مطالعات علوم سیاسی، حقوق و فقه

دوره ۹، شماره ۳، پاییز ۱۴۰۲

صفحات ۱۵۰-۱۳۹

Online ISSN: ٢٤٧٦-٤٤٦٩

Print ISSN: ٢٥٣٨-٢٠٣٩

www.irijournals.com

بزهکاری سایبری، شیوه ها و ساختار آن

محمد شریفانی

دانشیار دانشکده الهیات، دانشگاه علامه طباطبایی تهران، تهران، ایران

چکیده

این مقاله با روش توصیفی – تحلیلی و با ابزار کتابخانه ای به بررسی موضوع واکاوی بزهکاری سایبری و شیوه ها و ساختار آن می پردازد. شیوه های تحصیل آمار بزهکاری در جرایم سایبری شامل روش کمی، روش کیفی و شیوه های تکمیلی است. روش کمی شامل سه مرحله می باشد که مرحله اول، مرحله کشف جرم تلقی می شود که همه جرائم ارتکابی کشف نمی‌گردند و در نتیجه جرائم کشف نشده در آمار جنائی لحاظ نمی‌شوند. مرحله دوم، گزارش جرم است. و مرحله سوم را می توان ثبت جرم نامید. در این مرحله اعمالی که به نظر متضرر از عمل، مجرمانه تلقی می شوند، به مقامات انتظامی یا قضائی منعکس شده دستور تعقیب صادر می شود و تحقیقات لازم صورت می گیرد. در روش کیفی با پرونده‌ها و یا مستقیماً با خود مجرمین یا با ارگانها یا کسانی که به عنوان مسئولان اداره بزهکاری هستند سروکار داریم. مطالعه آرشیوها و پرونده‌های کیفری نشان می دهد که در یک پرونده کیفری، علاوه بر هویت متهم، یک سلسله اطلاعات حقوقی و کیفری وجود دارد که می‌تواند در مقام مطالعه مورد توجه جرم شناسی قرار گیرد که به خصوصیات مجرمین مربوط می‌شود.ساختار بزهکاری ظاهری و قانونی سایبری نیز شامل ساختار بر اساس بزه ارتکابی و ساختار جرایم سایبری بر اساس محل ارتکاب است.

واژه‌های کلیدی: بزهکاری، بزهکاری سایبری، قانون، جرم.

مقدمه

فضای سایبر دنیایی است که نه تنها هیچ نهاد و سازمان بین المللی مشخصی بر آن حکومت و کنترل ندارد، بلکه قابلیت کنترل و نظارت بر آن نیز دشوار است؛ لذا به همان اندازه که فضای سایبر از لحاظ فنی و تکنولوژیک پیشتاز است؛ اما نظارت بر آن همیشه یک گام عقب است. گستره‌ی این فضا به گونه ای است که امروزه تمام روابط زندگی بشر را در برگرفته و این امکان را فراهم ساخته است تا هر فردی به راحتی و با صرف کمترین زمان دست به ارتکاب جرم بزند بدون اینکه کنش گران نظام عدالت کیفری بدان پی ببرند، خصوصا آن که بدلیل فراملی بودن جرایم سایبری (و داشتن بزهکاران و قربانیان مربوط به کشورهای مختلف) امکان تشکیل باندهای سازمان یافته بزهکاری به صورت فراملی و غیره را فراهم آورده است.

یکی از تاثیرات محیط مجازی بر گرایش های مجرمانه به موضوع بزه دیدگان مربوط می باشد. در واقع گاه شرایط حاکم بر فضای مجازی به گونه است که احتمال بزه دیده شدن را افزایش می دهد. به عبارت بهتر فرد بزه دیده به واسطه حضور در زیست مجازی در ارتکاب جرم، به مجرم مساعدت می نماید.

به طور کلی شرایط حاکم بر زیست مجازی به خصوص از بعد ناشناختگی، با فراهم آوردن شرایط کاهش بازدارندگی، ایجاد شرایط تحریک و تشویق، اختلال در دوره های گذار زیستی و اجتماعی و اختلال در درک افراد نسبت به اعمال و تمایل به خود افشایی موجب اثرگذاری بر بزه دیدگی افراد می گردد. نکته مهم اینکه هیچ کدام از این رفتار های مجرمانه در آمار بزهکاری قانونی منعکس نمی شود. مساله ای که کمتر مورد توجه سیاسگذاران جنایی قرار می گیرد و البته آثار نامطلوبی برای شهروندان به طور عام و بزه دیدگان به طور خاص دارد.

۱-مفهوم سایبر

اصولا، واژه‌ی سایبر به لحاظ لغوی در فرهنگ‌های مختلف به معنای «مجازی» و «غیر ملموس» و از لغت یونانی kybernetes به معنی سکاندار یا راهنما مشتق شده است. «سایبرمحیطی مجازی و غیرملموس در فضای شبکه‌های بین‌المللی است که در این محیط تمام اطلاعات راجع به روابط افراد، فرهنگ‌ها، ملت‌ها، کشورها و به‌طور کلی هر آنچه در کره خاکی به صورت فیزیکی ملموس وجود دارد. (به صورت نوشته، تصویر، صوت، اسناد) در یک فضای مجازی به شکل دیجیتالی وجود داشته و قابل استفاده و دسترس کاربران هستند و از طریق رایانه، اجزا آن و شبکه‌های بین‌المللی به یکدیگر مرتبط هستند.» (باستانی، ۱۳۸۶: ۵۸) همچنین «سایبر» پیشوندی است برای توصیف یک شخص، یک شی، یک ایده و یا یک فضا که مربوط به دنیای کامپیوتر و اطلاعات است؛ این اصطلاح نخستین بار توسط ریاضیدانی به نام «نوربرت وینر» در کتابی با عنوان «سایبرنتیک و کنترل در ارتباط بین حیوان و ماشین» در سال ۱۹۴۸ بکار برده شد.

۲-بزه سایبری

اصطلاح «بزه سایبری» هنوز موضوع تعریف رسمی، (چه در اسناد بین المللی و چه در قوانین بسیاری از کشورها) قرار نگرفته است. این متون با تکیه بر رویکردی کاربردی ترجیح می دهند به جای ارائه ی تعریفی قانونی محتوای این بزهکاری را تبیین کرده جرایم تشکیل دهنده آن را دسته بندی نمایند. البته ازسال ۱۹۸۳ که نخستین تعریف از جرم سایبری از سوی سازمان همکاری اقتصادی اروپا منتشرگردید (عالی پور، ۱۳۹۵: ۱۲۵-۱۲۰) تاکنون تعریف های زیادی از جرم سایبری ارائه شده است. رهیافت های اتخاذ شده در این تعریف ها یا گسترده و یا محدود بوده، ممکن است همه ی مصادیق پیش بینی شده در قوانین

کیفری را شامل نشود و یا با توصیف های مضیق حقوقی تطابق نداشته باشد. (حاجی ده آبادی، ۱۳۹۳: ۱۲۴) وجه مشترک این تعاریف، ارتباط این جرایم با سامانه، اینترنت یا شبکه است.

از لحاظ حقوقی می‌توان این تعریف را برای جرایم سایبری ارائه داد: «هر اقدامی که از طریق فضای مجازی و با بهره گیری از ابزارهای اتصال به فضای مجازی صورت گرفته و حقوق شناسایی شده برای افراد را نقض می کند» به این ترتیب، تنها جرایمی در دامنه شمول این تعریف قرار می گیرند که از طریق فضای مجازی و با بهره گیری از ابزارهای اتصال به این فضا ارتکاب می-یابند.

جرایم سایبری در ایران، به موجب قانون جرایم رایانه ای مصوب ۱۳۸۸جرم انگاری شده است. این جرایم غالبا غیر قابل گذشت بوده‌اند و جز در یک مورد که جرم موضوع ماده ۷۴۴ این قانون می باشد، که وفق ماده ۱۱ قانون کاهش مجازات حبس تعزیری قابل گذشت دانسته شده است. در مواردی نیز درخصوص غیر قابل گذشت بودن این جرایم مانند سرقت رایانه ای میان قضات اختلاف نظر وجود دارد؛ اما تنها موردی که به صراحت قابل گذشت دانسته شده همان جرم موضوع ماده ۷۴۴ یعنی هتک حیثیت از طریق سامانه های رایانه ای یا مخابراتی است.

در رویه قضایی، بسیار مشاهده می شود که جرمی رایانه ای؛ مانند کلاهبرداری رایانه ای و... رخ داده و در مرحله دادسرا شاکی خصوصی رضایت متهم را می دهد.حال تکلیف چیست؟ در ابتدا باید خاطر نشان کرد که دقیقا همین موضوع تفاوت بزهکاری سایبری ظاهری و قانونی را نمایان می سازد.

در این مواقع، از آنجا که جرم غیر قابل گذشت بوده، طبیعتا رضایت شاکی تنها می تواند از موجبات تخفیف باشد؛ یعنی آنکه با رضایت شاکی پرونده مختومه نخواهد شد و قاضی ملزم به ادامه تحقیقات و در نهایت صدور قرار است. یک رویه میان قضات وجود دارد که در این مواقع جهت جلوگیری از سابقه دار شدن افراد و همچنین مسائلی از قبیل آمار گرایی و کمبود وقت کافی جهت رسیدگی، در صورتی که شاکی گذشت خود را اعلام نماید، با استفاده از شگردی که برخی از قضات به کار می برند و البته که با دیدی کلی می‌توان گفت اثار مطلوبی دارد، متهم را از ادامه مراحل دادرسی و صدور حکم و در نهایت مجازات معاف می نمایند.

آنان با استفاده از عبارت عدم کفایت ادله در انتساب رفتار به متهم قرار منع تعقیب صادر می کنند. در واقع ملزم هستند که اگر ادله کافی وجود دارد و شاکی هم رضایت داده باشد، بدون درنظر گرفتن رضایت شاکی به اتهام وی رسیدگی نموده و قرار جلب به دادرسی صادر نمایند تا مراحل دادرسی طی شود اما با به کار گرفتن این رویه نتایج مطلوبی شامل سیستم قضایی و بزهکار می شود.

این امر در جهت تعدیل امار سیستم قضایی تاثیر گذار بوده و در مقابل نیز متهم محکوم به مجازات های مختلف من جمله جزای نقدی یا حبس نخواهد شد. با کمی تامل به نظر منطقی می آید. وقتی شاکی خصوصی که متحمل ضرر و زیان شده رضایت می دهد، حاکمیت یا به تعبیری خاص تر دستگاه قضایی چرا نبخشد!

معمولا تجربه نشان داده که بزهدیده نیز، با گرفتن ضرر و زیان خود پیش از رضایت دادن به متهم، از او جبران خسارت می شود، حال اگر در مقابل قاضی بخواهد در این گونه موارد رویه فوق را پیش نگرفته و در چنین مواردی با وجود ادله کافی در انتساب رفتار به متهم، قرار جلب به دادرسی را صادر نماید و متهم وارد مرحله دادرسی و صدور حکم و در نهایت مجازات شود، نتایج مطلوبی شامل هیچ کدام از طرفین نخواهد شد. به نوعی می‌توان گفت: سیستم قضایی و حاکمیت نیز متحمل ضرر می شوند، زیرا با مجازات بزهکار، بدون شک هزینه هایی را برای حاکمیت به ارمغان خواهد آورد.

به عنوان مثال نگهداری وی در زندان برای دولت و حاکمیت هزینه آور خواهد بود و از طرفی دیگر برچسب مجرمیت بر پیشانی بزهکارخواهد خورد که در آینده اثرات نامطلوبی را برای وی در بردارد، این موارد که با رضایت شاکی و شگرد برخی از قضات در نهایت با قرار منع تعقیب پرونده مختومه می شود، جز آمار بزهکاری سایبری ظاهری محسوب شده که تعداد قابل توجهی را به خود اختصاص می دهد.

به تعبیر ساده تر، اگر این رویه توسط برخی از قضات محترم پیش گرفته نشود، به تبع به امار قانونی این جرایم تعداد قابل توجهی اضافه خواهد شد. لازم به ذکر است که در مواقعی نیز این جرایم در مرجع انتظامی حل و فصل شده و حتی به مرحله دادسرا نیز نمی رسد.

۳-شیوه های تحصیل آمار بزهکاری در جرایم سایبری

در این شیوه به سه روش کمی، کیفی و تکمیلی نسبت به جمع آوری آمار به شرح ذیل اقدام می گردد:

۳-۱-روش کمی

یکی از منابعِ مطالعات کمّی در جرم شناسی، آمار جنائی است؛ یعنی از ریاضی و محاسبات در هنگام مطالعه پدیده مجرمانه استفاده کنیم. «آمار جنایی، دانش نوظهوری است که تقریباً همزمان با پیدایش جرم‌شناسی فعالیت خود را آغاز کرده و اساس و پایه تحقیقات عینی امور جنایی قرار گرفته است.» (کی نیا، ۱۳۸۶: ۶۷) و عبارتست از «جمع‌آوری و تجزیه و تحلیل حقایق عینی تبهکاران، اعمال مجرمان، عوامل فردی و اجتماعی و... و تفسیر آن براساس منطق و استدلال. این آمار راجع به طبع جرم، تعداد جرایم و مجرمان، سن، جنس و سوابق قضایی آنها اطلاعات مفیدی به دست می‌دهد» (همان: ۷۲)

نخستین آمار سالانه‌ی ملی در زمینه جرم، در سال ۱۸۲۷ در فرانسه منتشر گردید، که از اهمیت بالایی برخوردار است و سپس آندیره میشل‌گری (Ander – Michel Guerry) به سال ۱۸۲۹ نتایج اولیه تحقیقات خود و در سال ۱۸۳۳ کتاب خود را تحت عنوان «پژوهش در آمار اخلاقی فرانسه» منتشر کرد که توانسته تاثیر به سزایی در این حوزه بگذارد. دومین فردی که به آمار جنایی توجه کرد آدولف کتله (Adolphe - Quetelet) می‌باشد که امروزه، به عنوان پدر آمار جنایی شناخته می‌شود، (ولد، ۱۳۸۰: ۶۹-۴۷) طبق نظر گری و کتله (لامبرآدولف ژاک کتله) آمار جنائی احصاء اعمالی است که جرم تلقی می‌شود و برای آن ضمانت اجرا پیش‌بینی شده است. در دنیای امروز برنامه ریزی از نکات کلیدی و اساسی به شمار می رود و پیش برد امور بدون آن ممکن و موفق نیست.

در کنار آمارهائی که عمدتاً ناشی از وزارت دادگستری بوده، آمارهائی داریم که به آنها آمار پلیسی یا بزهکاری ظاهری می‌نامند؛ یعنی تعداد افرادی که در رابطه با جرم و بزهکاری و انحراف توسط پلیس و نیروی انتظامی دستگیر شده‌اند و هنوز به مرحله دادسرا و محکومیت نرسیده‌اند. علاوه بر آمار پلیس، آمار نیروی انتظامی هم در حکم آمار پلیسی است.

این آمار اغلب توسط ضابطین کشف و مورد تحقیق و بررسی قرار می گیرند که گاه با کشف آن و پیگیری دقیق آن زمینه کشف جرایم دیگری نیز فراهم می گردد؛ چرا که پرونده چنین کسانی لزوماً به مراجع قضائی ارسال نمی‌شود. آمار دادسرای نظامی هم قابل توجه است که امروزه در قلمرو قوه قضائیه است. ایراد عمده بر آمار این است که آمار بیانگر واقعیت مجرمانه نیست، بلکه بیانگر میزان فعالیت ارگانها و اعمال کنترل اجتماعی است. (ابری، ۱۳۸۷: ۱۲۴)

با بررسی میدانی که در کلانتری ها انجام شده مشخص می گردد که؛ اولاً جرایم سایبر را بسیار کم گزارش نموده اند و نبود پلیس فتا در برخی شهرستان ها، دلیلی است برای اینکه به طور علمی پیگیری کشف و شناسایی مجرمین صورت نگیرد و عدم توانایی پلیس های غیر تخصصی در کشف و شناسایی مجرمین این تمایل را در مردم جهت پیگیری از بین برده است؛ لذا جا دارد که در کل کشور با توجه به افزایش جرایم سایبری و نیاز به پیگیری علمی و تخصصی این جرایم، نسبت به تشکیل پلیس فتا در همه شهرستانها با افراد با تجربه بالا و متخصص در حوزه مربوطه اقدام شود تا از سردرگمی مردم جلوگیری به عمل آید و زودتر به حقوق خود برسند.

البته ذکر این نکته ضروری است که همه ی این آمارها حاکی از وجود ارتکاب جرم و یا کشف آنها نمی باشد و در برخی از جرائم اصل جرم کشف نمی شود و کسی از آن مطلع نیست.

برای پی بردن به فرایند ثبت جرایم ارتکابی و تنظیم آمارجنائی لازم است مراحل مختلف این فرایند را مورد بررسی قرار دهیم:

الف) مرحله اول را می توان مرحله کشف جرم تلقی نمود. توضیح آنکه همه‌ی جرائم ارتکابی کشف نمی‌گردند و در نتیجه جرائم کشف نشده در آمار جنائی لحاظ نمی‌شوند.

ب) مرحله دوم «گزارش جرم» است. در این مرحله بزه دیده به دلایل عدیده از گزارش جرائم ارتکابی به مقامات قضائی یا انتظامی خود داری می کندکه دلیل عدم گزارش می تواند متفاوت باشد؛ لذا روشن می شود که بزهکاری قانونی در آمار جنائی دادگستری منعکس می شود، اما بزهکاری قانونی فقط جزئی کوچک از بزهکاری واقعی در جامعه را تشکیل می دهد و بزهکاری پلیسی به بزهکاری واقعی نزدیک تر است؛ زیرا همان گونه که گفته شد، عدم صدور حکم محکومیت در مورد جرائمی که به پلیس گزارش شده، الزاما به معنی عدم وقوع جرم نیست و ممکن است عدم صدور حکم محکومیت دلایل مختلفی داشته باشد و چه بسا در بسیاری از مواقع جرم کشف نشده، دارای ابعاد وسیع تر بوده و ریشه های پنهانی نیز داشته باشد.

مرحله سوم را می توان مرحله «ثبت جرم نامید» در این مرحله اعمالی که به نظر متضرر از عمل، مجرمانه تلقی می شوند، به مقامات انتظامی یا قضائی منعکس شده دستور تعقیب صادر می شود و تحقیقات لازم صورت می گیرد. اعمالی که مجرمانه تلقی می شوند، ممکن است برای رسیدگی تعیین مجازات به دادگاه گزارش شوند و دادگاه نهایتا حکم محکومیت صادر کند که مجموع احکام محکومیت صادره را که دلالت قطعی بر ارتکاب جرم دارد در جرم شناسی تحت عنوان «بزهکاری قانونی» یا قضایی مورد توجه قرارمی دهد که در مقایسه با بزهکاری واقعی ممکن است رقم بسیار ناچیزی را تشکیل دهد؛ چرا که در مورد هر پرونده امکان دارد شرایطی پیش آید که نتیجه محکومیت قطعی نشود؛ از جمله: گذشت شاکی و بزه دیده، مرور زمان در جرائم،کم بودن ادله یا جرم نبودن رفتار انجام شده است.

در زمینه مسائل کیفری، به خصوص پیشگیری از جرم، آمارجنائی ابزار کار محسوب شده و اساساً پیشگیری از بزهکاری، بدون استفاده از آن، میسر نمی‌گردد؛ ولی باید دید آمار جنائی تا چه حد می تواند به عنوان ابزاری مناسب برای پیشگیری موفقیت آمیز مورد استفاده قرار گیرد.

آمار جنائی دارای انواع مختلفی است و بر اساس محکومیتهای کیفری؛ یعنی مجرمینی که در دادگستری موضوع تحقیق و بازپرسی قرار گرفته‌اند به دست می‌آید. در دادگستری در کنار برگ محکومیت یا حکم معمولاً بایستی فیش هائی را مأمورِ دفترِ دادگاه پر کند که در آن، کلیه خصوصیات محکوم منعکس است. براساس این فیش ها آمار جنائی بوجود می‌آید و مورد استفاده محقق جرم شناسی قرار می‌گیرد.

امروزه، با توجه به بیشتر شدن دادگستری‌ها و ثبت کلیه جرایم در دفاتر خدمات قضایی و تشکیل اولیه پرونده در این دفاتر می‌توان به راحتی آمار جرایم اعلام شده به قوه قضاییه را مشخص کرد و با توجه به عنوان مجرمانه اعلامیه بزه‌دیده را به دست آورد؛ اما متاسفانه به دلیل عدم یک قانون جامع و کامل برای جرایم رایانه‌ای و انطباق آن به عنوان ماده قانونی، نمی‌توان میزان دقیق جرایم سایبری را مشخص نماییم؛ چرا که امروز هر دفتر خدمات قضایی شکایت اعلامی را با هر عنوان که خود تطبیق دهد ثبت می کند، ولی اگر مشخص باشد که عناوین سایبری چه جرایمی می باشند می توان نرخ واقعی جرایم را که منجر به صدور حکم محکومیت گردیده را از (سیستم cms دادگستری) اخذ نمود و مشخص کرد که چه نرخی از جرایم در مرحله دادسرا متوقف یا رسیدگی نهایی شده است و چه عناوینی در مرحله دادگاه منتهی به صدور حکم قطعی گردیده است.

در جرایم نمی توان به طور دقیق به آماری دست یافت، که بتواند به طور قاطع قابل اتکا بوده و بدون شک و شبهه باشد، لذا این سوال پیش می‌آید که ارزش داده های آماری به چه میزان است؟

در پاسخ می‌توان گفت: ارزش داده‌های آمار جنایی با توجه به وجود رقم سیاه و خاکستری در آمار جنایی معلوم می‌شود، «تحقیقات جرم‌شناسی براساس آمار، هیچ گاه دقیق و کامل نیست؛ زیرا آمار جنایی، تصویری از بزهکاری واقعی به ما نمی‌دهند بلکه تصویری را می‌دهد که تهیه کنندگان آنها موفق به اخذ آن شده‌اند.» (سوتیل، ۱۳۸۳: ۷۱-۷۰) آنچه ما به عنوان بزهکار رایانه ای می‌بینیم صرفا آن دسته از بزهکارانی است که دستگاه قضا موفق به کشف و مجازات آن شده است.

بسیاری از جرایم پنهان مانده و در لایه های زیرین جامعه ادامه پیدا می کنند و بعد از سالها، ابعاد گسترده آن‌ها در جامعه مشخص می‌شود که بعضا می توانند ضربه های جبران ناپذیری به جامعه وارد کنند. به همین جهت در جرم‌شناسی برای شناخت و برآورد رقم سیاه، روشهای مختلفی وجود دارد. «قبل از دهه ۱۹۶۰ جرم‌شناسان اغلب اوقات، نظریات خود را بر روی حقایقی که از آمار رسمی به دست می‌آوردند بنا می‌کردند ولی بعد از آن انتقادهایی مطرح شد که معتقد بودند آمارهای رسمی معیاری برای فعالیت سازمان‌هایی است که آمار ارائه می‌کنند تا اینکه معیاری برای نشان دادن میزان واقعی جرایم ارتکابی باشد؛ برای مثال اگر فعالیت نیروی پلیس زیاد باشد اینگونه به نظر خواهد رسید که جرایم بیشتری به وقوع پیوسته است.» (همان)

یکی از چالش‌های جرایم سایبری مشکل کشف این جرایم است. در این نوع از جرایم به دلیل واقع شدن در فضای مجازی و غیر واقعی، اثری ملموس و مادی از جرم و ردپای مجرم، آن گونه که در جرایم سنتی به جای می‌ماند، دیر نمی شود و در بیشتر موارد همان اندک آثار باقیمانده از جرم که قابلیت ردپای مجرم را دارد به راحتی قابل امحاء و پاک سازی است. به همین دلیل می توان با اطمینان گفت که رقم سیاه در جرایم سایبری در مقایسه با جرایم سنتی بسیار بالاست. (شاهمرادی، ۱۳۹۷: ۸۹)

در بررسی دلایل وجود رقم سیاه بزهکاری می‌توان به مواردی مانند عدم توانایی پلیس در کشف جرم، خودداری بزه دیده از طرح شکایت، خارج شدن پرونده از فرایند آمار جنایی به دلیل صدور قرارهای موقوفی تعقیب یا ترک تعقیب یا توقف تحقیقات به لحاظ عدم شناسایی مرتکب جرم اشاره کرد.

آمار جنائی وزارت دادگستری نیز جرائمی را در بر می‌گیرد که در مکان و زمان معین به وقوع پیوسته و بطور مفید در دادگاههای صالحه مورد رسیدگی قرار گرفتند و به محکومیت رسیدند؛ بنابراین آمار قضائی بیانگر بزهکاری واقعی که در یک جامعه به وقوع می‌پیوندند، نیست.

بسیاری از جرایم به دلیل ناشناخته ماندن جزء ارقام سیاه بزهکاری محسوب شده و دستگاه قضایی از کشف آن باز می ماند؛ این دسته از جرایم گاها اثرات جبران ناپذیری بر جامعه می گذارد. البته باید اشاره کرد، مضاف بر عدم کشف این جرایم یا هوش بزهکار، در بسیاری مواقع، عدم پیگیری بزه دیده موجب پنهان ماندن جرم شده و درصد زیادی را به خود اختصاص می-دهد.

متاسفانه آمار قضائی از سویی تعداد کسانی را که تبرئه می‌شوند، نشان نمی‌دهد و از سوی دیگر، در مورد محل دقیق ارتکاب جرم، اطلاعاتی نمی‌دهد در حالی که این موضوع حائز اهمیت است. آمار قضائی در واقع بیانگر رویه و عملکرد قضات کیفری است. چه بسا قضاتی که گرایش به تبرئه کردن دارند و بالعکس قضاتی هستند که با سخت گیری از کیفیات مخففه و یا مکانیزم های تعزیری، استفاده نمی‌کنند و این امر در میزان آمار پرونده های قضایی بی تاثیر نمی باشد؛ بنابراین آمار جنائی وزارت دادگستری باید با احتیاط تلقی شود.

آمار احتیاطی آماری است که از طرف وزارت دادگستری مطرح و بیان می شود و دارای ملاحظات عدیده ای است که در شمار آمار احتیاطی قرار می گیرد. جرایم سایبری دارای خصیصه های مختلفی می باشد یکی از مهمترین خصایص جرائم سایبری آن است که با توجه به ماهیت خاص فضای مجازی بزهکاران سایبری قابلیت شخصیت سازی مجازی و پنهان شدن در قالب یک شخصیت مجازی را دارند که شناسایی آنان را تا حدودی با سختی مواجه می سازد و گاه دیده می شود فرد با هویت مذکر خود را زن معرفی کرده و گاه زنی خود را مرد معرفی می کند، یا به طور کلی فردی بی سواد خود را دکتر یا مهندس معرفی کرده، محل سکونت و سن خود را غیر واقعی معرفی کرده و مخاطب را به اشتباه می اندازند؛ ولی این پیچیدگی در جرایم سنتی وجود ندارد.

با توجه به ماهیت خاص فضای مجازی، یک بزهکار سایبری می‌تواند در مدت کوتاهی قربانیان متعددی را متاثر از اقدامهای مجرمانه خود سازد. مانند فردی که می تواند با غیرفعال نمودن دیتابیس سایت یکی از دانشگاه های کشور هزاران دانشجو را مستاصل و با مشکل مواجه سازد.

۳-۲- روش کیفی

روش کیفی مطالعه جرم با توجه به تعداد محکومیت ها، انواع محکومیت ها و نوع جرائم ارتکابی یا اتهامات و میزان وقوع مجازاتهاست. در روش کیفی با پرونده‌ها و یا مستقیماً با خود مجرمین یا با ارگانها یا کسانی که به عنوان مسئولان اداره بزهکاری هستند سروکار داریم.

مطالعه آرشیوها و پرونده‌های کیفری نشان می دهد که در یک پرونده کیفری، علاوه بر هویت متهم، یک سلسله اطلاعات حقوقی و کیفری وجود دارد که می‌تواند در مقام مطالعه مورد توجه جرم شناسی قرار گیرد که به خصوصیات مجرمین، مربوط می‌شود.

روش دیگری که در چارچوب مطالعات کیفی قرار می‌گیرد، مصاحبه است. هدف در روش مصاحبه جبران عیوب روشهای مطالعاتی کمی است. مثلاً جرمی واقع می‌شود ولی منعکس نمی‌شود یا در محل مصاحبه صورت می‌گیرد و در نتیجه در آمار مورد عنایت قرار نمی‌گیرد؛ لذا از طریق مصاحبه می‌توان به کمّ وکیف آن دست یافت.

البته باید گفت هیچ وقت تمام اظهارات بزه دیده و بزهکار در پرونده منعکس نمی گردد تا بتوان در روش کیفی وضعیت و روحیات بزه دیده و بزهکار را مورد کنکاش قرار داد و بر اساس آن در خصوص پیشگیری از جرم و باز اجتماعی نمودن مجرمین اقدام نمود و بزه دیده که معمولاً در جرایم سایبری از نظر روحی و روانی با مشکلات زیادی مواجه می شود را درمان نمود.

نوعی دیگر از روش کیفی استخراج و کسب نظر از متخصصان بزهکاری یا مدیران پدیده بزهکاری از قبیل پلیس، وکلا، انجمن حمایت از زندانیان و بالاخره کسانی که مستقیم یا غیرمستقیم با مجرمین و وسائل انحراف زا سر و کار دارند.

آخرین روشی که می‌تواند در چهارچوب مطالعات کیفی مطرح شود، مطالعات تعقیب کننده است، که بعد از اتمام دوره مجازات باید نسبت به محکوم صورت گیرد. این مطالعه به منظور تاثیرحبس در ذهنیت مجرمین صورت‌می‌گیرد.

تک نگاری یا منوگرافی به منظور کشف یک سری واقعیتهای بخصوص مثل جرم سقط جنین یا زنا انجام می‌یابد. از آنجا که آمارهای بدست آمده به دلائلی نرخ واقعی بزهکاری را به ما نشان نمی‌دهد، پس همواره برای محقق جرم‌شناسی بخشی از بزهکاری تاریک می‌ماند که به آن «رقم سیاه» می‌گویند که با توجه به نوع جرم مختلف است مثلاً در قتل رقم سیاه نسبتاً کم بوده ولی رقم سیاه در جرائم تهدید به هتک حیثیت در جرایم سایبری، بسیار زیاد است، بنابر این می‌توان گفت: دو نوع بزهکاری داریم.

جرم‌شناسان برای رسیدن به رقم بزهکاری سعی کرده‌اند به روش‌هائی غیر از روشهای سنتی متوسل شوند و لااقل خواسته‌اند مقداری از رقم سیاه بعضی از جرائم را کشف کنند و اندکی خود را به بزهکاری واقعی نزدیک کنند. برای رسیدن به این هدف، دو روش به کار گرفته‌اند.

۳-۳- شیوه های تکمیلی

یکی از راه‌های اساسی برای از بین بردن شکاف میان آمار کیفری و آمار واقعی رویدادهای جنایی، برگزاری پیمایش‌های جنایی است. پیمایش های راجع به رویدادهای جنایی، به طورکلی در دو شاخه پیمایش های بزهکاری و بزه دیده گی قابل تقسیم می‌باشند. درهر دو مورد، پژوهشگران یا مجریان پیمایش بر پایه پرسش نامه یا سایر شیوه های کسب اطلاعات، به دنبال درک تجربه های جنایی جامعه نمونه خود به عنوان بزه کار یا بزه دیده یا شاهد یا آگاه از رویدادهای جنایی اند.

۳-۳-۱-روش پرس و جو

روش پرس و جو، عبارت است از تهیه پرسش‌نامه و توزیع بین یک گروه، بسته به موضوع و هدف از نظر سن، تحصیلات، شغل و... گروه می‌تواند، متفاوت باشد. این پرسش‌نامه شامل مواردی است که مورد نظر محققین بوده است. از این طریق فرد بنا بر اعتمادی که دارد بوقوع جرم اعتراف می‌کند؛ بنابر این اطلاعات می‌توان رقم سیاه را تخمین زد. در این روش اصل بر اعتماد و اطمینان می‌باشد و مهم‌ترین آن در خصوص بزهکاری اطفال می‌باشد.

۳-۳-۲-روش مبتنی بر اظهارات مجنی علیه

یکی از شیوه‌های تکمیلی، روش مبتنی بر اظهارات مجنی علیه است که اساس این روش، توسل به مجنی علیه است، البته نه مجنی علیهی که جرم آن به اطلاع پلیس رسیده باشد؛ محققین بنا به مصالحی وقوع جرم را به اطلاع پلیس نمی‌رسانند و جرائمی مثل جرائم علیه خانواده و ناموس در این حیطه قرار می‌گیرند که گاها به خاطر ترس از بی آبرویی و برچسب های

جامعه، پنهان مانده و رسیدگی نمی شوند. از این جا می‌توان به یک فرمول مهم دست یافت که عبارت است از رقم سیاه بزهکاری ظاهری؛ بنابراین می‌توان گفت: آمارجنائی فقط شامل بزهکاری گزارش شده نمی‌شود و شامل بزهکاری پنهان نیز می‌باشد.

۴- ساختار بزهکاری ظاهری و قانونی سایبری

برخی از علل ساختاری عامل رشد بزهکاری، ناامنی و به طورکلی تضعیف همزیستی مشترک می باشند. شهرسازی و زندگی شهری، رشد فزاینده داشته است، چنانچه بر اساس آمار سازمان ملل متحد، امروزه نیمی از جمعیت دنیا در محیط شهری زندگی می کنند؛ لذا توجه به این تحولات شهری، عاملی مهم، در انتخاب نوع تدابیر پیشگیرانه است، در واقع همزیستی فعالیت های شغلی مختلف، نوع مدیریت فضاهای عمومی، شکل نظارت و کنترل انبوه جمعیت، فی نفسه می تواند بر رفتار افراد و تعامل آنها با یکدیگر تاثیر گذارد؛ از این رو اگر چه شهر ممکن است خاستگاه مشکلات و مسایل باشد، لیکن به طور بالقوه از ظرفیت های پیشگیرانه ای نیز برخوردار نمی باشد.

تاکنون داده‌های کمی بررسی شده درباره مجموع تبهکاری کشورهای مختلف غربی بوده است. صفات برجسته ساختار تبهکاری کشورهای غربی را می توان از تجزیه تعداد کلی استنتاج کرد و مورد بررسی قرار داد. درواقع تاکنون به شرح این ساختار از نقطه نظر صرفا کیفی اکتفا شده بود و اینک شایسته است بیشتر به عمق مساله پرداخت.

۴-۱- ساختار بر اساس بزه ارتکابی

تجزیه و تحلیل جرائم درک ساختار تبهکاری غربی را در سه راستای مختلف شدت، طبیعت ، محل ارتکاب جرم میسر سازد: که به تجزیه و تحلیل آن‌ها خواهیم پرداخت.

شاید نتوان بر اساس شدت، برای ساختار جرایم سایبری تقسیم بندی کاملی کرد؛ زیرا ما قانون خاصی برای این جرایم نداریم، به نظر می رسد، پدیده تهدید برخط از شدت بیشتری برخوردار باشد؛ تهدید از منظرجرم‌شناسی هر نوع رفتار اعم از کلام فعل یا حرکت عمدی است که به طور مکرر مستقیم یا غیرمستقیم در فضای سایبری و در چهارچوب و بستر رابطه قدرت نابرابر بین افراد با هدف ایجاد رنج لطمه آزار رنجاندن و ستم صورت می‌گیرد.

بر اساس این تعریف تهدید بر خط مجموعه رفتارهایی را در بر می‌گیرد که می‌تواند به شکل مستقیم یا غیر مستقیم همچون ایجاد فشار و انتشار شایعه و یا طرح در فضای مجازی از طریق استفاده از فناوری اطلاعات و ارتباطات ارتکاب یابد، چنانچه اتفاقات بسیار شدیدی در پی این تهدیدات پیش آمده که اگر امروز مهمترین جرم را قتل و آن هم قتل های ناموسی به دلیل فرار از این جرم پیش آمده است و دختر برای خلاصی از این تهدیدات دست به خودکشی زده است. در کشور ما نباید جرایم سایبری را ساده انگاشت؛ زیرا خود زمینه ساز جرایم سنتی می باشد.

۴-۲- ساختار جرایم سایبری بر اساس محل ارتکاب

بزهکاری سایبری از پویایی خیره کننده ای برخوردار بوده و رفتارهای مجرمانه در این نوع بزهکاری، متنوع و پویا هستند؛ برخی از آنها کاملا و برخی دیگر همان جرایم متداولی بوده که در بستر سامانه و شبکه های اطلاعاتی به شکل دیگری ارتکاب پیدا می کنند. همان طور که تاکنون گفته شد، جرم اینترنتی جرمی است که در فضای مجازی واقع می شود. این جرایم در

حال حاضر در قوانین کیفری ایران تصویب شده و از طریق مجتمع قضایی ویژه و دادگاههای تخصصی که به منظور پیگیری این دسته از جرایم توسط قوه قضائیه در نظرگرفته شده اند، قابل تعقیب هستند.

بدیهی است که جرائم اینترنتی خاص کشور ایران نیست و در همه جای دنیا به عنوان چالش مطرح و به نوعی همه ی کشورها را درگیر و آسیب دیده این دسته از جرایم هستند، این جرایم می تواند حتی از نظر روحی و روانی، افراد را تحت تاثیر قرار دهد، آسیب های روانی، ایجاد خشونت و عصبانیت، افزایش انواع افسردگی و ایجاد حس تنهایی، حس های کاذب احساسی بزه دیده، از همین نوع آثارند که در اکثر مواقع، اثرات آن پنهان و نا محسوس است.

گسترش شبکه‌های جهانی رایانه‌ای، مرزهای جغرافیایی را با خلل روبه رو کرده است و استفاده از شبکه‌های جهانی اینترنتی به شدت رو به افزایش است. همین که پیوستن به شبکه‌های اینترنتی افزایش می‌یابد ـ یعنی جایی که بسیاری از افراد با هم تبادل اطلاعات دارند ـ مباحث حقوقی، اعم از کیفری و خصوصی به شکل تازه‌ای مطرح می‌گردد.

نامعین بودن حیطه‌های جغرافیایی قوانین و مقررات حاکم بر بستر عبور و مرور در فضای مبادلات اینترنتی بی شک، از مقررات موجود برای مبادلات تجاری در دنیای واقعی، بسیار متفاوت می باشد. بخش عمده‌ای از این تفاوت ناشی از خصوصیاتی است که در اینترنت، زمینه حضور راه دور را فراهم می‌آورند و شبکه را به لحاظ فن‌آوری از بُعد مکانی و فیزیکی متمایز می سازند. موقعیت شبکه آن چنان به موقعیت جغرافیایی بی‌ربط است که اغلب تعیین مکان فیزیکی یک منبع یا کاربر اینترنتی ناممکن است. اطلاع از این موقعیت مکانی برای عملکرد شبکه و ایجاد کنندگان آن اهمیتی ندارد، لذا در طراحی یک شبکه امکان تشخیص مکان جغرافیایی در نظر گرفته نشده است.

در فضا و مکان واقعی، یک شرکت یا طرف تجاری معمولاً می‌تواند مکانی واحد یا شخصی را که با او در تبادل است شناسایی نماید. چرا که این کار به شناسایی طرفین و اعتبار و مشروعیت مبادلات کمک خواهد کرد، اما انجام این کار در محیط مجازی رایانه‌ای بسیار دشوار است. فضای مجازی این امکان را برای افراد فراهم می کند که بتوانند به راحتی در فضای تبادل اطلاعات گام بردارند و هر آنچه می خواهند را جست و جو کنند؛ زیرا در اینجا طرفین یک مبادله ممکن است در دو اتاق هم جوار یا در دو سوی جهان باشند و شبکه هم راهی برای تشخیص این تفاوت ارائه نمی‌دهد. (حسینی، ۱۳۹۴: ۶۹) ماشین‌های اینترنتی «آدرس» دارند ولی این آدرس جایگاه آنها را در شبکه مشخص می‌کند نه در مکان و موقعیت اراضی. البته بعضی آدرس‌های اینترنتی مشخص‌کننده‌های جغرافیایی، یا مشخص‌کننده‌هایی که از نظر جغرافیایی قابل تعیین باشند را در خود دارند. برای مثال، یک آدرس اینترنتی که پسوند (UK) را داشته باشد در بریتانیای کبیر(United Kingdom) قرار دارد.

اغلب کشورهای اروپایی از جمله، فرانسه، بلژیک، آلمان و ... دارای رژیم حقوقی نوشته هستند. ولی متأسفانه اکثر آدرس‌های اینترنتی فاقد چنین تعیین‌کننده‌های جغرافیایی بوده اند. مهم تر از آن، تمام آدرس‌های اینترنتی به راحتی قابل انتقال هستند، زیرا برخلاف آدرس‌های فیزیکی در فضای واقعی زندگی آدرس‌هایی قراردادی در شبکه هستند.

به عبارت دیگر، هیچ گونه هماهنگی و هم سویی بین فضا و مکان واقعی از یک سو و فضای مجازی رایانه‌ای وجود ندارد مثلا در مورد مسائل مربوط به صلاحیت قضایی در قبال جرائم، تقریباً همیشه با در نظر گرفتن محل ارتکاب آنها بیان می‌شوند، توضیح آن که در جرائم کیفری همواره ملاک تشخیص صلاحیت در رسیدگی های قضای (محل وقوع جرم) است که با توجه به ماهیت خاص فضای مجازی تشخیص محل وقوع جرم در جرائم سایبری موضوعی مهم می باشد؛ این بدان دلیل است که صلاحیت قضایی جنایی همواره بر مبنای حضور واقعی و فیزیکی مجرم در درون حوزۀ استحفاظی و در مقابل میز محاکمه تعیین می‌شود. (نای، ۱۳۸۶: ۱۵۳)

براساس قواعد صلاحیت قضایی اگر عنصر مادی یک جرم درون حوزۀ قضایی شروع یا کامل شده باشد، آن حوزه قضائی صالح برسیدگی خواهد بود. اکنون در قانونگذار در فصل جرائم رایانه ای بیان می دارد؛ چنانچه جرم رایانه ای در محلی کشف یا گزارش شود؛ ولی محل وقوع آن معلوم نباشد، دادسرای محل کشف مکلف است تحقیقات مقدماتی را انجام دهد؛ چنانچه محل وقوع جرم مشخص نگردد، دادسرا پس از اتمام تحقیقات مبادرت به صدور قرار می کند و دادگاه مربوط نیزرای مقتضی را صادر خواهد کرد. یا در مورد جرائم چند صلاحیتی، مانند آدم‌ربایی، تنها کافی است که یک عنصر مادی از جرم، درون یک حوزه قضائی در حال انجام باشد تا آن حوزه صالح به رسیدگی شناخته شود. تعامل و ادغام این قوانین ممکن است کاربران اینترنتی را با احتمال مجرم بودن در هر حوزه ذی صلاحی که با اینترنت در ارتباط است روبرو کند.

همچنین ماهیت اینترنت امکان ارتباط متقابل بین چندین حوزۀ قضایی را فراهم آورده و عناصر یک جرم ممکن است نه تنها در مکان و حوزه‌ای با حضور فیزیکی مجرم شروع شده، و یا به نتیجه رسیده باشند، بلکه این امکان نیز هست که در تمام حوزه‌های دیگری که در اثر عملکرد کاربر به صورت الکترونیکی درگیر شده‌اند نیز بحث وقوع جرم مطرح باشد.

مسئله مهم اینجاست که با توجه به ماهیت جرایم اینترنتی تعیین محل وقوع جرم و یا محل حصول نتیجه همیشه و به آسانی مقدور نیست و به فرض شناسایی محل ارتکاب جرم و یا محل حصول نتیجه جرم (در صورت تعدد محلهای ارتکاب)، کدام حوزه صالح به رسیدگی خواهد بود و اگر چندین کشور درگیر چنین جرایمی شده باشند، اینکه کدام کشور و مهمتر اینکه داخل هر کشور، کدام‌یک از حوزه‌های قضایی داخلی، صالح به رسیدگی خواهند بود، موضوع بحث‌است!

آنچه حائز اهمیت است نحوه ی برخورد کشورها با این جرایم و جرم انگاری آن است تا بتوانند راه فرار برای بزهکار بسته و به خوبی با آسیب های این نوع جرایم برخورد کنند هر جامعه ای بر اساس اهمیتی که برای گروه های آسیب پذیر جامعه قائل است قوانین خاص خود را در این حوزه مشخص می کند. طبیعی است که در صورت عدم وجود قانون مصرح به قواعد عام جزایی رجوع می گردد. البته ذکر این نکته ضروری است که جرائم رایانه ای که قانون گذار محل وقوع جرم را ملاک قرار داده است به نفع بزه دیده می باشد؛ چرا که بزه دیده غالبا در همان محل وقوع جرم است و از طرفی در غالب موارد بزهکار در آن محل وجود و حضور فیزیکی ندارد.

۵-نتایج

روند رو به رشد جرایم رایانه‌ای و افزایش چشمگیر سوءاستفاده گسترده مجرمین از رایانه و سامانه های رایانه‌ای و مخابراتی و بالا بودن حجم خسارات وارده موجب بروز مشکلات عدیده ای در جوامع مدرن امروزی از جمله جوامع حقوقی گردیده است؛ چرا که فناوری اطلاعات باعث ایجاد ارزش های جدیدی در جامعه شده است که حمایت از آن نیازمند ضمانت اجرای کیفری می باشد. بدیهی است بروز چنین انقلابی سیاست جنایی نوینی می طلبد تا بتوان به طور موثر با چالش های آن مقابله کرد.

فضای سایبر خیلی متفاوت از فضای حقیقی که ما درآن زندگی می‌کنیم می باشد چرا که امروزه در فضای حقیقی اگر جرمی اتفاق بیفتد ضابطین و دستگاه قضایی سریعاً ورود پیدا می‌کنند و ادله جرم را جمع آوری و از امحا آن جلوگیری می کنند و متهم را دستگیر می کنند ولی این امکان در فضای سایبر وجود ندارد و با توجه به انعطاف پذیری عناصر تشکیل دهنده جرم در زمان و مکان یعنی اینکه اثری مادی و ملموس از جرم باقی نمی ماند و اینکه مشخص نیست بزهکار در چه زمانی و از چه مکانی این جرم را انجام داده است؛ چرا که فضای سایبر یک محیط عرضی است و نه طولی و افراد مختلف در گوشه و کنار دنیا

با هم ارتباط دارند و همه در این فضا به یک میزان صاحب حق هستند و ناشناس ماندن نسبی مرتکبان در این فضا باعث شده است تا دادستان و ضابطین در جرایم سایبری نتوانند سریعاً ورود پیدا کنند و ادله را جمع آوری یا مجرم را دستگیر نمایند.

منابع

۱. ابری، نسیبه. (۱۳۸۷). فضای مجازی عرصه ظهور خلاقیت. اولین کنفرانس ملی خلاقیت شناسی.

۲. باستانی، برومند. (۱۳۸۶). جرایم رایانه ای و اینترنتی . تهران: انتشارات بهنامی.

۳. حاجی ده آبادی، احمد. سلیمی، احسان. (۱۳۹۳). اصول جرم انگاری در فضای سایبر با رویکرد انتقادی به قانون جرایم رایانه ای. فصلنامه مجلس و راهبردها. شماره ۸۰.

۴. حسینی، محمد. (۱۳۹۴). جرایم رایانه ای، تهران: میزان.

۵. سوتیل، کیت. و دیگران. (۱۳۸۳). شناخت جرم شناسی. مترجم میرروح الله صدیق. تهران: نشر دادگستر.

۶. شاهمرادی، خیراله. طهماسبی،جواد. زمستان (۱۳۹۷). چالش ها و خلاهای موجود در فرایند رسیدگی به جرایم سایبری. مجله حقوقی دادگستری. شماره ۱۰۴.

۷. عالی پور، حسن. (۱۳۹۵). حقوق کیفری فناوری اطلاعات. چاپ چهارم. تهران: معاونت حقوقی و توسعه قضایی قوه قضاییه. مرکز مطالعات توسعه قضایی.

۸. فریبرزی، الهام. (۱۳۹۱). سیر تحول قوانین مرتبط با جرایم رایانه ای درایران و جهان. تهران:انتشارات میزان.

۹. کی نیا، مهدی. (۱۳۸۶). مبانی جرم شناسی. تهران:انتشارات میزان.

۱۰. مک کوئیل، دنیس. (۱۳۹۵). مخاطب شناسی. ترجمه مهدی منتظر قائم. تهران: مرکز مطالعات و تحقیقات رسانه.

۱۱. نای، جوزف. (۱۳۸۶). قدرت در عصر ارتباطات از واقع گرایی تا جهانی شدن. ترجمه سعید میرترابی. چاپ دوم. تهران: پژوهشگاه مطالعات راهبردی حسن جعفری.

۱۲. نجفی ابرند آبادی، علی حسین. (۱۳۸۹) از جرم شناسی حقیقی تا جرم شناسی مجازی. چاپ دوم. تهران: انتشارات میزان.

۱۳. ولد، جرج. و دیگران. (۱۳۸۰). جرم شناسی نظری. ترجمه علی شجاعی. تهران:انتشارات سمت.

۱۴. ویلیامز، ماتیو. (۱۳۸۷). بزهکاری مجازی بزه انحراف و مقررات گذاری برخط. مترجم امیر حسین جلالی فراهانی و محبوبه منفرد. تهران: انتشارات میزان.