

نیمرخ جرم‌شناختی بزه کاران سایبری

حسین محمد کوره‌پز* - سید محمود میرخلیلی** - عبدالعلی توجهی*** - حمید بهره‌مند****

(تاریخ دریافت: ۹۳/۸/۳ - تاریخ پذیرش ۹۴/۲/۱۹)

چکیده

فن نسبتاً نوین ترسیم نیمرخ جنایی با مشارکت جرم‌شناسان، روان‌شناسان و مأمورین اجرای قانون درصدد است با به تصویر کشیدن ویژگی‌های احتمالی بزه کاران پرخطر از گذر بررسی آمار و پرونده‌های محکومین پیشین و مصاحبه با بزه دیدگان مستقیم یا با مشاهده صحنه جرم و آثار به جای مانده از رفتار مرتکب، نیمرخ‌های جنایی از آنان ارائه و در نتیجه در راستای شناسایی آنان گام بردارد. این فن توان شناخت دقیق مرتکبین را ندارد، بلکه دایره مظنونین احتمالی را چنان محدود می‌کند تا مأمورین اجرای قانون بتوانند مرتکب واقعی را شناسایی کنند. استفاده از این فن تنها در ارتباط با جرایم پرخطر و آن دسته از بزه‌کارانی که به دشواری شناسایی می‌شوند، منطقی و امکان‌پذیر است. از این رو، می‌توان از این فن به منظور شناسایی برخی گونه‌های بزه‌کاران سایبری نیز بهره برد. رایج‌ترین گونه‌های طراحی نیمرخ جنایی عبارت است از: نخست؛ ایجاد یک نما از ویژگی‌های جمعیت‌شناختی - اجتماعی و روانی - رفتاری و نیز انگیزه‌های محکومین سابق (رویکرد استقرایی) و دوم؛ بررسی صحنه جرم و سپس تحلیل داده‌های گردآوری شده از آن (رویکرد استنتاجی). به دلایلی که اشاره خواهد شد، در این نوشتار بر گونه نخست، یعنی ترسیم نیمرخ جنایی به معنای خاص، تمرکز شده است. یافته‌های این پژوهش که با تمرکز بر مطالعه وضعیت متهمین و محکومین جرایم سایبری در ایران به دست آمده، برخلاف نظر برخی جرم‌شناسان، نشان می‌دهد که به‌طور کلی بزه کاران سایبری به‌مانند سایر بزه کاران از گروهی متجانس و همگن تشکیل نمی‌شوند و انگیزه‌های آنان نیز متفاوت از بزه کاران دنیای واقعی نیست. با این حال، برخی از ویژگی‌هایی که بدون پشتوانه علمی - تجربی نمایش داده می‌شود، می‌تواند به نحو بارزی در بزه کاران سایبری محض و نه بزه کاران بهره‌بردار از فضای سایبر، مشاهده شود.

واژگان کلیدی: نیمرخ جنایی، بزه کاران سایبری، شناسایی مجرم، ویژگی‌های جمعیت‌شناختی - اجتماعی، انگیزه‌های جنایی.

* کارشناس ارشد حقوق کیفری و جرم‌شناسی از پردیس فارابی دانشگاه تهران (نویسنده مسئول). kourepaz@ut.ac.ir
لازم به توضیح است که این نوشتار، برگرفته از پایان‌نامه کارشناسی ارشد این جانب با عنوان «نیمرخ جنایی بزه‌کاران سایبری» است.

** دانشیار گروه حقوق کیفری و جرم‌شناسی پردیس فارابی دانشگاه تهران mirkhalili@ut.ac.ir

*** استادیار گروه حقوق جزا و جرم‌شناسی دانشگاه شاهد. atavajjohi@yahoo.com

**** استادیار گروه حقوق کیفری و جرم‌شناسی دانشگاه تهران bahremand@ut.ac.ir

درآمد

۱. فن ترسیم نیمرخ جنایی^۱ در بستر پاسخ به یکی از بزرگ‌ترین دغدغه‌های اصلی مأمورین اجرای قانون؛ یعنی شناسایی بزهکاران جرایم سریالی ایجاد شده است (Rogers, 2003)؛ زیرا از یک سو ویژگی‌های جرایم سریالی نظیر انجام بزه به صورت انفرادی، وجود اختلالات رفتاری-روانی در مرتکبین و عدم وجود رابطه پیشینی بزهکار- بزه دیده، شناسایی مرتکبین این جرایم را در مقایسه با سایر جرایم دشوارتر می‌سازد. همچنین از سوی دیگر این دسته جرایم به سرعت خبرساز شده و تهدیدات گرانباری از جمله احساس ناامنی و ترس از بزه‌دیدگی را به جامعه تحمیل می‌کند. با این وجود، باید اشاره داشت که جرایم سریالی در اینجا موضوعیتی ندارند و چنانچه هر جرمی از این ویژگی‌ها برخوردار باشد، می‌توان از این فن به منظور کشف و شناسایی آن‌ها بهره برد.

۲. در عصر نوین شاید هیچ جرمی به مانند جرایم سایبری را نتوان سراغ داشت که بزهکاران آن بدین شکل معادلات شناسایی را برای مأمورین تحقیق پیچیده ساخته باشند. بستر سایبر به واسطه ویژگی‌های خاص خود، در وهله نخست شناسایی بزهکار و در مراتب پسینی، کشف بزه را دشوار ساخته است. افزون بر ویژگی‌هایی که فضای سایبر به بزهکاری اعطاء کرده است، ابزارهای سنتی تحقیقاتی نیز در رویارویی با این جرایم به شدت ناکارآمد و فاقد اثربخشی لازم می‌باشند؛ زیرا مسلم است که با رایانه‌ای شدن صحنه جرم^۲، تجهیز کنشگران عرصه بزهکاری به سلاح‌های نوین و بالطبع بهره‌برداری آنان از روش‌های ارتکاب جرم متناسب با آن، نمی‌توان از ابزارهایی که هیچ سنخیتی با آن ندارند، بهره جست. لذا پی‌جوئی جرایم سایبری مستلزم کاربست تدابیر روزآمد است. در این راستا، در چند سال اخیر فن ترسیم نیمرخ جنایی به واسطه امتیازات خاصی که دارد، ذهن پژوهشگران عرصه جرم‌شناسی فضای سایبر و مأمورین تحقیق واحد پلیس سایبری را به خود معطوف ساخته است و آنان را متقاعد ساخته که این شیوه، یکی از مؤثرترین و کم‌هزینه‌ترین روش‌های مبارزه با جرایم سایبری است. البته باید اشاره داشت که به جهت نوظهور بودن استفاده از این فن در جرایم سایبری ضروری است تا جرایم پرخطر سایبری و آن دسته از جرایمی سایبری که هزینه‌های سنگین سیاسی-اقتصادی را به بار می‌آورند، در اولویت قرار گیرند (Erbschloe 2001: 266)؛ زیرا استفاده از این فن حداقل در

1. Criminal Profiling
2. Scene of Crime

رویکرد استقرایی^۱ مستلزم آن است که دستگاه قضایی-پلیسی به گردآوری داده‌های تفصیلی این بزه‌کاران اقدام کند تا با استقراء بتوانند رفتار بزه‌کار موردنظر را پیش‌بینی نماید. حتی چنانچه این سازوکارها به طرز مطلوبی مهیا شوند، این فن همچنان به جهت آنکه مستلزم مشارکت متخصصین رشته‌های گوناگون است، روند انجام تحقیقات را تا حدی به درازا می‌کشاند.

۳. با این توضیحات مشخص می‌شود که ترسیم نیمرخ از بزه‌کار، مستلزم نگرشی عمیق به ویژگی‌های جمعیت‌شناختی-اجتماعی و رفتاری-روانی عموم مرتکبین قبلی، مشاهده صحنه ارتکاب جرم و نیز نشستن بر بالین بزه‌دیده‌ی مستقیم و گفتگو با وی است تا با تحلیل آن‌ها بتوان به سرخ‌هایی دست پیدا نمود که ما را در شناسایی بزه‌کار یاری‌رسان باشد (Matsumoto 401: 2009)؛ اما باید اشاره کرد که تمامی الگوهای ترسیم نیمرخ جنایی از مدل واحدی پیروی نمی‌کنند. فن ترسیم نیمرخ جنایی از دو الگوی اصلی برای طراحی نیمرخ جنایی بهره می‌برد: نخست؛ رویکرد استقرایی یا پایین به بالا که بر تعمیم بخشی ویژگی‌های جمعیت‌شناختی-اجتماعی و روانی-رفتاری محکومین سابق و نیز انگیزه‌های آنان تکیه دارد و رویکرد استنتاجی یا بالا به پایین^۲ که شواهد و مدارک به دست آمده از صحنه جرم و نه ملاحظات آماری را برای تجزیه و تحلیل مورد خاص و سپس برای بر ساخت یک نیمرخ رفتاری خاص (تنها برای همان پرونده تحت بررسی) کافی می‌داند. در رویکرد استقرایی، شناسایی مرتکبین احتمالی در سایه‌ی دو شاخص اصلی؛ یعنی شناخت رفتار عمومی بزه‌کاران سایبری و نیز انگیزه‌های آنان از گذر بهره‌برداری از اطلاعاتی که پیشتر در پایگاه داده‌های مجرمین موجود است، استفاده می‌شود و ویژگی‌های شخصیتی و رفتاری آنان با آن مورد تطبیق داده می‌شود.^۳ از میان این دو الگو، امروزه متخصصین امنیتی به‌طور فزاینده‌ای علاقه‌مند به استفاده از ویژگی‌های عمومی بزه‌کاران سایبری در چنین اقداماتی می‌باشند؛ یعنی شناسایی خود بزه‌کاران سایبری و شخصیت آن‌ها در

1. Inductive

2. Deductive

۳. از مهم‌ترین زیرگونه‌های الگوی استقرایی می‌توان به مدل روان‌شناسی تحقیقاتی (Investigative Psychology) و مدل اداره تحقیقات فدرال امریکا (اف.بی.آی) اشاره کرد. همچنین مدل تجزیه و تحلیل دلایلی رفتاری (Behavioral Evidence Analysis) از شاخص‌ترین زیرگونه رویکرد استقرایی است (جهت مطالعه تفصیلی کارکرد این دو گونه الگو بنگرید به: محمد کوره‌پز، حسین (۱۳۹۳)، **نیمرخ جنایی بزه‌کاران سایبری**، پایان‌نامه دوره کارشناسی ارشد حقوق کیفری و جرم‌شناسی، پردیس فارابی دانشگاه تهران (دانشکده حقوق)، صص ۱۴۱-۱۳۳).

معنای وسیع کلمه (Lickiewicz 2011)^۱. در واقع آنچه ما آن را «نیمرخ جرم شناختی بزهدکاران سایبری» نامیده‌ایم^۲. از مزایای الگوی استقرایی نسبت به الگوی استنتاجی می‌توان به این نکته اشاره کرد که در بیشتر موارد داده‌های مرتبط با صحنه جرم سایبری - حتی بیش از جرایم دیگر - شکننده، مبهم و غیرقابل دسترس و در نتیجه غیرقابل اعتبارند. همچنین، دسترسی دشوار به بزه دیده و مصاحبه با وی و حتی در صورت دسترسی، دستیابی به اطلاعات دقیق و واقعی و نه گمراه کننده بسیار دشوارتر است. از این رو، مدل استنتاجی حداقل در حال حاضر، کمتر مورد اقبال طراحان نیمرخ جنایی قرار گرفته است. این نوشتار، در چارچوب ترسیم نیمرخ جنایی استقرایی گام برمی‌دارد و با تکیه بر ویژگی‌های جرم شناختی بزهدکاران سایبری که از آمارها و یافته‌های پژوهشی داخلی و خارجی به دست آمده است، به تبیین و تحلیل این ویژگی‌ها و نیز انگیزه‌های جنایی آنان می‌پردازد.

۴. اگرچه در پژوهشی دیگر پیرامون ضرورت انعکاس یافته‌های روان شناختی در ترسیم نیمرخ جنایی بزهدکاران، به ویژه بزهدکاران سایبری سخن گفته شده است (محمد کوره‌پز ۱۳۹۳)، اما نه تنها نویسندگان حاضر در این زمینه در ادبیات پژوهشی ایران موردی را ملاحظه نکردند؛ بلکه در پژوهش‌هایی که در سایر نقاط دنیا انجام شده نیز تحقیقات صرفاً نظری و بدون پشتوانه‌های علمی-تجربی است یا بر پایه شبیه‌سازی ویژگی‌های یک گونه از بزهدکاران سایبری با هموعان کلاسیک خود صورت گرفته است. در این زمینه می‌توان نیمرخ روان شناختی تروریست‌های سایبری را مثال زد. برخی نویسندگان تنها بر مبنای اینکه چون یافته‌های پژوهش‌های اندک گذشته در ارتباط با تروریست‌ها نشان می‌دهد که آنان دارای ویژگی

۱. گفتنی است در گفتمان عدالت تخمینی یا سنجشی، بزهدکاران با توجه به عامل‌ها و متغیرهایی از قبیل پیشینه مجرمانه، نوع محکومیت کیفری، سن، مجرد و تأهل، جنسیت، بی‌کاری و اشتغال، خارجی یا بومی بودن، اعتیاد یا عدم اعتیاد، میزان تحصیلات، مسکن، محله، مهاجر بودن و غیره - شاخص‌های خطر - به منظور احتمال خطر ارتکاب و تکرار جرم گروه‌بندی می‌شوند و نیمرخ از این بزهدکاران خطرناک به منظور پیش‌بینی رفتار مجرمانه احتمالی شان ترسیم و طبقه‌بندی می‌گردد (نجفی ابرندآبادی ۱۳۸۸: ۷۲۹). در واقع، اگر کیفرشناسی نو که در این چارچوب شکل گرفت را از مرحله جرم‌یابی تا بعد از اجرای مجازات در امتداد بدانیم، نیمرخ‌سازی یکی از سیاست‌های کیفری است که در زمینه کشف زود هنگام از جرم ارتکابی، اعمال می‌گردد. از این رو به نظر می‌رسد گرچه پیشینه تکنیک نیمرخ‌سازی به سالیانی پیش از شکل‌گیری و بالندگی جرم‌شناسی نو - کیفرشناسی نو بازمی‌گردد اما نقطه اوج به کارگیری این تکنیک مصادف با پیدایش آن است؛ زیرا این تکنیک، اهداف این الگوی سیاست جنایی را به نحو آشکاری دنبال و سامان می‌بخشد.

۲. به نظر ما اصطلاح نیمرخ جرم شناختی می‌تواند بیش از هر دانش‌واژه‌ای، ذهن خواننده را از ملاحظاتی که مرتبط با شواهد و مدارک صحنه جرم است منصرف و بر ویژگی‌های جمعیت شناختی-اجتماعی و روانی-رفتاری معطوف نماید.

شخصیتی «هیجان‌طلبی»^۱ و «احساس حقارت»^۲ هستند، این ویژگی‌های روان‌شناختی را به تروریست‌های سایبری نیز تعمیم داده‌اند (Kirwan 2013: 202). در حالی که بدیهی است اگرچه برخی همسانی‌ها میان آن‌ها وجود دارد، اما باید گفت در میزان خطرپذیری و نیز نوع و شدت استفاده از حملات خشونت‌آمیز، کاملاً بر یکدیگر منطبق نیستند. از این رو، در اثر حاضر به ملاحظات روان‌شناختی بزه‌کاران سایبری پرداخته نشده است. با این حال، خلأ پژوهش مستقلی در این زمینه به شدت احساس می‌شود.

۵. گفتنی است طراحی جنایی از بزه‌کاران سایبری در مقایسه با سایر بزه‌کاران، به دلیل ماهیت پیچیده جرایم سایبری، مشکلات کشف جرم و شناسایی بزه‌کاران آن و همچنین دشواری‌های مربوط به مصاحبه و پیمایش از مجرمین، متخصصین این رشته را در بر ساخت. نیمرخ جنایی از بزه‌کاران سایبری، در شرایط پیچیده‌تری قرار می‌دهد. افزون بر این، رفتار مجرمان سایبری نیز به مانند خود این جرایم پویا و به سرعت در حال تغییر است.^۳ همان‌طور که این نکته را به آشکارا می‌توان در طبقه‌بندی‌های پیشینی از بزه‌کاران سایبری نسبت به طبقه‌بندی‌های نوین مشاهده نمود و ممکن است یافته‌های امروزی نتوانند برای مدت زیادی اساس تحقیقات جنایی قرار گیرند (Jahankhani and Al-Nemrat 2010). با این حال، چنانچه این نیمرخ‌ها به صورت علمی و دقیق طراحی شوند، ضمن آنکه می‌توانند ما را در درک جامع و دقیقی از رفتار بزه‌کاران سایبری کمک کنند (با یک رویکرد جرم‌شناختی) از آن می‌توان به منظور پیش‌بینی رفتار احتمالی بزه‌کاران و در نتیجه شناسایی بزه‌کار نیز بهره‌برداری نمود (با اتخاذ رویکرد جرم‌یابی).

بنابراین، در این نوشتار ابتدا به تفصیل به مهم‌ترین ویژگی‌های جمعیت‌شناختی-اجتماعی بزه‌کاران سایبری پرداخته می‌شود (بند الف) و سپس به انگیزه‌های اصلی ارتکاب جرم در

1. Sensation-Seeking

2. Feelings of Humiliation

۳. این پویایی و تنوع را به وضوح می‌توان در گونه‌های نوظهور جرایم سایبری مشاهده نمود. گونه‌های نخستین جرایم سایبری بیشتر به عنوان جرایم علیه محرمانگی، صحت و تمامیت داده‌ها مطرح بودند، اما با تصویب کنوانسیون جرایم سایبر در سال ۲۰۰۱ و گنجاندن «جرایم علیه محتوا» در این کنوانسیون، به نوعی حمله به عواطف انسانی نیز ممنوع گردید (جهت مطالعه بیشتر پیرامون گونه‌های مختلف سوءاستفاده برخط و جرایم سایبری بنگرید به: فیشر، بونی. اس و پی. لب. استیون، دانشنامه بزه‌دیده‌شناسی و پیشگیری از جرم (جلد اول)، ترجمه: اساتید حقوق کیفری و جرم‌شناسی سراسر کشور (زیر نظر: علی حسین نجفی ابرندآبادی)، تهران: میزان، ۱۳۹۴، صص ۳۵۵-۳۵۳.

فضای سایر اشاره می‌شود (بند ب)؛ زیرا در کنار این ویژگی‌ها، شناخت و طبقه‌بندی انگیزه‌های بزهکاران افزون بر این که تکمیل‌کننده ویژگی‌های مورد اشاره بوده و موجبات طراحی نیمرخ جرم‌شناختی دقیق‌تر و شناسایی فرد حمله‌کننده را فراهم می‌آورد، می‌تواند در شناسایی عوامل این برانگیختگی‌ها و در نتیجه به کارگیری تدابیر کنترل‌کننده یا بازپرورانه، یاری‌رسان باشد.

الف) ویژگی‌های جمعیت‌شناختی - اجتماعی بزهکاران سایبری

چنانچه از ما پرسیده شود «به نظر شما بزهکاران سایبری از چه ویژگی‌هایی برخوردارند»، به احتمال زیاد پاسخ خواهیم داد که آن‌ها برخلاف ویژگی‌های نوعی بزهکاران عادی، از هوش، دانش و سطح تحصیلات و نیز از تمکن مالی بیشتری نسبت به سایر بزهکاران برخوردارند (نجفی ابرندآبادی ۱۳۸۸: ۹). البته چنانچه کمی افراطی‌تر باشیم ممکن است آنان را گونه‌ای از بزهکاران یقه‌سفید بدانیم (عالی‌پور ۱۳۹۰: ۸۱). این گفتار درصدد است ضمن بررسی عمده ویژگی‌های بزهکاران سایبری، سازگاری این انگاره‌ها با یافته‌های علمی را محک بزند. همچنین به این پرسش پاسخ دهد که اساساً چه تفاوت‌هایی میان بزهکاران سایبری و عادی وجود دارد. در واقع، با دوزیستی انسان‌ها در فضای سایبر و دنیای خاکی، آیا بزهکاران این دو فضا از ویژگی‌های اجتماعی و جمعیت‌شناختی یکسانی برخوردارند یا خیر.

۱- بزهکاران سایبری: از قالب‌واره‌های ذهنی (کلیشه‌ها) تا انگاره‌های علمی

در اینجا به شاخص‌ترین ویژگی‌های جمعیت‌شناختی-شخصیتی بزهکاران سایبری اشاره می‌شود و در سنجش با پیمایش‌های صورت پذیرفته، آنان مورد ارزیابی علمی قرار می‌گیرند. با توجه به محدودیت‌ها و موانعی که پیشتر اشاره شد، از یک سو پیمایش و مصاحبه‌های اندکی پیرامون بزهکاران سایبری انجام شده و از سوی دیگر عمده پیمایش‌ها معطوف به هرزه‌نگاری است. لذا این یافته‌ها ناظر به بخشی از بزهکاران سایبری است. همچنین پژوهشگران اگرچه در سال‌های اخیر تمایل به مقایسه بزهکاران سایبری و کلاسیک پیدا نموده‌اند، اما این موارد بسیار نادر و بیشتر به توصیف تفاوت‌های جمعیت‌شناختی بزهکاران جنسی کلاسیک و سایبری پرداخته شده است که در ادامه به آن‌ها اشاره می‌شود.

۱-۱- سن

سن یک عامل جرم‌زای فردی گذرا و انتقالی است. این عامل در حقوق کیفری به‌منظور تمیز سن مسئولیت کیفری و در جرم‌شناسی و بزه‌دیده‌شناسی از لحاظ تفکیک بزهکاری اطفال و بزرگسالان، مورد توجه قرار می‌گیرد.^۱ از منظر جرم‌شناسی، یافته‌های تحقیقاتی نشان می‌دهند که در هر رده سنی، گونه‌ای از بزهکاری یا بزه‌دیدگی در میان افراد آن طبقه وجود دارد. برای نمونه در دوران طفولیت، کودکان ممکن است بزه‌دیده‌ی جرایمی چون تکدی‌گری (در این موارد فرد بزه‌کار- بزه‌دیده است)، ترک نفقه، آدم‌ربایی و غیره شوند. چنانکه وندالیسم یا خرابکاری در بین نوجوانان و جوانان شایع‌ترین جرم است و موارد معدودی از وندالیسم میان سالان و سالمندان گزارش شده است.^۲ یا برعکس، برخی جرایم مختص افرادی است که در طبقه سنی بالایی قرار دارند. بارزترین نمونه از چنین بزهکارانی، مجرمین یقه‌سفید هستند (فورچی‌بیگی ۱۳۹۲)؛ اما به‌عنوان یک قاعده کلی باید گفت که میان بزهکاری و سن (حداقل در فراوانی) رابطه‌ی معکوسی وجود دارد؛ به‌گونه‌ای که با افزایش سن، بزهکاری کاهش می‌یابد.

در ارتباط با کنشگران فضای سایبر نیز باید گفت در سنجشی که در سال ۲۰۰۳ میان برخی کشورها پیرامون رده‌ی سنی کاربران اینترنت انجام شد، نشان داد که در کشورهای نظیر کره (۹۵ درصد)، ایالات متحده آمریکا (۹۱ درصد)، ژاپن (۸۱ درصد) و انگلستان (۸۰ درصد) نوجوانان و جوانان ۱۶-۲۴ سال، بیشترین استفاده از اینترنت را داشته‌اند (توکل و کاظم‌پور ۱۳۸۴: ۱۲۰)؛ بنابراین، می‌توان گفت که علی‌الاصول بیشترین فراوانی بزه سایبری نیز باید متعلق به آنان باشد.

در ایران، از بررسی پرونده‌ی ۴۵ محکوم به تولید و انتشار تصاویر مستهجن مشاهده می‌شود که کمترین سن ۱۹ و بیشترین ۵۴ سال و در مجموع، میانگین سنی آن‌ها ۲۶/۲ است (معاونت آموزش و تحقیقات قوه قضائیه ۱۳۸۹: ۲۳۸-۲۰۹). همچنین، آمار پلیس فتا پیرامون میانگین

۱. جهت مطالعه بیشتر پیرامون جایگاه «سن» در علت‌شناسی بزهکاری و سیاست‌گذاری جنایی بنگرید به: نجفی ابرندآبادی، علی حسین، **درباره سن و علوم جنایی**، دیپاچه در: مبانی پیشگیری اجتماعی رشد‌مدار از بزهکاری اطفال و نوجوانان، نوشته محمود رجایی پور، تهران: نشر میزان (چاپ اول)، چاپ دوم کتاب، ۱۳۹۱: ۱۷-۱۳.

۲. تحقیق‌های انجام‌شده در ایران نشان می‌دهند که در ترکیب سنی افراد وندال دستگیر شده، ۶۷/۵ درصد آنان در گروه سنی ۱۰ تا ۲۵ سال قرار داشته‌اند، سهم گروه سنی کمتر از ۱۰ سال ۳/۶ درصد و بقیه متعلق به گروه ۲۶ سال به بالا است (شمسه، ۱۳۸۱).

سنی متهمان جرایم سایبری در بازه زمانی سال ۹۰ تا تیر ۹۱ نشان می‌دهد که ۷۷/۶ درصد متهمین دارای میانگین سنی ۱۷-۳۵ است (به نقل از: ابوذری ۱۳۹۱) شکل ۲-۲ به تفکیک گروه سنی، میزان متهمین جرایم سایبری را نشان می‌دهد.



شکل ۱- میانگین سنی متهمین جرایم سایبری در ایران

بررسی ۱۶۵ پرونده جرم سایبری در تایوان نیز نشان می‌دهد که بیشترین جرایم متعلق به گروه سنی ۳۰-۳۳ سال است و هرکدام از بزهکاران گروه سنی ۴۰-۳۰ و ۵۰-۴۱ سال، تنها ۴/۳ درصد از کل جرایم را مرتکب شده‌اند (Liao and Tasi 2006: 54).

البته نباید پنداشت که کل جرایم سایبری را نوجوانان و جوانان مرتکب می‌شوند. بر اساس اعلام بخش جرایم رایانه‌ای و مالکیت معنوی وزارت دادگستری ایالات متحده^۱، ۳۴ درصد از مجرمین درون‌سازمانی^۲ بین ۲۹-۲۰ سال، ۳۶ درصد بین ۳۵-۳۰ سال و ۲۷ درصد بیش از ۳۷ سال سن دارند. هرچند بیشتر مرتکبین بین ۳۰ و ۳۵ سال هستند، اما بیشترین آسیب، توسط افراد بیش از ۳۵ سال مانند راجردورونیو^۳ با ۶۰ سال سن متهم به سرقت ۳ میلیون دلار، تیموتی آلن لوید^۴ ۳۹ ساله متهم به بیش از ۱۰ میلیون دلار و کوین میتنیک^۵ ۳۷ ساله متهم به بیش از ۱ میلیون دلار وارد شده است (Nykodym, Taylor and Vilela 2005).

1. US Department of Justice (Computer Crime and Intellectual Property Section)
2. Insider criminal
3. Roger Duronio
4. Timothy Allen Lloyd
5. Kevin Mitnick

همچنین با توجه به بررسی بخش مذکور پیرامون سارقین سایبری، مشاهده می‌شود که الگوی معناداری در میان سن آنان وجود دارد. اگر سرقت کمتر از صد هزار دلار باشد، به احتمال زیاد مهاجم ۲۰ تا ۲۵ ساله است و هنوز در رده پایین سلسله‌مراتب سازمان قرار دارد. اگر ارزش جرم بین صد هزار تا یک میلیون دلار باشد، مرتکب جرم به احتمال زیاد بین ۲۵ تا ۳۵ سال و مرد است و چنانچه جرم بیش از یک میلیون دلار باشد، مهاجم بالای ۳۵ سال سن داشته و جزو کادر مدیریتی است (Nykodym, Taylor and Vilela 2005).

بنابراین به استثنای برخی جرایم (تروریست‌های سایبری، جاسوس‌های سایبری و نفوذ کارمندان که یا از متخصصین امنیت شبکه هستند یا بدین منظور شیوه‌های ارتکاب را به‌طور تخصصی می‌آموزند)، عمده جرائم ارتكابی توسط افراد زیر ۳۰ سال صورت می‌گیرد. دلیل این امر نیز روشن است؛ چراکه به جهت سطح پایین مهارت و تخصص افراد میان‌سال و سالمند، نه تنها ارتکاب جرم سایبری برای آنان بسیار دشوار بلکه حتی گاه انجام کارهای شخصی آنها با کمک سایرین صورت می‌گیرد! پس می‌توان گفت جوامعی که هرم سنی آنها در قاعده کم‌عرض‌تر است (جوامع به اصطلاح پیر) نرخ جرم سایبری کمتری دارند. با پذیرش این استدلال باید گفت، در یکی دو دهه آینده بزهکاری افراد میان‌سال نیز شایع‌تر خواهد بود.

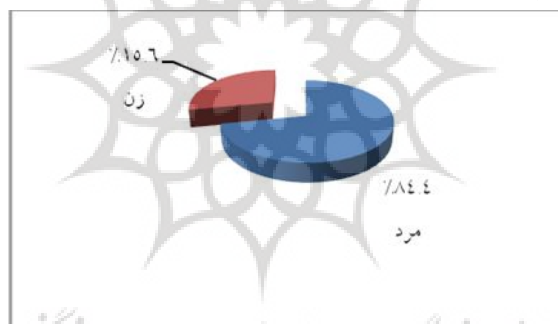
۲-۱- جنسیت

آنچه واضح است، نسبت نابرابری از بزهکاری میان مردان و زنان وجود دارد. هرچند در سال‌های اخیر با رشد مسئولیت‌پذیری و مشارکت زنان در جامعه نرخ بزهکاری زنان رشد یافته است، اما هنوز در بسیاری از جرایم فاصله‌ی ارقام بزهکاری مردان با زنان زیاد است (رستمی تبریزی ۱۳۸۸). به گونه‌ای که در سال ۲۰۰۹ اداره تحقیقات فدرال آمریکا گزارش داد که از ۳۰ میلیون متهم دستگیر شده، ۷۵ درصد مرد و تنها ۲۵ درصد آنها زن می‌باشند و ۸۱ درصد جرایم

۱. مارکوس رجز و همکاران وی نیز در دو پیمایش خود گزارشی (Self Report) دریافتند که در ارتباط با جرایم مرتبط بانفوذ و دسترسی غیرمجاز (هک)، افراد ۱۷-۳۰ سال بیشترین کسانی هستند که در این رفتار منحرفانه/مجرمانه سایبری مباشرت دارند.

look; Rogers, Marcus K. Seigfried, Kathryn, Tidke, Kirti, "Self-Reported Computer Criminal Behavior: A Psychological Analysis", Digital Investigation: The International Journal of Digital Forensics & Incident Response, vol.3, 2006, pp.116-119; and Rogers, Marcus, K. Smoak N. and Liu J. "Self-Reported Criminal Computer Behavior: A Big-5, Moral Choice and Manipulative Exploitive Behavior Analysis", Deviant Behavior, vol.27, No.3, 2006, pp.245-268;

خشن از سوی مردان ارتکاب یافته است (3: Britton 2011). اطلاعات آماری زندانیان ایران نیز نشان می‌دهد که بیش از ۹۶ درصد از محکومین به حبس، مرد هستند (احمدی ۱۳۸۴: ۲۱۴).
 وراى توجیہات زیست‌شناختی (کی‌نیا ۱۳۸۶: ۱۶۵-۱۵۶ و وفايي ۱۳۷۸) و جامعه‌شناختی (رستمی تبریزی ۱۳۸۸) که پیرامون بزهکاری زنان انجام شده است، باید گفت رویکرد پلیس و برخورد دستگاه عدالت کیفری با بزهکاران زن نیز متفاوت از مردان است و بخشی از این نابرابری آماری می‌تواند ناشی از نگاه مسامحه‌گر دستگاه عدالت کیفری به جنسیت زنان باشد.
 وضعیت بالا تا حد زیادی در ارتباط با جرایم سایبری نیز صادق است. برخی پژوهش‌ها بیانگر وجود رابطه‌ی مستقیم میان جنسیت کاربران و میزان مراجعه به سایت‌های هرزه‌نگاری است. بر اساس یافته‌های پژوهشی با عنوان «مواجهه با تصاویر هرزه‌نگارانه در اینترنت میان کودکان و بزرگسالان»، ۸۲ درصد سایت‌های هرزه‌نگاری را مردان جوان و تنها ۵ درصد از آن‌ها را زنان تشکیل می‌دهند (نگهی ۱۳۹۱). از بررسی ۴۵ محکوم هرزه‌نگاری که در بالا اشاره شد نیز ۸۴/۴ درصد مجرمان مردان و ۱۵/۶ درصد را زنان تشکیل داده‌اند (معاونت آموزش و تحقیقات قوه قضائیه پیشین: ۲۳۸-۲۰۹).



شکل ۲- جنسیت محکومین هرزه‌نگاری در ایران

همچنین پیمایش انجام شده در تایوان نشان می‌دهد که ۹۰ درصد مردان در جرایم سایبری مباشرت داشته‌اند و درصد کمی از زنان آن‌هم در جرایم غیرمالي، بزهکار شناخته شده‌اند (Liao and Tasi 2006: 53).

با وجود مواردی که در بالا اشاره شد، در اندک پژوهش‌های انجام شده نیز جنسیت بزهکاران سایبری مغفول واقع شده و بیشتر مطالعات به نژاد و رنگ پوست آنان معطوف است. برای نمونه تحقیقات در ایالات متحده نشان می‌دهند، مردان سفیدپوست اروپایی زیر ۲۶ سال،

رایج‌ترین نیمرخ مربوط به بزه‌کاران هرزه‌نگاریِ کودکان را دارا می‌باشند (Krone 2004: 5). شاید دلیل اصلی این پیش‌فرض که بزه‌کاریِ سایبری متعلق به مردان است _ در کنار توجهات بالا_ پیچیدگی، فنی و تخصصی بودن جرایم سایبری باشد؛ اما به نظر می‌رسد از آنجا که بیشتر جرایم سایبری تخصص و مهارت زیادی را نمی‌طلبد، نرخ کم بزه‌کاری سایبری زنان ریشه در همان عللی دارد که در ارتباط با جرایم کلاسیک مطرح شد.

۳-۱- سطح مهارت فنی و استعدادهای درونی

معمولاً انتظار می‌رود که بزه‌کار سایبری، فردی دارای دانش تخصصیِ بالا از علوم رایانه‌ای باشد؛ کسانی که حداقل با چند زبان برنامه‌نویسی و نیز به‌طور تخصصی از امنیت رایانه‌ها و سامانه‌ها آشنایی دارند. شاید بتوان این دیدگاه را در ارتباط با جرایم رایانه‌ای که در دهه‌های گذشته روی می‌داد، با اغماض بپذیریم. زمانی که دانش‌آموختگان دانشگاه ام.آی.تی^۱ با مهارت و تخصص دانشگاهی خود به برنامه‌نویسی و ویروس‌نگاری‌های پیشرفته اقدام می‌نمودند و جز خود آن‌ها، کسی توان مقابله با آن‌ها را نداشت (Shinder 2002: 138)؛ اما امروزه با پیشرفت‌های سخت‌افزاری و نرم‌افزاری رایانه‌ای و نیز پیدایش اینترنت، بزه‌کاران سایبری به راحتی یک اشاره بر موشواره می‌توانند آنچه را پیشتر به دشواری انجام می‌شد را عملی سازند.

اما تصور رایج نادرست‌تر آن است که سطح مهارت فنی^۲ تمامی بزه‌کاران سایبری، همگن و متجانس انگاشته شود. یافته‌های یک پژوهش نشان می‌دهد که از مجموع ۲۳۹ نفر مورد مطالعه، ۲۱ درصد مهارت فنی پایین، ۲۲ درصد مهارت بالا، ۲۴ درصد متخصص و ۳۲ درصد توان فنی متوسط دارند (Chiesa 2009: 45). در واقع، اگرچه هنوز برخی شیوه‌های ارتکاب^۳ نظیر حملات ممانعت از سرویس‌دهی توزیعی^۴ در گستره سایبر به جهت ایمن بودن سامانه‌ها و شبکه‌ها نیازمند مهارت‌های عالی رایانه‌ای است، اما امروزه بیشتر جرایم سایبری با حداقل مهارت و تلاش روی می‌دهند. در این زمینه می‌توان به مهارت حداقلی ریزه‌خواران^۵ اشاره نمود. حتی در حملاتی که از پیچیدگی زیادی برخوردارند، افراد می‌توانند با مشورت

1. Massachusetts Institute of Technology (MIT)
2. Technical Skills
3. Modus Operandi
4. Distributed Denial of Service (DDoS)
5. Script Kiddies

پیرامون مشکل خود در شبکه اجتماعی هکرها یا با خرید نرم افزارهای خود کار و از پیش طراحی شده‌ی نفوذ، نسبت به آن اقدام کند. از روش‌های جدید جبرانِ خلأ نداشتن مهارت لازم می‌توان به اجیر کردن نوجوانان به منظور طراحی حمله و برنامه‌نویسی اشاره کرد که به‌نوعی می‌توان آن را شکل جدیدی از «کودکان کار» دانست (Jahankhani and Al-Nemrat 2010).

با توضیحات بالا می‌توان به این پرسش که «آیا سطح هوش بزهاران سایبری نسبت به سایر بزهاران بیشتر است؟» نیز پاسخ داد؛ زیرا این کلیشه در ذهن ما رخنه کرده که «چون هکرها (ما بزهاران سایبری را همان هکرها می‌دانیم) دست به اعمال خارق‌العاده می‌زنند، پس توانمندی‌های ذهنی-هوشی بالا و استعدادهای ویژه‌ای دارند». درحالی که این تعمیم ناروا است. پس اگرچه هوش بالا یا به عبارتی توانایی استدلال، تجزیه و تحلیل و فکر منطقی، اثربخشی حمله را تضمین می‌کند، اما آن دسته از بزهارانی که از نرم افزارهای تألیفی دیگران یا برنامه‌های نفوذ بارگیری شده^۲ بهره می‌برند، لزوماً نباید ضریب هوش^۳ بالایی داشته باشند. با این وجود، پاسخ شفاف‌تر به این پرسش نیازمند ارزیابی‌های دقیق‌تر و مطالعات بیشتری است.

۴-۱- سطح تحصیلات

مطالعات گوناگون نشان می‌دهد که رابطه معکوسی میان سطح تحصیلات و بزهارکاری وجود دارد؛ به این صورت که هرچه سطح تحصیلات بالاتر رود، فرد کمتر به ارتکاب جرم اقدام می‌کند (مظلومان ۱۳۵۴)؛ اما به نظر ما این فرضیه حتمی و غیرقابل رد نیست؛ زیرا اگرچه سطح سواد یک جامعه می‌تواند شاخصی برای توسعه یافتگی یک کشور تلقی شود، اما ضرورتاً کاهش بزهارکاری را به دنبال ندارد. حتی با لحاظ عواملی نظیر توسعه‌ی شهرنشینی، افزایش جمعیت-به‌عنوان شاخص‌های افزایش جرم در دو سده اخیر- و در کنار آن پیشرفت‌های فناورانه و رشد علم در جوامع بشری و سطح تحصیلات مردم شاهد آن هستیم که به نسبت افزایش سطح سواد جوامع، نه تنها بزهارکاری کاهش نیافته بلکه در آشکال و فراوانی سیر صعودی داشته است.

از سوی دیگر حتی با چشم‌پوشی از یافته‌هایی که رابطه معکوسی میان بزهارکاری و سطح تحصیلات نشان نمی‌دهند، برای نمونه یافته‌های بوزا و پیناتل نشان می‌دهند که در یک بازه

1. Child Labor
2. Download
3. Intelligence Quotient (IQ)

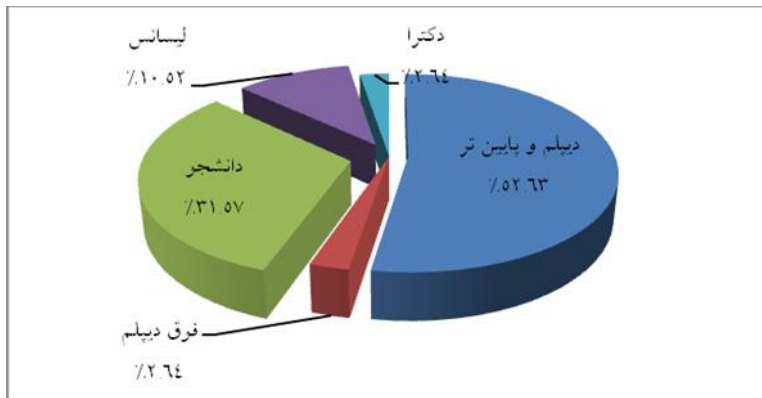
زمانی ۸۰ ساله اگرچه تعداد بی‌سوادها تا ۹۰ درصد کاهش یافته، اما از نرخ جرم کاسته نشده است. ممکن است انتقاد شود که میزان افزایش جمعیت و رشد شهرنشینی در این دوره زمانی لحاظ نشده است، اما به نظر می‌رسد حتی با وجود چنین نقیصه‌ای، نباید نرخ کاهش جرم تا این اندازه ناچیز باشد (مظلومان ۱۳۵۴). باید گفت موضوع مطالعه اکثر این پژوهش‌ها جرایم خشن یا مبتنی بر زور می‌باشند. لذا حداقل دستاورد این یافته‌ها آن است که سطح سواد با بزهکاری خشن رابطه معکوس دارد و نمی‌توان آن را به‌تمامی آشکال جرایم تسری داد.

یک پیمایش خود گزارشی در میان دانشجویان سال اول تا سال چهارم در کانادا نشان داد که ۸۸ درصد شرکت‌کنندگان در رفتارهای مجرمانه‌ی سایبری نظیر استفاده از رمز عبور دیگران بدون اجازه آن‌ها، تغییر و جستجو در فایل‌های دیگران بدون اجازه آن‌ها، استفاده از ویروس‌های تألیفی یا ویروس‌نگاری به منظور اعمال خرابکارانه و به‌دست آوردن رمز کارت اعتباری دیگران و غیره مباشرت داشته‌اند (Rogers, Seigfried and Tidk 2006). رجز و دیگران، هدف خود از انتخاب چنین جامعه آماری را جذابیت چنین رفتارهای منحرفانه نزد نوجوانان و جوانان بیان می‌دارند (Rogers, Seigfried and Tidk 2006)؛ بنابراین می‌توان گفت از آنجا که نوجوانان و جوانان بیش از هر رده‌ی سنی دیگر در اعمال مجرمانه سایبری دخالت دارند و از آن‌رو که بیشتر افراد در این سنین مشغول تحصیل در دانشگاه‌ها یا دانش‌آموخته می‌باشند، پس می‌توان نتیجه گرفت که افراد دانشجویی یا تحصیل کرده بیش از اقشار دیگر می‌توانند به‌عنوان بزهکار سایبری شناخته شوند.

در پژوهشی دیگر، میزان تحصیلات در کنار سایر ویژگی‌های جمعیت‌شناختی افرادی که به جستجو، دستیابی، بارگیری یا تبادل تصاویر هرزه‌نگاری کودکان اقدام نموده‌اند، سنجیده شد. از میان ۲۸ پرسش‌نامه، ۳/۶ درصد شرکت‌کنندگان مدرک تحصیلی خود را کمتر از دیپلم، ۱۴/۳ درصد دیپلم، ۶۰/۷ درصد فوق‌دیپلم یا لیسانس و ۲۱/۴ درصد فوق‌لیسانس یا دکتری اعلام نمودند (Seigfried, Lovely and Rogers 2008).

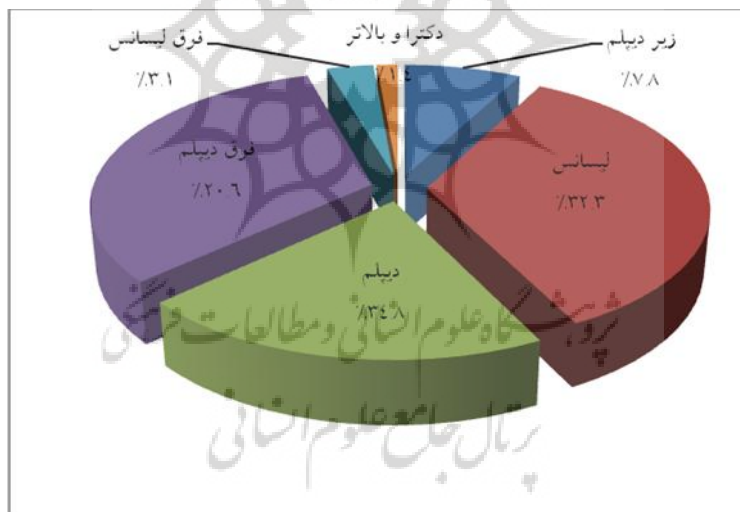
البته با ملاحظه‌ی ۳۸ پرونده‌ی محکومین هرزه‌نگاری از مجموع ۴۵ پرونده‌ی موجود (در ۷ پرونده میزان تحصیلات محکومین ذکر نشده بود) مشخص شد که این بررسی تا حدی با مطالعه اخیر همخوانی دارد. در ۲۰ پرونده محکومین تحصیلات دیپلم و کمتر داشتند و در ۱۸ پرونده آن‌ها فوق‌دیپلم به بالا - یک نفر فوق‌دیپلم، ۱۲ مورد دانشجویی، ۴ مورد لیسانس و یک دکتری -

می‌باشند (معاونت آموزش و تحقیقات قوه قضائیه ۱۳۸۹: ۲۳۸-۲۰۹).



شکل ۳- سطح تحصیلات محکومین هرزه‌نگاری در ایران

داده‌های آماری پلیس فتا نیز که در محدوده زمانی سال ۹۰ تا تیرماه ۹۱ به دست آمده است (به نقل از: ابوذری، ۱۳۹۲)، به شکل قابل توجهی با مورد پیشین همخوانی دارد.



شکل ۴- سطح تحصیلات متهمین جرایم سایبری در ایران

شاید دلیل اصلی این مشابهت، عدم لحاظ شرایط محدودکننده در جامعه آماری باشد؛ چراکه در مطالعه‌ی نخست، پژوهشگران جامعه آماری خود را تنها معطوف به دانشجویان

نمودند. البته باید اشاره کرد که جرایم مورد بررسی مطالعه‌ی نخست در زمره جرایم سایبری محض می‌باشند و این جرایم نسبت به سایر جرایم سایبری، به دانش و مهارت بیشتری نیاز دارند. لذا بدیهی است که معمولاً افراد تحصیل کرده‌تر این جرایم را مرتکب می‌شوند. موردی دیگری که نباید از یاد برد، آن است که رشد تحصیلات در کشورهای مختلف، یکسان نیست و در جوامع توسعه‌یافته یا دانشگاهی نظیر هند و مالزی، نرخ بیشتری از جرم در میان تحصیل کردگان را شاهد هستیم.

پس به‌طور کلی می‌توان گفت وضعیت تحصیل در تمامی بزه‌کاران از جمله بزه‌کاران سایبری نیز همگن نیست. برای نمونه پژوهشی که پنج سال به طول انجامید، نشان می‌دهد بزه‌کاران سایبری به‌مانند سایر بزه‌کارانی که به سایر جرایم نظیر ضرب و جرح و برگرگی محکوم شده‌اند، از سطح تحصیلاتی متفاوتی برخوردار می‌باشند (Durost 2006: 5-6). از سوی دیگر باید اذعان داشت در جرایم سایبری به دلیل آنچه در بالا آمد، اغلب افراد تحصیل کرده بیش از سایرین دست به ارتکاب جرم می‌زنند.

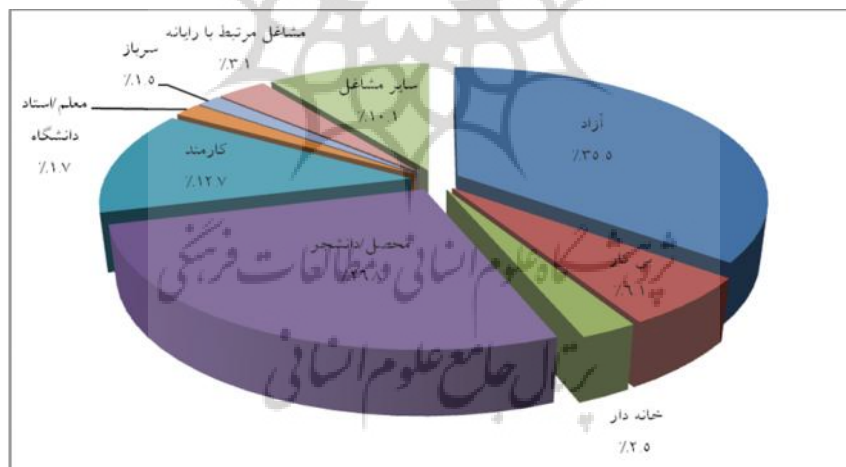
۵-۱- پیشینه خانوادگی و زمینه‌های شغلی

تصور رایج ما از خانواده‌ای که یک بزه‌کار سایبری/هکر در دامان آن پرورش یافته، خانواده‌ای محروم و سطح پایین است که پدر و مادر هیچ نظارتی بر فرزند خود ندارند، پدر و مادر از هم جدا شده یا طلاق گرفته‌اند یا به دلیل مشکلات روانی یا رفتاری به‌طور مداوم در حال مشاجره با یکدیگر می‌باشند. گاه فرزند مدت طولانی از آغوش پرمهر یکی از والدین محروم می‌شود و یا به جهت الکل‌بارگی و دیگر رفتارهای انحرافی والدین، کودک در دوران رشد خود دچار اختلال می‌گردد. پس به‌طور کلی، هکرها به‌مانند بیشتر بزه‌کاران در دوران کودکی و نوجوانی از سوی والدین خود حمایت عاطفی و مورد مراقبت نبوده‌اند. از این‌رو، معمولاً هکرها به خاطر شخصیت ضداجتماعی و درون‌گرایی خود در مدرسه نیز دوستان زیادی ندارند. آن‌ها با فرار از تمامی موج‌های نایمن زندگی، به ساحل امنی چون فضای مجازی رسیده‌اند؛ جایی که می‌تواند اظهار نظر کنند، قدرت از دست‌رفته خود را باز یابند و به عبارتی به تمامی آنچه در دنیای خاکی از آن محروم بوده‌اند، دست یابند.

1. Introversion

اما باید اشاره کرد که همواره وضعیت این گونه نیست. حتی در مواردی به جهت پیوند عمیقی که میان والدین و فرزند وجود دارد، کودک رفتار انحرافی را از والدین می آموزد. برای نمونه در یک پرونده، کودکی سه ساله توانست تحت آموزش و تشویق پدر و مادر خود با اجرای عملیات حملات ممانعت از سرویس دهی^۱ به داده های رایانه ای دیگر، دسترسی یابد (Chiesa, Ducci and Ciappi 2009: 93-94).

همان طور که در بالا اشاره شد بزهکاران سایبری ممکن است از هر قشری باشند و محصور کردن آنها به افرادی خاص، نادرست است. وضعیت اشتغال بزهکاران سایبری نیز از این حال خارج نیست. در واقع، برخلاف آنچه تصور می شود، بزهکاری سایبری منصرف به افراد بی کار و فاقد درآمد نیست. برای نمونه طبق آمار پلیس فتا تنها ۶/۱ درصد متهمین جرایم سایبری بی کار هستند (به نقل از: ابو ذری ۱۳۹۱) (بنگرید به شکل ۵). کما اینکه ملاحظه می شود حتی بعضی از حملات از سوی کسانی که در سازمان/شرکت دارای اختیارات گسترده هستند (بزهکاران درون سازمانی) انجام می شود. برای نمونه پیمایشی نشان داد که ۲۵/۱ درصد بزهکاران دانشجو، ۱۷/۵ درصد بیکار و بقیه مشغول به کار در سازمان های دولتی یا شرکت های خصوصی می باشند. شگفت آور اینکه حتی در چهار مورد، بزهکاران سایبری از استادان دانشگاه بودند (Liao and Tasi 2006: 54).



شکل ۵- زمینه های شغلی متهمین جرایم سایبری در ایران

1. Denial of Service (DoS)

۶-۱- پیشینه مجرمانه

یکی از برجسته‌ترین شاخص‌های سنجش خطرناکی در مطالعات جرم‌شناختی، سابقه‌دار بودن یا به عبارتی «تکرار بزهکاری» است. بررسی این عامل از این جهت مهم است که می‌تواند اساس سیاست‌گذاری‌های عمومی و مبنای راهبردهای جنایی قرار گیرد (غلامی ۱۳۸۲). برای نمونه در ارتباط با کدامین بزهکاران باید از راهبرد اصلاح و بازپروری سود جست یا در ارتباط با گونه‌های خطرناک‌تر بزهکاران، با سرکوب و سلب‌توان آنان را از جامعه حذف نمود.

اما گاه چنانچه این عامل را به‌عنوان تنها شاخص خطر موردنظر قرار دهیم، ممکن است گمراه شویم. برای نمونه مرتکبین جرایم خیابانی برعکس بزهکاران یقه‌سفید اغلب دارای سابقه مجرمانه هستند. از طرف دیگر، پژوهشی پیرامون جرایم یقه‌سفید نشان داد که هیچ‌یک از افراد تحت بررسی پیشتر دست به ارتکاب جرم نزده‌اند (قورچی‌بیگی ۱۳۹۲)؛ اما آیا به‌واقع گروه اخیر خطرناک‌تر نیستند؟^۱

مطالعه‌ای که پیرامون بزهکاران سایبری صورت گرفت نیز نشان داد که بیش از ۸۰ درصد بزهکاران هیچ سابقه‌ی مجرمانه‌ای نداشتند و تنها کمتر از ۲۰ درصد آن‌ها پیشتر به جرایمی همچون خرید و فروش مواد مخدر، توزیع لوح‌های فشرده هرزه‌نگاری، سرقت جزئی، قمار و غیره محکوم شده بودند (Liao and Tasi 2006: 54). در مطالعه دیگری که به مقایسه ویژگی‌های جمعیت‌شناختی-اجتماعی بزهکاران سایبری و بزهکاران کلاسیک پرداخت، نشان داده شد که هر دو آن‌ها، پیشتر بدون سابقه مجرمانه می‌باشند؛ اما همان‌طور که گفته شد، افراد باسابقه نیز در میان آنان ملاحظه می‌شود (Rogers 2001: 85).

در نتیجه، به‌صرف پاکی لوحه‌ی مجرمانه متهمین نمی‌توان بیان داشت آنان نسبت به سایرین کمتر خطرناک می‌باشند، بلکه عمل ارتكابی و میزان آسیب‌های وارده نیز باید موردبررسی قرار گیرند. برای نمونه نمی‌توان گفت یک تروریست سایبری که به‌طور سازمان‌یافته تأسیسات هسته‌ای یک کشور را هدف قرار می‌دهد به‌صرف نداشتن پیشینه مجرمانه خطرناک نیست. یا از آنجا که کسی چندین بار مرتکب نقض حق نشر شده است، خطرناک است. پس سابقه

۱. باید اشاره داشت که در یک سیاست جنایی عوام‌گرا، هر جرمی که بیشتر جامعه را ملتهب می‌سازد و مردم را متزجر کند به‌سرعت و مقطعی، بدون بهره‌گیری از متخصصین و بدون اتخاذ یک رویکرد علمی، با آن برخورد می‌شود (بابایی و عباسی ۱۳۹۰)؛ بنابراین در این چارچوب، میزان و معیار سنجش خطرناکی مردم هستند. بدین خاطر جای تعجب نیست که گاه به‌واسطه رسانه‌ای شدن یک رویداد جنایی، صحبت از اعدام حاملان سلاح سرد می‌شود و اولویت نخست دستگاه قضا مبارزه با «اشرار» قرار می‌گیرد و گاهی همه قوا در «مبارزه با مفسد اقتصادی» بسیج می‌شوند.

مجرمانه می تواند به عنوان اماره ای مبنی بر خطرناکی بزهکاران مورد لحاظ قرار گیرد، اما تنها دلیل موجود نیست.

آنچه در پژوهش حاضر آشکارا دیده می شود آن است که بزهکاری سایبری تنها از سوی یک گروه مشخص یا یک طرز فکر و باور واحد سر نمی زند. در واقع، همان طور که ما به هیچ وجه بزهکاران کلاسیک را یک کل متجانس و همگن نمی انگاریم، باید چنین رویکردی را نیز در برابر بزهکاران سایبری اتخاذ کنیم؛ بنابراین، حداقل می توان گفت نتایج تحقیقات تجربی انجام شده در این چارچوب و نیز نتایج تحقیقات میدانی مورد استناد این نوشتار، انگاره های برخی جرم شناسان درباره ویژگی های مجرمین سایبری را ثابت نمی کند.

لذا پژوهش حاضر نشان می دهد، گزاره های زیر به جهت تعمیم شاخص ها و ویژگی های عمومی به تمامی بزهکاران سایبری، نادرست و فاقد پشتوانه علمی-تجربی است:

- تمامی بزهکاران سایبری از ضریب هوشی بالایی برخوردارند و مهارت های فنی آنها در سطح بسیار بالایی است؛

- تمامی بزهکاران سایبری دارای کمترین مهارت اجتماعی می باشند، آنها افرادی گوشه گیر، منزوی و درون گرا می باشند؛

- تمامی بزهکاران سایبری سطح تحصیلات بالا دارند و به طبقه اجتماعی متوسط به بالا جامعه تعلق دارند؛

- تمامی بزهکاران سایبری، مرد و معمولاً پسرهای نوجوان می باشند؛

- تمامی بزهکاران سایبری خطرناک و همواره برای سامانه ها و رایانه ها در دسر ایجاد می کنند؛

- تمامی بزهکاران سایبری روابط عاطفی از هم گسیخته ای با والدین خود دارند یا اغلب

آنها کودکان طلاق یا فرزندخوانده^۲ می باشند؛

۱. شاید هیچ تعبیری به مانند «نرد» به وضوح از شخصیت آنها پرده بر نمی دارد. «نرد» به کسانی گفته می شود که دانشی قدرتمند در زمینه خاصی دارند ولی این دانش را نه برای پول و نه برای مقبولیت اجتماعی، بلکه به خاطر دل خودشان به دست می آورند. «نردها» معمولاً از طرف اجتماعات مختلف طرد می شوند، در ارتباط با جنس مخالف دچار مشکل هستند، ظاهر ژولیده ای دارند و به اصطلاح افرادی «سوسول» می باشند که اگر کسی پیدا نشود و از نبوغشان استفاده کند، از لحاظ مالی دچار بحران می شوند. در میان بزهکاران سایبری، جاسوس ها بیش از سایر آنها، افرادی ساکن و آرام به نظر می رسند. آنها کاملاً مراقب سخنان و نحوه نگاه خود هستند و نمی خواهند متفاوت به نظر برسند. لذا همیشه سعی می کنند با دیگران اختلاط کنند. برای به دام انداختن یک جاسوس، باید دنبال افرادی باشیم که همیشه کارهای خود را پنهان می کنند (Nykodym, Taylor and Vilela 2005: 413).

2. Adoption

- تمامی بزهکاران سایبری به‌مانند مجرمین یقه‌سفید، فاقد هرگونه پیشینه مجرمانه می‌باشند؛
- تمامی بزهکاران سایبری افرادی بی‌کار و فاقد درآمد مشخص می‌باشند؛
- بیشتر بزهکاران سایبری گونه‌ای از بزهکاران یقه‌سفید می‌باشند؛
- و به‌طور کلی:
- همه‌ی آن‌ها نیمرخ واحدی دارند.

البته باید اشاره کرد که برخی از پژوهش‌ها همسو با یافته‌های پژوهش‌های دیگر نشان می‌دهد که آنچه به‌طور کلیشه‌ای به‌عنوان ویژگی‌های بزهکاران سایبری از آن یاد می‌شود، به‌نحو بارزی در بزهکاران سایبری محض نظیر هکرها مشاهده می‌شود (محمدکوره‌پز ۱۳۹۳)؛ زیرا بزهکاران سایبری بهره‌بردار از فضای سایبر، در بیشتر موارد همان بزهکاران کلاسیک‌اند که به‌سلاح رایانه مجهز شده‌اند.

ازاین‌رو، سیاست‌گذاران و نهادهای اجرایی نیز باید نسبت به هریک از بزهکاران سایبری، سیاست و برنامه‌ی متناسب با آن را اساس کار خود قرار دهند (لزوم کاربست سیاست جنایی افتراقی). بی‌تردید رسوخ اندیشه‌های عوام‌گرا در بدنه‌ی برنامه‌ها و سیاست‌های فاقد پشتوانه علمی، بزرگ‌ترین مانع جهت موفقیت راهبردهای پیشگیرانه است. این کلیشه‌های ذهنی از آنجا ناشی می‌شود که ما به‌اشتباه ویژگی‌های یک دسته از بزهکاران سایبری (بخشی و نه همه بزهکاران سایبری محض) را به‌تمامی آنان قابل‌تعمیم می‌دانیم.

۲- بزهکاران سایبری و کلاسیک: همسانی یا گوناگونی

پس از ارائه توضیحاتی در ارتباط با ویژگی‌های اجتماعی و جمعیت‌شناختی بزهکاران سایبری، پرسش کلیدی که به‌ذهن‌خطور می‌کند آن است که آیا اساساً بزهکاران سایبری،

۱. اگرچه ممکن است گفته شود «بدیهی است که از هیچ‌گونه از بزهکارانی، نیمرخ واحدی وجود ندارد»، اما همان‌طور که در بالا به‌تفصیل اشاره شد، این‌انگاره در ارتباط با بزهکاران سایبری کمتر صدق می‌کند: زیرا با توجه به این‌که مطالعات کمتری این واقعیت را نشان داده‌اند و در این‌میان بیشتر رسانه‌ها ذهن عامه مردم نسبت به این بزهکاران را تسخیر کرده و جهت می‌دهند و نیز اینکه هویت یک بزهکار سایبری کمتر از سوی خود مردم - برخلاف سایر بزهکاران - به‌طور ملموس و عینی درک شده است، این امر ضرورت به‌تصویر کشیدن ویژگی‌های آنان بیش از گونه‌های دیگر بزهکاران را توجیه می‌کند. یکی از اهداف اصلی نیز که این پژوهش دنبال می‌کند، شفاف‌سازی این واقعیت است. بدیهی است باید مطالعات گوناگون بیشتری صورت گیرد تا حداقل واقعیت بزهکاران سایبری ایرانی مشخص شود و اساساً در چنین مطالعاتی، تعمیم پیمایش‌های دیگر، گمراه‌کننده و ناروا است.

همان بز هکاران کلاسیک هستند که امروزه به سلاح رایانه و اینترنت مجهز شده‌اند یا گونه‌ای متمایز از آن‌ها می‌باشند؟ پاسخ به این پرسش دشوار به نظر می‌رسد. اگرچه بدین منظور در برخی مطالعات تلاش‌هایی انجام شده است (به‌ویژه در ارتباط با تفاوت یا شباهت بز هکاران جنسی برخط و بز هکاران جنسی برون خط^۱)، اما پاسخ قطعی نیازمند مطالعات بیشتری است. برای نمونه در پژوهشی که در قالب یک «فرا تحلیل»^۲ صورت گرفت، نشان داد که بز هکاران جنسی برخط به احتمال زیاد سفیدپوست و تا حدی جوان‌تر از بز هکاران جنسی برون خط می‌باشند (Babchishin, Hanson and Hermann 2011).

با این وجود نباید پنداشت که ویژگی‌های بز هکاران سایبری و بز هکاران کلاسیک به‌طور کامل برهم منطبق و سازگار است؛ زیرا به جهت تفاوت عمیق بستر بی‌پیکر سایبر با فضای مادی، بی‌تردید ماهیت بزه و گونه‌های بز هکاران را دستخوش تغییر قرار داده است. برای نمونه گستره فضای مجازی نسبت به فضای مادی دارای اهداف مناسب بی‌شماری است و بالتبع این امر برانگیختگی مضاعف هر بز هکاری را در پی دارد. همچنین می‌توان به ویژگی‌هایی مانند ناشناختگی و مخفی ماندن هویت در فضای سایبر اشاره کرد. حتی به نظر ما ویژگی اخیر در ترغیب افراد از طبقات اجتماعی مختلف^۳ و ویژگی‌های جمعیت‌شناختی متفاوت نسبت به بز هکاران کلاسیک، در کنشگری و بالتبع بز هکاری یا بزه‌دیدگی بسیار حائز اهمیت است. چراکه افراد در پشت سپر ناشناختگی، اجتماعی‌تر و نسبت به ارتباطات رودررو آزادتر می‌باشند. آن‌ها به‌واسطه‌ی رشد شخصیت اجتماع‌پذیر، پرخاشگرتر می‌شوند و دیگر کم‌رو و خجالتی نیستند (منفرد و جلالی فراهانی ۱۳۹۱). از این رو ویژگی‌های محیطی، احتمال انحراف آن‌ها را تقویت می‌کند. همچنین، بدین لحاظ که بهره‌برداری سوء از بستر سایبر نیازمند حداقل مهارت و دانش فنی است، نوجوانان و جوانان - بیش از سایر گروه‌ها - باید مخاطب اصلی برنامه‌های کنشی و واکنشی قرار گیرند.^۴

1. Offline

۲. در آمار، فرا تحلیل (Meta-Analysis) داده‌ها عبارت است از ترکیب دو یا چند تحقیق آماری و پاسخ به پرسش تحقیق بر مبنای ترکیب انجام شده است. با تجمع و تحلیل حجم زیادی از داده‌ها، امکان اعتماد به نتایج به‌طور قابل‌توجهی بیشتر می‌شود. به این ترتیب می‌توان گفت که یافته‌های «فرا تحلیل»، اساسی‌تر از یافته‌های مطالعات پژوهشی منفرد هستند.
۳. برای نمونه درحالی‌که برخی بیمایش‌ها نشان می‌دهند آن‌هایی که در خانه‌های سازمانی و سایر ناحیه‌های با درآمد پایین زندگی می‌کنند، نسبت به کسانی که به خانواده‌های ثروتمند و ناحیه‌های حومه و روستایی تعلق دارند، محتمل‌تر است که ریسک ارتکاب جرم را بپذیرند، پژوهش‌های دیگر، وارونه آن را اثبات کرده‌اند (منفرد و جلالی فراهانی، ۱۳۹۱).
۴. در ارتباط با تدابیر واکنشی باید گفت، بدین خاطر که دسته‌ای از این کودکان به سن مسئولیت کیفری نرسیده‌اند، مقابله با

در تأیید آنچه در بالا آمد می‌توان به پژوهش رجرز که به بررسی و مقایسه ۶۶ بزه‌کار سایبری با همین تعداد بزه‌کار کلاسیک اختصاص داشت، اشاره کرد. این مطالعه نشان می‌دهد که جرم سایبری نسبت به سایر جرایم مردانه‌تر است. همچنین، گروه سنی ۲۵-۱۸ بیشترین فراوانی ارتکاب جرم سایبری را دارند درحالی‌که بیشترین فراوانی جرایم کلاسیک متعلق به گروه سنی ۲۶-۳۵ است (Rogers 2001: 86).

ب) گونه‌شناسی انگیزه‌ها

با وجود تعاریف گوناگونی که از انگیزه ارائه شده است،^۱ تمامی آن‌ها به گونه‌ای بر هدف نهایی و آنچه فرد را به انجام کاری سوق می‌دهد، اشاره دارند. به نظر می‌رسد انگیزه «مقصودی است که فرد به منظور آن دست به ارتکاب جرم می‌زند». عوامل مختلفی ممکن است ما را به ارتکاب جرم برانگیزد اما انگیزه اصلی، «هدفی است که چنانچه نباشد، جرم تکوین نمی‌یابد».^۲

اگرچه در حقوق کیفری جز در موارد استثنائی به انگیزه توجه نمی‌شود، اما برعکس این عنصر در علت‌شناسی جرم و پیشگیری از بزه‌کاری بسیار حائز اهمیت است؛^۳ زیرا جرم‌شناسان و سیاست‌گذاران همواره به دنبال آن‌اند تا از گذر انحراف در فرآیند گذار اندیشه به عمل^۴ (پویایی یا دینامیک جنایی) زمینه‌ی تحقق فرصت‌های ارتکاب جرم را خنثی سازند و از آماج

رفتارهای آن‌ها دشوار به نظر می‌رسد. حتی گاه جبران خسارت مدنی نیز از عهده آن‌ها خارج و به‌ناچار والدین آن‌ها باید تاوان آن را بپردازند. به نظر می‌رسد همان‌طور که در شریعت اسلام در سایر جرایم، فرد فاقد مسئولیت تأدیب می‌شود و نه ضرورتاً تنبیه بدنی یا روانی. در این مورد نیز قانون‌گذار ایرانی می‌توانست در قانون جرایم رایانه‌ای، تدابیر تأدیبی این چنینی را برای آنان لحاظ کند. البته به نظر ما هیچ تأدیبی اثربخش‌تر از آموزش؛ یعنی تقویت اخلاقی و برونی‌سازی هنجارها نیست (بنگرید به: بهره‌مند، محمد کوره‌پز و سلیمی، ۱۳۹۳).

۱. برای نمونه مرحوم دکتر نوربها معتقدند «انگیزه تمایلات خودآگاه یا ناخودآگاهی هستند که رغبت، شوق، گرایش‌های مثبت یا منفی را برای شخص در مورد فعالیت‌هایش و برای مجرم در ارتکاب جرم ایجاد می‌کنند» (نوربها ۱۳۸۶: ۱۸۲). همچنین انگیزه به‌عنوان «امری روانی که علت غائی یا هدف یا مقصد نهایی مورد نظر فاعل جرم است»، تعریف شده است (کی‌نیا ۱۳۸۶: ۸۰).

۲. به نظر می‌رسد انگیزه در حقوق کیفری و مدنی واجد یک مشخصه باشد. از این رو به نظر همان تعریف ارائه شده از «جهت» یا انگیزه در حقوق قراردادها، مناسب‌ترین برداشت از انگیزه به‌عنوان عامل ارتکاب جرم است (بنگرید به: کاتوزیان ۱۳۸۶: ۱۴۲).

۳. اولین مکتبی که به انگیزه در ارتکاب جرم توجه ویژه‌ای داشت، مکتب تحقیقی یا پوزیتیویستی بود. به عقیده بنیان این مکتب، انگیزه عنصری است که می‌تواند از حالت خطرناک فرد پرده بردارد (کی‌نیا ۱۳۸۶: ۸۱).

4. Acting Out

آسیب‌پذیر محافظت نماید (پیشگیری وضعی^۱) یا در پیشگیری اجتماعی به‌ویژه پیشگیری رشدمدار با از بین بردن انگیزه‌های مجرمانه، فرد را از ارتکاب جرم در آینده باز دارند (منفرد و جلالی فراهانی، ۱۳۹۱). در حال حاضر نیز با تحول در مفهوم حالت خطرناک و پیدایش یک سیاست جنایی امنیت‌مدار، شاهد آن هستیم که انگیزه در گفتمان نوین سیاست‌گذاری جنایی همچنان کانون توجه است (نجفی ابرندآبادی ۱۳۹۲: ۲۷-۲۳).

اما افزون بر آنچه در بالا بدان اشاره شد، در این گفتار بر آنیم تا بدین پرسش اساسی پاسخ دهیم که آیا انگیزه‌ها در فضای سایبر متنوع‌تر از فضای مادی هستند یا خیر. پیش از بیان این گونه‌ها باید اشاره کرد که طبقه‌بندی‌های متنوعی از انگیزه‌های بزهکاران سایبری انجام شده است. برای نمونه رجرز بر اساس مصاحبه‌هایی که با بزهکاران سایبری و کلاسیک انجام داده است، آن‌ها انگیزه‌ی خود را یکی از چهار مورد زیر بیان کرده‌اند: ۱- انتقام‌جویی (Revenge)؛ ۲- مالی (Financial)؛ ۳- شهرت (Notoriety) و ۴- کنجکاوی (Curiosity) (Rogers: 2010: 221). به نظر می‌رسد، این انگیزه‌ها تنها انگیزه‌های موجود نیستند ولی می‌توان - صرف نظر از انگیزه جنسی - تمام انگیزه‌ها را در این تقسیم‌بندی گنجانده.

اما چنانچه بخواهیم بر اساس گونه‌های رایج جرایم سایبری، انگیزه‌های بزهکاران سایبری را به گونه‌ای طبقه‌بندی کرد که با یکدیگر هم‌پوشانی نداشته باشند، آن‌ها عبارت‌اند از^۲:

۱- پاسخ به گرایش‌های درونی: کنجکاوی - لذت طلبی

یکی از اولین روانشناسانی که پیرامون ابعاد لذت‌طلبی انسان‌ها مطالعه کرد، بیان نمود: «برخی از رفتارها به خاطر لذت حاصل از انجام آن‌ها، صورت می‌گیرند» (Kshetri 2010: 22)؛ بنابراین انسان‌ها همواره سعی دارند در فعالیت‌هایی مباشرت کنند که بتواند حس لذت طلبی و

۱. باین حال نباید تصور شود که تنها با کاربرد تدابیر وضعی می‌توان از جرایم سایبری پیشگیری نمود؛ زیرا چنانچه فرد مصمم به ارتکاب جرم باشد، به‌محض شکست یا ناکامی در یک روش، با جابه‌جایی شیوه ارتکاب به‌منظور دور زدن و از میان برداشتن آماج اقدام می‌نماید.

۲. برخی نویسندگان عمده‌ترین انگیزه‌های جنایی سایبری را به ترتیب: سرگرمی، انگیزه مالی، انگیزه انتقام‌جویانه یا خشونت‌بار و انگیزه جنسی می‌دانند (منفرد ۱۳۹۱)؛ اما آن‌ها بیان نمی‌کنند که چرا این ترتیب را رعایت کرده‌اند. آیا آن‌ها این ترتیب را بر مبنای یک مطالعه تجربی انتخاب کرده‌اند؟ همچنین باید از آن‌ها پرسید چرا انگیزه جنسی در نقطه پایانی این شمارش قرار گرفته است. در حال حاضر به نظر می‌رسد، از لحاظ فراوانی، بیشتر بزهکاران که اکثراً نوجوان و جوان می‌باشند با انگیزه جنسی به ارتکاب جرم برانگیخته می‌شوند. به‌رحال بدون پشتوانه‌ی آماری قطعی، سخن گفتن از این فراوانی دشوار است.

سرگرمی آنان را تأمین کند. البته گاه کسب این حس به قیمت تضییع حقوق دیگران انجام می‌پذیرد و با هنجارهای اجتماعی برخورد می‌کند.

فضای سایبر نیز مملو از محرک‌های گوناگون است که تنوع آن‌ها، تمامی سلايق را پاسخگو است و به نحو خیره‌کننده‌ای انسان تفریح‌گر قرن بیست و یکم را راضی نگه می‌دارد. این محرک‌ها بسته به نوع نگرش و انگیزه مجرم از ارزش متفاوتی برخوردارند. بزه‌کاران پس از برانگیختگی، به سوی این آماج حرکت می‌کنند و هدف خود را نهایی می‌سازند. گاه این کنجکاوی و هیجان‌طلبی به شکل جزئی و در قالب شوخی‌های آزاردهنده با اعضای شبکه و گاه به صورت امنیت‌سنجی سیستم دفاعی یک دولت/شرکت ظهور پیدا می‌کند. با این وجود، این افراد به جهت غیر پیچیدگی حملاتشان، شناسایی آنان دشوار نیست. از این رو، در زمره مشتریان همیشگی دستگاه عدالت کیفری قرار دارند.^۱ مثال‌های فوق نشان می‌دهند که ممکن است افراد با سطح مهارت‌های گوناگون به دنبال سرگرمی و کنجکاوی باشند. در این راستا یک هکر ۱۹ ساله‌ی سرباز ارتش رژیم اشغالگر قدس انگیزه خود از هک را این‌گونه بیان می‌دارد:

«هک، انجام یک کار غیرقانونی و نامشروع پرهیجان، حیرت‌آور و لذت‌بخش است. این عمل به‌مانند زمانی که ما بچه بودیم و دوستانمان بیرون از مغازه‌های کوچک منتظر می‌ماندند و کیک‌های شیرین و جعبه‌هایی از شکلات‌های شیرین می‌دزدیدند، هیجان‌انگیز است» (Goldschmidt 2011: 45).

باید به این نکته اشاره کرد که این افراد از آسیب‌های روانی و خسارات مالی که از رفتارشان ناشی می‌شود، درک کاملی ندارند. به‌جز آن دسته افرادی که احتمالاً از اختلال آزارگری (Sadism) رنج می‌برند، نسبت به سایرین می‌توان با برنامه‌های آموزش محور و یا با کاربردی‌ترین تدابیر وضعی - به‌ویژه با جاذبه‌زدایی - تا حد زیادی فراوانی رفتار آنان را تقلیل داد.

۲- طمع‌ورزی و کسب منافع مالی

با وابستگی فزاینده‌ی روابط تجاری میان مردم - دولت به ارتباطات از راه دور و شکل‌گیری دولت الکترونیک (E-Government)، جرایم مالی سایبری وارد مرحله‌ی نوینی شده است؛

۱. بر اساس آمار سازمان ملی جوانان، بیش از ۴۴ درصد کاربران ایرانی باهدف تفریح و سرگرمی وارد فضای مجازی می‌شوند (حاجیلی ۱۳۸۸: ۱۲۸).

بنابراین در کنار سرقت نرم افزار و استفاده غیرمجاز از آثار ادبی و هنری دیگران، بزهکاران با موج وسیعی از اطلاعات دیجیتالی مالی کاربران رویارو شده‌اند. هزینه‌ی پایین ارتکاب جرم، کثرت بزه دیدگان و بالطبع عواید بالا نه تنها بزهکاران سایبری بلکه دیگران را نیز به این عرصه گسیل داشته است.^۱ از رایج‌ترین جرایم که با انگیزه مالی صورت می‌گیرند می‌توان به کلاه برداری، سرقت اطلاعات مالی و نیز دسترسی به اطلاعات محصولات پر فروش، تقلب مالیاتی و پول‌شویی اشاره نمود.

به نظر می‌رسد افرادی که به دلیل جلب توجه و کسب شهرت به رفتارهای مخرب دست می‌زنند را نیز می‌توان در این دسته جا گنجاند؛ زیرا انگیزه غائی آنان از رفتارهایشان آن است تا یک سازمان یا شرکت نسبت به استخدام آنان اقدام کند. البته گاه آن‌ها فاقد انگیزه مالی و تنها حس برتری جوئی آن‌ها را به ارتکاب جرم برمی‌انگیزاند. از این رو می‌توان گفت که جلب توجه و کسب شهرت از انگیزه‌های بنیادین یا مختلط محسوب می‌شوند.

۳- انتقام‌جویی

گاه کارمندان یک سازمان/شرکت به جهت نادیده گرفته شدن حقوق و یا بی‌توجهی به شایستگی آن‌ها، ممکن است با اطلاعاتی که در دسترس دارند نسبت به انتقام‌جویی از کارفرمایان خود اقدام کنند. بنا بر پیمایش انجام شده، بیش از ۷۰٪ از جرایمی که سامانه‌ها و رایانه‌های یک سازمان/شرکت را هدف قرار می‌دهند، از سوی کارمندان خودی صورت می‌گیرند (Nykodym, Taylor and Vilela 2005).

یکی دیگر از جرایمی که با انگیزه انتقام‌جویی روی می‌دهد، تعقیب ایدئاتی^۲ است. تعقیب

۱. «در سال ۲۰۰۸، ۷۸٪ از تهدیدات مربوط به اطلاعات محرمانه، داده‌های کاربری را به فرمت دیگری تبدیل کرده و ۷۶٪ از موارد ورود به سیستم، به منظور سرقت اطلاعات نظیر اعتبارنامه‌های حساب بانکی برخط انجام شد. همچنین، ۷۶٪ از تله‌های فیشینگ، برندهایی را در بخش خدمات مالی هدف قرار دادند و این بخش نیز اکثر شناسه/هویت‌ها را به سبب رخنه در داده‌ها از دست داده بود. به همین منوال، در سال ۲۰۰۸، ۱۲٪ از همه نفوذهای داده‌ای در مورد اطلاعات کارت‌های اعتباری روی داد. در این سال، میانگین هزینه وارده برای هر نفوذ داده‌ای در ایالات متحده ۶،۷ میلیون دلار بود- که افزایش ۵ درصدی نسبت به سال ۲۰۰۷ را نشان می‌دهد- و زیان آن به کسب‌وکار به‌طور میانگین بالغ بر ۴،۶ میلیون دلار بود» (Jahankhani and Al-Nemrat 2011: 85). در همین زمینه، مدیرکل طرح و برنامه سازمان قضایی نیروهای مسلح کل کشور بیان می‌دارد که ۸۱ درصد از جرایم سایبری با انگیزه مالی رخ می‌دهند. ر.ک:

<http://www.cyberpolice.ir/news/18841>

2. Cyber Stalking

ایذائی رفتاری است که فرد با استفاده از ارتباطات از راه دور به آزار و اذیت دیگری می‌پردازد (پیتارو ۱۳۹۲: ۱۰۱۶-۱۰۱۵). انگیزه اصلی بزه‌کاران از تعقیب بزه‌دیده به‌ویژه زنان آن است که عاشق عقده‌ای، تعقیب ایذائی را بهترین روشی می‌داند که بدین وسیله می‌تواند به دیگران ثابت کند که هنوز از عشق دیرینش دست نکشیده است. همچنین ممکن است رابطه زناشویی از هم گسیخته، شوهر سوءاستفاده‌گر یا حتی شوهر سابق را به انتقام از زن خود تحریک کند (رایجیان اصلی، محمد کوره‌پز و سلیمی، ۱۳۹۳). مثال زیر نمونه‌ی بارزی از تعقیب ایذائی است:

«یک زن مطلقه جوان به شهر دیگری نقل مکان می‌کند تا زندگی بهتری داشته باشد. مرتکب نام او را در اینترنت جستجو کرده و اقدام به استخراج آدرس محل سکونت جدید و محل کار او کرد. او نامه‌ای حاوی اطلاعات تنفرآمیز درباره آن زن به کارفرمای او فرستاده و نمایه‌های دروغین را آماده کرده تا نه تنها به او ناسزا گفته، او را تمسخر کرده و به او توهین و هتک حرمت کند» (رایجیان اصلی، محمد کوره‌پز و سلیمی، ۱۳۹۳)

مزاحمت سایبری و تجاوز به عنف سایبری (Cyber Trespass) از دیگر جرایمی است که می‌تواند با انگیزه انتقام‌جویی روی دهند؛ بنابراین، تحلیلی عمیق از انگیزه‌های مرتکبین - اعم از زنان و مردان - در جرم سایبری بر ضد زنان نشان می‌دهد که حسادت اصلی‌ترین و زیربنایی‌ترین انگیزه به‌منظور بزه‌دیده ساختن زنان است.

۴- انگیزه جنسی

چنانکه آمارها گواهی می‌دهند، بخش بزرگی از کاربران - به‌ویژه نوجوانان و جوانان - به‌منظور پاسخ به نیازهای جنسی خود به فضای سایبر سفر می‌کنند.^۱ چراکه این فضا با ناشناختگی اعطائی به کاربران و عدم ملاقات چهره به چهره، محدودیت‌های دنیای خاکی برای ابراز این تمایلات را از بین برده است. این انحرافات بیشتر با آنچه امروزه از آن با عنوان صنعت مقاربت جنسی یاد می‌شود، مرتبط می‌باشند. این صنعت از ماهیت متخلفانه‌ی محتوای

۱. متأسفانه آمارهای تکان‌دهنده زیر بیانگر آن‌اند که ۱۲ درصد از کل وب‌گاه‌ها، اختصاص به مسائل هرزه‌نگاری دارند (نزدیک به ۴ میلیون و ۲۰۰ هزار وب‌گاه)، روزانه بیش از ۲ و نیم میلیارد رایانامه حاوی هرزه‌نگاری ردوبدل می‌شود (بیش از ۸ درصد تمامی رایانامه‌های ارسالی) و بیش از ۲۵ درصد جستجوهای کاربران به‌منظور رصد این وب‌گاه‌ها است. همچنین باید اشاره کرد این صنعت چنان پردرآمد است که در سراسر دنیا سالانه دست‌کم ۵۷ میلیارد دلار سودآوری دارد. ر.ک:

<https://wsr.byu.edu/pornographystats>

هرزه‌نگاری زنان و کودکان بهره می‌گیرد و چیزهایی را که در زمان قدیم فقط در بازی‌های کثیف و فرعی هرزه‌نگاری یافت می‌شد، قابل قبول می‌سازد. نگران‌کننده‌ترین موضوع در مورد تمام این اطلاعات، آن است که صنعت مذکور نه تنها تجارت بزرگی است، بلکه فروش محصولات آن - هرزه‌نگاری، خودفروشی، سیاحت جنسی و عروس‌های پستی - اکثراً به زنان و کودکان مربوط می‌شود (زینالی ۱۳۸۸: ۲۸۵). افزون بر هرزه‌نگاری، از دیگر جرایم مرسوم که با انگیزه جنسی روی می‌دهند می‌توان به سیاحت گری جنسی^۱ و کودک دوستی اشاره نمود.

بنابراین، افراد زیادی با درجات خطرناکی مختلف (از کاربران عادی گرفته تا کسانی که به‌طور سازمان‌یافته به تولید و توزیع این محتویات می‌پردازند) در این چرخه‌ی بزهکاری مباشرت دارند تا بتوانند نیازهای جنسی خود را در این فضا برآورده سازند. چنانکه گروه‌های دیگری نظیر آزارگر - آزارپذیرها (Sado-Masochist)، متجاوزان به عنف سریالی و قاتلین سریالی جنسی از جمله بزهکاران جنسی سنتی هستند که به جهت مزایای فضای سایبر، پا به این دنیا گذاشته‌اند (منفرد ۱۳۹۱). بدیهی است ممکن است این اعمال باهدف کسب منافع مالی صورت گیرد و پیگیری اهداف جنسی به‌عنوان انگیزه ثانویه‌ی آنان، تلقی شود.

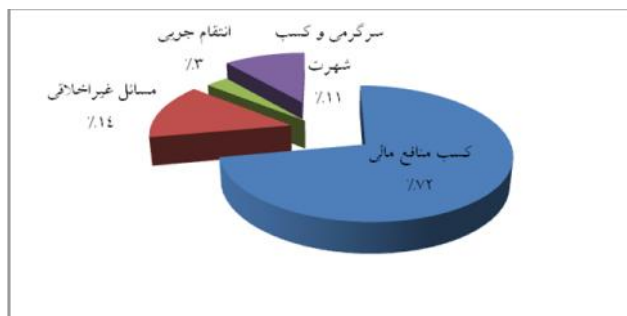
۵- باورهای ایدئولوژیک

اگرچه به نظر برخی نویسندگان، انگیزه سیاسی هیچ‌گاه انگیزه ابتدایی و اولیه نیست (Rogers 2010: 221)؛ اما گاه اعمال مجرمانه سایبری تنها باهدف حمایت از اعتقادات یا باورهای فردی-جمعی صورت می‌پذیرد. تروریست‌ها و جنگاوران سایبری از بارزترین نمونه‌های این گروه می‌باشند. گاه تحریکات اشخاص یا حتی دستگاه‌های دولتی می‌تواند زمینه‌ساز تهدیدهای سایبری آن‌ها شود؛ بنابراین، در صورت بروز رفتار غیرمعمول از طرف هکرها و بزهکاران احتمالی، رفتارهایی از قبیل مقابله به مثل کردن یا انتشار بیانیه در رسانه‌های گروهی، بستر را برای شکل‌گیری حملات سایبری فراهم می‌کند؛ زیرا این اقدام باعث ترغیب بیشتر بزهکاران به انجام رفتارهای غیرقانونی می‌شود. نمونه بارز اقدامات تحریک‌آمیز را می‌توان در کشورهایی که دارای ساختار قومیتی هستند، ملاحظه کرد. درواقع، هرگونه تبعیض نژادی یا اختلافات مذهبی-عقیدتی (Mansour Maghaireh, Alaeldin 2013: 137-150) می‌تواند

بزه‌کاران سایبری را تحریک به حمله به وبگاه‌های دولتی و حتی زیرساخت‌های حیاتی یک دولت کند تا به همگان ثابت کنند که در این جنگ سایبری، آن‌ها فاتح بلامنازع می‌باشند. افزون بر این، گاه این جرایم به واسطه تنفر از یک گروه نژادی-جنسی یا یک اندیشه سیاسی-مذهبی معارض صورت می‌گیرد.^۱ برای نمونه مردان علاقه‌چندانی به اندیشه‌های فمینیستی ندارند و رشد این طرز فکر را به ضرر خود می‌دانند. از این رو، ممکن است به شبکه‌های اجتماعی مروجین این باورها حمله کنند. باید اشاره کرد که اگرچه این جرایم به مانند جرایم کلاسیک اغلب همراه با خشونت می‌باشند، اما برخلاف نظر برخی نویسندگان (منفرد ۱۳۹۱) باید گفت انگیزه‌ی اولیه‌ی آن انتقام‌جویی یا ارتکاب اعمال خشونت‌بار نیست. چنانچه ما عملیات انتحاری یا شهادت‌طلبانه یک مجاهد را در ذهن تداعی کنیم، پی می‌بریم که چیزی جز مقدسات و باورهایش او را به ارتکاب جرم تحریک نکرده است.

نتیجه‌ی بحث مذکور آن است که بزه‌کاران سایبری به مانند هم‌تایان کلاسیک خود، طیف وسیعی از انگیزه‌ها را در سر می‌پرورانند؛ زیرا هم‌اکنون همان انگیزه‌های سنتی که همواره با بشر همراه بوده است در پوششی نوین-در فضای سایبر-رخ‌نمایی می‌کند. فرضیه این مدعی آن است که اگرچه گاه طبایع و کشش‌های انسانی و بالطبع بزه‌کاران ممکن است در مواردی تمایل بیشتری به یک پدیده داشته باشد اما این محرک‌ها همواره ثابت و غیرقابل تغییر می‌باشند. برای نمونه میل به شهوت جنسی همواره در طول تاریخ همراه انسان‌ها بوده است و همواره عده‌ای (بزه‌کاران جنسی) از راه‌های نامشروع دینی و نامقبول اجتماعی در صدد اطفای آن برآمده‌اند. در حال حاضر نیز گستره سایبر با تغییر در کیفیت و بدون دگرگونی در ماهیت، به نحو گسترده‌ای عرصه را برای هر منحرفی با هر نوع طبع و انگیزه‌ای گشوده است. (شکل ۵) به میزان و تنوع انگیزه بزه‌کاران سایبری در محدوده زمانی فروردین تا دی‌ماه ۱۳۹۰ که توسط پلیس فتا ارائه شده است، اشاره دارد. این آمار از ۱۹۰۸ مورد مکشوفه از مجموع ۴۰۰۰ پرونده موجود، به دست آمده است (به نقل از: ناصرآبادی ۱۳۹۱).

۱. در واقع این جرایم، گونه‌ی سایبری جرایم مبتنی بر نفرت (Hate Crime) می‌باشند. اغلب کشورهایی که به‌طور گسترده مقصد مهاجرین می‌باشند، در راستای کنترل اجتماعی از قوانین منسجمی در حمایت از نژاد، رنگ پوست و مذهب مهاجرین استفاده می‌کنند. شاید به همین خاطر است که در حقوق ایران، نفرت نژادی یا مذهبی به‌عنوان یک انگیزه‌ی مشدده لحاظ نشده است.



شکل ۶- انگیزه مجرمین سایبری در ایران

پس از آنکه داده‌های مربوط به نیمرخ جنایی محکومین پیشین گردآوری شد، باید از آن‌ها در تحلیل رویداد مجرمانه و در نهایت در طراحی نیمرخ جنایی کمک گرفت. اگرچه این داده‌ها در وهله نخست خام و بی‌ارزش به نظر می‌رسند؛ اما زمانی که آن‌ها به‌مانند تکه‌های پازل با دقت، تجربه، ظرافت و هوشیاری کنار یکدیگر چسبانیده شوند، روابط معناداری را آشکار می‌سازند. در غیر این صورت، نه تنها این اطلاعات ارزشی ندارند بلکه می‌توانند گمراه‌کننده نیز باشند.

در مرحله تحلیل داده‌ها این مأمورین تحقیق واحد جرایم رایانه‌ای می‌باشند که بیش از هر متخصصین دیگری می‌توانند با پردازش داده‌ها، برونداد/خروجی (Output) مناسب و مفیدی را از آن‌ها به دست آورند؛ زیرا این امر تنها از سوی مأمورین تحقیق زبده یا کسانی که به‌اصطلاح دارای «شم پلیسی» اند، برمی‌آید. در تأیید این نکته، سخنگوی واحد ملی جرم فناوری پیشرفته‌ی انگلستان بیان می‌دارد: «این کار نسبتاً راحتی است که مأموران خوبی انتخاب و به آن‌ها در امور فناوری‌های رایانه [ای] آموزش کافی دهیم، اما بسیار سخت است که افراد باهوش و [با] دانش در حوزه رایانه را انتخاب و آن‌ها را به مأموران خوبی تبدیل کنیم» (جوکز و همکاران ۱۳۸۹: ۱۶۰). با این حال، در این مرحله نیز مأمورین پلیس از مشاوره با متخصصین علوم رایانه مستغنی نمی‌باشند.

در مرحله تحلیل داده‌ها، افزون بر نگرشی عمیق به نیمرخ‌های بزهکاران بزه‌های مشابه، مأمورین تحقیق باید به بررسی و تحلیل داده‌ها و رفتارهای مرتکب در صحنه جرم نیز توجه ویژه‌ای داشته باشند؛ زیرا اگرچه گونه‌های مختلفی از نیمرخ‌سازی وجود دارد، با این وجود یکی از بهترین و کامل‌ترین گونه‌های آن، شیوه ترکیبی است. در این رویکرد، تنها به داده‌های

گردآوری شده از صحنه جرم یا اطلاعاتی که طراحان نیمرخ از بزهکاران پیشینی به دست آورده‌اند، بسنده نمی‌شود. به این صورت که پس از شناسایی ماهیت جرم ارتكابی، با بررسی صحنه‌ی جرم - که شامل شیوه، مکان، زمان ارتكاب، ملاحظات بزه‌دیده‌شناختی و غیره است - سرنخ‌های مهم گردآوری می‌گردند. سپس این داده‌ها با وضعیت بزهکاران جرایم مشابه پیشین - ویژگی‌های جمعیت‌شناختی - روانی مقایسه می‌شوند. سرانجام کارآگاهان و مأمورین تحقیق با تلفیق این دودسته اطلاعات با یکدیگر، از آن‌ها به منظور شناسایی بزهکاران بهره‌برداری می‌کنند.^۱ برای نمونه زمانی که فردی از اتاق‌های گپ به منظور تعقیب ایدایی و یا آزارگری استفاده می‌کند، در کنار برخی قرائن و شواهد فنی و ملاحظات بزه‌دیده‌شناختی که از صحنه جرم به دست می‌آیند، توجه به این امر که در موارد پیشینی این دسته بزهکاران چه ویژگی‌های جمعیت‌شناختی - اجتماعی داشته‌اند و چه افرادی را با چه انگیزه‌ای قربانی می‌سازند، بسیار تعیین‌کننده است؛ زیرا اگرچه این داده‌ها به‌طور قطعی بزهکار را تعیین نمی‌کنند اما می‌توانند در پاسخ به این پرسش که «بزهکار کیست؟» احتمال‌ها و گمان‌های که قابل اعتنا نیستند و یا با دیگر داده‌ها همخوانی ندارند را کنار نهند.

در این مرحله مشخص می‌شود که تا چه اندازه داده‌هایی که هریک به‌تنهایی ارزش خاصی نداشتند (به‌ویژه داده‌های جمعیت‌شناختی - اجتماعی) می‌توانند راهگشا باشند. درحالی که در بادی امر این‌طور به نظر می‌رسید که اگرچه شناخت این ویژگی‌ها تنها برای یک جرم‌شناس یا سیاست‌گذار عرصه فضای سایبر بسیار اهمیت دارد، اما وجه ضرورت گردآوری آن داده‌ها در شناسایی بزهکار احتمالی کمی دور از ذهن به نظر می‌رسید. نگاه پرننگ این نوشتار به ویژگی‌های بزهکاران سایبری نیز از همین واقعیت حکایت دارد؛ زیرا پیش از ابداع این روش نیز در هر دو جرایم کلاسیک و سایبری، توجه به صحنه جرم و داده‌های مرتبط با آن، یک اقدام ابتدایی و ضروری به‌شمار می‌رفت. پس کمینه وجه تمایز فن نیمرخ جنایی با دیگر روش‌های تحقیقی، در گنجاندن چنین ویژگی‌هایی در اقدامات تحقیقی است.

۱. نکته بسیار مهم که نباید فراموش گردد آن است که این داده‌ها باید بر اساس میزان اهمیت و ارزش «تفسیرپذیری» طبقه‌بندی و تدوین شوند؛ زیرا تمامی داده‌ها از ارزش و اهمیت یکسانی برخوردار نیستند؛ اما در عین حال مأمورین نباید داده‌های جزئی را به بهانه این که آن‌ها «غیر مهم» اند، از تحلیل خود کنار گذارند؛ زیرا گاه همین ملاحظات جزئی می‌توانند مفید واقع شوند. دیگر تدابیر و اقداماتی که مأمورین تحقیق جرایم سایبری مکلف به رعایت آن می‌باشند تا حد زیادی به‌به مانند دیگر جرایم است که به جهت پرهیز از اطاله کلام از آن صرف‌نظر می‌کنیم.

نتیجه گیری

در ارتباط با نیمرخ جنایی بزهکاران سایبری باید گفت، طبقه‌بندی‌هایی که از بزهکاران سایبری ارائه شده است (محمدکوره پز ۱۳۹۳)، نشان می‌دهند که بزهکاران سایبری برخلاف تصور رایج جرم‌شناسان، گروهی همگن و متجانس نیستند. به بیانی دیگر، یافته‌های پژوهش‌های جدیدتر و پژوهش حاضر، اساساً هر گزاره‌ای که ویژگی خاصی را به تمامی بزهکاران سایبری تعمیم دهد، عوامانه و فاقد پشتوانه علمی می‌دانند؛ زیرا آنان نیز به مانند بزهکاران کلاسیک به گونه‌های متنوعی تقسیم می‌شوند. پس نباید پنداشت که تمامی بزهکاران سایبری، نوجوان و جوان، مرد، یقه‌سفید، باهوش، دارای مهارت فنی بالا، برخوردار از تحصیلات مطلوب و به طور کلی «حرفه‌ای» می‌باشند بلکه در میان بزهکاران سایبری نیز هم کسانی که مبتدی‌اند و به راحتی شناسایی می‌شوند و هم بزهکاران حرفه‌ای که شناسایی و ردیابی آنان دشوار است، وجود دارد. البته این تصور نیز نادرست است که ویژگی‌های آنان به طور کامل همسان و سازگار با بزهکاران کلاسیک فرض شود؛ زیرا حداقل، تفاوت عمیق بستر سایر فضاهای مادی، ماهیت بزه و گونه‌های بزهکاران را دستخوش تغییر کرده است. البته این گوناگونی در انگیزه‌های بزهکاران سایبری کم‌رنگ‌تر است. چنانکه ملاحظه شد، همان انگیزه‌های جنایی که در سایر بزهکاران وجود دارد، در بزهکاران سایبری نیز البته با تغییر در فراوانی مشاهده می‌شود. از این رو، شایسته است که سیاست‌گذاران، یک راهبرد یا سیاست جنایی افتراقی را به منظور مبارزه و پیشگیری در برابر بزهکاران سایبری، اتخاذ کنند.

در کنار تمرکز بر ویژگی‌های اجتماعی - روانی بزهکاران که اساس این نوشتار را تشکیل داد، باید اشاره کرد که بررسی صحنه جرم می‌تواند به طور مؤثری طراحان نیمرخ را در رمزگشایی و تعیین بزهکار احتمالی کمک کند. شیوه‌ی ارتکاب، مکان و زمان حمله و ملاحظات بزه‌دیده‌شناختی از مهم‌ترین عواملی‌اند که در ذیل صحنه جرم بررسی می‌شوند. نکته بسیار مهم اینکه بررسی این عوامل زمانی معنا پیدا می‌کنند که طراحان نیمرخ به ویژگی‌های اجتماعی - روانی بزهکاران نیز نگاه پررنگی داشته باشد. کما اینکه تنها نمی‌تواند به ویژگی‌های اجتماعی - روانی بسنده نمایند. برای نمونه شیوه‌ی ارتکاب بزه می‌تواند تعیین کند بزهکار به چه رده‌ی سنی متعلق است، حرفه‌ای است یا مبتدی، مهارت فنی بالایی دارد یا خیر - این دو بدین خاطر جداگانه مطرح شد که لزوماً کسی که مهارت فنی بالایی دارد حرفه‌ای



نیست زیرا حرفه‌ای بودن مرتکب بیشتر ناظر به آن است که رد پای سایبری خود را تغییر یا حذف کند تا شناسایی نشود. سطح تحصیلات او چگونه است و غیره. همچنین، از گذر مصاحبه با بزه‌دیده، ضمن آنکه می‌توان به منظور آشکارسازی روابط پیشینی بزه‌کار-بزه‌دیده، میزان تقصیر وی و به‌طور کلی سرنخ‌هایی که طراح نیمرخ را به تعیین بزه‌کار احتمالی استفاده نمود، موجبات پیشگیری از آسیب‌های ثانویه و حمایت از بزه‌دیدگان را فراهم می‌آورد.



پژوهشگاه علوم انسانی و مطالعات فرهنگی
پرتال جامع علوم انسانی

منابع

الف) منابع فارسی

- آس، کاتیا فرانکو (۱۳۹۰)، *جهانی‌سازی و جرم*، ترجمه: یوسف بابایی و اصلی عباسی، تهران: معجد.
- ابوذری، مهرنوش (۱۳۹۱)، *جرم‌شناسی جرایم سایبری*، پایان‌نامه دوره کارشناسی ارشد دانشگاه تهران، دانشکده حقوق و علوم سیاسی، حقوق کیفری و جرم‌شناسی.
- احمدی، حبیب (۱۳۸۴)، *جامعه‌شناسی انحرافات*، تهران: سمت.
- بهره‌مند ح؛ و محمد کوره‌پزح؛ و سلیمی ا (۱۳۹۳)، *راهبردهای وضعی پیشگیری از جرایم سایبری*، آموزه‌های حقوق کیفری (۷): ۱۷۶-۱۴۷.
- پیتارو، میشل (۱۳۹۲)، *مزاحمت سایبری: گونه‌شناسی، علت‌شناسی و بزه‌یاده‌شناسی*، ترجمه: لمیاء رستمی تبریزی، سودابه رضوانی و مرضیه السادات آقا میرسلیم، در: *دایرة المعارف علوم جنایی* (مجموعه مقاله‌های تازه‌های علوم جنایی)، کتاب دوم، زیر نظر: علی حسین نجفی ابرندآبادی، تهران: میزان.
- توکل، محمد؛ و کاظم پور، ابراهیم (۱۳۸۴)، *دگرگونی‌های اجتماعی در یک جامعه‌ی اطلاعاتی*، تهران: انتشارات کمیسیون ملی یونسکو.
- حاجیلی، محمود (۱۳۸۸)، *وضعیت فناوری ارتباطات در حوزه جوانان*، تهران: دبیرخانه شورای عالی اطلاع رسانی.
- رستمی تبریزی، لمیاء (۱۳۸۸)، «درآمدی بر رویکرد جنسیتی جرم‌شناسی»، *تحقیقات حقوقی*، (۵۵)، ۳۱۷-۲۷۹.
- زینالی، امیرحمزه (۱۳۸۸)، *حمایت کیفری از کودکان در برابر هرزه‌نگاری از واکنش‌های جهانی تا پاسخ‌های نظام‌های کیفری ملی*، در: *حقوق فناوری اطلاعات و ارتباطات* (مجموعه مقالات)، گردآوری: امیرحسین جلالی فراهانی، تهران: روزنامه رسمی جمهوری اسلامی ایران.
- شمس، مجید (۱۳۸۱)، «وندالیسم اعتراض به جامعه»، *مجله اصلاح و تربیت*، (۹)، ۱۹-۱۷.
- عالی‌پور، حسن (۱۳۹۰)، *حقوق کیفری فناوری اطلاعات*، تهران: انتشارات خرسندی.
- غلامی، حسین (۱۳۸۲)، «تکرار جرم به‌عنوان حرفه مجرمانه»، *فصلنامه حقوق (مجله دانشکده حقوق و علوم سیاسی سابق)*، (۶۲)، ۳۱۶-۲۸۵.

- فیشر، بونی. اس؛ و پی. لب. استیون (۱۳۹۴)، *دانشنامه بزه‌دیده‌شناسی و پیشگیری از جرم (جلد اول)*، ترجمه اساتید حقوق کیفری و جرم‌شناسی سراسر کشور (زیر نظر: علی حسین نجفی ابرندآبادی)، تهران: میزان.
- قورچی‌بیگی، مجید (۱۳۹۲)، *تحلیل و بررسی جرم‌شناختی جرایم یقه‌سفیدها*، رساله دوره دکتری، دانشگاه تهران، دانشکده حقوق و علوم سیاسی، حقوق کیفری و جرم‌شناسی.
- کاتوزیان، ناصر (۱۳۸۶)، *حقوق مدنی (اعمال حقوقی، قرارداد-ایقاع)*، دوره مقدماتی، تهران: انتشارات سهامی انتشار.
- کی‌نیا، مهدی (۱۳۸۶)، *مبانی جرم‌شناسی*، جلد اول، تهران: انتشارات دانشگاه تهران.
- محمد کوره‌پز، حسین (۱۳۹۳)، *نیمرخ جنایی بزه‌کاران سایبری*، پایان‌نامه دوره کارشناسی ارشد، پردیس فارابی دانشگاه تهران، دانشکده حقوق، حقوق کیفری و جرم‌شناسی.
- مظلومان، رضا (۱۳۵۳)، «نقش تحصیل در کمیت و کیفیت جرم»، نشریه کاوه (مونیخ)، (۵۴)، ۳۱-۱۹.
- معاونت آموزش و تحقیقات قوه قضائیه (۱۳۸۹)، *مسائل قضایی هرزه‌نگاری در محیط سایبر*، تهران: راه نوین.
- منفرد، محبوبه (۱۳۹۱)، «بررسی جرم‌شناختی بزهکاری رایانه‌ای»، فصلنامه مطالعات پیشگیری از جرم، (۲۵)، ۴۷-۷۶.
- منفرد؛ و جلالی فراهانی (۱۳۹۱)، «کدهای رفتاری و پیشگیری از بزهکاری»، پژوهشنامه حقوق کیفری. (۶): ۱۳۴-۱۰۵.
- ناصرآبادی، سید پاشا (۱۳۹۱)، *سخنرانی در: سمینار آموزشی پیشگیری از سرقت اطلاعات رایانه‌ای*، قابل دسترسی در:
- [http://fad.tehran.ir/Default.aspx?tabid=163&articleid=3341&dnnprintmode=true&mid=631&SkinSrc=\[G\]Skins%2F_default%2FNo+Skin&ContainerSrc=\[G\]Containers%2F_default%2FNo+Container](http://fad.tehran.ir/Default.aspx?tabid=163&articleid=3341&dnnprintmode=true&mid=631&SkinSrc=[G]Skins%2F_default%2FNo+Skin&ContainerSrc=[G]Containers%2F_default%2FNo+Container)
- نجفی ابرندآبادی، علی حسین (۱۳۸۸)، «درباره‌ی بزهکاری و جرم‌شناسی سایبری (گفتگو)»، *مجله تعالی حقوق*، (۳۶)، ۱۱-۷.
- نجفی ابرندآبادی، علی حسین (۱۳۸۸)، *کیفرشناسی نو- جرم‌شناسی نو در آمدی بر سیاست جنایی مدیریتی خطرمدار*، زیر نظر علی حسین نجفی ابرندآبادی، در: تازه‌های علوم جنایی (مجموعه مقاله‌ها)، تهران: میزان
- نجفی ابرندآبادی، علی حسین (۱۳۹۲)، *تقریرات درس جرم‌شناسی (از جرم‌شناسی*

انتقادی تا جرم‌شناسی امنیتی)، دوره دکتری، دانشکده حقوق دانشگاه شهید بهشتی، نیم سال دوم تحصیلی، ۱۳۹۲-۱۳۹۱. قابل دسترسی در: www.lawtest.ir.

- نجفی ابرندآبادی، علی حسین (۱۳۹۱)، *درباره سن و علوم جنایی، دیپاچه در: مبانی پیشگیری اجتماعی رشدمدار از بزهکاری اطفال و نوجوانان*. نوشته محمود رجبی پور، تهران: نشر میزان (چاپ اول)، چاپ دوم کتاب.

- نگهی، مرجان (۱۳۹۱)، «مقابله با هرزه‌نگاری کودکان: بررسی تطبیقی اسناد بین‌المللی و قوانین کیفری ایران»، پژوهشنامه حقوق کیفری، (۶)، ۱۶۰-۱۳۵.

- نوربها، رضا (۱۳۸۶)، *زمینه حقوق جزای عمومی*، تهران: گنج دانش.

- وفایی، فریبا (۱۳۷۸)، «زنان بزهکارترند یا مردان؟»، *مجله اصلاح و تربیت* (دوره قدیم)، (۲۸)، ۲۲-۲۰.

- ویلیامز، ماتيو (۱۳۹۱)، *بزهکاری مجازی: بزه، انحراف و مقررات‌گذاری برخط*، ترجمه: امیرحسین جلالی فراهانی و محبوبه منفرد، زیر نظر علی حسین نجفی ابرندآبادی، تهران: میزان.

- هالدر، دباراتی؛ و جیشنکار، جی (۱۳۹۳)، *جرم رایانه‌ای و بزه‌دیدگی زنان: قانون‌ها، حق‌ها و مقرره‌ها*، ترجمه: مهرداد رایجیان اصلی، حسین محمدکوره‌پز و احسان سلیمی، تهران: مجد.

ب) منابع انگلیسی

- Britton, Dana M. (2011). *the Gender of Crime*, New York: Rowman & Littlefield Publishers.

- Babchishin, Kelly M. Hanson, R. Karl and Hermann, Chantal A. (2011). *The Characteristics of Online Sex Offenders: A Meta-Analysis*, *Sexual Abuse: A Journal of Research and Treatment*, 23 (1), 92-123.

- Chiesa, Raoul (2009). *Profiling Hackers: Real Data, Real Experiences, Wrong Myths and the Hacker Profiling Project (HPP)*. Virus Bulletin. Available at: www.virusbtn.com/pdf/conference.../Chiesa-VB2009.pdf.

- Chiesa, Raoul, Ducci, Stefania and Ciappi, Silvio. (2009). *Profiling Hackers: The Science of Criminal Profiling as Applied to the World of Hacking*, Boca Raton: Taylor & Francis Group Auerbach Publications.

- Durost, Shane (2005), *Profiling a Hacker*, Capstone Project, available at: ciag.umfk.maine.edu/Shane%20Durost.pdf.

- Erbschloe, Michael. (2001), *Information Warfare: How to Survive Cyber Attacks*, New York: McGraw Hill.

- Goldschmidt, Orly Turgeman (2011). *Identity Construction among Hackers*, In: Jaishankar, K. (Ed), *Cyber Criminology: Exploring Internet Crimes*

and Criminal Behavior. Boca Raton: CRC Press.

- Jahankhani, Hamid, and Al-Nemrat, Ameer (2011). *Cybercrime Profiling and Trend Analysis*. In: Akhgar, Babak and Yates, Simeon (Eds), *Intelligence Management: Knowledge Driven Frameworks for Combating Terrorism and Organized Crime*, London: Springer.

- Jahankhani, Hamid and Al-Nemrat, Ameer (2010). *Examination of Cyber-Criminal Behavior*. *International Journal of Information Science and Management (Special Issue)*, 41-48.

- Kirwan, Gráinne and Power, Andrew. (2013). *Cybercrime: the Psychology of Online Offenders*. New York: Cambridge University Press.

- Krone, Tony. (2004). *Typology of Online Child Pornography Offending*. Trends and Issues in Crime and Criminal Justice. (279), available at: <http://aic.gov.au/documents/4/F/8/%7B4F8B4249-7BEE-4F57-B9ED-993479D9196D%7Dtandi279.pdf>

- Kshetri, Nir. (2010). *the Global Cybercrime Industry: Economic, Institutional and Strategic Perspectives*, London: Springer.

- Liao, You-lu, Tsai, Cynthia (2006). *Analysis of Computer Crime Characteristics in Taiwan*, In: Chen, H. and et al. (Eds): *Intelligence and Security Informatics*, London: Springer.

- Lickiewicz, Jakub (2011). *Cyber Crime Psychology – Proposal of an Offender Psychological Profile*. *Problems of Forensic Sciences*, (87), 239-252.

- Mansour Maghaireh, Alaeldin. (2013). *Arabic Muslim Hackers: Who Are They and What Is Their Relationship with Islamic Jihadists and Terrorists?* In: Jaishankar, K. and Ronel, Natti (Eds), *Global Criminology: Crime and Victimization in a Globalized Era*, Boca Raton: CRC Press.

- Matsumoto, David. (2009). *the Cambridge Dictionary of Psychology*, New York: Cambridge University Press.

- Nykodym, Nick, Taylor, Robert and Vilela, Julia (2005). *Criminal profiling and insider cyber crime*. *Computer Law & Security Report*, (21), 261-267.

- Rogers, Marcus K. (2001). *A Social Learning Theory and Moral Disengagement Analysis of Criminal Computer Behavior: An Exploratory Study*. a Thesis Submitted to the Faculty of Graduate Studies in Partial Fulfillment of the Requirements for the Degree of Doctor of Philosophy, University of Manitoba.

- Rogers, Marcus, (2003). *The Role of Criminal Profiling in the Computer Forensics Process*. *Computers & Security*. 22(4), 292-298.

- Rogers, Marcus K. Seigfried, Kathryn, Tidke, Kirti. (2006). *Self-Reported Computer Criminal Behavior: a Psychological Analysis*. *Digital Investigation: the International Journal of Digital Forensics & Incident Response*. (3), 116-120.

- Rogers, Marcus, K. Smoak N. and Liu J. (2006). *Self-Reported Criminal Computer Behavior: A Big-5, Moral Choice and Manipulative Exploitive Behavior Analysis*. *Deviant Behavior*, 27(3), 245-268.

- Rogers, Marcus K. (2010). *The Psyche of Cybercriminals: A Psycho-Social Perspective*. In: Sumit Ghosh, and Elliot Turrini (Eds), *Cyber Crimes: A Multidisciplinary Analysis*, London: Springer.

- Seigfried, Kathryn, Lovely, Richard W. and Rogers, Marcus K. (2008). *Self-Reported Online Child Pornography Behavior: A Psychological Analysis*. International Journal of Cyber Criminology. 2 (1), 286-297.
- Shinder, Debra Littlejohn. (2002). *Scene of the Cybercrime: Computer Forensics Handbook*, Rockland: Syngress Publishing.

