این امر قانونگذاران را از جرم‌انگاری گسترده رفتارها منع می‌کند و آنها را ملزم می‌سازد تا جرم‌انگاری را به مواردی که یک رفتار، صدمه و سرزنشی شدید در پی دارد محدود سازند. بنابراین پیش‌شرط جرم‌انگاری، رعایت اصل صدمه و سرزنش است. اگر رفتاری که قانونگذار آن را جرم شناخته است به‌قدر کافی صدمه و سرزنش در پی نداشته باشد حقوق و آزادی‌های افراد جامعه مخدوش خواهد شد و مردم عملاً از دستور قانونگذار مبنی‌بر عدم ارتکاب چنین رفتاری سرپیچی خواهند کرد. برای مثال جرم‌انگاری قتل عمدی، کلاهبرداری، سرقت و خیانت در امانت قابل توجیه‌اند و از مبنایی مشروعیت‌بخش بهره می‌برند. جرائم مذکور با هر دو اصل صدمه و سرزنش مطابقت دارند زیرا ازیک‌سو به امنیت، جان یا مال افراد صدمه وارد می‌سازند و ازسوی‌دیگر تقبیح و سرزنش اخلاقی و اجتماعی را برمی‌انگیزند.

هرچند مشروعیت جرم‌انگاری منوط به سرزنش‌آمیز بودن رفتار و زیانبار بودن آن است، اما وزن هریک از اصول سرزنش و صدمه نزد حقوقدانان و مفسرین قانون یکسان نیست. قطع نظر از ترجیح یکی از این اصول در فرایند جرم‌انگاری، باید به این مطلب یقین داشت که جرم‌انگاری و مجازات همچون هر نهاد دیگری تنها در جای خود می‌تواند رسالت خویش را ایفا کند و گسترده کردن حدود و ثغور آن موجب پیامدهای نامطلوب دیگری می‌شود. استفاده ابزاری از حقوق کیفری برای ارزش‌گذاری یک مهم در جامعه، نه‌تنها بی‌اثر است بلکه موجب پایمال شدن ارزش مورد نظر و لوث شدن ابزارهای حقوق کیفری و درمجموع نقض غرض قانونگذار می‌شود.

۲. اصول عام جرم‌انگاری در فضای سایبر

۲-۱. اصل مشروعیت جرم‌انگاری

مطابق مبانی فقهی چون مجازات نوعی تصرف در مال، جان، عضو، آزادی و حیثیت دیگری می‌باشد، پس نوعی ولایت بر دیگری است و اصل اقتضای آن را دارد که کسی بر دیگری

ولایت ندارد مگر اینکه دلیل قطعی بر آن وجود داشته باشد. این امر قانونگذاران را از جرم‌انگاری دلبخواه و گسترده رفتارها منع و آنان را ملزم می‌کند تا جرم‌انگاری را به مواردی محدود سازند که یک رفتار، صدمه و سرزنشی شدید در پی دارد. هر جرم‌انگاری نوعی مداخله و ایجاد محدودیت فراروی حقوق و آزادی‌های افراد است. لذا در حقوق کیفریِ کرامت‌محور که پاسداری از حرمت و کرامت افراد، دل‌مشغولی سیاستگذاران کیفری است، در هر مورد از جرم‌انگاری باید چنان مصلحتی در حمایت از حقوق و آزادی‌های افراد وجود داشته باشد که بر مفسده ناشی از محدود کردن این حقوق و آزادی‌ها چیرگی داشته باشد (شمس ناتری، ابوالمعالی و علیزاده، ۱۳۹۰: ۲۷۲). به‌عبارت‌دیگر جرم‌انگاری درمجموع باید مانع افزایش خودمختاری و [باعث افزایش] حرمت و حیثیت شهروندان گردد (نوبهار، ۱۳۸۷: ۲۲۳).

در محیط سایبر به اقتضای ویژگی‌های خاص و از جمله سهولت ارتکاب جرم و فرمانرانی آزادی در این فضا، امکان رخ دادن پدیده نامطلوب مجرمانه بیشتر می‌شود چرا که یکی از ویژگی‌های به‌واقع متمایز و درعین‌حال ارزشمند فناوری اطلاعات و ارتباطات الکترونیکی نسبت به دیگر فناوری‌ها، مانند فناوری هسته‌ای، زیستی و ریزفناوری، حداقل در برهه کنونی این است که اکثر افراد با حداقل مهارت فنی می‌توانند از قابلیت‌های متنوع آن استفاده کنند (جلالی‌فراهانی، ۱۳۸۹: ۱۵). به‌تبع این امر ارتکاب جرم در محیط سایبر نیز بسیار راحت است. هرکس با داشتن یک رایانه که امکان اتصال به اینترنت را دارد و با اندک آشنایی به سواد رایانه‌ای می‌تواند مجرمی بالقوه باشد (فضلی، ۱۳۸۹: ۷۲). درواقع امکان ارتکاب جرم برای شهروندان اینترنت (نتیزن)[1] بسیار بیشتر از شهروندان دنیای واقعی است. لکن زمانی باید به جرم‌انگاری از این پدیده نامطلوب پرداخته شود که آن فعل یا ترک فعل صدمه و سرزنش قابل توجهی را در پی داشته باشد. درواقع «شناسایی جامع مخاطرات محتمل از ناحیه جرائم سایبری در ابعاد مختلف زندگی اجتماعی، پیش‌شرط قانونگذاری خوب و اجرای موفق قانون در این زمینه است» (جوان‌جعفری، ۱۳۸۵: ۳۱). برخی جرائم موجود در

---

۱. اصطلاح نتیزن (Netizen) در برابر سیتیزن (Citizen)، توسط مایکل هابن وضع شده است. یک نتیزن از لحاظ لغوی، یک شهروند اینترنت است. اینها کسانی هستند که از آزادی استفاده از شبکه و تمام چیزهای دیگری که به آن مربوط است مثل گروه‌های خبری، نامه‌های الکترونیکی و مانند اینها بهره می‌برند و می‌دانند که این امر، مرحله‌ای جدید از توانایی ارتباط را تماماً فراهم می‌کند (Jaishankar, 2011).

قانون جرائم رایانه‌ای فاقد قباحت ذاتی هستند و به این جهت وقوع آنها سرزنشی را در پی نخواهد داشت. برای مثال ماده (۲۴) قانون جرائم رایانه‌ای درخصوص استفاده بدون مجوز از پهنای باند بین‌المللی، بدین صورت اقدام به جرم‌انگاری نموده است: «هرکس بدون مجوز قانونی از پهنای باند بین‌المللی برای برقراری ارتباطات مخابراتی مبتنی‌بر پروتکل اینترنتی از خارج ایران به داخل یا برعکس استفاده کند، به حبس از یک تا سه سال یا جزای نقدی از یکصد میلیون تا یک میلیارد ریال یا هر دو مجازات محکوم خواهد شد». این درحالی است که در اکثر کشورهای پیشرفته در عرصه داده‌پردازی، استفاده از فضای سایبر با پهنای باند پرسرعت بین‌المللی و بهره‌گیری از این‌گونه ارتباطات، به‌عنوان یک حق شهروندی پذیرفته شده است (الهی‌منش و سدره‌نشین، ۱۳۹۱: ۱۳۹). بنابراین پیش‌شرط جرم‌انگاری، رعایت «اصل صدمه»[۱] و «اصل سرزنش»[۲] است. اگر رفتاری که قانونگذار آن را جرم شناخته است به‌قدر کافی صدمه و سرزنش در پی نداشته باشد حقوق و آزادی‌های افراد جامعه مخدوش خواهد شد و مردم عملاً از دستور قانونگذار مبنی‌بر عدم ارتکاب چنین رفتاری سرپیچی خواهند کرد؛ کمااینکه در مورد استفاده از فیلترشکن‌ها این سرپیچی نمودار شده است.

۲-۲. اصل ضرورت

مهمترین بایسته درزمینه جرم‌انگاری از یک عمل، ضرورت و ناگزیر بودن جرم شمردن آن عمل است لذا برای جرم‌انگاری از یک عمل پس از آنکه ثابت شد «که رفتار براساس یک سلسله اصول نظری راجع به جرم‌انگاری (مثلاً اصل منع صدمه) در حیطه صلاحیت قضایی جامعه یا اقتدار دولتی قرار دارد؛ به‌عبارت‌دیگر باید اثبات شود که دولت به مداخله در حوزه حقوق و آزادی‌های شهروندان از طریق ممنوعیت یا ایجاد محدودیت کیفری مجاز می‌باشد. باید دید که آیا راه‌های موفقیت‌آمیز دیگری وجود دارد که وقوع عمل را بدون به‌کارگیری ماشین نظام عدالت کیفری تقلیل دهد، یا نه؟» (زینالی، ۱۳۸۷: ۳۰۷-۳۰۶). به بیانی دیگر جرم

---

۱. مفهوم اصل صدمه: رفتاری را می‌توان به حوزه جرم راه داد که با نقض یک تکلیف و الزام قانونی سبب ایراد لطمه و صدمه شود.

۲. مفهوم اصل سرزنش: رفتاری را می‌توان به حوزه جرم راه داد که افراد جامعه در قضاوتی اخلاقی و اجتماعی مرتکب رفتار را تقبیح و سرزنش کنند.

شمردن یک فعل یا ترک فعل باید آخرین حربه برای نیل به خواسته مقنن باشد. لذا باید گفت استفاده از ضمانت اجراهای کیفری برای حمایت از ارزش‌ها و ایدئال‌ها آنگاه مجاز است که نتوان از سایر ضمانت اجراها بهره جست. اتکای اصل ضرورت هم بر ادله حقوقی و هم بر مبانی فقهی است تا آنجا که می‌توان ادعا کرد «مقررات جزایی اسلام، کیفر را برای نفس مجازات مقرر نداشته بلکه آن را به‌عنوان آخرین اقدام در جهت تأدیب و تربیت افراد، اصلاح جامعه و از بین بردن تباهی‌ها مدنظر قرار داده است» (گلدوزیان، ۱۳۸۶: ۲۷). از منظر حقوقی قطع نظر از نظریه‌هایی چون «تسامح صفر» و «پدرسالاری قانونی» مطابق با اغلب نظریه‌هایی همچون «پالایش»،[1] «اصل منع صدمه»، «اصل ضرر» و ...، که درخصوص اصول جرم‌انگاری ابراز شده، می‌توان گفت در هر جامعه‌ای که برای آزادی‌اش ارزش قائل است باید از حقوق جزا تنها به‌عنوان آخرین راه‌حل برای کنترل اجتماعی استمداد شود. استفاده ابزاری از حقوق کیفری و ضمانت اجرای مجازات، علاوه‌بر آنکه اقتدار حقوق کیفری را درهم می‌شکند، تأثیر چندانی هم در القای ارزش‌های مدنظر قانونگذار به جامعه ندارد.

اصل ضرورت در جرم‌انگاری جرائم سایبری جایگاه ویژه‌ای دارد و با اعمال این اصل به یک جرم‌انگاری حداقلی دست خواهیم یافت. چه آنکه به اقتضای شرایط خاص حاکم بر فضای سایبر و امکانات ویژه آن، به‌راحتی می‌توان قبل از رسیدن کار به مرحله جرم‌انگاری، از وقوع بسیاری از جرائم پیشگیری کرد. درواقع امکان پیشگیری از جرم در عرصه سایبر اعم از پیشگیری اجتماعی یا وضعی بسیار مساعد است. پیشگیری اجتماعی و مقوله آموزش که در «رهنمود عملی پیشگیری از جرم سازمان ملل متحد»[2] هم بر آن تأکید شده، امر خطیری است که به چند شکل به پیشگیری از جرائم رایانه‌ای کمک می‌کند. توضیح بیشتر اینکه، می‌توان مدعی بود «با توجه به اینکه جرائم سایبری عمدتاً توسط نیروهای سازمان‌یافته و طراحی و نقشه قبلی و نیز توسط اشخاص رقیب یا اخراج شده از سازمان‌های مزبور صورت می‌گیرد» (رضوی، ۱۳۸۶: ۱۲۴) آموزش به اشخاص و شرکت‌هایی که احتمالاً در معرض

---

۱. جانتان شنشک نظریه سه فیلتر یا پالایش را چنین مطرح می‌کند: زمانی که درصدد جرم‌انگاری رفتاری هستیم باید آن رفتار را به‌طور متوالی و موفقیت‌آمیز از سه صافی یا فیلتر مجزا به اسم فیلتر اصول، فیلتر پیش‌فرض‌ها و فیلتر کارکردها عبور دهیم (Schonsheck, 1994).

2. The Guidelines for the Prevention of Crime (Council Resolution 2002/13 annex).

جرائم سایبری هستند برای مقابله با این جرائم بسیار سودمند است. علاوه‌بر این، آموزش‌های عمومی در رسانه‌های گروهی برای مقابله با ویروس‌ها[۱] و کرم‌های[۲] رایانه‌ای بسیار سودمند است زیرا درصورتی‌که مقابله عمومی با این ویروس‌های رایانه‌ای صورت گیرد هزینه‌های پیشگیری از این جرائم به‌مراتب کاهش می‌یابد. آموزش تدابیری که به‌وسیله آنها امنیت رایانه تأمین می‌شود نیز بسیار ضروری است و بدین وسیله از بسیاری جرائم، که در ارتباط با محرمانگی داده‌هاست، جلوگیری به‌عمل می‌آید. پیشگیری وضعی نیز در جرائم رایانه‌ای بسیار کارآمد است. به بیان ساده، پیشگیری وضعی در جرائم رایانه‌ای از جایگاه خاصی برخوردار است.[۳] یکی از دلایلی که موجب اهمیت این نوع پیشگیری برای جرائم رایانه‌ای شده، مقید به وسیله بودن این جرائم است. به‌عبارت‌دیگر بدون استفاده از رایانه و فضای سایبر ارتکاب این جرائم محال است در نتیجه با اعمال محدودیت‌های لازم بر وسیله، می‌توان ارتکاب این جرائم را به نحو چشمگیری کاهش داد. نصب دیوار آتشین[۴] و پالایه استفاده از پروکسی[۵] و استفاده از کوکی[۶] را می‌توان روش مناسبی از نوع پیشگیری وضعی برای جرائم سایبری دانست. ملاحظه می‌شود که در محیط سایبر شیوه‌های متفاوتی برای پرهیز از جرم‌انگاری وجود دارد و با به‌کارگیری تدابیر پیشگیری به‌راحتی می‌توان اهداف مورد نظر مقنن را تأمین کرد. تدابیری که به نسبت جرم‌انگاری کمترین لطمه را به منافع و آزادی‌های خصوصی وارد می‌آورد.

---

۱. Virus: یک برنامه مخرب رایانه‌ای که توسط خرابکاران (هکرها) برای اهداف مختلفی به‌کار می‌رود (الهی‌منش و سدره‌نشین، ۱۳۹۱: ۲۰۶).

۲. Worm: برنامه‌های نرم‌افزاری مخربی که به‌سرعت کپی‌هایی از خود را در شبکه و سامانه تکثیر نموده و در سطح آن پراکنده می‌شوند (همان: ۲۰۵).

۳. برای مطالعه بیشتر در این زمینه رک.: امیرحسین جلالی فراهانی (۱۳۸۴). «پیشگیری وضعی از جرائم سایبر در پرتو موازین حقوق بشر»، *مجله فقه و حقوق*، سال دوم.

4. Fire Wall

۵. Proxy: سرور پروکسی، تماس با اینترنت را به تمام رایانه‌هایی که به شبکه محلی متصل می‌باشند، تقسیم می‌کند. به‌طورکلی پروکسی سروری است که به‌عنوان یک واسطه بین کاربر و سرور عمل می‌کند. هنگامی که رایانه‌ای از طریق پروکسی به اینترنت وصل است و می‌خواهد به یک فایل دسترسی پیدا کند، ابتدا درخواستش را به یک سرور پروکسی می‌فرستد و سپس پروکسی به رایانه مقصد متصل شده، فایل درخواستی را دریافت می‌کند.

6. Cookie

۳-۲. احترام به حریم خصوصی و رعایت موازین حقوق بشری

جرم‌انگاری و مجازات اگرچه مطلوب یک جامعه نیستند، اما اهدافی آرمانی را دنبال می‌کنند که اصلاح بزهکار، حمایت از جامعه در مقابل بزه و تحقق عدالت‌بخشی از آنهاست. به‌دلیل والا بودن این اهداف باید جرم‌انگاری، مجازات و برخورد با بزهکار به‌گونه‌ای باشد که موجبات نقض غرض را فراهم نکند. از این حیث، رعایت حریم خصوصی، کرامت انسانی و موازین بین‌المللی حقوق بشر حائز اهمیت ویژه‌ای هستند. کنوانسیون جرائم سایبری در ماده (۱۵) خود با عنوان شروط و تضمین‌ها، دولت‌های عضو را موظف کرده به هنگام وضع قوانین و مقررات مطابق این کنوانسیون، حقوق و آزادی‌های فردی از جمله حریم خصوصی افراد را مطابق قوانین و مقررات بین‌المللی دقیقاً رعایت کنند. در بخشی از این ماده آمده است: «اعضا باید اطمینان دهند که حمایت شایسته‌ای از حقوق و آزادی‌های بشری به‌عمل می‌آورند که شامل حقوق برخاسته از تعهداتی است که آنها در کنوانسیون شورای اروپا راجع به حمایت از حقوق و آزادی‌های اساسی بشر (۱۹۵۰) و سایر اسناد لازم‌الاجرای حقوق بشری پذیرفته‌اند» (جلالی‌فراهانی، ۱۳۸۹: ۵۸). همچنین سازمان همکاری و توسعه اقتصادی اروپا[1] در سال ۱۹۸۰ یک رشته راهبردهای حریم خصوصی را به‌کار گرفت و آنها را ارائه کرد. این راهبردها به‌طور خاص طراحی شده بودند تا به مشکلات روزافزون جریان فرامرزی داده‌ها و حرکت اطلاعات شخصی از کشوری که داده‌های شخصی در آن به‌شدت تحت حفاظت قرار دارند به کشوری دیگر که داده‌های شخصی در آن از حفاظت کمتری برخوردارند بپردازند. راهبردهای این سازمان در مورد حفاظت از حریم خصوصی و جریان فرامرزی داده‌ها از هشت اصل تشکیل شده است[2] (سادوسکای و دیگران، ۱۳۸۴: ۱۷۶). با توجه به آنچه گفته شد ملاحظه می‌شود که چه در کنوانسیون جرائم سایبری و چه در راهبردهای سازمان همکاری و توسعه اقتصادی اروپا به‌نحو بارزی بر رعایت حریم خصوصی تأکید شده است لذا با توجه به اینکه «علاوه‌بر بخش اعظم ارتباطات الکترونیکی در فضای سایبر شامل صحبت در محیط‌های گپ و کنفرانس‌های شبکه‌ای و پست‌های الکترونیکی،

---

1. Organization for Economic Co-operation and Development

۲. این اصول عبارتند از: محدودیت جمع‌آوری، کیفیت داده‌ها، تعریف هدف، محدودیت استفاده، حفاظت‌های امنیتی، باز بودن، مشارکت فردی و پاسخ‌گویی.

شکل‌های دیگری از ارتباطات سایبری وجود دارد [که می‌توان هریک از این محیط‌ها را مصداق حریم خصوصی دانست] لازم است از هرگونه تفتیش، شنود و دستیابی غیرمجاز مصون باشند» (یزدانی‌زنور، ۱۳۸۸: ۱۴۶).

نکته قابل تأملی که نباید از آن غافل بود این است که علاوه‌بر اینکه قانونگذار خود ملزم به رعایت حریم خصوصی افراد و کاربران فضای سایبر می‌باشد باید نگهبان حریم خصوصی کاربران در مقابل دیگران اعم از سایر کاربران یا ارائه‌دهندگان خدمات دسترسی و ... هم باشد. بااین‌حال، متأسفانه در قانون جرائم رایانه‌ای تمهید مناسبی جهت جلوگیری از نقض حریم خصوصی کاربران و کاوش در فعالیت‌های صورت گرفته توسط آنان به‌وسیله ارائه‌دهندگان خدمات دسترسی اندیشیده نشده است. ماده (۳۲) قانون جرائم رایانه‌ای ارائه‌دهندگان دسترسی را ملزم به نگهداری داده‌ها نموده است، این ماده مقرر می‌دارد: «ارائه‌دهندگان خدمات دسترسی موظفند داده‌های ترافیکی را حداقل تا شش ماه پس از ایجاد و اطلاعات کاربران را حداقل تا شش ماه پس از خاتمه اشتراک نگهداری کنند». هرچند مصادیق نقض حریم خصوصی کاربران توسط ارائه‌دهندگان خدمات دسترسی به‌موجب مواد (۱ و ۲) قانون جرائم رایانه‌ای قابل مجازات است، اما بهتر بود قانونگذار تبصره‌ای را ذیل ماده (۳۲) مبنی‌بر مجازات شدیدتر تفتیش غیرقانونی حریم خصوصی کاربران توسط ارائه‌دهندگان خدمات دسترسی قرار می‌داد.

یکی از تضمین‌های رعایت حریم خصوصی، به رسمیت شناختن حق شکایت از اقدامات مأموران تفتیش و بازرسی است. خوشبختانه در ماده (۴۷) قانون جرائم رایانه‌ای به این امر توجه شده است. مطابق ماده (۴۷) «متضرر می‌تواند در مورد عملیات و اقدام‌های مأموران در توقیف داده‌ها و سیستم‌های رایانه‌ای و مخابراتی، اعتراض کتبی خود را همراه با دلایل ظرف ده روز به مرجع قضایی دستوردهنده تسلیم نماید». پیش‌بینی این ماده در قانون، رفتار مأموران را ضابطه‌مند و محدود به ثغور مقرر در قانون می‌نماید.

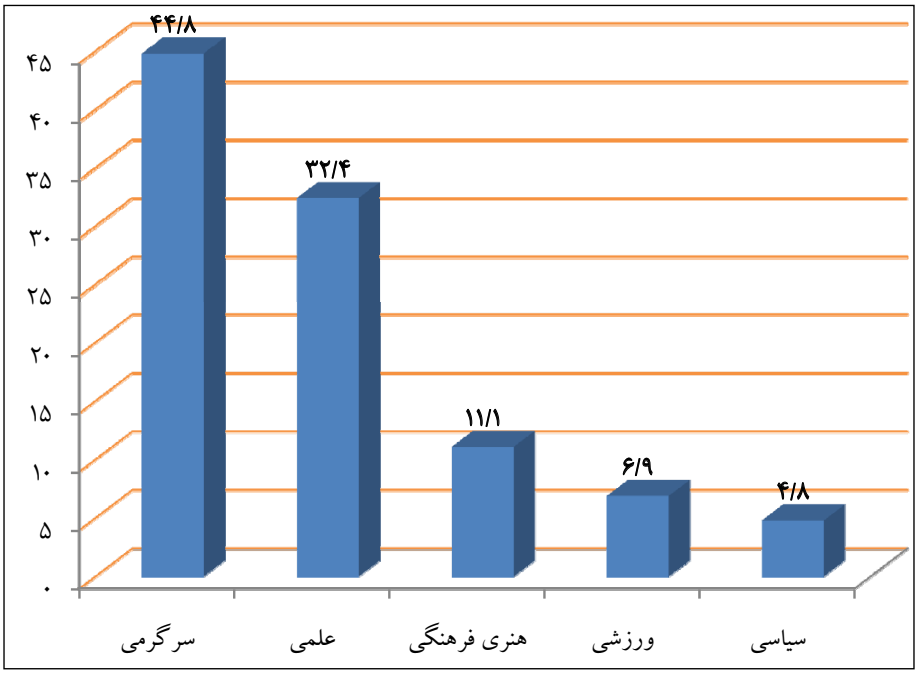
٤-۲. اصل تناسب جرم و مجازات

«تئوری تناسب جرم و مجازات تحت تأثیر آموزه‌های مکاتب مختلف کیفری و جرم‌شناختی از جمله مکتب کلاسیک، نئوکلاسیک، مکتب تحققی و مکتب دفاع اجتماعی همواره در

حال تحول و تکامل بوده است» (حبیب‌زاده و رحیمی‌نژاد، ۱۳۸۷: ۱۱۶). اهمیت این اصل باعث شده است که در سال‌های اخیر و با پیدایش نهادهای بین‌المللی «در سطح بین‌المللی و منطقه‌ای ماده (۵) اعلامیه جهانی حقوق بشر (۱۹۴۸)، ماده (۷) کنوانسیون بین‌المللی حقوق مدنی و سیاسی (۱۹۶۶)، مواد (۲ و ۴) کنوانسیون بین‌المللی منع شکنجه و رفتارها و مجازات‌های ظالمانه غیرانسانی و وحشیانه (۱۹۸۴)، بند «۲» ماده (۵) کنوانسیون آمریکایی حقوق بشر (۱۹۶۹)، ماده (۳) کنوانسیون اروپایی حقوق بشر (۱۹۵۰)، ماده (۵) منشور آفریقایی حقوق بشر (۱۹۸۱) و ماده (۴۹) منشور حقوق بنیادین اتحادیه اروپا (۲۰۰۰)، اصل تناسب جرائم و مجازات‌ها و ممنوعیت مجازات‌های نامتناسب را به‌صورت صریح یا ضمنی مورد تأکید قرار دهند» (همان: ۱۱۶). میزان صدمه مستقیم و غیرمستقیم ناشی از بزه، فایده اجتماعی مجازات، نوع جرم ارتکابی، خصوصیات شخصیتی مجرم با مطالعه پرونده شخصیت و درجه تقصیر بزه‌دیده مهمترین معیارهای تناسب جرم با مجازاتند. منظور از تناسب جرم و مجازات تنها تناسب در درجه شدت کیفر نیست بلکه «تناسب میان جرم و مجازات هم در انتخاب نوع مجازات و هم در تعیین مقدار مجازات باید رعایت شود» (حاجی‌ده‌آبادی، ۱۳۸۹: ۳۴). چرا که «اگر فرشته عدالت در مقابل هر رفتاری به‌طور یکسان شمشیر از نیام برکشد و [همیشه] به سلاح کیفر متوسل گردد، اولین نتیجه آن مخدوش شدن چهره عدالت است. وقتی که صحبت از حبس می‌شود، باید در ذهن مردم شدیدترین جرائم و تجاوز به اساسی‌ترین ارزش‌ها تداعی گردد، نه اینکه برای هر رفتار کم‌اهمیت، جزئی و مربوط به حریم خصوصی و حق زیستن مردم براساس سبک‌های مختلف زندگی، به کیفر حبس متوسل شویم» (حبیب‌زاده و زینالی، ۱۳۸۴: ۱۲). شدت مجازات نه‌تنها تأمین‌کننده اهداف حقوق کیفری نمی‌تواند باشد بلکه به این جهت که حتمیت و قطعیت مجازات را منتفی می‌سازد مانع تحقق اهداف مجازات هم هست و بدین جهت است که منتسکیو معتقد است: «شقاوت قوانین، اغلب مانعِ اجرای آن است، وقتی مجازات حد و مرزی ندارد، اغلب مجبور می‌شوند مجازات نکردن را به‌جای آن ترجیح دهند» (بکاریا، ۱۳۸۰: ۸۰). در بسیاری موارد انگیزه مرتکبان جرائم سایبری برخلاف سایر مجرمین، انگیزه مالی، انتقام‌جویی و کینه، ناموسی و مواردی ازاین‌دست نیست بلکه درصد بالایی از شهروندان اینترنت، با انگیزه تفریح و سرگرمی وارد این فضا می‌شوند و گاهی به جهت سهولت ارتکاب جرم

و بی‌چهرگی و ناشناخته بودن، مرتکب جرائم رایانه‌ای می‌شوند. نمودار زیر این مطلب را به‌خوبی نشان می‌دهد.

نمودار ۱. موضوعات مورد علاقه جوانان در اینترنت



مأخذ: محمود حاجیلی (۱۳۸۸).

مدل واکنشی معمول در جهان سنتی، برای جهان آنلاین مناسب نیست (جوان‌جعفری، ۱۳۸۵: ۳۲). با توجه به ویژگی‌های منحصربه‌فرد جرم و مجرم سایبری باید اظهار داشت به آن اندازه که جرائم و مجرمان رایانه‌ای از جهت سن و انگیزه مجرمانه متمایز از سایر مجرمان هستند مجازات این جرائم نیز باید متفاوت باشد «اصل تقصیر (قابل مجازات بودن) مستلزم تفکیک بر طبق مصالح مربوط، اعمال ارتکابی، وضعیت مرتکب، اهداف و دیگر عناصر روانی است» (زیبر، ۱۳۹۰: ۱۹۰). اعمال مجازات‌های قدیمی برای جرائم نوین سایبری نه‌تنها اهداف مجازات را برآورده نمی‌کند بلکه تمامی آثار منفی اعمال مجازات، از قبیل معاشرت با بزهکاران حرفه‌ای، دوری از خانواده و پیامدهای منفی ناشی از آن و ... را به‌همراه دارد.

اعمال مجازات‌های شدید در این جرائم، علاوه‌بر اینکه سودمند نیست، در عمل نمی‌تواند ممکن باشد زیرا درصد بالایی از مجرمان سایبری را نوجوانانی که به سن مسئولیت کیفری نرسیده‌اند تشکیل می‌دهند. همچنین «فردی کردن مجازات» درخصوص این جرائم ضروری به‌نظر می‌رسد. مجازات این بزهکاران باید شناور باشد زیرا این مجرمان از تنوع و گوناگونی شخصیتی بیشتری نسبت به سایر مجرمان برخوردارند. لذا باید اختیار قضات را در تعیین کیفر افزود تا بزهکاران را نه بیش از آنچه که سودمند است و نه بیش از آنچه عدالت اقتضا دارد مجازات کنند. درواقع دادرسان باید بتوانند در دعواهای مختلف، متناسب با شرایط و اوضاع‌واحوال حاکم بر آن کیفر را تعیین کنند. «نظام نرمش‌ناپذیر مبتنی‌بر قانون، احساس بی‌عدالتی ایجاد می‌کند زیرا توانایی دستیابی به همه معیارهای بالقوه مرتبط با تعیین کیفر عادلانه را ندارد؛ صرف‌نظر از اینکه نمی‌تواند نیازهای بازپرورانه مجرم را دربربگیرد» (محمودی‌جانکی، ۱۳۸۸: ۶۷۲). این امر در مورد جرائم سایبری که دارای بزهکاران متنوع و با شرایط مختلف است نمود بیشتری دارد.

انجام خدمات عام‌المنفعه به‌جای مجازات، یکی از جلوه‌های نوین عدالت ترمیمی است. عدالت ترمیمی که به آن عدالت احیاکننده نیز گفته می‌شود، تفکر جدیدی است که بر ترمیم و مقابله با آثار جرم در جامعه و به‌ویژه از طریق مشارکت ارکان مختلف جامعه مدنی (بزه‌دیده، بزهکار و مردم) تکیه می‌کند (رستمی، ۱۳۸۶: ۱۵۲). کار عام‌المنفعه درعین‌حال یکی از مصادیق مهم مشارکت مردم در فرایند اصلاح و درمان بزهکاران است و به مجرم نشان می‌دهد که هرچند جامعه از مجرمیت او متأثر شده است، می‌تواند به او به‌عنوان عنصری سودمند و سازنده ـ نه مخرب و زیانبار ـ نیز بنگرد. فرایند مزبور یک فلسفه عدالت ترمیمی را به‌همراه دارد که برمبنای آن بزهکار یک سری خدمات عام‌المنفعه عمومی را انجام می‌دهد که این امر منجر به اشتغال و کسب تجربه‌های نوین می‌شود (جمشیدی، ۱۳۹۰: ۲۴۱). خوشبختانه بستر اجرای این راهبرد درخصوص مجرمین رایانه‌ای به جهت برخورداری از تخصص کافی کار با رایانه، بسیار هموار و مساعد است. به‌جرئت می‌توان ادعا کرد درجه مهارت و تخصص برخی از این بزهکاران از بسیاری مهندسان و تکنسین‌های رایانه‌ای بالاتر است. لذا خدمات عام‌المنفعه این افراد به جامعه، به‌ویژه پلیس سایبری ازیک‌طرف و همکاری و اعتمادپذیری نظام عدالت کیفری ازطرف‌دیگر، گام مهمی در جهت پیشگیری از وقوع مجدد و اصلاح بزهکار تلقی می‌شود.

وضعیت قانون جرائم رایانه‌ای از حیث اختیار قضات در تعیین مجازات مطلوب می‌باشد

زیرا در غالب جرائم برشمرده شده در این قانون قاضی بین سه گزینه حبس، جزای نقدی یا هر دو مجازات مخیر است. لکن عملکرد قانونگذار از جهت میزان مجازات در برخی موارد به‌هیچ‌وجه قابل دفاع نیست. برای مثال حبس به مدت سه سال و جزای نقدی به مقدار یک میلیارد ریال، موضوع مجازات ماده (۲۴) این قانون برای صرف استفاده از پهنای باند بین‌المللی بدون مجوز قانونی است که شدت این مجازات به‌هیچ‌وجه قابل مسامحه نیست.

۵-۲. جرم‌انگاری با توجه به امکانات دستگاه عدالت کیفری

جرم‌انگاری بدون توجه به امکانات، زیربناها و ساختار دستگاه عدالت کیفری، تبعات و پیامدهای سنگینی در پی خواهد داشت. درواقع هنگامی جرم‌انگاری به‌صورت صحیح و بدون نقض اهداف و اغراض قانونگذار محقق می‌شود که مقنن به تمام وسایل و امکاناتی که از مرحله کشف جرم تا اعمال مجازات نیاز هست توجه داشته باشد و با عنایت به واقعیت‌های موجود اقدام به قانونگذاری کند. برخی نظریه‌پردازان حقوق کیفری به این موضوع تحت عنوان «فیلتر کارکردها»[1] پرداخته‌اند. در این فیلتر عواقب عملی جرم‌انگاری یک رفتار مورد بررسی قرار می‌گیرد. تصویب و اجرای قوانین موضوعه کیفری، پیامدهای عملی در پی دارد که برخی از آنها واضح بوده، به‌سرعت خود را نمایان می‌سازند و اثر برخی دیگر ممکن است در زمان و مکان به طول بینجامد و درعین‌حال بسیار غافلگیرکننده و عجیب باشد. درواقع باید سود و زیان اجتماعی اجرا و عدم اجرای قانون کیفری پیشنهادی را ارزیابی و سبک و سنگین کرد (Schonsheck, 1994: 70). مسلماً اجرای کامل حقوق کیفری غیرممکن است زیرا هزینه‌های اقتصادی آن و نیز هزینه‌های اجتماعی زیستن در یک نظام پلیسی، که لزوماً همراه با از میان رفتن آزادی‌های مدنی و حقوق انسانی خواهد بود، غیرقابل تصور است (کلارکسون، ۱۳۹۰: ۲۵۴). بی‌توجهی به وضعیت و شرایط دستگاه عدالت کیفری از جهت بودجه، امکانات فنی و ظرفیت اعمال مجازات مسلماً آثار و تبعات منفی زیادی در پی خواهد داشت. از جمله این آثار می‌توان به مواردی همچون افزایش رقم‌های سیاه و خاکستری بزهکاری، بازنمایی اجتماعی منفی دستگاه عدالت کیفری، تورم جمعیت کیفری زندان‌ها (حبیب‌زاده و زینالی، ۱۳۸۴: ۱۲-۶) تضعیف قدرت حقوق کیفری به جهت عدم حتمیت مجازات اشاره کرد. در عرصه سایبر، جرم‌انگاری توجه جدی به امکانات

1. The Pragmatics Filter

و ظرفیت‌های نظام عدالت کیفری را طلب می‌کند. به جهت ساختار نوین فضای سایبر امکانات کشف جرم و دستگیری مجرم در حال پیشرفت است لکن متأسفانه این امکانات هنوز به آن مرحله از پیشرفت نرسیده است که پاسخ‌گوی دستگاه عدالت کیفری باشد زیرا پیشرفت فوق‌العاده سریع فناوری‌های رایانه‌ای باعث ناشناس و مجهول بودن شیوه‌های نوین بزه شده است. همچنین در جرائم سایبری، مجرم پس از ارتکاب جرم نه‌تنها احساس ندامت ندارد، بلکه به عکس به هوش و توانایی خود در ارتکاب این اعمال مجرمانه می‌بالد و به نوعی احساس زرنگی می‌کند. به همین دلیل می‌توان گفت «جرائم سایبری نسبت به نظایر فیزیکی‌شان از رقم سیاه بالاتری برخوردارند» (جلالی فراهانی، ۱۳۸۳: ۱۱۸) و احتمالاً تکرار و تعدد جرم در این جرائم بالاتر است. برای دفع این احساس مجرمان، باید بر حتمیت و قطعیت مجازات تأکید و تمرکز کرد. به‌گونه‌ای که هیچ بزهکاری خود را دورزننده مجازات نبیند. درمجموع باید نظر داد که مجازات جرائم سایبری باید به‌دور از شدت و دارای حتمیت و قطعیت در اعمال باشد. شاید بتوان گفت به‌دلیل سرعت بالای این پیشرفت، قانونگذار کیفری همیشه یک گام، بلکه بیشتر، عقب‌تر از فناوری سایبر در حرکت است. به‌طور مثال اگرچه ماده (۲۴) قانون جرائم رایانه‌ای درخصوص استفاده بدون مجوز از پهنای باند بین‌المللی بدین‌صورت اقدام به جرم‌انگاری نموده است: «هرکس بدون مجوز قانونی از پهنای باند بین‌المللی برای برقراری ارتباطات مخابراتی مبتنی‌بر پروتکل اینترنتی از خارج ایران به داخل یا برعکس استفاده کند، به حبس از یک تا سه سال یا جزای نقدی از یکصد میلیون تا یک میلیارد ریال یا هر دو مجازات محکوم خواهد شد» لیکن «کشف و پیگیری چنین ارتباطی نیاز به دانش و فناوری نوین دارد که در ایران به‌ندرت در دسترس می‌باشد؛ به‌ویژه در مواردی که از خارج از کشور این‌گونه تماس‌ها برقرار شود، پیگیری و کشف آن دشوار است» (الهی‌منش و سدره‌نشین، ۱۳۹۱: ۱۳۸). حتی شناخت مفهومی برخی از این جرائم برای حقوقدانان تا حدی دشوار است. این امر ناشی از سرعت بالای پیشرفت فناوری و تکنولوژی اطلاعات و ارتباطات است.

۳. اصول خاص جرم‌انگاری در فضای سایبر

در کنار اصول عام جرم‌انگاری که هم در مورد جرائم سایبری و هم سایر جرائم موضوعیت دارد، باید اصول دیگری را مورد توجه قرار داد که ارتباط مستقیمی با ویژگی‌های خاص و

منحصربه‌فرد جرائم سایبری دارا هستند. به‌بیان‌دیگر، ویژگی‌های ممتاز و بی‌نظیر فضای سایبر اقتضا می‌کند که قانونگذاران و سیاستگذاران این عرصه اصول خاصی را رعایت کنند که این اصول در مورد سایر جرائم یا موضوعیت ندارد و یا به‌اندازه جرائم سایبری اهمیت ندارد.

۱-۳. لزوم توجه به راهبردها، رویکردها و همکاری‌های بین‌المللی

هماهنگی با قوانین بین‌المللی به‌ویژه با توجه به استاندارد شدن نسبی فناوری‌های اطلاعات و شیوه‌های ارتکاب جرم در صحنه جهانی، گستردگی جرائم و عدم توجه به مرزها به‌عنوان مانعی برای ارتکاب جرم، ضروری به‌نظر می‌رسد چرا که فضای سایبر و اینترنت فارغ از مرزهای جغرافیایی عمل می‌کند؛ محدود به چارچوب خطوطی که دولت‌مردان در طراحی نقشه‌های سیاسی رسم می‌کنند نیست و از هیچ‌گونه محدودیت مکانی تبعیت نمی‌کند. سایبر یک گستره بدون مرز است که نمی‌توان در برابر آن خطوط مقسّم کشید یا با مرزهای طبیعی یا مصنوعی آن را تکه‌تکه و جدا ساخت (فضلی، ۱۳۸۹: ۶۶). ازیک‌سو بسیاری از مصادیق جرائم سازمان‌یافته بین‌المللی همچون پولشویی و قاچاق انسان استفاده از ابزار رایانه و شبکه جهانی اینترنت و ارتکاب جرائم رایانه‌ای اقدام به جرم سازمان‌یافته می‌کنند و از تسهیلات فناوری اطلاعات و ارتباطات برای ارتکاب جرائم سازمان‌یافته بهره‌برداری می‌کنند (Keenan, 2006: 514) و ازسوی‌دیگر خود جرائم سایبری هم کاملاً جنبه فرامرزی دارند. برای مثال می‌توان به واقعه زیر، که جنبه فرامرزی بودن سایبر را بهتر نشان می‌دهد، اشاره کرد: «یک ایمیل تهدیدآمیز دایر بر تهدید به بمب‌گذاری در یک فروشگاه مواد غذایی در لتونی دریافت شد. پس از بررسی‌های فراوان مشخص شد که مرتکب ساکن استونی است و با استفاده از امکانات و فضای سایبر اقدامات خود را عملی می‌کرده است. یا در قضیه دیگر فردی ناشناس از طریق ایمیل تهدیدآمیز مقر ستاد پلیس نروژ را تهدید به بمب‌گذاری کرد. در پیگیری ماجرا، فرد مرتکب شناسایی نشد. با استمداد پلیس نروژ از پلیس اینترپل،[1] دولت کانادا دریافت که آن شخص در این کشور ثبت دامنه کرده و از خطوط آن کشور بهره می‌برد، درحالی که پلیس اینترپل انتظار داشت آن شخص ساکن کانادا باشد، پس از بررسی‌های فراوان مشخص شد که مرتکب ساکن

1. Enterpol Police

نروژ و در همان خیابان محل مقر ستاد پلیس نروژ بوده است» (شیرزاد، ۱۳۸۸: ۳۰-۲۹). در بخشی از رهنمود عملی پیشگیری از جرم سازمان ملل متحد، تحت عنوان همکاری فنی آمده است: «دولت‌های عضو و سازمان‌های بین‌المللی مسئول تأمین بودجه مربوطه، باید به‌منظور اجرایی کردن اصول ناظر بر تأمین امنیت گروهی و پیشگیری از جرم در سطح ملی و منطقه‌ای، زمینه همکاری مالی و فنی درخصوص تقویت ظرفیت‌ها، ساختارها و آموزش را با کشورهای در حال توسعه، گروه‌ها و سایر سازمان‌های ذی‌ربط فراهم کنند». بنابر آنچه در این زمینه گفته شد، استفاده از تعاریف استاندارد جهانی، استفاده از تجربیات دیگر کشورها و وجود همکاری‌های دو یا چندجانبه در مواجهه با جرائم سایبری، از پیش‌شرط‌های توفیق در جرم‌انگاری است (جوان‌جعفری، ۱۳۸۵: ۳۱). فصل سوم کنوانسیون جرائم سایبری (۲۰۰۱) تحت عنوان همکاری بین‌المللی چند اصل کلی را در ماده (۲۳) در این خصوص برمی‌شمارد که حدود و سمت و شیوه همکاری‌های بین‌المللی را معین می‌کند. این اصول عبارتند از:

- همکاری بین‌المللی در میان اعضا باید در گسترده‌ترین وضعیت تأمین شود.
- همکاری باید تمامی جرائم مرتبط با سیستم‌های رایانه‌ای و همچنین جمع‌آوری ادله الکترونیک را دربربگیرد.
- همکاری باید براساس توافق‌نامه‌های بین‌المللی در موضوعات کیفری و ترتیبات توافق شده براساس قانونگذاری متحدالشکل یا دوجانبه و قوانین داخلی به‌عمل آید.

۲-۳. لزوم توجه ویژه مقنن به اقشار آسیب‌پذیر در فضای سایبر

۱-۲-۳. زنان

هرکسی ممکن است قربانی جرائم سایبری باشد، اما گروه‌های جمعیتی خاص بیشتر از دیگران در معرض خطرند. این گروه‌ها عبارتند از: زنان، نوجوانان، تازه‌واردان اینترنت، و سایر گروهای خاص آسیب‌پذیر (Hutton and Haantz, 2003). بنابراین جنسیت می‌تواند به‌عنوان عاملی باشد که احتمال بزه‌دیدگی افراد نسبت به برخی جرائم را بالا ببرد (نجابتی، ۱۳۷۹: ۳۵). در مطالعاتی که در سال ۲۰۰۲ توسط گروهی از وکلای قربانیان آنلاین تحت عنوان تلاش برای توقف سوءاستفاده آنلاین (Halder and Jaishankar, 2010) صورت گرفت، ۷۱ درصد قربانیان مزاحمت سایبری زن بودند، و ۵۹ درصد آنان در گذشته

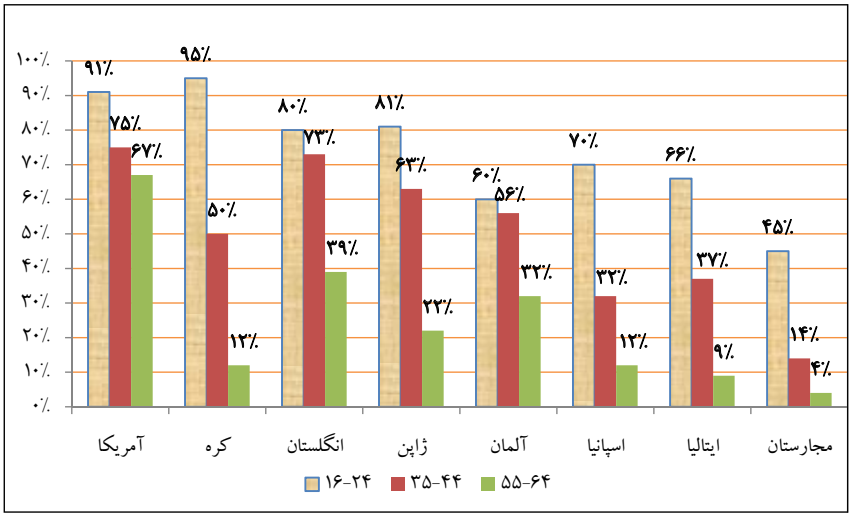
نوعی از روابط را با مزاحم تجربه کرده بودند (Hutton and Haantz, 2003). تقریباً از هر پنج قربانی، چهار تن زن هستند و زنان هشت‌برابر بیشتر از مردان در معرض مزاحمت سایبری توسط همسران سابق یا آشنایان قرار دارند (Ibid.; Reno, 1999). با این وجود، نویسندگان کنوانسیون اتحادیه اروپا و قانونگذاران کشورهای مختلف، هیچ‌گاه بزه‌دیده شدن زنان در فضای مجازی را، مسئله‌ای به بزرگی جرائم دیگر در نظر نگرفته‌اند. بنابراین بزه‌دیدگان زن به‌عنوان یک نگرانی ثانویه برای تمام جوامع مجهز به سیستم‌های مجازی باقی مانده‌اند. این ازقلم‌افتادگی به‌وضوح در رشد میزان رخدادهای مجرمانه، که زنان را در شبکه‌های اجتماعی مورد هدف قرار می‌دهند، قابل مشاهده است (Jaishankar, 2011: 300). در ایران هم، آمار موجود نشان می‌دهد که ۷۰ درصد کاربران مرد و تنها ۳۰ درصد آنها زن هستند (حاجیلی، ۱۳۸۸: ۱۲۷). همچنین اکثر قریب‌به‌اتفاق جرائم سایبری نیز توسط مردان ارتکاب می‌یابد. به همین جهت زنان بیشتر در معرض بزه‌دیدگی هستند، موضوع نگران‌کننده این است که ۹۵ درصد متهمان جرائم رایانه‌ای در ایران را مردان تشکیل می‌دهند که بیشتر این متهمان در گروه سنی ۱۸ تا ۳۵ سال قرار دارند. دلیل عمده برای رشد بزه‌دیده شدن آنلاین زنان در شبکه‌های اجتماعی عبارت است از: آسان بزه‌دیده شدن زنان و مطلوب بودن وضعیت زنان برای ارتکاب بزه. قوانین افتراقی حساس به جنسیت بزه‌دیدگان که در آنها جرائم علیه دسته خاصی از بزه‌دیدگان مجازات بیشتری در پی دارد ابزاری مناسب برای کنترل نرخ جرم می‌باشد چرا که مجرمان محاسبه‌گر را از ارتکاب جرم علیه این دسته خاص از بزه‌دیدگان منصرف می‌کند. بنابراین ضروری است با جرم‌انگاری ویژه و خاص درخصوص بزه‌دیدگی زنان به مقابله جدی با وضعیت اسفبار موجود در فضای مجازی پرداخت.

۲-۲-۳. کودکان

میزان استفاده از اینترنت و شبکه‌های مجازی چنان رو به گسترش است که نسل کنونی را نسل اینترنت یا نسل شبکه نام نهاده‌اند. این نسل متولدین اواسط دهه ۱۹۹۰ میلادی به بعد هستند. بین استفاده نسل‌های مختلف از شبکه‌های اجتماعی و همچنین انگیزه‌های آنها از پیوستن به فضای مجازی تفاوت‌های قابل توجهی وجود دارد (Bartholomew and et al., 2012). نمودار زیر به‌خوبی نشان می‌دهد که در تمام کشورهایی که درخصوص سن کاربران اینترنت

سنجش به‌عمل آمده است جوانان ۱۶ تا ۲۴ ساله بیشترین استفاده از اینترنت را دارند (توکل و کاظم‌پور، ۱۳۸۴: ۱۲۰).

نمودار ۲. استفاده از اینترنت براساس سن



Source: http://www.worldinternetproject.net.

متأسفانه کاربران جوان اینترنت، اغلب بدون مواجه شدن با یک ارتباط ناخوانده ازسوی سایر مجرمان اینترنتی، قادر به شرکت در فعالیت‌های آنلاین نیستند. براساس مطالعات مختلف[1] بر روی استفاده جوانان از اینترنت، تعداد کثیری از جوانان، درحالی که از روش‌های ارتباط رایانه‌ای استفاده می‌کنند، گونه‌های ذیل از بزه‌دیدگی را تجربه کرده‌اند:

- قرار گرفتن ناخواسته در معرض داده‌های جنسی،
- تقاضای جنسی،
- مزاحمت‌های ناخواسته غیرجنسی.

ازسوی‌دیگر، یکی از ویژگی‌های جرائم اینترنتی که هشداری جدی برای جوامع امروزی است روبه‌رو شدن با دسته بزرگی از مجرمان نوجوان است که بعضاً به سن مسئولیت

1. Mitchell, Finkelhor and Wolak, 2003, 2007; O´Connell, Barrow and Sange, 2002; Quayle and Taylor, 2003; Wolak, Mitchell and Finkelhor, 2007; Ybarra, Mitchell, Finkelhor and Wolak, 2007.

کیفری نرسیده‌اند. درحالی که جرائم ارتکابی آنان در عرصه اینترنت، از نظر صدمه و آسیب بسیار گسترده‌تر از جرائم سنتی می‌باشد. به‌طور مثال یک نوجوان پانزده‌ساله که به حساب شرکت‌های دیگر مبلغ ۸۹ هزار دلار مکالمه تلفنی انجام داده بود، شناسایی و دستگیر شد. این بزهکار نوجوان با استفاده از یک دستگاه مودم و رایانه شخصی خود از منزل وارد سیستم‌های رایانه‌ای شرکت‌های تجاری می‌شد و گذرواژه آنها را به‌دست می‌آورد و سپس با استفاده از آن گذرواژه در هر مکانی می‌توانست به حساب آن شرکت تلفن کند یا در موردی دیگر، می‌توان به قضیه شبکه‌های رایانه‌ای «تله‌نت» و «دیتاپک» اشاره کرد. استفاده‌کنندگان از این دو شبکه، ظرف مدت یک هفته شکایت‌هایی به مسئولان شبکه تسلیم کردند و متعرض شدند که افرادی به‌صورت غیرمجاز به سیستم آنها دست یافته و مشکلاتی ایجاد کرده‌اند. چون سوءاستفاده الکترونیکی یاد شده وضع فراملی داشت، پلیس کانادا با همکاری پلیس آمریکا از طریق خطوط الکترونیکی شبکه‌ها، چهار نوجوان سیزده‌ساله مدرسه دالتون نیویورک را دستگیر کرد (پاکزاد، ۱۳۷۵: ۱۸).

بنابر آنچه گفته شد باید اذعان داشت فضای سایبر چالش‌های نگران‌کننده‌ای را درخصوص کودکان و نوجوانان به‌وجود آورده است. ازیک‌سو با حضور کثیری از کودکان در این فضا، امکان بزه‌دیدگی این افراد بالا می‌رود و ازسوی‌دیگر در برخی موارد همین کودکان جرائمی را با خسارت‌هایی که امکان ایجاد آن توسط آنها در جرائم سنتی نزدیک به محال است به‌وجود می‌آورند. لذا قانونگذار کیفری باید اولاً با اعمال تشدید مجازات نسبت به مجرمانی که بزه‌دیده خود را از میان کودکان انتخاب می‌کنند از این افراد حمایت ویژه‌ای به‌عمل آورد و ازسوی‌دیگر تدابیری بیندیشد که بدون توسل به اقدامات کیفری موجبات کاستن از مجرمان صغیر رایانه‌ای و به حداقل رساندن خسارات و صدمات آنان را فراهم آورد.

۳-۳. لزوم اتخاذ راهبردهای علمی و دانش بین‌رشته‌ای برای مقابله با جرائم رایانه‌ای

جرائم رایانه‌ای در فضا و بستری ارتکاب می‌یابند که امکان شناسایی و مقابله با آنها بسیار دشوار است و از این لحاظ نسبت به نظایر فیزیکی‌شان از رقم سیاه بالاتری برخوردارند (جلالی‌فراهانی، ۱۳۸۴: ۱۱۸). رهنمود پیشگیری از جرم سازمان ملل متحد تأکید می‌کند که برای شناخت وضعیت فعلی جرائم و راه‌حل‌های پیشگیری از آنها، از دانش و اطلاعات مناسب استفاده شود.

(جوان‌جعفری و سیدزاده ثانی، ۱۳۹۱: ۱۲۴). برخلاف جرائم سنتی، علل و عوامل جرائم سایبری و طرق ارتکاب آنها مختلف است. مثلاً جرم سرقت سنتی به چند شیوه از قبیل کیف‌قاپی، سرقت مسلحانه از بانک، سرقت ساده و ... ارتکاب می‌یابد و متناسب با این شیوه‌های سرقت، قانونگذار اقدام به جرم‌انگاری انواع مختلف سرقت در قانون مجازات اسلامی نموده است، اما در جرائم رایانه‌ای علاوه‌بر طرق مختلف ارتکاب یک جرم، بعضاً با جرائم جدیدی روبه‌رو می‌شویم که حتی شناخت مفهومیِ این جرائم برای حقوقدانان و قضات دشوار می‌باشد. این امر ناشی از سرعت بالای پیشرفت فناوری و تکنولوژی اطلاعات و ارتباطات است. شاید بتوان گفت به‌دلیل سرعت بالای این پیشرفت، قانونگذار کیفری همیشه یک گام عقب‌تر از فناوری است و پس از قربانی شدن شهروندان بسیاری توسط مجرمین باهوش رایانه‌ای، به پیشگیری و یا جرم‌انگاری می‌پردازد (سلیمی، ۱۳۹۱: ۱۷).

ازاین‌رو ضروری است که علوم مختلف را در شناسایی این جرائم و مجرمین و بزه‌دیدگان آن به‌کار گیریم و با یک مبنای علمی دقیق به مقابله با وقوع این جرائم بپردازیم. به‌بیان‌دیگر، مشارکت همه بخش‌های ذی‌نفع و به‌ویژه متخصصان و کارشناسان فناوری اطلاعات در این حوزه (حوزه سایبر)، بیش از سایر حوزه‌های قانونگذاری ضروری به‌نظر می‌رسد. یکی از مشکلات اساسی بخش‌های مختلف درگیر در نظام حقوقی کشور، عدم آشنایی کافی با موضوع است. لذا حضور متخصصان سایبر درزمینه‌های مختلف قانونگذاری، قضاوت، تحقیق و کشف جرم، اجتناب‌ناپذیر است (جوان‌جعفری، ۱۳۸۵: ۳۱). راهبردها، سیاست‌ها، برنامه‌ها و اقدامات پیشگیری و مقابله با جرم به‌ویژه امر تقنین، قبل از هرچیز باید بر پایه تحقیقات علمی و دانش بین‌رشته‌ای درخصوص علل جرم و راهکارهای قطعی و احتمالی معضل جرم بنا شود. در غیر این صورت هرگونه سیاستگذاری و یا قانونگذاری، به‌ویژه در عرصه جرائم نوپدید مجازی برای اهل فن و مجرمان حرفه‌ای ناکارآمد، بی‌فایده و حتی مضحک خواهد بود. لذا برای کارآمد شدن هرچه بیشتر قوانین توصیه می‌شود در جرم‌انگاری از جرائم سایبری، از نظرات تخصصی متخصصان و کارشناسان نرم‌افزارها و سخت‌افزارهای رایانه‌ای بیشتر استفاده شود. رخصت مقنن برای حضور متخصصان و کارشناسان فناوری اطلاعات در مرحله رسیدگی به جرم و تعیین مجازات و یاری رساندن به قضات در شناسایی مفهوم جرم در قالب «هیئت منصفه» بسیار ضروری به‌نظر می‌رسد.

٤-۳. لزوم شناسایی مسئولیت کیفری اشخاص حقوقی

حتی اگر در شناسایی مسئولیت کیفری برای اشخاص حقوقی در جرائم سنتی تردید داشته باشیم، فراوانی حضور و بزهکاری اشخاص حقوقی در فضای سایبر، تردیدی در شناسایی مسئولیت کیفری اشخاص حقوقی باقی نمی‌گذارد. درواقع فضای سایبر بستر مناسبی را برای فعالیت‌های اشخاص حقوقی پدید آورده است که درصورت عدم شناسایی مسئولیت اشخاص حقوقی، جرائم این اشخاص صدمات و خسارت‌های جبران‌ناپذیری به بار خواهد آورد. شرکت‌های تولیدکننده و واردکننده سخت‌افزارهای رایانه‌ای، شرکت‌های مخابراتی، توزیع‌کنندگان کلی و جزئی نرم‌افزار، شرکت‌های خدمات دسترسی، اتحادیه‌ها و اصناف مرتبط، آموزشگاه‌های رایانه‌ای و کلیه نهادهای مرتبط با فعالیت‌های رایانه‌ای بخشی از اشخاص حقوقی فعال درزمینه سایبر هستند. ماده (۱۲) کنوانسیون جرائم سایبری (۲۰۰۱) به مسئولیت اشخاص حقوقی پرداخته است و قانونگذاران کشورها را مکلف به شناسایی مسئولیت کیفری و مدنی اشخاص حقوقی می‌نماید. این ماده مقرر می‌دارد: «هریک از اعضا باید به‌گونه‌ای اقدام به وضع قوانین و سایر تدابیر نمایند که درصورت لزوم اطمینان دهند چنانچه اشخاص حقوقی در راستای منافع خود مرتکب جرائم مصوب این کنوانسیون شدند، آنها را تحت قوانین کیفری تحت تعقیب قرار خواهند داد». خوشبختانه قانون جرائم رایانه‌ای به مسئولیت کیفری اشخاص حقوقی توجه داشته و مواد (۱۹ تا ۲۳) این قانون به بحث پیرامون اشخاص حقوقی و مسئولیت کیفری اشخاص حقوقی پرداخته است.

٥-۳. جرم‌انگاری در پرتو سیاست جنایی مشارکتی

یکی از چالش‌های جدید حقوق کیفری مقابله با جرائم سایبری است. به‌بیان‌دیگر با توجه به گستردگی و شبکه‌ای بودن فضای سایبر، باید اذعان داشت مقابله با جرائم سایبری به جهت گستردگی خسارت و کثرت بزه‌دیدگان، فرامرزی بودن و مشکلات کشف و تعقیب مجرم و بسیاری ویژگی‌های دیگر تنها با یک «راهبرد جنایی مشارکتی» می‌تواند کارآمد و مؤثر صورت گیرد. آنچه این نظر را تقویت می‌کند این است که جرائم سایبری در غیاب جرائم سنتی اتفاق نمی‌افتند و درواقع جایگزین جرائم سنتی نمی‌شوند، بلکه در کنار آنها قرار می‌گیرند. یعنی جرائم سنتی مانند قتل، ضرب و جرح، زنا، سرقت و کلاهبرداری‌های سنتی کماکان اتفاق می‌افتند. نتیجه

این است که منابع، نیروها و امکانات موجود دستگاه عدالت کیفری دچار فرسایش و کمبود می‌شوند و امکان مواجهه با همه این جرائم از آنها سلب می‌شود (همان: ۲۶).

برای مقابله همه‌جانبه و کارآمد با این جرائم، اتخاذ یک سیاست جنایی فراگیر با مشارکت گسترده جامعه مدنی، کاربران سایبر و سازمان‌های مردم‌نهاد ضروری است. در پرتو یک سیاست جنایی مشارکتی هریک از این گروه‌ها باید در مراحل مختلف فرایند جنایی یعنی پیشگیری و مقابله با جرم، کشف جرم و تعقیب مجرم، مرحله رسیدگی به جرم و مجازات مجرم نقش‌آفرینی کنند تا ضمن کاستن از بار دستگاه عدالت کیفری به مقابله هرچه گسترده‌تر و دقیق‌تر با جرم پرداخته شود. چرا که کنترل بزه به جهات مختلف فراتر از ظرفیت نهادهای رسمی عدالت کیفری است و باید به واگذاری بخشی از سازکارهای تأمین‌کننده امنیت و عدالت به مردم، سازمان‌های مردم‌نهاد و نهادهای غیردولتی پرداخت. اهمیت پیشگیری مشارکتی تا جایی است که بکاریا در رساله جرائم و مجازات‌های خود درخصوص این مفهوم چنین بیان می‌دارد: «می‌خواهید از وقوع جرم پیشگیری کنید؟ پس بکوشید تا قوانین روشن و ساده باشد و تمام قدرت ملت در دفاع از آن بسیج شود و هیچ قدرتی برای نابودی آن به‌کار گرفته نشود» (بکاریا، ۱۳۸۰: ۱۳۲). یکی از نمودهای سیاست جنایی مشارکتی درزمینه سایبر، کاستن از اختیار نهادهای دولتی و نظارتی در امر فیلترینگ و تفویض حداقل قسمتی از این امر به برخی از شهروندان و کاربرانِ شریف فضای سایبر، که رویکردی سنجیده و ملایم‌تر نسبت به مسئله فیلترینگ دارند، می‌باشد. این امر موجب افزایش دقت و هوشمندی سامانه‌های فیلترکننده برای اجتناب از اشتباه در فیلترینگ نیز می‌شود. نمود دیگری از سیاست جنایی مشارکتی در جرائم رایانه‌ای رعایت ادب و نزاکت در اتاق‌های گپ و گفت‌وگو است که درصورت عدم پایبندی به آن، کاربران دیگر، شخص هنجارشکن را از ادامه حضور در اتاق گپ محروم می‌کنند. قانونگذار کیفری باید با به رسمیت شناختن عرف‌های مطلوبِ موجود در عرصه مجازی، زمینه مشارکت اجتماعی شهروندان اینترنت را در ساماندهی این فضا فراهم آورد. ترغیب کاربران به ایمن‌سازی محیط سایبر با تفهیم این مهم به ایشان که سایبر زیستگاه دوم ما و فرزندان ماست در ایمن‌سازی و مقابله با هنجارشکنان آن بسیار مؤثر و راهگشاست. باید بپذیریم که هیچ سیاستی در قبال جرائم سایبری بدون مشارکت تمام بخش‌های درگیر یعنی حکومت، بخش خصوصی،

جامعه و به‌طورکلی، تمام کسانی که به‌نحوی از فضای سایبر ذی‌نفع و متأثر می‌باشند، قابلیت اجرا و تداوم نخواهد داشت. بنابراین قانونگذاری در فضای سایبر با اتخاذ راهبرد «سیاست جنایی مشارکتی» در کلیه مراحل یعنی کشف جرم، تعقیب مجرم، رسیدگی و اجرای مجازات و حتی بازپروری مجرم بسیار کارآمد و مؤثر می‌باشد لذا قانونگذار کیفری باید به‌گونه‌ای قانونگذاری نماید که در هریک از این مراحل امکان بهره‌گیری از مشارکت مردم و سازمان‌های مردم‌نهاد وجود داشته باشد و از بار دستگاه عدالت کیفری تا حد امکان بکاهد.

٤. جمع‌بندی و نتیجه‌گیری

قانونگذار کیفری از جرم‌انگاری یک رفتار اهداف خاصی را دنبال می‌کند لکن هنگامی که این جرم‌انگاری بدون معیار و ضابطه صورت گیرد نه‌تنها این اهداف محقق نمی‌شود بلکه چهره دستگاه عدالت کیفری مخدوش می‌گردد. بنابراین برای جرم شمردن یک رفتار ضروری است اصول و قواعد حقوق کیفری و اقتضائات خاص یک جرم کاملاً رعایت شود. به همین جهت قانونگذار کیفری می‌بایست با رعایت معیارهایی همچون «اصل مشروعیت جرم‌انگاری» و «اصل ضرورت جرم‌انگاری» اولاً از فعل یا ترک فعلی جرم‌انگاری کند که به‌قدر کافی دارای «صدمه» برای جامعه و «سرزنش» اجتماعی باشد و ثانیاً به هیچ طریق دیگری نتوان از ارتکاب و وقوع آن جلوگیری کرد. درواقع جرم‌انگاری از فعل یا ترک فعل کاربران فضای سایبر باید به‌عنوان آخرین حربه نگریسته شود. «احترام به حریم خصوصی و رعایت موازین حقوق بشری» مقوله مهم دیگری است که برای جرم شمردن یک رفتار در محیط سایبر باید کاملاً مورد توجه قرار بگیرد. به جهت ویژگی‌های خاص بزه‌های رایانه‌ای «تناسب بین جرم و مجازات» و فردی کردن مجازات ضرورتی مضاعف دارد. همچنین با توجه به نوین بودن جرائم رایانه‌ای جرم‌انگاری بدون عنایت به ابزار و وسایل موجودِ دستگاه عدالت کیفری از مرحله شناسایی جرم تا تعقیب و دستگیری مجرم و در نهایت اعمال مجازات، موجب ناکامی در عمل و لطمه به اقتدار حقوق کیفری می‌شود. برخی از ویژگی‌های جرائم سایبری که ازیک‌سو بر ضرورت رعایت دقت و ضابطه در جرم‌انگاری می‌افزاید و ازسوی‌دیگر اقتضائات خاصی را در امر جرم‌انگاری موجب می‌شود عبارتند از: سن و جنس مجرمان، فرامرزی بودن جرم، گستردگی خسارت و بزه‌دیده این جرائم، پیشرفت سریع و به‌روز این فناوری و انگیزه و روحیه خاص مجرمان سایبر.

در کنار اصول عمومی جرم‌انگاری که پیشتر اشاره شد، با توجه به ویژگی‌ها و شرایط منحصربه‌فرد فضای سایبر برای نیل به یک قانون مؤثر، کارآمد و عادلانه ضروری است قانونگذار کیفری اصول خاصی را برای جرم شمردن یک رفتار در فضای سایبر رعایت کند. بنابراین باید از «هماهنگی با قوانین بین‌المللی» به‌ویژه با توجه به استاندارد شدن نسبی فناوری‌های اطلاعات و شیوه‌های ارتکاب جرم در صحنه جهانی و فرامرزی بودن جرم، سخن گفت. همچنین «توجه ویژه مقنن به اقشار آسیب‌پذیر» در فضای سایبر و جرم‌انگاری به‌گونه‌ای که به سن و جنسیت حساس باشد به جهت کثرت بزه‌دیدگی این افراد در فضای مجازی ضروری است. با توجه به نوین بودن این جرائم و پیشرفت خیره‌کننده فناوری اطلاعات و ارتباطات ضروری است که علوم مختلف را در شناسایی این جرائم و مجرمین و بزه‌دیدگان آن به‌کار گیریم و با یک مبنای علمی دقیق به مقابله با وقوع این جرائم بپردازیم. حضور پررنگ اشخاص حقوقی در فضای سایبر اقتضائات خاص خود را طلب می‌کند درواقع فضای سایبر بستر مناسبی را برای فعالیت‌های اشخاص حقوقی پدید آورده است که درصورت عدم شناسایی مسئولیت اشخاص حقوقی، جرائم این اشخاص صدمات و خسارت‌های جبران‌ناپذیری به بار خواهد آورد و در نهایت «جرم‌انگاری در پرتو سیاست جنایی مشارکتی» که اعمال آن در مورد جرائم سایبری هم ممکن و هم ضروری است ضمن کاستن از بار سنگین دستگاه عدالت کیفری به‌دستیابی به یک قانون کارآمد کمک خواهد کرد.

منابع و مآخذ

۱. الهی‌منش، محمدرضا و ابوالفضل سدره‌نشین (۱۳۹۱). *محشای قانون جرائم رایانه‌ای*، چاپ اول، تهران، انتشارات مجد.

۲. بکاریا، سزار (۱۳۸۰). *رساله جرائم و مجازات‌ها*، ترجمه محمدعلی اردبیلی، چاپ دوم، تهران، انتشارات میزان.

۳. پاکزاد، بتول (۱۳۷۵). «جرائم رایانه‌ای»، پایان‌نامه کارشناسی ارشد، دانشگاه شهید بهشتی.

۴. پیکا، ژرژ (۱۳۹۰). *جرم‌شناسی*، ترجمه علی حسین نجفی ابرندآبادی، چاپ دوم، تهران، انتشارات میزان.

۵. توکل، محمد و ابراهیم کاظم‌پور (۱۳۸۴). *دگرگونی‌های اجتماعی در یک جامعه اطلاعاتی*، تهران، انتشارات کمیسیون ملی یونسکو.

۶. جلالی‌فراهانی، امیرحسین (۱۳۸۳). «پیشگیری از جرائم رایانه‌ای»، مجله *حقوقی دادگستری*، ش ۴۷.

۷. ـــــــ (۱۳۸۴). «پیشگیری وضعی از جرائم سایبری در پرتو موازین حقوق بشر»، مجله *فقه و حقوق*، سال دوم.

۸. ـــــــ (۱۳۸۹). *کنوانسیون جرائم سایبری و پروتکل الحاقی آن*، چاپ اول، تهران، انتشارات خرسندی.

۹. جمشیدی، علیرضا (۱۳۹۰). *سیاست جنایی مشارکتی*، چاپ اول، تهران، انتشارات میزان.

۱۰. جوان‌جعفری، عبدالرضا (۱۳۸۵). «جرائم سایبر و چالش‌های نوین سیاست کیفری»، مجموعه *مقالات همایش جهانی شدن حقوق و چالش‌های آن*، مشهد، دانشگاه فردوسی.

۱۱. جوان‌جعفری، عبدالرضا و مهدی سیدزاده ثانی (۱۳۹۱). *رهنمودهای عملی پیشگیری از* جرم، معاونت پیشگیری از وقوع جرم قوه قضائیه، چاپ اول، تهران، انتشارات میزان.

۱۲. حاجی‌ده‌آبادی، احمد (۱۳۸۹). «مقررات کیفری لایحه حمایت از خانواده در بوته نقد»، مطالعات *راهبردی زنان* (کتاب *زنان* سابق)، ش ۴۸.

۱۳. حاجیلی، محمود (۱۳۸۸). *وضعیت فناوری ارتباطات در حوزه جوانان*، دبیرخانه شورای عالی اطلاع‌رسانی.

۱۴. حبیب‌زاده، محمدجعفر و اسماعیل رحیمی‌نژاد (۱۳۸۷). «مجازات‌های نامتناسب مجازات‌های مغایر با کرامت انسانی»، فصلنامه *حقوق دانشگاه تهران*، دوره ۳۸، ش ۲.

۱۵. حبیب‌زاده، محمدجعفر و امیرحمزه زینالی (۱۳۸۴). «درآمدی بر برخی محدودیت‌های عملی جرم‌انگاری»، *نامه حقوقی*، جلد اول، ش ۱.

۱۶. حسن‌بیگی، ابراهیم (۱۳۸۴). *حقوق و امنیت در فضای سایبر*، تهران، مؤسسه مطالعات و تحقیقات بین‌المللی ابرار معاصر.

۱۷. رستمی، ولی (۱۳۸۶). «مشارکت مردم در فرایند کیفری» (بررسی سیاست جنایی کشورهای غربی)، فصلنامه *حقوق دانشگاه تهران*، سال ۳۷، ش ۲.

۱۸. رضوی، محمد (۱۳۸۶). «جرائم سایبری و نقش پلیس در پیشگیری از این جرائم و کشف آنها»، فصلنامه *دانش انتظامی*، سال نهم، ش ۱.

۱۹. زیبر، اولریش (۱۳۹۰). *جرائم رایانه‌ای*، چاپ دوم، تهران، انتشارات گنج دانش.
۲۰. زینالی، امیرحمزه (۱۳۸۷). «ارزیابی گستره مداخلات قانونگذار کیفری ایران در حوزه آسیب‌ها و انحرافات اجتماعی»، فصلنامه علمی پژوهشی *رفاه اجتماعی*، سال نهم، ش ۳۴.
۲۱. سادوسکای، جورج، جیمز اکس دمپزی، آلن گرین برگ، جی مک باربارا و آلن شوارتز (۱۳۸۴). *راهنمای امنیت فناوری اطلاعات*، ترجمه مهدی میردامادی، زهرا شجاعی و محمدجواد صمدی، دبیرخانه شورای عالی اطلاع‌رسانی.
۲۲. سلیمی، احسان (۱۳۹۱). «خطر مضاعف جرائم رایانه‌ای»، مجموعه *مقالات اولین کنگره فضای مجازی و آسیب‌های اجتماعی نوپدید*، تهران، انتشارات وزارت رفاه و تأمین اجتماعی.
۲۳. شمس‌ناتری، محمدابراهیم، وحید ابوالمعالی و زهراسادات علیزاده (۱۳۹۰). «ویژگی‌های جرم‌انگاری در پرتو اسناد و موازین حقوق بشر»، فصلنامه *راهبرد*، سال بیستم، ش ۵۸.
۲۴. شیرزاد، کامران (۱۳۸۸). *جرائم رایانه‌ای از دیدگاه حقوق جزای ایران و حقوق بین‌الملل*، چاپ اول، تهران، نشر بهینه.
۲۵. فضلی، مهدی (۱۳۸۹). *مسئولیت کیفری در فضای سایبر*، چاپ اول، تهران، انتشارات خرسندی.
۲۶. کلارکسون، کریستوفر (۱۳۹۰). *تحلیل مبانی حقوق جزای عمومی*، ترجمه حسین میرمحمد صادقی، چاپ اول، انتشارات جنگل.
۲۷. گلدوزیان، ایرج (۱۳۸۶). *بایسته‌های حقوق جزای عمومی*، جلد اول، دوم و سوم، چاپ پانزدهم، تهران، نشر میزان.
۲۸. محمودی‌جانکی، فیروز (۱۳۸۸). *نظام کیفردهی هدف‌ها و ضرورت‌ها، تازه‌های علوم جنایی* (مجموعه مقالات)، چاپ اول، تهران، انتشارات میزان.
۲۹. نجابتی، مهدی (۱۳۷۹). «نقش طراحی واحدهای مسکونی در پیشگیری از جرم»، مجله *امنیت*، سال چهارم، ش ۱۵ و ۱۶.
۳۰. نوبهار، رحیم (۱۳۸۷). *حمایت حقوق کیفری از حوزه‌های عمومی و خصوصی*، انتشارات جنگل.
۳۱. یزدانی‌زنور، هرمز (۱۳۸۸). «حریم خصوصی در فضای سایبر»، مجموعه *مقالات حقوق فناوری اطلاعات و ارتباطات؛ گرامیداشت مرحوم دزیانی*، گردآوری امیرحسین جلالی فراهانی، چاپ اول.

32. Bartholomew, Mitchell K., Sarah J. Schoppe-Sullivan, Michael Glassman, Claire M. Kamp Dush and Jason M. Sullivan (2012). "New Parent's Facebook Use at the Transition to Parenthood", *Family Relations*, Vol. 61, No. 3.
33. Halder, D. and K. Jaishankar (2010). *Cyber Crime and Victimization of Women: Laws, Rights, and Regulations*, Hershey, PA, USA: LGL Global.
34. Hutton, S. and S. Haantz (2003). "Cyber Stalking", Retrieved from http://www.nw3c.org.

35. Jaishankar, K. (2011). *Cyber Criminology, Exploring Internet Crimesand Criminal Behavior*, Boca Raton, CRC Press.

36. Jaishankar, K. and Uma V. Sankary (2005). "Cyber Stalking: A Global Menace in the Information Super Highway", *ERCES Online Quarterly Review*, 2 (3), Retrieved from http://www.erces.com/journal/articles/archives/Volume2/v03/v02.htm.

37. Keenan, Patrick James (2006). "The New Deterrence: Crime and Policy in the Age of Globalization", *Iowa Law Review*, Vol. 91, Available at SSRN: http://ssrn.com/abstract.

38. Mitchell, K., D. Finkelhor and J. Wolak (2003). "The Exposure of Youth to Unwanted Sexual Material on the Internet: A National Survey of Risk, Impact. and Prevention", *Youth and Society*, 34.

39. _____ (2007). "Youth Internet Users at Risk for the more Serious Online Sexual Solicitations", *American Journal of Preventive Medicine*, 32.

40. O'Connell, R., C. Barrow and S. Sange (2002). *Young People's Use of Chat Rooms: Implications for Policy Strategies and Programs of Education*, Preston, United Kingdom, University of Central Lancashire.

41. Quayle, E. and M. Taylor (2003). "Model of Problematic Internet Use in People with a Sextual Interest in Children", *Cyber Psychology and Behavior*, 6.

42. Reno, J. (1999). "Report on Cyber Stalking: A New Challenge for Law Enforcement and Industry", Retrievedfrom http://www.usdoj.gov/criminal/cybercrime/cyberstalking.htm.

43. Schonsheck, jonathan (1994). *On Criminalization; An Essay in the Philosophy of the Criminal Law,* Netherland, Kluwer Academic Publisher.

44. The Guidelines for the Prevention of Crime (Council Resolution 2002/13 annex).

45. Wolak, J., K. Mitchell and D. Finkelhor (2007). "Unwanted and Wanted Exposure to Online Pornography in National Sample of Youth Internet Users", *Pediatrics*, 119.

46. www.worldinternetproject.net.

47. Ybarra, M., K. Mitchell, D. Finkelhor and J. Wolak (2007). "Internet Prevention Messages: Targeting the Right Online Behaviors", *Archives of Pediatric and Adolescent Medicine*, 161.