مجله علمی پژوهش در حقوق، فقه، فلسفه و الهیات ، شماره ۱۴ ، زمستان ۱۳۹۷جلد۲، ص ۶۷-۴۳
http://www.jrse.ir

مجله علمی پژوهش در حقوق، فقه، فلسفه و الهیات (سال چهارم)
شماره ۱۴ / زمستان ۱۳۹۷ / ص ۶۷-۴۳

راهبردهای پاسخ دهی قضایی کیفری به جرایم ارتکابی در فضای مجازی

سید نعمت اله موسوی[1] سیده زهره موسوی[2]

[1]دکتری دانشگاه علامه طباطبایی وعضو هیأت علمی دانشگاه
[2]دانشجوی کارشناسی ارشد فقه و مبانی حقوق واحد تهران جنوب
نویسنده مسؤول:

سید نعمت اله موسوی

چکیده

فناوری اطلاعات تمام ابعاد زندگی اجتماعی، اقتصادی، فرهنگی و از جمله حقوق کیفری را تحت تأثیر عمیق خویش قرار داده است.یکی از مشکلاتی که جامعهٔ بشری بطور جدی با پیامدهای آن دست و پنجه نرم می‌کند و روز به روز بر مشکلات ناشی از آن افزوده می‌شود، در دست گرفتن ابتکار عمل‌های سایبری از سوی برخی هنجارشکنان است. پیش‌بینی ضمانت اجراهای کیفری در مجموعه‌ای به نام قوانین کیفری، علاوه بر حفظ و پایداری نظم وامنیت جامعه،موازین حقوق بشری شهروندان راهم تضمین می‌کند؛به ویژه در حوزه‌های جدیدی مانند فناوری اطلاعات و ارتباطات که در مواردی شهروندان نمی‌دانند کدام افعال را مرتکب نشوند و از انجام کدام اعمال سرپیچی نکنند. بدیهی است که بهره‌وری ضمانت اجراهای کیفری علیه جرایم ارتکابی در فضای مجازی در گرو مطالعه‌ای عمیق، بسیط و چندبُعدی بود. این مقاله به بیان عوامل و الزامات تأثیرگذار درتعیین مجازات ازسوی قاضی در جرایم ارتکاب در فضای مجازی پرداخته است. مطابق نتایج این پژوهش، در عرصهٔ ضمانت اجراهای کیفری، علاوه بر ضرورت اصلاح و بازنگری نظام‌مند و پیوستهٔ قوانین کیفری و روزآمدسازی آن‌ها برپایهٔ نوآوری‌ها و پویایی‌های سایبری و حفظ پاسخ‌گویی نظام عدالت کیفری در برابر تهدیدهای جنایی، ضروری است . سیاست کیفری این عرصه نیز متناسب با شرایط، اقتضائات و ملاحظات حاکم بر آن بازتعریف شود . صرف‌نظر از اینکه کیفرهای رایجی همچون حبس و جزای نقدی نسبت به سایر جرایم تا چه‌اندازه از بازدارندگی، تناسب و اثربخشی برخوردارند، با توجه به ویژگی‌های متمایز جرایم و کنشگران جنایی سایبری، می‌توان به دستاوردهای آن‌ها در این حوزهٔ خاص نیز امیدوار بود. بر این اساس، برای رشد کارآیی و اثربخشی ضمانت اجراهای کیفری، اجرایی بودن برخی نظریه‌های نوین حقوق کیفری را می‌توان آزمود و کاستی‌ها و نارسایی‌های آن را به آزمون گذارد. از جملهٔ این آموزه‌ها، عدالت ترمیمی است که افزون بر بازگرداندن مرتکب به جامعه، توجه اصلی آن، حمایت همه‌جانبه از بزه‌دیده می‌باشد؛ با امعان‌نظر به شرایط خاص و منحصربه‌فرد حاکم بر فضای سایبر،ویژگی‌های شخصیتی مرتکبان انواع جرایم سایبری،میزان زیان‌های مادی و معنوی عموماً گسترده‌ای که به بار می‌آورند و تحول ساختار نظام عدالت کیفری ملی ، طراحی مجموعه ساختارمند نظام پاسخ‌دهی به جرایم فضای مجازی که در عین تضمین سلامت جامعه، از تحمیل هزینه‌های ناشایست یا بروز پیامدهای ناگوار نیز جلوگیری کند،ضرورت دارد.

کلیدواژه ها:فضای مجازی،نیمرخ جنایی،پاسخ کیفری،پاسخ غیرکیفری عدالت ترمی

مقدمه

پیدایش و ظهور اشکال مدرن بزهکاری طی سالیان اخیر،تنوع و کثرت در اعمال تدابیر،واکنش ها و رویکردهای مختلفی را در پی داشته است. یکی از پدیده‌های شگفت‌انگیز معاصر که در بروز یک تحول جهانی نقشی اساسی ایفا کرده است، «فناوری اطلاعات و ارتباطات» است. بیش از دو دهه از کاربری گسترده و روزافزون سامانه‌های رایانه‌ای و همچنین ارتباطات الکترونیکی، به ویژه سیار و داده‌ای، و دسترسی شهروندان ایرانی به شبکه‌های اطلاع‌رسانی رایانه‌ای، بویژه شبکهٔ جهانی اینترنت می‌گذرد و متناسب با رشد ضریب نفوذ دسترسی، یادگیری الکترونیکی و همچنین تأمین برنامه‌ها و نرم‌افزارهای کاربردی بومی موردنیاز آن‌ها، امور خرد و کلان اجتماعی به دنیای سایبر راه یافته‌اند و هم‌اینک کمتر حوزه‌ای مانده که جلوهٔ الکترونیکی آن نمایان نشده باشد. از دیگر سو، به دلیل حذف محدودیت‌های مکانی و مرزی در معماری فضای سایبر از گذر پیدایش ارتباطات الکترونیکی،[1] رایانه‌های سراسر گیتی توانستند بسان نوع بشر با یکدیگر ارتباط زنده و پویایی برقرار کنند و این اتصال و ارتباط یکپارچه، خود به خود شبکه‌ای جهانی را پدید آورده که انسان‌های آغاز هزارهٔ سوم را برآن داشته تا بسیاری از جنبه‌های زندگی خاکی‌شان را به این دنیا منتقل کرده و یک زندگی دوم[2] را رقم بزنند.[3]

بی‌تردید این وضعیت با بهینه‌سازی باورنکردنی امور، افق جدیدی را در مقابل جامعهٔ بشری گشوده است. اما ویژگی‌های منحصربفرد آن فرصت‌های مغتنمی را برای هنجارشکنان پدیدآورده است. این‌چنین کوچ فراگیر و همگانی به دنیای نوپدید سایبر، بهمراه خود ناهنجاری‌ها و هنجارشکنی‌های زیان‌بار مادی و معنوی دنیای خاکی[4] را نیز آورده و حتی جلوهٔ کارآمدتر و اثربخش‌تری نیز به آن‌ها بخشیده است. چراکه هنجارشکنان، همانند دیگران و البته شاید بهتر از آن‌ها، از توانمندی‌ها و مزیت‌های منحصربفرد این فضا برای پیشبرد اهداف شوم و تبهکارانه‌شان بهره‌برداری می‌کنند.

این گوناگونی آماج‌ها در فضای سایبر، درکنار سستی تدابیر و ابزارهای امنیتی حفاظت از سامانه‌ها و داده‌ها، موجب آسیب‌پذیری بیشتر و رشد خطرپذیری این فضا شده است. بزه‌کار، برای ارتکاب جرایم رایانه‌ای از یک سو بر فرصت‌هایی که فضای سایبر به عنوان یک جهان نوپدید پیش روی وی نهاده، تکیه می‌کند و از رهگذر مجازی انگاشتن این فضا و هرچه در آنست، واقعیت‌ها و ارزش‌های اجتماعی آن را نادیده گرفته و به لطف گمنامی اعطاشده دراین فضا با بهره‌گیری ازابزارهای پنهان‌نگاری[5] و رمزنگاری،[6]درمقایسه با جهان خاکی بسیار آسان-تر و کم‌هزینه‌تر[7] مرتکب جرم می‌شود.

تمامی این امور، معضلات نوینی‌اند که بخش‌های مختلف نظام حقوق کیفری را به چالش کشیده‌اند. بزه در فضای مجازی به دلیل تفاوت‌هایی که با بزه‌های دنیای واقعی دارد نیازمند قوانین خاص متناسب با فناوری‌هایی است که در چشم به هم زدنی تغییر کرده و باید در راستای تحولات، قوانین آن وضع شود تا بتوان مجازاتی درخور خلاف انجام شده را برای آن در نظر گرفت. در واقع، آنچه که باید در اینجا مورد توجه قرار گیرد، نوع و میزان واکنش کیفری در قبال این طیف از جرایم است. قدری تأمل در مفهوم و ماهیت جرایم سایبری آشکار می‌سازد که مقابلهٔ کیفری با عوامل آن‌ها تفاوت‌های اساسی با سایر مرتکبان جرایم دارد. البته در مواردی که وجوه اشتراکی وجود دارد، باید از تجربیات موجود بهره برد.

توجه به اینگونه مسایل آشکار می‌سازد که بهره‌وری ضمانت اجراهای کیفری علیه جرایم سایبری در گرو مطالعه‌ای عمیق، بسیط و چندبُعدی است. لذا باید از فرصت‌های موجود کمال بهره‌برداری را به عمل آورد و در عین حال به ظرفیت‌سازی لازم نیز اندیشید.

این تحقیق راهبردهای پاسخ دهی قضایی کیفری به جرایم ارتکابی در فضای مجازی هدف بررسی و تحلیل خویش قرار داده است. امروزه کمتر کسی است که با این گونه هنجارشکنی‌های زیان‌بار آشنا نشده یا دست کم گونه‌هایی از آن‌ها را تجربه نکرده باشد. تفاوت‌های جرایم ارتکابی در فضای مجازی با جرایم سنتی به گونه‌ای است که رویکرد کیفری متعارف و اصول و مبانی شناخته شده آن برای مقابله با این

1. Electronic Communication
2. Second Life

۳. پیکا، جرج، «**جرم‌شناسی**»، ترجمهٔ نجفی ابرندآبادی، علی‌حسین، چاپ نخست، تهران، نشر میزان، ۱۳۹۵، ۱۰.

4. Terrestrial World
5.Steganography
6. Encryption/Cryptography

7. به هنگام محاسبهٔ هزینهٔ جرم دو مؤلفه مورد توجه قرار می‌گیرد: ۱. نتیجه‌ای که عاید می‌شود؛ و ۲. احتمال دستگیری و مجازات.

جرایم پاسخگو نیستند و پاسخ‌های تعیین شده بیشتر جنبه‌ای گذرا، تسکینی و جبرانی دارد و بازدارندگی مطلوب را که هدف غایی نظام پاسخ‌ها است ندارند.

برای دست‌یابی به الگویی منسجم و قابل اتکا در پاسخ‌دهی به جرایم ارتکابی در فضای مجازی باید عوامل گوناگونی را مورد بررسی و تجزیه و تحلیل قرار داد. برای مثال، تنوع ضمانت‌اجراهای کیفری پیش‌بینی شده از سوی قانون‌گذار چقدر است؟ مرتکبان جرایم هدف از لحاظ شخصیتی و موقعیت اجتماعی چه وضعیتی دارند؟ به طور مشابه وضعیت بزه‌دیدگان این جرایم چگونه است؟ چه تدابیر دیگری غیر از پاسخ‌های کیفری برای واکنش نسبت به اینگونه جرایم قابل استفاده هستند؟ آیا عوامل دیگری از جمله بزه‌دیدگان و آماج جرایم در تعیین پاسخ‌ها نسبت به جرایم سایبری مؤثرند؟

1) نظام پاسخ‌ها؛ ماهیت و اقسام

برپایهٔ یک نگاه جامع و فراگیر در مبارزه همه‌جانبه با جرایم، نظام سیاست جنایی مجموعه‌ای از تدابیر پیشگیرانه یا کنشی و سزاده یا واکنشی است که از سوی جامعه در برابر آن‌ها اتخاذ می‌شود. در این نظام، «پاسخ» عبارت است از هر نوع واکنشی که جامعه در مقابل رفتار ضد اجتماعی اتخاذ می‌کند؛ در هر کشوری برخی رفتارها جرم تلقی می‌شوند که ابتدایی‌ترین عکس العمل در مقابل آن‌ها، اجرای مجازات است. در واقع، تنها آن دسته از رفتارها یا ترک رفتارهایی باید مجازات شوند که از سوی قانون‌گذار تعریف شده‌اند. بنابراین، نه تنها تعریف جرایم در صلاحیت ذاتی و انحصاری قانون‌گذار است، بلکه تدبیرهای قابل اتخاذ در برابر آن‌ها، اعم از پیشگیرانه و واکنشی نیز باید با اجازهٔ آن صورت گیرد.

تا پیش از پیدایش مکتب تحققی، ویژگی سزادهی کیفر تنها مؤلفه‌ای بود که در نظام عدالت کیفری سرکوبگرانه جایگاه داشت؛ اما با تولد این مکتب، تحولات شگرفی در واکنش به پدیده مجرمانه به وجود آمد و تدبیرهای اصلاحی ـ درمانی محکومان به منظور بازپروری و بازپذیری آن‌ها جهت بازگشت بدون آسیبشان به اجتماع نیز پیش‌بینی شد. در واقع نظام عدالت کیفری دو شأن یافت: سرکوبگر و اصلاحی ـ درمانی. دست آخر گروه دیگری که بسیاری از نظام‌های حقوقی خود را پیرو آن می‌دانند و سرمایه‌های خود را بسوی آن سوق داده‌اند، تأکید بر پیشگیری در کنار ضمانت اجراهای کیفری را در دستور کار خویش قرار داده‌اند؛ با این باور که چنانچه جامعه در عرصهٔ پیشگیری از وقوع جرایم پیروز شود، نیازی به هزینه‌های گزاف اعمال ضمانت اجراهای کیفری نیست، گرچه نمی‌توان از آن‌ها چشم پوشید و جامعه به یک نظام عدالت کیفری مقتدر، آگاه و مستقل نیازمند است.

1-1 نظام دوگانه پاسخ‌ها

در این بند، انواع گوناگون پاسخ به پدیده مجرمانه احصا و بررسی شده است. پیش از ورود به بحث، توضیح این نکته ضروری به نظر می‌رسد که تقسیم دوگانه و این‌چنینی نظام پاسخ‌ها لزوما به معنای تفکیک صد در صدی و غیر قابل اشتراک این پاسخ‌ها نیست. نگارنده اذعان دارد که ممکن است این طبقه‌بندی‌ها در برخی موارد با یکدیگر همپوشانی داشته باشند و نوع مشخصی از پاسخ در آن واحد در چند گروه قرار بگیرد. برای مثال، ممکن است یک پاسخ هم غیر کیفری، هم خاص و هم پیشینی باشد. با این حال، در این قسمت با ذکر انواع پاسخ‌ها و طبقه‌بندی دو دویی آن‌ها تلاش شده تا ذهن خواننده محترم با انواع پاسخ‌ها آشنا شده و در نظام وسیع و گسترده پاسخ‌ها به طور منظم و طبقه‌بندی شده جایابی گردد.

1-1-1 پاسخ‌های کیفری و غیرکیفری

از میان انواع گوناگون پاسخ به پدیده مجرمانه، کیفر رایج‌ترین پاسخ به جرم است؛ تا آنجا که مفهوم جرم در ذهن افراد مجازات و کیفر را در پی دارد. با این حال درک درست مفهوم پاسخ‌های کیفری و وجه افتراق آن‌ها با پاسخ‌های غیرکیفری در گرو پاسخ به این پرسش است که معیار تشخیص پاسخ کیفری از غیر کیفری چیست؟ گفته می‌شود که کیفر آن واکنشی است که موجب تحصیل درد، رنج، سلب آزادی و محدودیت نسبت به مال و جان می‌شود. لیکن همواره اینگونه نیست و در بسیاری از موارد واکنش کیفری به جرم به معنای واقعی کیفر یا مجازات نبوده و بیشتر جنبه الزام به مهارت آموزی، اقامت یا عدم اقامت در مکان معین، اشتغال به حرفه‌ای خاص و ... دارد. نکته جالب توجه اینجاست که در مجموعه قوانین جزایی کشور ما حتی توبیخ و تذکر و یا الزام به اقامه نماز در مساجد نیز در ردیف مجازات‌های تکمیلی قرار گرفته و به نوعی پاسخ کیفری به جرم محسوب می‌شود. بنابراین واکنش به پدیده مجرمانه چه در قالب سرکوبگرانه و سزاده آن و چه در

قالب اصلاحی آن هر دو پاسخ کیفری به جرم به شمار می‌آیند. در برابر، آنجا که هدف از واکنش جرم از ارعاب و سزادهی و حتی اصلاح و بازپروری به ترمیم آسیب‌های وارده و مشارکت طرفین پدیده جنایی تغییر می‌یابد، آنجا که پاسخگویی بزهکار، بازسازی آسیب‌های وارد شده به بزه‌دیده و همیاری کامل بزه‌دیده، بزهکار و جامعه هدف فرایند کیفری قرار می‌گیرد، با «پاسخ‌های غیرکیفری» به جرم مواجه هستیم.

کیفر، ابزار اجرایی گفتمان عدالت کیفری و ترمیم آسیب ابزار اجرایی گفتمان عدالت ترمیمی است. کیفر ابزار قهرآمیز جامعه برای اجرای عدالت و برقراری نظم است که اجرای آن باید با احتیاط کامل صورت بگیرد. از این رو لازم است تا جز در مواردی که نوع و میزان آن از سوی حاکم شرع مشخص شده است، به مسألهٔ «بهره‌وری کیفری» توجه کرد؛ به این معنا که با هزینهٔ کمتر درصد تحقق اهداف کیفری افزایش یابد. از جملهٔ این اهداف می‌توان به اصلاح مجرمان در پرتو بازپذیرسازی اجتماعی آن‌ها، پیشگیری از تکرار جرم در پرتو ارعاب‌انگیزی و پیشگیری از ارتکاب جرم از سوی سایر افراد جامعه در پرتوی عبرت‌آموزی اشاره کرد.

برای دست‌یابی به این مهم باید عوامل گوناگونی را مورد بررسی و تجزیه و تحلیل قرار داد. برای مثال، تنوع ضمانت‌اجراهای کیفری پیش‌بینی شده از سوی قانون‌گذار چقدر است؟ مرتکبان جرایم از لحاظ شخصیتی و موقعیت اجتماعی چه وضعیتی دارند؟ به طور مشابه وضعیت بزه‌دیدگان این جرایم چگونه است؟ برای مثال، گروهی از دانشمندان حقوق کیفری و جرم‌شناسی، جرایم را به دو دستهٔ جرایم اصطلاحاً «فسفری» و «کلسیمی» تقسیم کرده‌اند. گروه نخست که از آن‌ها به مجرمان «یقه سپید» نیز یاد می‌شود، با اندیشهٔ خود هنجارهای اجتماعی را نقض می‌کنند، نمونهٔ آشکار آن کلاهبرداری است. اما گروه دوم که به مجرمان «یقه آبی» نیز موسومند، عمدتاً مرتکب جرایم خشونت‌بار می‌شوند. از این تقسیم‌بندی به ظاهر ساده نتایج ارزشمندی عاید می‌شود. برای مثال، گروه اول نسبت به گروه دوم از وضعیت مالی مطلوب‌تری برخوردارند و این مسأله باید بر نوع و میزان ضمانت‌اجراهای کیفری تأثیر گذارد. بنابراین، سیر تحول اجتماعی باید از سوی قانون‌گذاران کیفری مورد ملاحظهٔ مستمر قرار گیرد.

پاسخ‌های کیفری عمدتاً از سوی دولت، یعنی نهادهای رسمی با رعایت تشریفات، علیه پدیده مجرمانه اعمال می‌شود. در برابر، پاسخ‌های غیرکیفری پاسخ‌هایی برآمده از جامعه مدنی و نهادهای مختلف مردمی‌اند که بصورت غیر رسمی و با روش‌های مختلف در مدیریت پدیده مجرمانه و پاسخ به آن نقش‌آفرینی می‌کنند. این پاسخ‌ها که از آن‌ها تحت عنوان «پاسخ‌های غیرکیفری» یاد می‌شود، به منظور افزایش بهره-وری هرچه بیشتر پاسخ به پدیده مجرمانه و مشارکت دولت و جامعه مدنی به موازات یکدیگر برای اجرای سیاست جنایی پویا و اثربخش طراحی و اجرا می‌شوند. راهبردهای ترمیمی، بهره‌گیری از کارکرد نهادهای اجتماعی مانند مدارس و مساجد، افزایش و ارتقای کمی و کیفی برنامه‌های تلویزیونی و رشد آگاهی و سواد عمومی جامعه نسبت به موقعیت‌های جنایی، نمونه‌هایی از پاسخ غیرکیفری هستند.

2-1-1 پاسخ‌های سنتی و نوین

گرچه «کیفر» شایع‌ترین نوع پاسخ به جرم می باشد، اما علاوه برآن می‌توان ازسایر انواع پاسخ به جرم نیز یاد کردکه ضرورتا دارای ویژگی‌های مجازات یا کیفر نیستند.پاسخ‌های کیفری درمعنای سنتی شامل مجازات‌هایی می‌شوندکه یا به صورت بدنی برجسم و جان محکومٌ علیه بار می‌شود؛مانند:شلاق یا قطع عضو و یا شامل انواع مجازات‌هایی است که سایر جنبه‌های وجودی بزهکار، اعم از مال یا آزادی وی را هدف قرار داده یا وی را ملزم به جبران خسارت از بزه‌دیده می‌نماید. در برابر پاسخ سنتی، نوع نوینی از پاسخ به جرم وجود دارد که به عنوان پاسخ‌های اجتماعی نیز مطرح می‌شوند. در این گروه می‌توان از انواع جایگزین‌های حبس مانند تعلیق اجرای مجازات، حبس‌های خانگی یا نظام نیمه آزادی و همچنین مجازات‌های مستقلی همچون خدمات میانجی‌گری، خدمات عام‌المنفعه و رویکردهای نظارتی بر فرد بزهکار نام برد. در واقع وجه مشترک پاسخ سنتی و سایر انواع پاسخ به جرم، اینست که هر دو در مقام واکنش نسبت به جرایم و مجرمان

و توسط نهاد قضایی مورد حکم قرار گرفته و عمدتا توسط نهادهای وابسته به دستگاه عدالت کیفری همانند زندان، اجرای احکام، پلیس و ... به اجرا گذاشته می‌شود.

3-1-1 پاسخ‌های پیشینی و پسینی

طی دهه‌های اخیر، یکی از دگرگونی‌های بزرگی که در کشورها رخ داده، این است که برای ریشه‌کنی یا کاستن از میزان جرایم و زیان‌ها و آسیب‌های ناشی از آن‌ها، به جای تأکید بیشتر بر نظام عدالت کیفری و آزمودن گزینه‌های گوناگون برای کارآمدتر کردن آن و اثربخش‌تر کردن تدابیر کیفری، اندیشهٔ مبارزه با جرایم، به یک مرحله پیش‌تر، یعنی مرحلهٔ وقوع آن‌ها تمرکز یافته است. به عبارت دیگر، به جای اینکه جامعه و نظام عدالت کیفری به نمایندگی از آن در انتظار وقوع جرایم باشد و سپس وارد عمل شود، پیش‌دستی کرده و شرایط، موقعیت‌ها و عوامل جرم‌زا را از جامعه می‌زداید. به این ترتیب، در چنین شرایطی جامعه از رویکرد منفعلانه و صرفاً واکنشی خارج شده و موضعی فعالانه و کنش‌گر اتخاذ کرده است.

بر این اساس، می‌توان گفت پاسخ به جرم به دو گروه قابل تقسیم است: «پاسخ‌های پسینی و پاسخ‌های پیشینی». پاسخ‌های پسینی اصولاً جنبه واکنشی ویا دفاعی دارند و به عبارت دیگر پس از ارتکاب جرم ویا وقوع آن مورد توسل قرار گرفته ویا قابل استفاده می‌باشند. پاسخ‌های پیشینی به منظور پیشگیری از جرم و کاهش احتمال بزه و بزهکاری مورد استفاده قرار می‌گیرند[۸].

با تثبیت این رویکرد و دستیابی به یک اجماع نسبتاً جهانی راجع به آن، تاکنون الگوهای مختلفی از سوی صاحب‌نظران و فعالان این حوزه ارائه شده است. برخی از آن‌ها با الهام از سایر برنامه‌های مقابله با عوارض اجتماعی، نظیر پیشگیری از بیماری‌ها تدوین و برنامه‌ریزی شده‌اند. برخی دیگر، با گردآوری مزیت‌ها و ویژگی‌های تدابیر گوناگون، جلوهٔ تکامل‌یافته‌ای پیدا کرده‌اند و با نگاه جامع به تمامی عواملی که می‌توانند در پیشگیری از وقوع جرم مؤثر باشند، رویکرد نسبتاً جامع و فراگیری را اتخاذ کرده‌اند.

از میان تدابیر گوناگون پیشگیری از وقوع جرم، الگوی پیشگیری اجتماعی[۹] و وضعی[۱۰] از جرم جایگاه برجسته‌ای یافته است. لازم به یادآوری است، هم‌اکنون در اسناد گوناگون بین‌المللی و منطقه‌ای مبارزه با جرایم به اصطلاح شدید یا مهم، مانند سازمان‌یافتهٔ فراملی و فساد، پایه‌ریزی برنامه‌های پیشگیرانه براساس این الگو به چشم می‌خورد و در اسناد تفصیلی پشتیبان آن‌ها، نحوهٔ پیاده‌سازی اختصاصی اینگونه تدابیر شرح داده شده تا کشورهای عضو به آسانی آن‌ها را اجرا کنند و با مشکل خاصی مواجه نشوند.[۱۱]

4-1-1 پاسخ‌های دولتی و جامعوی

تقسیم‌بندی دیگر نظام پاسخ‌ها، پاسخ دولتی و پاسخ جامعوی است. در پاسخ دولتی که از رهگذر ساختار رسمی و برخاسته از هیات سیاسی حاکمه نشات می‌گیرد، نهادهای دولتی قضایی و اداری نظر به سیاست کلان حاکم بر خویش و با عنایت به سیاست‌ها و راهبردهای از پیش تعیین شده نظام سیاسی در برابر جرم و انحراف از خود پاسخی به نمایش می‌گذارند که مبتنی بر اصل وزین و بنیادین «قانونی بودن» است. زیرا، در پرتو همین اصل است که پاسخ دولتی نمایان می‌گردد و جلوه رسمی خود را به بازیگران و تابعان حقوقی نشان می‌دهد. در چنین حالتی، آن گاه که تابعی حقوقی یعنی بازیگر فعال اجتماعی در فراگرد اجتماع، ارزش‌ها و هنجارهای موصوف به جرم را نقض می‌کند، از

---

۸. غلامی، حسین، **کیفرشناسی (کلیات و مبانی پاسخ شناسی جرم)** ، تهران، نشر میزان، چاپ اول ۱۳۹۵. ص ۴۴

۹. Social Prevention

۱۰.Situational Prevention

۱۱.جلالی فراهانی، امیرحسین و بهره‌مند بگ‌نظر، حمید (مترجمان)، لانگست، پیتر و دیگران، «**برنامه‌های جهانی مبارزه با فساد**»، انتشارات مرکز پژوهش‌های مجلس شورای اسلامی، چاپ نخست، پاییز ۱۳۸۷، ص ۳۵۱ به بعد.

رهگذر نهادهای رسمی نظیر پلیس و محاکم به جزای کرده مجرمانه خویش خواهد رسید و با واکنش مطلوب آن نوع نظـام سیاسـی مواجـه می‌گردد.

با این حال، در پاسخ جامعوی، نوع واکنش به گونه‌ای دیگر نمودار می‌گردد و اگرچه می‌توان در این وادی نیز نهادهایی اما غیررسمی و مردم بنیاد متصور گشت، ولی از واکنش نظیر نهاد دولت، خبری نیست. در این وضعیت که به نوعی چهره غالب امر به معروف و نهـی از منکـر بـه صورت خاصی نمایان می‌شود، جامعه در پرتو ارزش‌ها و هنجارهای راسخ و نهادینه خویش، به شهروندان می‌آموزد که به چـه اعمـالی دسـت زند و از دستیابی به کدامین نباید سرباز زنند؛ در صورت تخلف نیز با چه پاسخ‌های احتمالی جامعه که در قالب «پاسخ‌های جامعوی» متبلور می‌گردند، مواجه خواهند شد.

2-1 پاسخ‌دهی کیفری؛ الگوی پیشتاز در پاسخ به پدیده جنایی

پاسخ کیفری یا مجازات در لغت به معنای جزا دادن و یا دانش آمده است.[۱۲] در اصطلاح حقوقی تعاریف متعددی بیان شده است. «تنبیه و کیفری است که بر مرتکب جرم تحمیل می‌شود...».[۱۳] مراد از پاسخ‌های کیفری پاسخ‌هایی است که نسبت به جرایم بالفعل یا بالقوه ابراز شده و یا قابل ارائه می‌باشند و باید توجه داشت که امروزه شخصیت افراد و موقعیت آن‌ها می‌تواند در مجازات آن‌ها مؤثر باشد ولی از جهت نظری همه افراد در مقابل قانون با یکدیگر مساوی هستند و اجرای کیفر بدون توجه به فرد باید انجام شود.[۱۴]

پیش‌بینی ضمانت اجراهای کیفری در مجموعه‌ای به نام قوانین کیفری، علاوه بر حفظ و پایداری نظم و امنیت جامعه، موازین حقوق بشری شهروندان را هم تضمین می‌کند، به ویژه در حوزه‌های جدیدی مانند فناوری اطلاعات و ارتباطات که در مواردی واقعاً شهروندان نمی‌دانند کدام افعال را مرتکب نشوند و از انجام کدام اعمال سرپیچی نکنند.

در این طبقه‌بندی، نظام پاسخ‌های کیفری از یک سو شامل واکنش‌های سزاگونه‌ای است که در قالب‌هایی مانند مجازات‌های حدی، قصاص، حبس، جزای نقدی و یا جایگزین‌های حبس بر مرتکب بار می‌شود؛ و از سوی دیگر، پاسخ‌های کیفری شامل مجموعه‌ای از تدابیر و اقدامات-اند که گاه به منظور جایگزینی کیفر و کاهش آثار زیانبار آن و گاه تحت تأثیر اصول بنیادین حقوق کیفری مانند اصل حداقل بودن حقوق جزا و در نتیجه توسل حداقلی به مجازات (به عنوان یکی از آثار و جنبه‌های اصل حداقل بودن)، توسط دستگاه عدالت کیفری و در برخی موارد با مشارکت بزهکار یا جامعه مورد توسل قرار می‌گیرد. تعویق صدور حکم، تعلیق مجازات، نظام نیمه آزادی نمونه‌هایی از وجه دیگر پاسخ‌های کیفری‌اند. پاسخ‌هایی که نسبت به مجرمین بالقوه یا بالفعل اعمال شده است و یا قابل اعمال هستند اما لزوما دارای وصف و ماهیت کیفری نمی‌باشد. این نوع پاسخ‌ها نیز فقط نسبت به بزهکار اعمال می‌شوند و نسبت به سایر اشخاص صرف نظر از هر گونه رابطه‌ای که با بزهکار دارند چنانچه در وقوع جرم مباشرت یا معاونتی نداشته باشند قابل اعمال نیستند. راهبردهای غیرکیفری نسبت به پدیده مجرمانه، ماهیتی متفاوت از مجازات دارند؛ بدین معنا که رنج آور و محروم کننده نبوده و با مشارکت شخص بزهکار برای اصلاح هرچه بیشتر وی و ترمیم خسارت‌های حاصل از جرم به ویژه خسارت‌های بزه‌دیده اعمال می‌شوند. در این طبقه از پاسخ‌ها به طور خاص می‌توان به راهبردهای ترمیمی اشاره کرد.

1-2-1 هدف‌های پاسخ کیفری

پاسخ‌های کیفری ویژگی‌هایی دارند که از یک طرف می‌توانند موجبات آزار و اذیت شخص را فراهم نموده و او را از جامعه طرد کنند و از طرف دیگر می‌توانند موجب اصلاح شخص شوند. در حقوق جزای اسلامی به فطرت انسانی توجه فراوانی شده است و آن را پاک و منزه معرفی کرده است. در حاکمیت اسلام، برای ارشاد مجرمین، راه‌های فراوانی در نظر گرفته شده است اما گاهی اسلام، در آخرین مرحله، اجازه اعمال پاسخ‌های کیفری داده است.

---

[۱۲]. عمید، حسن، **فرهنگ فارسی**، تهران، انتشارات امیرکبیر، ۱۳۸۷، ص ۹۴۷.

[۱۳]. علی آبادی، عبدالحسین، **حقوق جنایی**، جلد دوم، تهران، انتشارات فردوسی، ۱۳۶۹، ص ۱.

[۱۴]. نوربها، رضا، **زمینه حقوق جزای عمومی**، تهران، گنج دانش، ۱۳۸۷، ص ۳۷۴.

در هر نظام حقوقی، پاسخ‌های کیفری به دلیل ارتباط نزدیکی که با جان، مال و ناموس مردم دارند از اهمیت بالایی برخوردار می‌باشند. زیرا از یک طرف با تعیین کیفر و نحوه رسیدگی به جرایم و شیوه اجرای مجازات‌ها و از طرف دیگر با حفظ حیثیت و کرامت انسانی می‌تواند نقش مؤثری را در نظم و امنیت اجتماعی ایفاء نماید.

نظام کیفری اسلام یک نظام دوگانه و ترکیبی است که هم به اجتماع و هم به افراد جامعه توجه دارد. در این نظام مجازات‌های مختلف و متفاوتی وجود دارند که هدف از هرکدام در برخی موارد متفاوت است. مثلا در مجازات قصاص، حفظ حیات انسانی، جلوگیری از انتقام خصوصی و تشفی خاطر بزه‌دیده مد نظر می‌باشد. اما در مجازات‌هایی مثل تعزیرات، بیشتر اصلاح بزهکار، اجرای عدالت و بیم تجری دیگران مد نظر می‌باشد. هر چند که برخی از این موارد در قصاص هم وجود دارد اما در قصاص، اصلاح بزهکار مد نظر نمی‌باشد.

صاحب کتاب احکام زندان در اسلام چنین می‌گوید: «با توجه به اینکه مناط در کیفر دادن، ملاحظه صلاح و فساد جامعه است، پس هر گونه عقوبتی که به این هدف تحقق بدهد،مشروع خواهد بود به شرط اینکه از چهارچوبی که شارع تعیین کرده خارج نباشد و به این منظور شارع تعزیرات را در اختیار امام قرار داده است.[۱۵]

2-2-1 اقسام پاسخ کیفری

در یک طبقه‌بندی کلی، می‌توان پاسخ کیفری به پدیده مجرمانه را در سه دسته جای داد:

۱. پاسخ کیفری سزاده

۲. پاسخ کیفری ارفاقی

۳. پاسخ کیفری تأمینی و تربیتی

مطابق قانون مجازات اسلامی مصوب ۱۳۹۲ کیفرهای اصلی عبارتند از حدود، قصاص، دیات و تعزیرات. این کیفرها همان‌هایی هستند که آن‌ها را در دسته پاسخ‌های کیفری سزاده قرار می‌دهیم. از گونه‌های مختلف کیفر، سه قسم آن برگرفته از شرع مقدس می‌باشد، حد، قصاص و دیه. اما تعزیر با شرع تطبیق داده شده است به عبارت دیگر تعزیر نیز به صورت غیرمستقیم از شرع اقتباس شده است.

با این حال، در طول جریان دادرسی،قاضی از ابتدای رسیدگی تا زمان صدور حکم ممکن است از نهادهای مختلفی برای اعمال کیفر استفاده کند که هدف از استفاده از همه نهادهای مزبور بازگشت بزهکار به جامعه و اصلاح نهایی اجتماع به وسیله دستگاه قضایی است و این برخورد خود نوعی جبران و اصلاح ساختارهای رفتاری افراد جامعه تلقی می‌شود. با توجه به اینکه امکان دارد اشخاص تحت شرایط خاصی مثل گفتار تحریک آمیز بزه‌دیده، وجود انگیزه شرافتمندانه در ارتکاب جرم و امثالهم مرتکب رفتار مجرمانه شده باشند و یا اینکه بلافاصله بعد از وقوع جرم ابراز ندامت نموده و یا اقرار مؤثری در حین تحقیق داشته باشند و یا اینکه شاکی اعلام گذشت نماید در چنین شرایطی نیاز به ارفاق و ایجاد فرصت و زمینه مناسب دارد تا مرتکب بار دیگر به جامعه برگردد. در اینجا بکارگیری تدابیری تحت عنوان «تدابیر ارفاقی» می‌تواند راه را برای برگشت بزهکار به جامعه به نحو مطلوب فراهم نماید.

استفاده از تدابیر ارفاقی مانند معافیت از مجازات، تعویق صدور حکم، تعلیق اجرای مجازات می‌تواند در جهت کاهش آسیب‌های جدی زندان به افراد زندانی، خانواده‌های زندانیان و جامعه کمک کند.

پاسخ‌های تأمینی و تربیتی نوع دیگری از پاسخ‌های کیفری‌اند که از آن‌ها تعریف‌های متعددی از سوی حقوقدانان و کارشناسان ارائه شده است. «اقدامات تأمینی و تربیتی، اقدامی است فردی، الزام آور و بدون رنگ اخلاقی و فقط برای افرادی به مورد اجرا گذاشته می‌شود که حالت خطرناک برای جامعه داشته باشد.»[۱۶] یا «این اقدامات تدابیر پیشگیرانه‌ای هستند که برای اصلاح مجرم، رفع حالت خطرناک و جلوگیری از ارتکاب جرم در آینده و بازسازی اجتماعی مجرم وضع می‌شوند. البته این اقدامات در مورد اشیاء خطرناک نیز قابلیت اجرا دارند

---

[۱۵]. واثلی، احمد، **احکام زندان در اسلام**، ترجمه محمد حسن بکایی، نشر فرهنگ اسلامی، ۱۳۶۷، ص ۲۰۳.

[۱۶]. شامبیاتی، **هوشنگ، حقوق جزای عمومی**، جلد دوم، تهران، انتشارات مجد، ص ۴۱۲.

و به طور کلی هدف تأمین امنیت جامعه را دنبال می‌کنند.»[۱۷] بنابراین می‌توان اظهار داشت اقدامات تأمینی، تدبیرهای فردی و یا وضعی الزامی بدون رنگ اخلاقی می‌باشند که در مورد افراد خطرناکی که نظم جامعه را با حالات و رفتار خود تهدید می‌کنند و یا نسبت به یک وضع خطرناک به موجب حکم دادگاه اتخاذ می‌شوند اطلاق می‌شود.

مکتب تحققی بنیانگذار اقدامات تأمینی و تربیتی می‌باشد. امروزه هیچ کشوری وجود ندارد که مجازات را امری بیهوده و عبث تلقی نماید و صرفاً اعتقاد به تجویز اقدامات تأمینی و تربیتی باشد. اجرای این اقدامات گاهی ممکن است از طریق جدا کردن مجرم از کسانی که توانایی بالقوه برای ارتکاب مجدد جرم را دارند صورت می‌گیرد، مثل نگهداری مجرمان دیوانه در تیمارستان، منع اشخاص خطرناک در نقاط معین، در قانون مجازات عمومی مصوب ۱۳۰۴ با اقتباس و الهام از قانون جزای فرانسه صرفاً مجازات و انواع مختلف آن پیش بینی شده بود ولی به تدریج اشکال جدیدی از واکنش بر ضد جرم وارد مقررات کیفری شد. اقدام تأمینی در کشور ما با اقتباس از قانون جزای ۱۹۳۷ میلادی سوئیس تهیه و در سال ۱۳۳۷ هجری شمسی به مجلس شورای ملی تقدیم شد و در نهایت در ۲۱ ماده تحت عنوان «قانون اقدامات تأمینی» در مورخ ۱۳۳۹/۲/۱۲ به تصویب مجلسین وقت رسید.

در حال حاضر در اکثر کشورها اقدامات تأمینی و تربیتی با کمیت و کیفیت گوناگون مورد پذیرش واقع شده و به مرحله اجرا در آمده است، نکته قابل توجه آن است که مجازات بیشتر و غالبا بر ضد جرم داده می‌شود در صورتیکه جهت‌گیری اقدامات تأمینی که پیشگیری فردی است باید از کیفرها تفکیک و در بخش خاصی از قوانین جزایی پیش‌بینی شود. در واقع جهت‌گیری اقدامات تأمینی و تربیتی جلوگیری از حدوث جرایم با اعمال راه‌های اصلاحی، درمانی، تربیتی و یا خنثی کردن خطرهای احتمالی اشخاص و یا اشیا و مؤسسه‌هایی است که وضعیت خطرناک (مجرمانه) دارند. همچنین از جمله مسایل مهم سیاست جنایی کیفرزدایی می‌باشد که بدنبال اقدامی غیرکیفری درباره عمل بزهکارانه است که اقدامات تأمینی و تربیتی از ابزار مهم سیاست جنایی محسوب می‌شود.

با این حال، نباید نادیده انگاشت که ادعای دوری مطلق ویژگی‌های اقدامات تأمینی و تربیتی از مجازات‌ها قابل پذیرش نیست. زیرا در کلیه اقدامات تأمینی نیز رنگی از ویژگی‌های مجازات می‌توان دید و به همین دلیل است که این اقدامات در زمره پاسخ‌های کیفری تقسیم‌بندی می‌شوند.[۱۸]

3-2-1 پیامدهای پاسخ کیفری

هر تدبیری که اندیشه و اجرا می‌شود، پیامدهایی[۱۹] دارد. در اینجا پیامد مفهومی فراتر از هزینه[۲۰] دارد و آسیب‌ها یا زیان‌های احتمالی را نیز دربرمی‌گیرد. پیامد یک تدبیر می‌تواند مادی یا معنوی و هریک از اینها می‌توانند مستقیم یا غیرمستقیم باشند؛ به این معنا که تنها کنشگران یا موضوعات[۲۱] آن‌ها را دربرگیرند یا اینکه به اشخاص یا موضوعات مرتبط یا وابسته به آن‌ها نیز سرایت یابند.

کیفر در مفهوم فراگیر خود و به عنوان یک تدبیر حاکمیتی نیز از این قاعده مستثنی نیست و با پیامدهای خرد و کلانی روبروست، تا آنجا که ممکن است جلوه‌ای فراملی و بین‌المللی نیز بیابد. یک تدبیر کیفری می‌تواند پیامدهای سیاسی، اجتماعی و اقتصادی زیان‌بار و حتی جبران-ناپذیری داشته باشد. لذا باید در تعیین نوع و میزان کیفرها ملاحظات بسیاری را درنظر داشت و براستی چنانچه این مسایل از نگاه واضعان احکام کیفری بگذرد، بسیار محتاطانه‌تر اقدام خواهند کرد.

علاوه‌براین، پیامدهای پیش روی کنشگران جرم، یعنی بزهکاران و بزه‌دیدگان را نیز نباید از نظر دور داشت. ممکن است پرسیده شود چرا پیامدهای پیش روی بزهکاران نیز باید مورد توجه قرار گیرد؟ پاسخ این پرسش را باید در حضور و نقش اجتماعی آن‌ها یافت. چنانچه با ابزار

---

[۱۷]. ابراهیمی، جواد، **بررسی محدوده اقدامات تأمینی و تربیتی در قانون مجازات اسلامی ۱۳۹۲ با مقایسه قانون مجازات اسلامی ۱۳۷۰**، پایان‌نامه دوره کارشناسی ارشد، دانشگاه قم، ۱۳۹۳، ص ۱۰.

[۱۸]. نوربها، رضا، **زمینه حقوق جزای عمومی**، پیشین، ص ۵۰۸.

[19]. Consequence

[20]. Cost

[21]. Subjects

کیفر به راندن بزهکار از جامعه می‌اندیشیم و قصد بازگرداندن او را نداریم، این احتمال را باید بدهیم که بطور مستقیم یا غیرمستقیم پیامدهایی را به جامعه تحمیل خواهیم کرد.

استفاده گسترده از حبس به منظور سلب توان بزهکاری، موجب حبس تعداد بسیار زیادی از بزهکارانی می‌شود که ضرورتاً نباید مشمول چنین کیفری قرار گیرند. این وضعیت موجب توسعه شبکه حبس و افزایش تعداد زندانیان و ازدحام جمعیت کیفری در زندان می‌شود که آثار و عواقب سوئی در مدیریت زندان، ایجاد فرهنگ زندان و تکرار جرم زندانیان خواهد داشت.[۲۲]

2)عوامل و الزامات تأثیرگذار بر تعیین پاسخ کیفری از سوی قاضی

کیفر، ابزار قهرآمیز جامعه برای اجرای عدالت و برقراری نظم است که اجرای آن باید با احتیاط کامل صورت بگیرد. از این رو لازم است تا جز در مواردی که نوع و میزان آن از سوی حاکم شرع مشخص شده است، به مسألهٔ «بهره‌وری کیفری» توجه کرد؛ به این معنا که با هزینهٔ کمتر درصد تحقق اهداف کیفری افزایش یابد. از جملهٔ این اهداف می‌توان به اصلاح مجرمان در پرتو بازپذیرسازی اجتماعی آن‌ها، پیشگیری از تکرار جرم در پرتو ارعاب‌انگیزی، پیشگیری از ارتکاب جرم از سوی سایر افراد جامعه در پرتوی عبرت‌آموزی و ترمیم خسارت بزه‌دیدگان جرایم اشاره کرد.

برای دست‌یابی به این مهم باید عوامل گوناگونی را مورد بررسی و تجزیه و تحلیل قرار داد. برای مثال، تنوع ضمانت‌اجراهای کیفری پیش‌بینی شده از سوی قانون‌گذار چقدر است؟ مرتکبان جرایم از لحاظ شخصیتی و موقعیت اجتماعی چه وضعیتی دارند؟ به طور مشابه وضعیت بزه‌دیدگان این جرایم چگونه است؟ برای مثال، گروهی از دانشمندان حقوق کیفری و جرم‌شناسی، جرایم را به دو دستهٔ جرایم اصطلاحاً «فسفری» و «کلسیمی» تقسیم کرده‌اند. گروه نخست که از آن‌ها به مجرمان «یقه سپید» نیز یاد می‌شود، با اندیشهٔ خود هنجارهای اجتماعی را نقض می‌کنند، نمونهٔ آشکار آن کلاهبرداری است. اما گروه دوم که به مجرمان «یقه آبی» نیز موسومند، عمدتاً مرتکب جرایم خشونت‌بار می‌شوند. از این تقسیم‌بندی به ظاهر ساده نتایج ارزشمندی عاید می‌شود. برای مثال، گروه اول نسبت به گروه دوم از وضعیت مالی مطلوب‌تری برخوردارند و این مسأله باید بر نوع و میزان ضمانت‌اجراهای کیفری تأثیر گذارد.

در این گفتار، بر آنیم تا عوامل تأثیرگذار بر گزینش پاسخ کیفری مناسب از سوی قاضی را بررسی کنیم. در بند نخست، لزوم توجه قاضی به ویژگی‌های مجرمان سایبری بحث و بررسی شده و در بند دوم ویژگی‌های بزه‌دیدگان سایبری و خسارت‌های وارده برشمرده خواهد شد.

۲-۱ ضرورت توجه به ویژگی‌های مجرمان سایبری

جرایم سایبر یا حتی نسل پیشین آن‌ها، یعنی جرایم رایانه‌ای، به دنبال بکارگیری فناوری نوین اطلاعات و ارتباطات در جرایم سنتی یا سوءاستفاده از خود آن‌ها به وجود آمده‌اند. لذا طبیعی است به مرتکبین آن‌ها سوای از دیگر مرتکبین جرایم نگریسته شود. زیرا عمدتا آن‌ها را متخصصین و تحصیل‌کرده‌هایی تشکیل می‌دادند که حتی به زعم عده‌ای در راستای اهداف خیرخواهانه مرتکب این جرایم می‌شدند. هرچند از سوی دیگر گروهی معتقد بودند این گروه در زمره **مجرمین یقه سفید** قرار می‌گیرند و باید ساز و کارهای مقابله با این گروه از مجرمین را در مورد آن‌ها پیاده کرد. با اینکه نمی‌توان این مدعا را حداقل نسبت به نسل اول این جرایم رد کرد، اما خواهیم دید که امروزه تحول شگرفی در گستره مجرمین سایبر به وقوع پیوسته است.

در مجموع یک سری برداشت‌های غلط درباره شخصیت مجرمین سایبر رواج یافته است که معمول‌ترین آن‌ها عبارتنداز:

۱. مجرمین سایبر از لحاظ اجتماعی بی‌کفایت، اما انسان‌های باهوشی هستند.
۲. مجرمین سایبر از بهره هوشی و دانش فنی بسیار بالایی برخوردارند.
۳. مجرمین سایبر را مردان و معمولاً جوانان طیف ۲۰ سال تشکیل می‌دهند.
۴. پسران جوانی که کامپیوتر دارند، مجرمین سایبر خطرناک محسوب می‌شوند.
۵. مجرمین سایبر، مجرمین واقعی محسوب نمی‌شوند، زیرا آن‌ها در دنیای واقعی مرتکب جرم نمی‌شوند.
۶. مجرمین سایبر هرگز مرتکب خشونت نمی‌شوند.
۷. مجرمین سایبر را می‌توان به دقت در یک نیم‌رخ مجرمانه[۲۳] مورد بررسی قرار داد.

[۲۲]. ماری لین، **پذیرش فرهنگ زندان**. ترجمه حسین غلامی، مجله پژوهش حقوق و سیاست، شماره ۷، ۱۳۸۱، ص ۱۷۵-۱۵۹.

در ادامه به بررسی هر یک از این برداشت‌ها می‌پردازیم:

۲-۱-۱ باهوشی و در عین حال بی‌کفایتی مجرمان سایبری

همانند بسیاری از نگرش‌های غلط، این تفکر نیز در گذشته که مصادیق صحیح آن به مراتب بیش از امروز بوده، رواج داشته است. همانطور که در تاریخچه سیستم‌های رایانه‌ای بیان شد، در ابتدا معدودی افراد بودند که به ابررایانه‌های بسیار بزرگ، گران و ناخوشایند دسترسی داشتند. کار با کامپیوترهای نخستین مستلزم دانش بالای ریاضی بود. پشت این کامپیوترها هرگز کاربرانی به مفهوم امروزین قرار نمی‌گرفتند و تنها کسانی می‌توانستند از آن‌ها استفاده کنند که برنامه‌نویس ماهری بودند. برنامه‌نویسی هم یک فرایند مشقت‌بار بود که به صبر و اراده‌ای پولادین نیاز داشت تا در مدت زمانی طولانی کدگذاری‌های مربوطه انجام شود. در آن زمان به سختی می‌شد راجع به فعالان این حوزه مطلبی در صفحات اجتماعی روزنامه‌ها پیدا کرد. هنگامی که این افراد پس از آن فعالیت بسیار خسته‌کننده شب هنگام به دنیای خارج پا می‌گذاشتند، هیچ حرفی برای گفتن به افراد جامعه نداشتند. تمام زندگی آن‌ها در میان انبوه لامپ‌های خلاء و نسخه‌های چاپی صفر و یک سپری می‌شد. یعنی چیزهایی که هیچ کس نه می‌توانست و نه می‌خواست به آن‌ها توجه کند.

اما اکنون سیستم‌های رایانه‌ای تقریبا در همه جا یافت می‌شوند. مهارت‌های مورد نیاز جهت بهره‌برداری‌های ناشایست از این سیستم‌ها به مراتب نسبت به گذشته از پیچیدگی بسیار کمتری برخوردار شده است. البته اکنون از آنگونه متخصصان اولیه نیز یافت می‌شود. اما بسیاری از مجرمین سایبر امروزین، به ویژه حقه‌بازان کامپیوتری و آنهایی که ارضای تمایلات جنسی خود را در این فضا جستجو می‌کنند، انسان‌هایی مؤدب و جذاب هستند و مهارت‌های اجتماعی را به خوبی فراگرفته‌اند.

۲-۱-۲ بهره هوشی و دانش فنی بالای مجرمان سایبری

با توجه به توضیحاتی که داده شد، درمی‌یابیم این نگرش نیز تنها در مورد متخصصین سیستم‌های اولیه رایانه‌ای صادق بوده است. امروزه دسترسی به فضای آنلاین به آسانی یک کلیک کردن شده است. با اینکه بعضی جرایم سایبر، نظیر نگارش و نشر ویروس‌های جدید یا تهاجم به شبکه‌های فوق امنیتی همچنان مستلزم دانش فنی بالایی است، اما طیف وسیعی از جرایم سایبر هستند که اشخاص عادی که بهره هوشی متوسط دارند و دانش فنی‌شان ناچیز است یا حتی از آن برخوردار نیستند نیز می‌توانند آن‌ها را مرتکب شوند.

حقه‌بازی‌های سایبری را هر کسی که قادر به ارسال پست الکترونیک باشد یا بتواند از برنامه‌های گپ اینترنتی استفاده کند، می‌تواند مرتکب شود. سرقت داده نیز غالبا به سادگی یک کپی کردن است. حتی جرایمی که مستلزم تخصص فنی پیچیده هستند را هم هکرهای غیرحرفه‌ای می‌توانند مرتکب گردند. این افراد فقط از کدی که دیگران در راستای اهداف شوم خود نگارش کرده‌اند استفاده می‌کنند. صدها وب سایت و گروه خبری به هکرهایی که هیچ‌گونه دانش فنی در اختیار ندارند، ابزارهای از پیش پیکربندی شده یا خودکاری ارائه می‌دهند که می‌توانند با استفاده از آن‌ها سیستم‌های رایانه‌ای را مورد تعرض قرار دهند.

۲-۱-۳ مردان جوان؛ پیشتاز در ارتکاب جرایم سایبری

این نگرش نیز از آنجا ناشی می‌شود که دانش ریاضی به طور عام و فناوری کامپیوتر به طور خاص از همان ابتدا در انحصار مردان بوده است. هرچند آمارهای مجریان قانون نیز حاکی از این است که در تمامی جرایم، مردان بیش از زنان مستعد ارتکاب جرم هستند. با این حال، آمارهای اخیر حاکی از پر شدن این شکاف جنسیتی است. البته این موضوع از این جهت نیز قابل تأمل است که از آنجا که جرایم رایانه‌ای در ابتدا در زمره جرایم یقه سفید قرار گرفته بود و مرتکبین این جرایم را عمدتاً مردان تشکیل داده بودند، این نگرش به وجود آمده است. هرچند باید خاطرنشان کرد که این حوزه نیز متحول شده است. هم‌اکنون زنان بسیاری در مناصب مدیریتی و اجرایی قرار گرفته‌اند که مستعد ارتکاب جرایم یقه سفید هستند و آمارها نیز حاکی از رشد ارتکاب این جرایم نزد آنان است[۲۴].

به این ترتیب، واقعیت این است که دیگر دانش کامپیوتر در انحصار مردان نیست. آمارهای وزارت بازرگانی امریکا نشان می‌دهد که ۲۸/۵ درصد برنامه‌نویسان را زنان تشکیل می‌دهند که البته درصد ناچیزی از آن‌ها به دنبال بهره‌برداری نامشروع از مهارت خود هستند. هرچند به

---

[23]. Criminal Profiling

[۲۴]. نجفی ابرندآبادی، علی حسین، **تقریرات درس جرم‌شناسی (بزهکاری زنان)**، تنظیمی حسن قاسمی مقدم، دانشگاه امام صادق (ع)، دوره کارشناسی ارشد، نیم‌سال نخست ۸۴-۱۳۸۳، ص ۱۷۷۲.

هر حال ابزار ارتکاب طیف وسیعی از جرایم سایبر در اختیارشان قرار گرفته است. بنابراین، این نکته مهم را نباید فراموش کرد که جرایم سایبر توسط هر جنسیت، نژاد و هر گروه سنی قابل ارتکاب است.[۲۵]

۲-۱-۴ پسران جوان مجهز به رایانه؛ مجرمان سایبری خطرناک

بی‌تردید هیچ‌کس با این واقعیت که اشخاص جوانی که سعی می‌کنند وب‌سایت‌ها را تخریب کنند یا به سیستم‌های کامپیوتری دولتی نفوذ کنند، مجرم محسوب می‌شوند، مخالفتی ندارد و حتی همگان اذعان دارند که این معضل باید رفع شود. اما این مسأله هرگز به این معنا نیست که طیف عظیم جوانانی که از مهارت‌های کامپیوتری برخوردارند، همگی از کامپیوترهایشان در راستای مقاصد نامشروع استفاده می‌کنند. اکثر آن‌ها عمده فعالیت شبکه‌ای‌شان در پیاده کردن موسیقی یا نرم‌افزاری خلاصه می‌شود که از آن برای مصارف شخصی استفاده می‌کنند. هرچند این اقدام نیز خود می‌تواند جلوه مجرمانه به خود بگیرد. اما به هر حال، هیچگاه نمی‌توان چنین انگ مجرمانه‌ای را به طیف عظیم کاربران شبکه‌ای زد.

۲-۱-۵ واقعی نبودن مجرمان سایبر

بسیاری از مجرمین سایبر این نگرش را ترویج کرده‌اند که مجرمین سایبر، مجرمین واقعی محسوب نمی‌شوند، زیرا آن‌ها در دنیای واقعی مرتکب جرم نمی‌شوند. دلیل ترویج این ادعا این بود که شاید از این طریق بتوانند اقدامات خود را توجیه کنند. حتی اشخاصی که در دنیای فیزیکی اقدامات غیرقانونی را مرتکب می‌شوند، چنین تصوری نسبت به فضای سایبر ندارند و به همین دلیل، بسیار راحت‌تر دروغ می‌گویند، تقلب می‌کنند یا حتی مرتکب اعمال وقیحانه یا نفرت‌انگیز می‌شوند.

به همین دلیل، اکنون مطالعات بسیاری در خصوص **روان‌شناسی جنایی سایبر** آغاز شده است تا از این طریق بهتر بتوان در خصوص رفتارهایی که در فضای سایبر بروز می‌یابند اظهار نظر کرد. به عنوان مثال، مرکز مطالعات **ارتباطات میان‌کامپیوتری** (CMC)، جلوه دوگانه غیرواقع‌گرایانه و ناشناس ماندن رفتارهای افراد که هویت متفاوتی به آن‌ها در فضای سایبر بخشیده است را در دستور کار مطالعات خود قرار داده است.

فناوری‌هایی نظیر گپ آنلاین، سیاه‌چال‌های چندکاربره (MUDs) و برنامه‌های واقعیت مجازی باعث شده‌اند برخی کاربران توانایی تفکیک دنیای واقعی از سایبر را از دست بدهند. بسیاری از کاربران اینترنت، به ویژه آنهایی که به تازگی به فضای آنلاین ملحق شده‌اند، تصور می‌کنند اشخاص مقابل آن‌ها در آن سوی مودم در حکم یک برنامه کامپیوتری هستند و حتی با آن‌ها به مثابه یک بازی رایانه‌ای تعامل برقرار می‌کنند. این افراد هویتی که در دنیای واقعی از خود بروز می‌دهند را در تعاملات آنلاین بکار نمی‌گیرند. زیرا تصور می‌کنند در آن سوی مودم کسی وجود ندارد. از این رو، به خود اجازه می‌دهند هرگونه حقه و نیرنگی را در این تعاملات به کار برند. همچنین، از آنجا که این افراد می‌توانند در فضای آنلاین برای خود هویت دیگری تعریف کنند و حتی برخلاف دنیای فیزیکی به سرعت آن را تغییر دهند و هویت‌های دیگری با ویژگی‌های کاملا متقلبانه را برای خود برگزینند، این بستر بیشتر برای آن‌ها فراهم می‌شود که به اقدامات متقلبانه آنلاین خود با خیال آسوده‌تر ادامه دهند.

به این ترتیب، این ایده که هیچ‌چیز در فضای آنلاین واقعیت ندارد، می‌تواند مروج یک واقعیت تلخ دیگر نیز باشد که هیچ‌کس در برابر اقدامات خود مسئول نیست. البته خود بستر فضای سایبر به مجرمین جرأت مضاعفی را اعطا کرده است. زیرا آن‌ها برخلاف دنیای فیزیکی، بی‌آنکه نتایج شرم‌آور و اسف‌بار جرایم خود را مشاهده کنند یا صدای فغان قربانیان خود را گوش کنند، با خیال راحت به ارتکاب جرایم می‌پردازند و به واقع می‌توان گفت تنها چیزی که مشاهده می‌کنند یک سری اعداد و ارقام و عبارات است که بر روی صفحه نمایشگرشان ظاهر شده است.

۲-۱-۶ فقدان خشونت در رفتار مجرمان سایبری

با توجه به توضیحاتی که در فوق داده شد، درمی‌یابیم از آنجا که به فضای سایبر بیشتر به عنوان یک فضای مجازی یا حداقل دنیای متمایز و متفاوت از دنیای فیزیکی نگریسته می‌شود، نتیجه منطقی آن این است که هیچ یک از مصادیق جرایم سایبر از ماهیت خشن برخوردار نباشند. زیرا از فاصله دور ارتکاب می‌یابند و در نگاه اول این مسأله به ذهن متبادر نمی‌شود که قابلیت اتصاف به خشونت را داشته باشند.

---

[۲۵]. جلالی فراهانی، امیرحسین، **پیشگیری از جرایم رایانه‌ای**، پایان‌نامه کارشناسی ارشد، دانشگاه امام صادق، ۱۳۸۴، ص ۲۱.

با قبول این واقعیت که بخش عمده‌ای از جرایم سایبر گزارش شده، کلاهبرداری، سرقت، و دسترسی غیرمجاز هستند، اما نباید از یاد برد که گزارشات مکرری نیز در خصوص هرزه‌نگاری کودکان به ثبت رسیده که به طور کلی در زمره جرایم خشن یا بالقوه خشن قرار می‌گیرد. تعرضات هکرها نیز جرایم خشونت‌باری هستند که گزارش‌های بسیاری از خسارات آن‌ها شده است. همچنین **تعقیب ایذایی در فضای سایبر**[۲۶] نیز یکی دیگر از مصادیق بارز خشونت در فضای سایبر است. یا **تروریسم سایبر**[۲۷] یکی از نمادهای بارز خشونت سایبری است که به طور جدی فضای سایبر و وابستگان به آن را مورد تهدید قرار می‌دهد.

۷-۱-۲ نیم‌رخ جنایی واحد برای مجرمین سایبر

این ادعا که مجرمین سایبر را می‌توان به دقت در یک نیم‌رخ مجرمانه مورد بررسی قرار داد قابل دفاع نیست. ممکن است بتوانیم برای اشخاصی که مرتکب جرایم سایبر خاصی می‌شوند، نیم‌رخ مشترکی تهیه کنیم، اما غیرممکن است تمامی آن‌ها را در یک نیم‌رخ به تصویر کشیم. درست مانند متخلفین و مجرمین رانندگی که نمی‌توان از آن‌ها یک نیم‌رخ تهیه کرد. یک راننده که به طور اتفاقی سریع رانندگی کرده است، احتمالا با یک راننده که عادتا مست است از شخصیت و انگیزه‌های متفاوتی برخوردار است و راننده‌ای که به شدت عصبانی است و از وسیله نقلیه مانند یک سلاح جهت از بین بردن عابران استفاده می‌کند نیز از شخصیت متفاوتی برخوردار است. به همین ترتیب، یک اوباش اینترنتی ویژگی‌های کاملا متمایزی با یک تعقیب‌گر ایذایی سایبری دارد که او نیز به نوبه خود هیچ شباهتی با یک هکر ندارد.

این تمایزات زمانی نمود بیشتری پیدا می‌کند که ویژگی‌های روان‌شناختی، جامعه‌شناختی و انگیزه‌های هر یک از مجرمین سایبر را نیز مد نظر قرار دهیم. به این ترتیب، ناگفته پیداست اگر بخواهیم بخشی از توده مجرمین سایبر را به تصویر کشیم، با طیف گسترده‌ای از ویژگی‌ها و خصائص متمایز مواجه خواهیم بود که برای درک دقیق‌تر آن‌ها نیازمند طبقه‌بندی مشخص و دقیقی هستیم.[۲۸]

۲-۲: ضرورت توجه به ویژگی‌های بزه‌دیدگان سایبری

اصطلاح بزه‌دیده یا victim از واژه لاتین victima اقتباس شده که به معنی حیوانی است که برای کشته شدن تقدیم می‌گردد. امروزه این واژه به شخص یا چیزی اطلاق می‌شود که توسط شخص یا تحت تأثیر شرایطی آسیب می‌بیند. در حوزه جرم‌شناسی، بزه‌دیده جرم به کسی گفته می‌شود که جرم علیه وی ارتکاب می‌یابد، یعنی کسی که فعل غیرقانونی مجرم به او آسیب می‌رساند.[۲۹]

امروزه گستره بزه‌دیده‌شناسی شامل جمع‌آوری داده‌ها راجع به قربانیان جرم و متأثر از نیم‌رخ‌شناسی جرم است. این اطلاعات به چند دلیل بسیار مفید هستند:

۱. به مجریان قانون امکان می‌دهد نوع شخصیت افرادی که احتمال دارد قربانی طیف خاصی از جرایم شوند را پیش‌بینی کنند و به آن‌ها هشدارهای لازم را بدهند. این امر به نوبه خود به قربانیان بالقوه امکان می‌دهد اقدامات لازم را جهت حفاظت از خود انجام دهند.
۲. به مجریان قانون امکان می‌دهد نیم‌رخ مجرمانه دقیق‌تری تهیه کنند، زیرا الگوهای گزینش قربانی بخش مهمی از نیم‌رخ مجرم را تشکیل می‌دهند.
۳. به مجریان قانون امکان می‌دهد با استفاده از نیم‌رخ قربانی مجرمین را به دام اندازند[۳۰].

قربانیان جرایم غالبا شاهدان اصلی محسوب می‌شوند. با اتخاذ فنون بزه‌دیده‌شناسی، حتی یک قربانی مرده هم می‌تواند نشانه‌های مهمی را به مجریان قانون ارائه دهد. به عقیده **اِمی گلدمن**[۳۱] نویسنده کتاب «**اهمیت بزه‌دیده‌شناسی در نیم‌رخ‌نگاری مجرمین**» هر سؤالی که در رابطه با قربانیان پاسخ داده می‌شود، به واقع پنجره‌ای به روی ذهن مجرم است که به نوبه خود سؤالات بسیاری را پاسخ می‌دهد.

---

26. Cyber Stalking
27. Cyber Terrorism

۲۸. جلالی فراهانی، امیرحسین، **پیشگیری از جرایم رایانه‌ای**، پایان‌نامه کارشناسی ارشد، دانشگاه امام صادق، ۱۳۸۴، صص ۲۳-۱۹.

۲۹. نجفی ابرندآبادی، علی حسین، **تقریرات درس جرم‌شناسی (بزه‌دیده‌شناسی)**، تنظیمی فاطمه قناد، دوره کارشناسی دانشکده حقوق دانشگاه شهید بهشتی، نیم‌سال دوم ۷۴-۱۳۷۳، ص ۲۲۳.

۳۰. همان، ص ۲۲۴.

31. Amy Goldman

شناخت بزه‌دیده، نوع رفتارها و میزان خطرپذیری وی در هنگام فعالیت‌های رایانه‌ای و اینترنتی در کنار بسترهای جرم‌برانگیز و آسیب‌ساز فضای سایبر، می‌تواند در شناخت علت‌های بزه‌دیدگی رایانه‌ای به مأموران تحقیق کمک کند. طرح پرسش‌هایی مانند پرسش‌های زیر چیستی، چرایی، کجایی، چگونگی و زمان فعالیت‌های اینترنتی بزه‌دیده را مشخص می‌کند:

۱. بزه‌دیده در اینترنت چه فعالیتی انجام می‌داده است؟
۲. بزه‌دیده از اینترنت چه استفاده‌ای می‌کرده که در غیر آنصورت نمی‌توانسته به آن دسترسی یابد؟
۳. بزه‌دیده چگونه به اینترنت دسترسی یافته است، برای مثال، از رهگذر حساب خود، والدین، دوستان یا از حساب سرقتی؟
۴. بزه‌دیده از چه مکانی به اینترنت دسترسی یافته است، برای نمونه، منزل، محل کار، کافی‌نت و ... ؟
۵. چرا بزه‌دیده آن محل را برای دسترسی به اینترنت برگزیده است، برای نمونه، حفظ حریم خصوصی خود، اقتضای شغل یا ملاقات حضوری با دیگران؟
۶. بزه‌دیده از چه نوع خدمات اینترنتی استفاده می‌کرده و چرا؟
۷. آیا بزه‌دیده می‌کوشیده تا بوسیلهٔ اینترنت پول بدست آورد؟
۸. آیا بزه‌دیده رفتاری از خود بروز داده که بتواند وضعیت روانی، تمایلات جنسی، سبک زندگی، هوش و یا خود ـ انگاره‌اش را نشان دهد؟ برای نمونه، آیا وی به سوءاستفاده از بازیابی گروه‌های خبری یا فهرست‌های پست الکترونیکی می‌پرداخته است؟ در صورت مثبت بودن پاسخ، چرا؟
۹. آیا بزه‌دیده به دستورالعمل‌های امنیتی پایبند بوده است؟
۱۰. آیا سامانه رایانه‌ای بزه‌دیده در برابر تهاجم‌های اینترنتی از ایمنی نسبی برخوردار بوده است؟[۳۲]

وجود برخی ویژگی‌های ذاتی و اکتسابی در افراد بویژه در فضای سایبر سبب می‌شود که احتمال بزه‌دیدگی آنان بالا رود و توجه بزه‌کاران بیشتر به آن‌ها جلب شود.

۱-۲-۲ بزه‌دیدگی برپایه ویژگی‌های ذاتی بزه‌دیده

به باور فون هانتیگ، سردمدار مطالعات بزه‌دیده‌شناسی، برخی از طبقات سنی و اجتماعی مانند زنان، کودکان، جوانان، اقلیت‌های قومی، مهاجران در زمرهٔ «پیش‌استعدادها یا پیش‌زمینه‌های بزه‌دیدگی» قرار دارند که با چنین ویژگی‌هایی، کشش و جاذبهٔ ارتکاب جرم را برای بزه-کار فراهم می‌کنند، درست همانند جاذبه‌ای که بره برای گرگ ایجاد می‌کند. در این افراد که از آن‌ها با عنوان «زیرهنجار»[۳۳] یاد می‌شود، نوعی آمادگی و استعداد ذاتی برای بزه‌دیده‌شدن وجود دارد که بزه‌کار بالقوه را به سوی ارتکاب رفتار مجرمانه سوق می‌دهد. این ویژگی‌ها در دنیای سایبر نسبت به دنیای خاکی اهمیتی دوچندان می‌یابد، چرا که به دلیل نبودن همگرایی‌های زمانی و مکانی موجود بین بزه‌کار و بزه‌دیده در دنیای خاکی، بزه‌دیدگان به لطف ناشناخته‌ماندن هویتشان با بی‌احتیاطی هرچه بیشتر به موقعیت‌های خطرزا وارد شده و خود را در معرض بزه‌دیدگی قرار می‌دهند. این ویژگی‌ها عبارتند از:

الف: سن

سن همواره به عنوان یکی از عوامل تأثیرگذار بر بزه‌دیدگی شناخته شده است. آسیب‌پذیری فرد از نظر معیار آسیب‌شناسانهٔ سن، نه تنها در برخی شاخه‌های علوم جنایی (مانند جرم‌شناسی و حقوق کیفری فنی یا خاص گرایش کودکان و نوجوانان) جایگاه ویژه‌ای دارد، بلکه موضوع یکی از شاخه‌های سیاست جنایی افتراقی نیز هست. در حقوق کیفری، از کودکان و نوجوانان به عنوان انسان‌های کاملی یاد می‌شود که از نظر ویژگی‌های بدنی، روانی و شخصیتی با بزرگسالان متفاوتند. این تفاوت، آن‌ها را بیش از بزرگسالان در برابر کژروی‌ها و بزه‌کاری‌ها آسیب-پذیر می‌سازد. از دیدگاه جرم‌شناسی نیز گسترهٔ تدابیر روانشناسانه ـ اجتماعی برای مداخله در پیشگیری از رفتارهای کژروانه یا پایان دادن به عواملی که فرد را از دوران کودکی در آستانهٔ خطر قرار می‌دهد، دربردارندهٔ افراد آسیب‌پذیری است که امکان بزه‌دیدگی‌شان را در آینده بیشتر می‌سازد.

---

[۳۲]. منفرد، محبوبه، **پیشگیری از جرایم رایانه‌ای از گذر کدهای رفتاری رایانه‌ای**، پایان‌نامه کارشناسی ارشد، موسسه غیرانتفاعی شهید اشرفی اصفهانی، ۱۳۹۱، ص ۱۰۶.

[33]. Subnormal

علاوه‌بر کودکان، سالمندان نیز یکی دیگر از گروه‌های سنی آسیب‌پذیر به شمار می‌آیند که به واسطه ضعف قوای جسمی و ناتوانی از دفاع خود در برابر دیگران توجه بزه‌کاران را بخود جلب می‌کنند. هم کودکان و هم سالمندان در فضای سایبر نیز بیشتر در معرض سوءاستفاده‌های احتمالی هستند. روحیه کاوشگر و در عین حال آسیب‌پذیر کودکان منجر می‌شود با حضور در اتاق‌های گفتگو و عضویت در تارنماهای نامناسب، به شیوه‌های گوناگون در معرض خطرهایی قرار بگیرند و به یک بزه‌دیده بالقوه تبدیل شوند. همچنین، بی‌اعتمادی سالمندان در به بکارگیری ابزارهای فناورانه و درخواست کمک از جوان‌ترها ممکن است موجبات بزه‌دیدگی آن‌ها را فراهم کند.

ب: جنسیت[۳۴]

همانطور که در جرایم فضای واقعی نیز مشاهده می‌شود، جنسیت افراد نقش تعیین‌کننده‌ای در بزه‌دیدگی آن‌ها دارد. زنان یکی دیگر از گروه‌های آسیب‌پذیری هستند که به دلیل ویژگی‌های فردی (ذاتی) در معرض بزه‌دیدگی‌های نوین و گسترده‌ای قرار گرفته‌اند. در دنیای خاکی، زنان به دلیل برخورداری از عوامل خاص زیست‌شناختی و اجتماعی، پیش‌زمینه و استعداد قبلی برای بزه‌دیده شدن را دارند و براساس یافته‌های جرم‌شناختی، بزه‌کاران بالقوه قربانیان خود را غالبا از میان افرادی انتخاب می‌کنند که ارتکاب جرم بر روی آن‌ها دارای خطر و هزینه بالایی نباشد. البته در اینجا لازم است که قائل به تفکیک شویم. برخی جرایم فی‌نفسه جنسیت‌محورند، بدین معنا که صرف داشتن جنسیت مؤنث یا مذکر عاملی برای بزه‌دیدگی به شمار می‌آید؛ لیکن گاهی جنسیت به ناتوانی جسمی تعبیر می‌شود. برای مثال، اینگونه پنداشته می‌شود که به دلیل ناتوان بودن زنان نسبت به مردان، ارتکاب جرایم مالی علیه آن‌ها در شرایط مشابه کم‌خطرتر و کم‌هزینه‌تر است. با این حال، بطورکلی، زنان به عنوان افراد بالقوه آسیب‌پذیرتر از مردان، آماج‌های مطلوبی برای بزه‌کاران محسوب می شوند. این قاعده در جرایم فضای سایبر و بزه‌دیدگی سایبری نیز به چشم می‌خورد. هرزه‌نگاری، تعقیب ایذایی سایبری، آزار جنسی و تحقیر منزلت نمونه‌هایی از اینگونه بزه‌دیدگی‌هایند.

پ: قومیت[۳۵] و نژاد[۳۶]

هرگونه تمایز، کنار گذاشتن، محدود کردن یا برتری دادن بر مبنای نژاد، رنگ پوست، نسب، یا اصالت قومی یا ملی که هدف بی‌اعتباری یا تضعیفِ پذیرش، بهره‌مندی یا استفادهٔ برابر از حقوق بشر و آزادی‌های اساسی در حوزه‌های سیاسی، اقتصادی، اجتماعی، فرهنگی و سایر حوزه‌های زندگی عمومی را دنبال می‌کند، با عنوان تبعیض نژادی شناخته می‌شود. رفتارهای برآمده از تنفر، تبعیض یا خشونت نسبت به هر شخص یا گروهی از اشخاص که به دلیل تعلق به یک گروهی با نژاد، اصالت قومی یا ملی خاص دستاویز این عوامل قرار می‌گیرد، از دیرباز تا کنون وجود داشته است. نقطه پیوند بزه‌دیدگی اقلیت‌ها جرم‌های برخاسته از نفرتند که به دلیل نژاد، قومیت، مذهب یا خاستگاه ملی بزه‌دیده رخ می‌دهند.

در این راستا، به دنبال نزدیک‌تر شدن مردم دنیا به یکدیگر در اثر پیشرفت‌های فناوری، تجاری و اقتصادی، تبعیض نژادی، بیگانه‌ستیزی و سایر اشکال تحمل‌ناپذیر به موجودیت خود در جوامعمان ادامه می‌دهند. جهانی‌شدن خطرهایی دارد که ممکن است به طرد افراد و افزایش نابرابری‌هایی منجر شود که بیشتر از جریان‌های نژادی و قومیتی ناشی می‌شوند. در این میان، پیدایش شبکه‌های ارتباطات بین‌المللی برای برخی افراد ابزارهای پیشرفته و توانمندی بمنظور اِعمال نژادپرستی و بیگانه‌ستیزی فراهم آورده و به آن‌ها امکان داده به راحتی و در سطحی گسترده اینگونه دیدگاه‌ها را منتشر کنند. تبادل محتوای نژادپرستانه و بیگانه‌ستیزانه در محیط‌های گپ، ارسال پیام‌های مشابه در گروه‌های خبری یا بحث‌های اینترنتی، به منظور تهدید، اهانت یا انکار نسل‌کشی و جنایت علیه بشریت نمونه‌هایی از اینگونه تهدیدها به شمار می‌آیند.

---

34. Gender

جنس (Sex) و جنسیت (Gender) از واژه‌هایی هستند که به ویژه در مباحث زنان، بسیار از آن‌ها استفاده می‌شود. این دو واژه، نزد کارشناسان امور زنان، معانی کاملا متفاوتی دارند. واژهٔ «جنس» به ابعاد بیولوژیکی مردانگی و زنانگی فرد محدود می‌شود و واژه «جنسیت» به صفات و ویژگی‌های اجتماعی دو جنس اطلاق می‌گردد. به بیان دیگر، واژهٔ «جنسیت» به اجزای غیرفیزیولوژیکی جنس اشاره دارد که از نظر فرهنگی، برای مردان یا زنان مناسب تشخیص داده می‌شود.

35. Ethnic

36. Race

بیان اینگونه دیدگاه‌ها، اشخاصی که قربانی آن جنایات عظیم شده‌اند و همچنین بستگان آن‌ها و در نهایت، حیثیت جامعهٔ بشری را تهدید می‌کند.

ت:مذهب

مذهب یکی دیگر از ویژگی‌هایی است که به بزه‌دیدگی بیشتر برخی از افراد دامن می‌زند. تبادل باورها و اندیشه‌های مذهبی در فضای سایبر همواره با احترام و ارزش‌گذاری به نظرات سایرین همراه نیست. توهین، استهزاء و دشنام به فرد یا گروهی از افراد با هدف به چالش کشیدن پایه‌های اعتقادی آن‌ها و تحت تأثیر قراردادن افکار عمومی دربارهٔ آن مذهب خاص از رفتارهایی است که در روابط اجتماعی برخط به چشم می‌خورد. در تازه‌ترین نمونهٔ اینگونه تعرض‌ها، می‌توان به توهین علیه پیامبر مکرم اسلام اشاره کرد که خشم مسلمانان جهان را به همراه داشت.

۲-۲-۲ بزه‌دیدگی برپایه ویژگی‌های اکتسابی بزه‌دیده

ویژگی‌های اکتسابی شامل آن دسته از ویژگی‌هایی می‌شود که اشخاص از تعامل با محیط و دیگران کسب می‌کنند. در ادامه به برخی از مهم‌ترین ویژگی‌های اکتسابی کاربران در فضای سایبر که فرصتی مناسب برای دام‌گستری بزه‌کاران به شمار می‌آیند، اشاره می‌شود:

الف: شغل

حساسیت‌های حاکم بر برخی متصدیان و سمت‌های حساس مرتبط با سامانه‌های رایانه‌ای بگونه‌ای است که همواره خطرات احتمالی علیه آن‌ها را افزایش می‌دهد و به لحاظ موقعیت شغلی توجه بزه‌کاران بیشتری به آن‌ها جلب می‌شود. نمونهٔ بارز این تهدید، **مهندسی اجتماعی**[۳۷] و **مهندسی اجتماعی معکوس**[۳۸] است. منظور از مهندسی اجتماعی هرگونه تلاش جهت برقراری ارتباط با مسئولین سامانه‌های‌های مورد نظر و فریب دادن آنهاست تا اطلاعاتی که جهت نفوذ به سامانه مورد نیاز هستند را از آن‌ها به دست آورد. به عنوان مثال، ممکن است بزهکار با مسئول مربوطه تماس بگیرد و اینگونه وانمود کند که از کارمندان جدید است و با مشکلی مواجه شده است. این کار خود باعث می‌شود اطلاعات بسیار سودمندی نظیر نام‌های رایانه‌ای، سامانه‌های عامل و حتی اطلاعاتی راجع به اعتبار کارمندان بدست آید. یا اینکه می‌توان خود را یک تکنیسین رایانه‌ای معرفی کرد که در تلاش است مشکلی را حل کند و از این طریق اطلاعات بسیار سودمندی را به دست آورد.

اما مهندسی اجتماعی معکوس اقداماتی است که باعث می‌شود افراد مورد نظر بزهکاران با آن‌ها تماس بگیرند. به عبارت دیگر، به جای اینکه بزهکاران با این کارمندان تماس بگیرند و به نحوی آن‌ها را بفریبند، زمینه را طوری فراهم می‌کنند که آن کارمندان مجبور به تماس با آن‌ها شوند. به عنوان مثال، ارسال یک یادداشت به همراه یک نسخه نرم‌افزار پشتیبان جدید از طریق پست الکترونیک می‌تواند موجب سرازیری سیلی از اطلاعات شود. مهندسی اجتماعی معکوس نسبت به مهندسی اجتماعی از این مزیت برخوردار است که کمتر شک‌برانگیز است. در جایی که خود کارمندان با بزهکار تماس می‌گیرند تا مشکلشان را حل کنند، بعید است نگاه شک‌برانگیزی به وی داشته باشند تا به این ترتیب این وضعیت را به مقامات مافوق خود گزارش کنند.

ب: تجارت

در سال‌های اخیر، یکی از آسیب‌پذیرترین جنبه‌های وجودی اشخاص حقوقی در فضای سایبر، به عرصهٔ کسب‌وکار و تجارت الکترونیکی مربوط می‌شود. امروزه تجارت، به طور چشمگیری به شبکه‌های فناوری اطلاعات و ارتباطات وابسته شده است؛ فناوری‌هایی که ستون فقرات خرید، فروش، یافتن منابع، عملیات و سامانه‌های مالی محسوب می‌شوند. از این‌رو، آسیب‌پذیری زیرساخت سامانه‌های شبکه‌ای در برابر کنش‌های متفاوت جرایم رایانه‌ای غیرقابل انکارست. روشن است که شرکت‌های تجاری، مؤسسه‌های غیردولتی و دستگاه‌های اجرایی در هر حد واندازه‌ای که باشند، از حملات رایانه‌ای در امان نیستند. هرساله سازمان‌های بسیاری هدف جرایم مرتبط با امنیت داده‌ها و اطلاعات قرار می‌گیرند، از حملات ویروسی گرفته تا کلاهبرداری‌های تجاری و سرقت اطلاعات حساس تجاری و اطلاعات محرمانه کارت‌های اعتباری. اینگونه حملات موجب میلیون‌ها دلار ضرر و اخلال در فعالیت شرکت‌ها می‌شوند.

---

[37]. Social Engineering
[38]. Reverse Social Engineering

بانک‌ها و مؤسسه‌های مالی نمونه‌های بارزی از بنگاه‌های اقتصادی‌اند که در معرض بزه‌دیدگی سایبری قرار می‌گیرند. تهاجم‌هایی مانند ورود و نفوذ به سامانه‌های بانکی و برداشت‌های غیرمجاز مالی از حساب‌های پرتراکنش، گشایش حساب‌های بانکی غیرواقعی و انجام تراکنش‌های غیرواقعی (نادرست)، سوءاستفاده از کارت‌های اعتباری و خرید و فروش‌های مجازی، جعل و تغییر در اسناد مالی و بانکی با نفوذ به سامانه‌های مالی از تعرض‌هایی هستند که اینگونه اشخاص حقوقی را تهدید می‌کنند.

پ: خدمات اداری و دولتی

نوع و ماهیت برخی فعالیت‌های سایبری بیشتر توجه بزه‌کاران بالقوه را به خود جلب می‌کند. با گسترش خدمات دولت الکترونیک و کاربری روزافزون فناوری‌های اطلاعات و ارتباطات در سازمان‌های دولتی و غیردولتی، ابعاد آسیب‌پذیری نهادهایی که خدمات اداری و دولتی را در قالب خدمات الکترونیکی انجام می‌دهند، افزایش یافته است. با پیدایش دولت‌های الکترونیک کشورها در بسیاری از جنبه‌های حکمرانی وابستگی بالایی به سامانه‌های رایانه‌ای یافته‌اند، خطرهایی که در اثر رفتارهای مجرمانه علیه این سامانه‌ها ایجاد می‌شوند، قابل توجهند. حمله‌های رایانه‌محور می‌توانند سامانه‌های رایانه‌ای که مسئولیت ادارهٔ سامانه‌های تأمین برق، حمل و نقل هوایی، راه‌آهن یا دیگر سامانه‌های کنترل آن‌ها، رایانه‌های بیمارستان یا تسلیحات نظامی، شرکت‌های تولیدات غذایی یا دارویی، سدهای برقی آبی یا ایستگاه‌های انرژی هسته-ای را به عهده دارند، هدف قرار دهند. اخلال در اینگونه سامانه‌ها می‌تواند آنچنان شدید و جدی باشد که ادامهٔ خدمات امکان‌پذیر نباشد. به خطر افتادن هریک از این سامانه‌های عملیاتی و اطلاعاتی ویا سامانه‌های مشابه می‌تواند درکنار اخلال در کارکردشان، موجب پیامدهای منفی از لحاظ اجتماعی، سیاسی و امنیت ملی شود.

ت: میزان آگاهی و سواد رایانه‌ای

همان اندازه که داشتن دانش و سواد سوءاستفاده از ابزارهای فناورانه عاملی تعیین‌کننده در بزه‌کاری به شمار می‌آید، دانش رویارویی با این تهدیدها نیز برای کاهش خطر بزه‌دیدگی افراد اهمیت دارد. نبود یا کاستی آگاهی و سواد رایانه‌ای دربارهٔ سوءاستفاده‌های رایانه‌ای و شبکه‌ای می‌تواند عامل مؤثری در تحقق بزه‌دیدگی کاربر باشد. البته دانش و سواد رایانه‌ای برای همهٔ کاربران در یک سطح تعریف نمی‌شود. این اصطلاح از یک سو به دانستن چگونگی بکارگیری رایانه و انجام کار مفید با آن اشاره دارد. در برخی موارد، صرف داشتن دانش پایه و نه شناخت کامل رایانه برای محافظت کاربر از تهدیدهای سایبری کافی است. اما در سطحی دیگر، سواد رایانه‌ای، به توانایی برنامه‌ریزی و شناخت علم رایانه یا «جایی که تخصص آنجاست» اطلاق می‌شود. بدین‌سان، روشن است که داشتن دانش و تخصص در رویارویی با بزه‌دیدگی، امری نسبی است. در واقع اگر پرسیده شود که نبود یا کاستی دانش و تخصص به چه معناست، درپاسخ باید آن را با دومفهوم روشن ساخت. در اینجا نبود دانش و تخصص با توجه به دو عامل سطح کاربری و سطح تهدیدها تعریف می‌شود. به عبارت دیگر، هرچه نوع کاربری پیشرفته‌تر و اهمیت تهدیدها بالاتر باشد، آسیب‌پذیری افراد دربرابر جرایم رایانه‌ای بیشتر خواهد شد.

منظور از سطح کاربری اینست که بسته به کاربردی که رایانه و شبکه‌های ارتباطی برای افراد و سازمان‌ها دارند، میزان دانش و تخصص آن‌ها برای طراحی و راه‌اندازی ابزارهای امنیتی و حفاظتی گوناگون است. برای یک سامانهٔ رایانه‌ای ساده با کاربری ساده، به دانش رایانه‌ای پیشرفته‌ای نیاز نیست. از سوی دیگر، ممکن است شخص به دانش بسیار پیشرفته‌ای مجهز باشد، لیکن این دانش برای تأمین امنیت و حفاظت از سامانه‌ای که دراختیار دارد، ناکافی یا لازم باشد که همواره دانش رایانه‌ای خود را روزآمد نگاه دارد. در این صورت آن سامانه از امنیت کافی برخوردار نیست.

آنچه که به سطح کاربری افراد و لزوم آشنایی با چگونگی ایمن داشتن سامانه‌ها اهمیت دوچندان می‌بخشد، نوع اطلاعاتی است که در سامانه بایگانی و نگهداری می‌شود. به عبارت بهتر، هرچه داده‌ها و اطلاعاتی که کاربر در سامانهٔ خود نگهداری می‌کند، ارزش بیشتری برای آن فرد یا سازمان داشته باشد، به همان نسبت به دانش فراتری برای حفظ محرمانگی‌شان نیاز خواهد بود. برای مثال، چنانچه سازمانی تصمیم بگیرد امور مربوط به بایگانی اسناد، مدارک و پرونده‌ها را رایانه‌ای و به دنبال آن نرم‌افزاری را برای پردازش آن‌ها طراحی کند، نباید به صرف اینکه تنها کاربری آن سامانه داده‌پردازی است، شیوهٔ مصون‌سازی ابتدایی و ساده را درنظر بگیرد. معمولاً گفته می‌شود که امنیت در سامانه‌های رایانه‌ای مؤلفه‌ای است از هزینه؛ هرچه حفظ امنیت و دسترس‌ناپذیری یک سامانه برای کاربر مهم‌تر و ارزشمندتر باشد، به همان میزان هزینه بیشتری نیز برای حفظ داده‌ها و اطلاعات موجود در آن درنظر گرفته می‌شود.

علاوه بر سطح کاربری، عامل دیگری که در تعیین میزان دانش و تخصص رایانه‌ای نقش قابل توجهی دارد، سطح تهدیدهای بالقوه است. بطور کلی، هر عملی که موجب اخلال در امنیت رایانه شود، تهدید رایانه‌ای بشمار می‌آید. هنگامی می‌توان از آسیب‌های بکارگیری سامانه‌های

رایانه‌ای و فعالیت در شبکه‌های ارتباطی در امان بود که بسته به تهدیدها و خطرهای بالقوه‌ای که پیش‌بینی می‌شوند، دانش و تخصص متناسب برای تأمین امنیت سامانهٔ رایانه‌ای را نیز به کار برد.

ث:میزان اراده در رویارویی با تهدیدها و تهاجم‌های سایبری

ارزیابی میزان خطرپذیری بزه‌دیدهٔ بالقوه در هنگام فعالیت‌های رایانه‌ای و اینترنتی به عنوان یکی از علت‌های بزه‌دیدگی رایانه‌ای از اهمیت بسیاری برخوردار است. به دیگر سخن، بی‌پروایی و خطرآفرینی برخی از بزه‌دیدگان هنگام حضور در فضای سایبر که رابطهٔ مستقیم با خواست و ارادهٔ آن‌ها دارد، نقش مؤثری در بزه‌دیدگی‌شان ایفا می‌کند. این دسته از بزه‌دیدگان افرادی هستند که عموماً به دلیل ساده‌انگاری زیان‌های احتمالی و با بی‌توجهی به هشدارهای امنیتی و با جرأتی که از گذر گمنامی هویت در این فضا بدست آورده‌اند، مرتکب رفتارهای پرخطری می‌شوند که آن‌ها را در معرض بزه‌دیدگی قرار می‌دهد. این افراد همزمان بزه‌دیدهٔ بی‌احتیاطی، سهل‌انگاری، ساده‌لوحی و رفتار مجرمانه بزهکار می‌شوند.

۳-۲-۲ بزه‌دیدگی برپایه آماج‌های سایبری

بطور کلی، آماج‌های تهدید و تجاوز سایبری در دو گروه دارایی‌های مادی و معنوی سایبری قرار می‌گیرند. این دارایی‌ها می‌توانند به یک شخص خاص یا به یک گروه یا به کل جامعه تعلق داشته باشند که در ادامه به آن‌ها اشاره خواهد شد.

منظور از **دارایی مادی**، آن بخش از داشته‌هاست که مستقل از وی موجودیت دارد و تنها حق مالکیت (اعم از عین یا منفعت) است که میان آن و شخص مالک (اعم از حقیقی یا حقوقی) رابطه مالکیت معنادار و مشروعی را برقرار می‌سازد. برای مثال، ملک، خودرو، پول یا اوراق بهادار، نرم‌افزار یا محتوای چندرسانه‌ای و مانند اینها پدیدآورنده ویا دارنده مشخصی دارد که نوعا مالک آن نیز شناخته می‌شود. بطور کلی، در پرتو اهداف این نوشتار، دارایی‌های مادی سایبری را می‌توان به دارایی‌های حیاتی؛ دارایی‌های حساس؛ دارایی‌های مهم و دارایی‌های عادی تقسیم‌بندی کرد. لطمه به هریک از این دارایی‌ها پیامدهای زیان‌بار و بعضا غیرقابل جبرانی را برای بزه‌دیده به دنبال خواهد داشت.

منظور از **دارایی‌های معنوی**، آن بخش از داشته‌هاست که وجود مستقلی ندارند و به وجود دیگری متکی‌اند و با حیات آن پدید می‌آیند و با زوال آن از بین می‌روند. البته این وابستگی به معنای کم‌ارزش یا بی‌ارزش بودن آن‌ها نیست و گاهی ارزش آن‌ها به حدی می‌رسد که هرگونه دارایی مادی را تحت‌الشعاع خود قرار می‌دهند. لیکن از لحاظ حقوقی چنین تقسیم‌بندی اعمال می‌شود تا بتوان آثار گوناگون آن را بررسی و تحلیل کرد. بطور کلی، دارایی معنوی را می‌توان در دو شکل فردی (حیثیت، حریم و ...) و عمومی یا ملی (فرهنگ، باورها، ارزش‌های ملی و محلی) قرار داد.

در خصوص قربانیان جرایم سایبر نیز می‌توان گونه دیگری از طبقه‌بندی را مطرح کرد. بدیهی است بعضی از این طبقات با یکدیگر هم‌پوشانی دارند. این بزه‌دیدگان عبارتنداز: اشخاصی که به تازگی وارد فضای شبکه‌ای شده‌اند؛ اشخاصی که ساده و بی‌تجربه هستند؛ اشخاصی که ناتوان یا آسیب‌پذیرند؛ اشخاصی که حریص یا تنها هستند یا از دیگر نیازهای روانی رنج می‌برند؛ قربانی‌نماها که بی‌آنکه واقعا قربانی جرمی شده باشند، آن را گزارش می‌کنند؛ اشخاصی که آنقدر بدشانس هستند که در یک زمان و مکان، به اشتباه بر سر راه مجرمین قرار می‌گیرند.[۳۹] در ادامه به بررسی هر یک از این طبقات می‌پردازیم تا با آسیب‌پذیری آن‌ها در برابر مجرمین سایبر بیشتر آشنا شویم:

الف: تازه‌واردهای شبکه‌ای

کسانی که به تازگی مبادرت به استفاده از اینترنت کرده‌اند، کمتر احتمال می‌رود با حقه‌های رایج آن آشنا باشند. همچنین این افراد غالبا با تدابیر امنیتی رایج و حفره‌های امنیتی نرم‌افزارها نیز آشنایی ندارند. ممکن است این افراد ندانند که سیستم‌هایشان با باز کردن ساده یک ضمیمه پست الکترونیک یا مشاهده یک وب سایت غیرقانونی ویروسی می‌شود. حتی ممکن است ندانند که می‌توان ویروس‌ها را از طریق سیستم‌هایشان منتشر کرد.

کاربران کامپیوتری که تجربه زیادی در تعاملات آنلاین ندارند، برای آنهایی که در محیط‌های گپ ملاقاتشان می‌کنند، بیشتر قابل اعتمادند. ممکن است آن‌ها چنین اعتقاد داشته باشند که از آنجا که خود در ارتباطات آنلاین صداقت به خرج می‌دهند، دیگران نیز چنین خواهند بود. مجرمین سایبر هر ساله با خیل عظیمی از تازه‌واردهای اینترنتی مواجهند که هر یک از آن‌ها می‌تواند یک قربانی بالقوه ارزشمندی برای آن‌ها

[39]. Shinder, Debra Littlejohn; **Scene of the Cyber Crime, Computer Forensics Hand Book**; Syngress Publication; 2002; p 129.

به شمار آیند. به همین دلیل، متولیان آموزشی کاربران اینترنت باید توجه ویژه‌ای به تازه‌واردها داشته باشند و باید به آن‌ها به خوبی گوشزد کنند که ممکن است هدف اقدامات متقلبانه کلاهبرداران و دیگر مجرمین قرار گیرند و در این خصوص اطلاعاتی جهت شناسایی آن‌ها و نحوه جلوگیری از به دام افتادن آن‌ها ارائه دهند.

ب: ساده‌لوح‌ها

بعضی افراد نسبت به بقیه ساده‌تر هستند. معمولاً اشخاص بسیار جوان و مسن‌ها گزینه‌های مطلوبی برای کلاهبردارها به شمار می‌آیند. اینگونه ترجیح‌ها به فضای آنلاین نیز تسری یافته است. اشخاص جوان غالباً دیدگاه‌های ناقصی از دنیای پیرامون خود دارند، به ویژه اگر در یک محیط بسته پرورش یافته باشند. ممکن است هنوز این بینش در آن‌ها نهادینه نشده باشد که بدکارانی هستند که می‌خواهند به دیگران لطمه بزنند. ممکن است تصور آن‌ها این باشد که اگر برای دیگران مثبت باشند، دیگران نیز برای آن‌ها مثبت خواهند بود. مضافا اینکه، کودکان طبیعتا کنجکاو و مشتاق تعامل با دیگران هستند که این خود می‌تواند برای مجرمین سایبر یک موقعیت عالی را رقم بزند. یکی از بدترین اشکال جرایم سایبر که کودکان را تهدید می‌کند **کودک‌دوستی**[40] است.

بسیاری از افراد مسن چندان با فناوری نوین مأنوس نشده‌اند. زیرا با آن رشد نکرده‌اند. ممکن است آن‌ها از کمک به دیگران لذت ببرند، خصلتی که می‌تواند منجر به سوء استفاده کلاهبرداران شود. زمانی که افراد مسن قربانی یک رفتار مجرمانه می‌شوند، ممکن است چندان رغبتی به گزارش آن نداشته باشند، حتی اگر در اثر کلاهبرداری مبلغ هنگفتی را از دست بدهند. استدلال این افراد می‌تواند این باشد که خودشان تا حدودی حماقت به خرج داده‌اند. طرح‌های کلاهبرداری پستی سنتی که افراد مسن را هدف قرار می‌دادند، هم‌اکنون در جلوه جدیدی ظاهر شده‌اند و آن کلاهبرداری از طریق پست الکترونیک است.

پ: ناتوان‌ها و آسیب‌پذیرها

این افراد نیز می‌توانند اهداف خاصی را برای مجرمین سایبر به وجود آورند. مجرمین سایبر با جستجو در پایگاه‌های داده آنلاین و پیوستن به فهرست‌های پستی که برای گروه‌های حامی افراد ناتوان و آسیب‌پذیر تدوین می‌شوند، این افراد را شناسایی کرده و به دام می‌اندازند. تشکل‌های آنلاین می‌توانند در تعاملات اجتماعی نقش مهمی ایفا کنند و یک منبع مهم آشنایی افراد ناتوان که قادر به حرکت نیستند، نظیر فلج‌های حرکتی، با یکدیگر به شمار آیند. متولیان آموزشی این گروه از افراد باید با اتخاذ تدابیر شایسته نه تنها زمینه‌های بزه‌دیدگی آن‌ها را از بین ببرند که امکان بهره‌برداری هرچه بیشتر آن‌ها را از فضای سایبر فراهم آورند.

ت: سیبل‌آفرینان

این افراد بهترین اهداف را برای مجرمین سایبر به وجود می‌آورند. ممکن است آن‌ها در تمامی محیط‌های بدنام آنلاین به دنبال یک عشق برای خود باشند؛ یا به طور مستمر به سایت‌های مستهجن مراجعه کنند؛ یا برای رستگاری خود، گروه‌های مذهبی را در اینترنت جستجو کنند؛ یا واقعا نیازمند کمک‌های مالی باشند؛ یا نیازهای روانی یا فیزیکی داشته باشند. در هر صورت، وضعیت بحرانی آن‌ها می‌تواند آن‌ها را آسیب‌پذیر کند. ممکن است آن‌ها به دام کلاهبرداران بیفتند یا فریب مبلغین مذهبی منحرف اخلاقی را بخورند یا اینکه با جذب شدن به طرح‌هایی که به سرعت موجبات پولدار شدن، دریافت وام‌های باصرفه از طریق اینترنت یا استخدام را فراهم می‌کنند، خود را در معرض کلاهبرداری قرار دهند.

ث: قربانی‌نماها

ممکن است این جمله زیگموند فروید که گفته سیگار همیشه سیگار است، اما قربانی همیشه قربانی نیست تا حدودی صحیح باشد. اشخاصی هستند که به دلایل خاصی جرایمی را گزارش می‌دهند که هرگز به وقوع نپیوسته است یا خود را به جای قربانیان معرفی می‌کنند. این در حالی است که ممکن است خودشان مرتکب آن جرم یا جرایم باشند. انگیزه این قربانی‌نماها می‌تواند موارد ذیل باشد: انتقام از دیگران؛ جلب توجه دیگران، این کار به آن‌ها موقعیت خاصی می‌بخشد؛ لاپوشانی جرم ارتکابی توسط خودشان؛ و تحصیل پول از مرتکبین غیرواقعی، سازمان‌های خیریه یا شرکت‌های بیمه.

با اینکه بخش عمده‌ای از گزارش‌های قربانیان واقعی تلقی می‌شود، اما باز هم مأموران پی‌جویی این احتمال را مد نظر داشته باشند که احتمال بروز چنین مسأله‌ای وجود دارد. در بعضی کشورها چنین عملی جرم‌شناخته می‌شود.

---

[40]. Pedophilia

ج: قربانیان اشتباهی

این یک واقعیت است که مرتکبین جرایم، همانند گرگ‌ها یا دیگر درندگانی که به گله‌های حیوانات حمله می‌کنند، به دنبال ضعیف‌ترین قربانی یا آنکه در ظاهر چنین است می‌گردند. اما این واقعیت را هم نمی‌توان کتمان کرد که تمامی قربانیان از پیش انتخاب نشده‌اند و به این دلیل قربانی جرم قرار گرفته‌اند که یک سری آسیب‌پذیری‌ها را از خود نشان داده‌اند. گاهی اوقات، فقط به این دلیل یک نفر قربانی جرم سایبر می‌شود که در زمان خاصی در موقعیت خاصی قرار گرفته است.[۴۱]

[۴۱]. جلالی فراهانی، امیرحسین، **پیشگیری از جرایم رایانه‌ای**، پایان‌نامه کارشناسی ارشد، دانشگاه امام صادق، ۱۳۸۴، صص ۲۷-۲۵.

بحث و نتیجه‌گیری

رایانه بزرگ‌ترین فناوری عصر حاضر است و سایر فناوری‌های نوین یا به‌وسیله آن یا بر بستر آن شکل می‌گیرند. البته فناوری‌ها در کنار مزایای خود می‌توانند بسترساز سوء استفاده‌هایی نیز باشند به‌ویژه اگر این فناوری، رایانه باشد دامنه خطرهای آن افزایش می‌یابد. حقوق کیفری نوین، امروزه با بزه‌ها و بزهکاران رایانه‌ای روبروست. جرایم و مجرمانی که در اغلب موارد دارای ماهیت و ویژگی‌هایی به نحو اساسی متفاوت با جرایم سنتی‌اند. جرایمی که در عرصه‌های خرد و کلان فردی و عمومی، زیان‌ها و آسیب‌های مادی و معنوی بسیاری را پدید می-آورند و هرآنچه وابستگی مردمان به این عرصه نوپدید بیشتر می‌شود، این زیان‌ها و آسیب‌ها شدیدتر می‌گردند و بزه‌دیدگان را بیشتر متأثر می‌سازند.

در چنین شرایطی، پاسخ جامعه چه می‌تواند باشد؟ آیا جامعه به عنوان متولی نظم و امنیت عمومی دربرابر این عرصه نوپدید نیز تعهدی دارد یا اینکه خود را تنها دربرابر موضوعات و مسائل دنیای مادی مسئول می‌داند؟ بی‌شک چنین است و هرگونه عقب نشینی از قلمروها[۴۲] و مرزهای مجازی[۴۳] به زیان نظام‌های حاکمیتی خواهد بود و معنایی جز تسلیم یا گذشتن از دارایی‌ها و داشته‌های باارزش ملی و یکایک اعضایش ندارد.

به گواه تاریخی که عمرش کمی بیش از یک نیم سده می‌گذرد، نظام‌های حاکمیتی پس از مدتی نسبتاً کوتاهِ سردرگمی، سرانجام به خویشتن آمده و در پی چاره‌جویی برآمدند. در نخستین گام، برخی رفتارهای زیان‌بار شدید را با قوانین سنتی دردسترس به کیفر رساندند تا تب در حال تشدید جامعه را فرونشانند. برای نمونه، دخل و تصرف در دارایی‌های دیگری از گذر دستکاری اسناد دیجیتالی بنگاه‌ها را گاه سرقت و گروهی کلاهبرداری و برخی نیز خیانت در امانت پنداشتند و مرتکبانش را به سزای اعمالشان رساندند. یا ورود غیرمجاز به سامانه‌های دیگران را همان ورود به عنف[۴۴] انگاشتند و سزاوار کیفر دانستند. شاید در این میان، دادرسانی بودند که اعتقادی به چنین تفسیر موسع نداشتند، اما دربرابر خواست و خواهش جامعه ناگزیر به چنین واکنش‌هایی بودند. سپس با توان و آگاهی‌یابی گروه‌های معارض، یعنی مرتکبان و مدافعان آن‌ها (یعنی مشاوران و وکلای حقوقی‌شان)، به تدریج کاستی‌ها و نارسایی‌های نظام عدالت کیفری در پاسخ به این رفتارهای سرزنش‌آمیز جنایی نمایان گشت و چاره‌جویی‌ها رنگ و بوی تقنینی به خود گرفت و تمرکز اصلی اصلاحات و الحاقات تقنینی، بر جبران کاستی‌ها و نارسایی‌های عناصر و اجزای تشکیل‌دهنده رفتارها یا ترک رفتارهای جنایی اختصاص یافت. به این ترتیب که کلاهبرداری‌های سنتی و مرسوم، کلاهبرداری‌ها یا سوء استفاده‌های مالی رایانه‌ای را بنیان نهادند یا اینکه تنها چنین جرم انگاشتند که احکام اسناد کاغذی بر نمونه‌های دیجیتالی آن‌ها نیز قابل اعمال است. تخریب، مختل‌کردن و ورود غیرمجاز به داده‌ها و سامانه‌های رایانه‌ای نیز به همین ترتیب ساماندهی شدند و نظام حقوق کیفری ماهوی کشورها از آمادگی نسبی دربرابر گونه‌های نوپدید زیان‌بار سایبری تضمین گشت.

واقعیتی که نمی‌توان و نباید از آن گذشت آنست که فضای مجازی ویژگی‌هایی دارد که اگر نظام پاسخ‌ها خود را با آن هماهنگ و همسو نسازد، کارآیی و اثربخشیش در اندازه همان شعار پوشالی توخالی باقی خواهد ماند. در اینجا نه تنها زمین و قاعده بازی دگرگون شده‌اند، بلکه بازیگران این صحنه، یعنی مجرمان و بزه‌دیدگان نیز هویت‌ها و ماهیت‌هایی یافته‌اند که لزوماً همان هویت‌ها و ماهیت‌های دنیای مادی نیستند و به‌راستی نمی‌توان شفابخشی آن‌ها را با همان نسخه‌های حاوی کیفرهای قبلی که برای همه هنجارشکنی‌های جنایی سنتی می‌نوشتیم، برای جرایم و جنایات فضای مجازی انتظار داشته باشیم. حتی حکومت‌ها نیز این دو محیط را به یک شکل و شیوه رهبری و راهبری نمی‌کنند که دست کم از این جهت بتوان وجه مشترکی را میان آن‌ها برقرار کرد. حال آیا در چنین وضعیتی، سخن از پاسخ‌های غیرکیفری که جلوه بارز آن عدالت ترمیمی سایبری است، زودهنگام نیست و به سخره گرفته نمی‌شود؟! یا اینکه باید گفت شتاب انطباق‌پذیری جوامع به اندازه‌ای بالارفته که می‌توان ایده‌ها و گزینه‌های نوین را در کنار آزموده‌های سنتی قرار داد و اتفاقاً در قیاسی شفاف‌تر و نتیجه بخش‌تر، زودتر و آسان‌تر به دستاوردهای مورد انتظار رسید.

---

[42]. Cyber Frontiers
[43]. Cyber Territories
[44]. Trespass

نگاه گذرا به آیینه سیاست‌های راهبردی، تقنینی، قضایی و اجرایی ایران گواهی می‌دهد که به‌رغم کارهای پرتراکم و البته پراکنده‌ای که به شکل سینوسی عموماً در دهه گذشته و ماقبل آن به انجام رسیده، راهٔ برای پیمودن بسیار است.

البته از حق که نگذریم، در این سالیان برخی تمهیدات شکلی نیز از تصویب قانون‌گذار گذشت که گروهی از آن‌ها به همکاری‌های فراملی دلالت داشتند، مانند معاهده همکاری امنیتی ایران و ایتالیا مصوب ۱۳۸۲ مجلس شورای اسلامی که به جرایم رایانه‌ای در کنار جرایم سازمان‌یافته و تروریستی و خشونت‌بار فراملی توجه داشته است. با این حال، تا سال ۱۳۸۸ و با تصویب قانون جرایم رایانه‌ای، نظام عدالت کیفری، به‌رغم برخورداری از همه قانون‌گذاری‌های پیشین، نقطه عطفی را در مبارزه ضابطه‌مند و هدفمند با این جرایم شاهد نبود. هرچند این نکته را هم نباید از یاد برد که وجود قوانین پیشین و نیازها و تعارض‌های شکلی و ماهوی برآمده از آن‌ها، زمینه پذیرش و ارزش قانون جرایم رایانه‌ای را فراهم و دوچندان کرده بودند و به همین دلیل در عرصه‌های مختلف قضایی و اجرایی در کوتاه‌ترین زمان نقش و جایگاه درخور خویش را یافت. با این حال، به‌رغم همه این مزیت‌های انکارناپذیر، این قانون نیز از آزمودن پاسخ‌های نوآورانه به جرایم و جنایات فضای مجازی سرباز زد و همان رویکرد سنتی واکنش‌های کیفری را در پیش گرفت و از گزینه‌های مرسوم حبس و جزای نقدی و اعدام و مانند آن سخن گفت. حتی جانب احتیاط را تا آنجا پیش گرفت که تدابیر مکمل کیفری اجتماعی، یعنی محرومیت از خدمات عمومی الکترونیکی را نیز تنها در مرحله پاسخ به جرایم مکرر پیش‌بینی کرد و این جرأت را نیافت که در همان مرحله آغازین دست مراجع صلاحیتدار قضایی را برای اعمال این پاسخ باز گذارد. امروزه در نقاط دنیا سعی می‌شود که از ضمانت اجراهای غیر کیفری که سازنده‌تر و کم هزینه‌تر از مجازات (به‌ویژه زندان) هستند استفاده شود اما متأسفانه در قانون جرایم رایانه‌ای تنها دو شکل از ضمانت اجراها یا همان مجازات وجود دارد: ۱ـ زندان ۲ـ جزای نقدی. این مسئله به ما نشان می‌دهد که نظام پاسخ کیفری تقنینی کشورمان در برابر جرایم قابل ارتکاب در فضای مجازی از کارآیی، کارآمدی و اثربخشی مطلوبی برخوردار نمی‌باشد.

مطالب مذکور مقدمه‌ای بود برای رسیدن به این نتیجه منطقی که برای رشد کارآیی و اثربخشی ضمانت اجراهای کیفری، در وهله نخست باید به ویژگی‌های فردی کنشگران جرم رایانه‌ای از یک سو و ویژگی‌های فناورانه جرم مزبور و اثرات سوء آن بر نظم اجتماعی از سوی دیگر تمرکز کرد. به دیگر سخن، اینکه بزهکار سایبری از چه ویژگی‌های مجرمانه‌ای برخوردار بوده که وی را به سوی ارتکاب جرم سوق داده است، یا اینکه چه آسیب‌پذیری‌هایی در بزه‌دیده وجود داشته که او را آماج جرم قرار داده است، نشانه‌های معناداری برای تعیین پاسخ مناسب نسبت به رفتار مجرمانه هستند. تعیین دو ضمانت اجرای محدود حبس یا جزای نقدی به‌هیچ عنوان در رسیدن به چنین مقصودی کافی نخواهد بود. صرف‌نظر از اینکه کیفرهای رایجی چون حبس و جزای نقدی نسبت به سایر جرایم تا چه اندازه از بازدارندگی، تناسب و اثربخشی برخوردارند، با توجه به ویژگی‌های متمایز جرایم و کنشگران جنایی سایبری، آیا می‌توان به دستاوردهای چنین پاسخ‌هایی در این حوزهٔ خاص امیدوار بود؟

اینجاست که برای پاسخ نسبت به رفتارهای مجرمانه سایبری می‌توان اجرایی بودن برخی نظریه‌های نوین حقوق کیفری را آزمود و کاستی‌ها و نارسایی‌های آن را به آزمون گذارد. از جملهٔ این آموزه‌ها، عدالت ترمیمی است که با حمایت از بزه‌دیده از یک‌سو و استفاده از راهبردهای بازپذیرکننده نسبت به بزهکار، حفظ و ارتقای سطح نظم اجتماعی را دنبال می‌کند.

منابع

۱ـ فارسی

الف) کتاب‌ها

۱. اردبیلی، محمدعلی. (۱۳۹۵). **حقوق جزای عمومی**. جلد سوم، تهران: نشر میزان.

۲. السان، مصطفی. (۱۳۹۳). **حقوق فضای مجازی**. تهران: انتشارات موسسه مطالعات و پژوهش‌های حقوقی شهر دانش.

۳. انزالی، امیراسعد. (۱۳۷۴). **کامپیوترهای امروزی**. تهران: مجتمع فنی تهران.

۴. آزاد ارمکی، تقی. (۱۳۸۶). **فرهنگ و هویت ایرانی و جهانی شدن**. تهران: تمدن ایرانی.

۵. آشوری، محمد. (۱۳۸۲). **جایگزین‌های زندان یا مجازات‌های بینابین**. تهران: نشر گرایش.

۶. آنسل، مارک. (۱۳۹۵). **دفاع اجتماعی**. ترجمه محمد آشوری و علی حسین نجفی ابرندآبادی ، تهران: انتشارات گنج دانش.

۷. آیکاو، دیوید جی و همکاران. (۱۳۸۳). **راهکارهای پیشگیری و مقابله با جرایم رایانه‌ای**. ترجمه اکبر استرکی و همکاران، تهران: انتشارات دانشگاه علوم انتظامی.

۸. بابایی، محمدعلی. (۱۳۹۰). **جرم‌شناسی بالینی**. تهران: نشر میزان.

۹. بادامچی، حسین. (۱۳۸۸). **مسأله تکامل حقوق کیفری.تازه‌های علوم جنایی (مجموعه مقاله‌ها)**. تهران: نشر میزان.

۱۰. باهری، محمد و داور، علی اکبرخان. (۱۳۸۳). **نگرشی بر حقوق جزای عمومی**. مقارنه و تطبیق رضا شکری ، تهران: مجمع علمی و فرهنگی مجد.

۱۱. بکاریا، سزار. (۱۳۹۵). **رساله جرایم و مجازات‌ها**. ترجمه محمدعلی اردبیلی، تهران: نشر میزان.

۱۲. بولک، برنار. (۱۳۸۷). **کیفرشناسی**. ترجمه علی‌حسین نجفی ابرندآبادی، تهران: نشر مجد.

۱۳. پیکا، جرج. (۱۳۹۵). **جرم‌شناسی**. ترجمهٔ علی حسین نجفی ابرندآبادی، تهران: نشر میزان.

۱۴. تحیری، فرزاد. (۱۳۸۴). **دسترسی غیرمجاز؛ جلوه‌ای از جرمهای رایانه‌ای نوین [مقاله در] مجموعه مقاله‌های همایش بررسی جنبه‌های حقوقی فناوری اطلاعات**. قم: سلسبیل.

۱۵. توجهی، عبدالله. (۱۳۸۸). **اندیشه حمایت از بزه‌دیدگان و جایگاه آن در گستره جهانی و سیاست جنایی تقنینی ایران»؛ علوم جنایی (مجموعه مقالات در تجلیل از استاد دکتر محمد آشوری**. تهران: سازمان مطالعه و تدوین کتب علوم انسانی دانشگاه‌ها (سمت).

۱۶. جاویدنیا، جواد. (۱۳۸۹). **جرایم تجارت الکترونیکی**. تهران: نشر خرسندی.

۱۷. جلالی فراهانی، امیرحسین. (۱۳۸۸). **مجموعه مقالات حقوق فناوری اطلاعات و ارتباطات**. تهران: انتشارات روزنامهٔ رسمی کشور.

۱۸. جلالی فراهانی، امیرحسین. (۱۳۸۹). **درآمدی بر آیین دادرسی کیفری سایبری**. تهران: نشرخرسندی.

۱۹. جوانمرد، بهروز. (۱۳۸۸). **تسامح صفر: سیاست کیفری سختگیرانه در قبال جرایم** خرد. تهران: نشر میزان.

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

۲۱. حسینقلی نژاد، حسین. (۱۳۷۳). **حقوق کیفری** بین‌المللی. تهران: نشر میزان.

۲۲. حسینی، علیرضا و پهلوانی فرد، احسان. (۱۳۹۳). **بررسی تطبیقی قانون جرایم رایانه‌ای در حقوق ایران و حقوق بین‌الملل**. تهران: انتشارات مجد.

۲۳. خالقی، علی. (۱۳۹۰). **جستارهایی از حقوق جزای بین‌الملل**. تهران: نشر شهر دانش.

۲۴. خالقی، علی. (۱۳۹۴). **آئین دادرسی کیفری**. جلد دوم، تهران: نشر شهر دانش.

۲۵. خانی جزنی، جمال. (۱۳۸۵). **مجموعه مقالات دومین همایش منطقه‌ای اخلاق و فناوری اطلاعات**. تهران: انتشارات مرکز تحقیقات مخابرات ایران.

۲۶. دبیرخانهٔ شورای عالی انفورمایتک کشور. (۱۳۷۶). **جرایم کامپیوتری**. به کوشش محمدحسن دزیانی، تهران: بی‌نا.

۲۷. دزیانی، محمدحسن. (۱۳۷۳). **ابعاد جزایی کاربرد کامپیوتر و جرم کامپیوتر و جرم کامپیوتری**.تهران: خبرنامه انفورماتیک شورای عالی انفورماتیک کشور.

۲۸. دزیانی، محمدحسن. (۱۳۷۶). **جرایم کامپیوتری**. جلد اول، تهران: سازمان برنامه و بودجه دبیرخانه شورای عالی انفورماتیک کشور.

۲۹. عالی‌پور، حسن. (۱۳۹۰). **حقوق کیفری فناوری اطلاعات**. تهران: انتشارات خرسندی.

۳۰. عباسی، مراد. (۱۳۹۴). **فضای سایبری: جرم‌زا یا جرم‌زدا**. تهران: انتشارات معاونت حقوقی و امور مجلس ناجا.

۳۱. دزیانی، محمدحسن. (۱۳۷۶). **جرایم کامپیوتری**. جلد دوم، تهران: سازمان برنامه و بودجه دبیرخانه شورای عالی انفورماتیک کشور.

۳۲. رحیمی مقدم، احمد. (۱۳۸۸). **گزیده‌های اخبار جرایم سایبری**. تهران: معاونت حقوقی و توسعهٔ قضایی قوهٔ قضائیه، مرکز مطالعات توسعهٔ قضایی؛ انتشارات روزنامهٔ رسمی کشور.

۳۳. زمانی، سیدقاسم و بهرام‌لو، مهناز. (۱۳۸۶). **حقوق بشر و اینترنت**. تهران: انتشارات خرسندی.

۳۴. زندی، محمدرضا. (۱۳۹۳). **تحقیقات مقدماتی در جرایم سایبری**. تهران: انتشارات جنگل.

۳۵. زهر، هوارد. **کتاب کوچک عدالت ترمیمی**. ترجمهٔ حسین غلامی (۱۳۸۸)، تهران: نشر مجد.

۳۶. زیبر، اولریش.**جرایم رایانه‌ای**. ترجمه محمدعلی نوری، رضا نخجوانی، مصطفی بختیاروند و احمد رحیمی مقدم (۱۳۹۰)، تهران: انتشارات گنج دانش.

۳۷. **کنوانسیون جرایم سایبر و پروتکل الحاقی آن**. ترجمهٔ امیرحسین جلالی‌فراهانی(۱۳۸۸)، تهران: انتشارات خرسندی.

۳۸. **کنوانسیون جرایم سایبر و پروتکل الحاقی آن**. ترجمه امیرحسین جلالی فراهانی (۱۳۸۹)، تهران: نشر خرسندی

۳۹. میرمحمدصادقی، حسین. (۱۳۷۸). **جرایم علیه اموال و مالکیت**. تهران: نشر میزان.

۴۰. نجفی ابرندآبادی، علی‌حسین. (۱۳۸۸). **کیفرشناسی نو ـ جرم‌شناسی نو؛ درآمدی بر سیاست جنایی مدیریتی خطرمدار. تازه‌های علوم جنایی (مجموعه مقاله‌ها)**. تهران: نشر میزان.

۴۱. نکونام، محمدرضا. (۱۳۹۳). **حقوق نوبنیاد**. اسلام‌شهر: انتشارات صبح فردا.

۴۲. نوربها، رضا. (۱۳۸۷). **زمینه حقوق جزای عمومی**. تهران: انتشارات کانون وکلای دادگستری.

مقاله ها

۱. ابراهیمی، سیدفتاح. (۱۳۹۴). عدالت قضایی و دادرسی عادلانه. همایش ملی، عدالت، اخلاق، فقه و حقوق: دانشگاه آزاد اسلامی واحد میبد یزد.

۲. ابراهیمی، شهرام. (۱۳۸۷). بازدارندگی از منظر حقوق و جرم شناختی. مجله کارآگاه ۲(۵).

۳. اردبیلی، محمدعلی. (۱۳۶۶). نیمه آزادی. حق (مطالعات حقوقی و قضایی) (۱۰).

۴. الهام، غلامحسین و منوچهری، مریم. (۱۳۹۳). تخصصی شدن رسیدگی در دادگاه‌های ایران و ایتالیا. مطالعات حقوقی و جرم‌شناسی ۱ (۱).

۵. بابایی، محمد علی و غلامی، میثم. (۱۳۹۱). مهمترین جلوه‌های کیفرزدایی در قانون جدید مجازات اسلامی. پژوهش نامه اندیشه‌های حقوقی (۳).

۶. تحیری، فرزاد. (۱۳۸۴). دسترسی غیرمجاز، جلوه‌ای از جرایم رایانه‌ای نوین. مجموعه مقالات همایش بررسی ابعاد حقوقی فناوری اطلاعات؛ معاونت حقوقی و توسعه قضایی قوه قضائیه. تهران: نشر سلسبیل.

۷. حاجی ده آبادی، احمد و سلیمی، احسان. (۱۳۹۳). اصول جرم‌انگاری در فضای سایبر (با رویکرد انتقادی به قانون جرایم رایانه‌ای). فصلنامه مجلس و راهبرد ۲۱ (۸۰).

۸. خرم‌آبادی، عبدالصمد. (۱۳۸۴). سابقه پیدایش، تعریف و طبقه‌بندی جرایم رایانه‌ای. مجموعه مقالات همایش بررسی ابعاد حقوقی فناوری اطلاعات؛ معاونت حقوقی و توسعه قضایی قوه قضائیه: تهران.

۹. دزیانی، محمدحسن. (۱۳۷۳). ابعاد جزایی کاربرد کامپیوتر و جرم کامپیوتر و جرم کامپیوتری. خبرنامه انفورماتیک شورای عالی انفورماتیک کشور (۵۸).

10.عالی‌پور، حسن. (۱۳۸۴). جرایم مرتبط با محتوا: محتوای سیاه فناوری اطلاعات. مجموعه مقالات همایش بررسی ابعاد حقوقی فناوری اطلاعات؛ معاونت حقوقی و توسعه قضایی قوه قضائیه. تهران: نشر سلسبیل.

۲ـ انگلیسی

الف) کتاب‌ها

1. August Ray. (2002). **International Cyber-Jurisdiction: A Comparative Analysis**; American Business Law Journal.
2. Buchanan, James, Congletonp, Roger. (1998). **Politics by Principle, Not Interest: Toward Nondiscriminatory Democracy**. Cambridge: Cambridge University Press.
3. Casey، Eoghan. (2001). **Digital Evidence and Computer Crime**; Academic Press; First Edition.
4. Council of Europe. (1990). European Committee on Crime Problems; **Extraterritorial Criminal Jurisdiction**; Strasbourg.
5. DeAngelis, Gina. (2000). **Ciber Crimes**. Chelsea House
6. Engel .(2012). **Low self-control**, Maxplank institute.
7. Hill, Joshua B; & Marion, Nancy E. (2016). **Introduction to cybercrime: computer crimes, laws, and policing in the 21st century**. CA: Praeger: Santa Barbara.
8. Jenson, Gerber. (2007). **encyclopedia of white collar crimes** .greenwood press.
9. L. Carter، David. (1992). **Computer Crime Categories، How Techno-Criminals Operate**; FBI Law Enforcement Bulletin.
10. Law Reform Commission of Canada. (1984). **Extraterritorial Jurisdiction**
11. P. N. Grabosky. (2001). **Virtual Criminality: Old Wine in New Bottles?** Social & Legal Studies، 10 (2).
12. S. D. Moitra (2005). "**Developing Policies for Cybercrime: Some Empirical Issues**" European Journal of Crime، Criminal Law and Criminal Justice، 13 (3).

Shover, neal. (1999). **White collar crime**, in the handbook of crime and punishment edited