پژوهش حقوق کیفری، سال سوم، شماره نهم، زمستان ۱۳۹۳، ص ۱٤٦ - ۱۱۱

نیمرخ جرم‌شناختی بزه‌کاران سایبری

حسین محمدکوره‌پز* - 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 احتمالیِ بزه‌کارانِ پرخطر از گذرِ بررسیِ آمار و پرونده‌های محکومین پیشین و مصاحبه با بزه‌دیدگان مستقیم یا با مشاهده صحنه جرم و آثار به‌جای مانده از رفتارِ مرتکب، نیمرخی از آنان ارائه و درنتیجه در راستای شناساییِ آنان گام بردارد. این فن توان شناخت دقیقِ مرتکبین را ندارد، بلکه دایرهٔ 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 به‌دشواری شناسایی می‌شوند، منطقی و امکان‌پذیر است. ازاین‌رو، می‌توان از این فن به‌منظور شناساییِ برخی گونه‌های بزهکاران سایبری نیز بهره برد. رایج‌ترین گونه‌های طراحیِ نیمرخ جنایی عبارت است از: نخست؛ ایجادِ 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 گردآوری‌شده 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 به‌دست‌آمده، برخلاف نظر برخی جرم‌شناسان، نشان می‌دهد که به‌طورکلی بزه‌کاران سایبری به‌مانند سایر بزه‌کاران از گروهی متجانس و همگن تشکیل نمی‌شوند و انگیزه‌های آنان نیز متفاوت از بزه‌کاران دنیای واقعی نیست. بااین‌حال، برخی از ویژگی‌هایی که بدون پشتوانه علمی-تجربی نمایش داده می‌شود، می‌تواند به نحو بارزی در بزه‌کاران سایبری محض و نه بزه‌کاران بهره‌بردار از فضای سایبر، مشاهده شود.

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

---

* کارشناس ارشدِ حقوق کیفری و جرم‌شناسی از پردیس فارابی دانشگاه تهران (نویسنده مسئول). kourepaz@ut.ac.ir

لازم به توضیح است که این نوشتار، برگرفته از پایان‌نامهٔ کارشناسی ارشد این‌جانب با عنوان «نیمرخ جنایی بزهکاران سایبری» است.

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

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

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

درآمد

۱. فن ترسیم نیمرخ جنایی[1] در بستر پاسخ به یکی از بزرگ‌ترین دغدغه‌های اصلیِ مأمورین اجرای قانون؛ یعنی شناسایی بزهکاران جرایم سریالی ایجاد شده است (Rogers, 2003)؛ زیرا از یک‌سو ویژگی‌های جرایم سریالی نظیر انجام بزه به‌صورت انفرادی، وجود اختلالات رفتاری- روانی در مرتکبین و عدم وجودِ رابطه پیشینیِ بزهکار- بزه دیده، شناسایی مرتکبین این جرایم را در مقایسه با سایر جرایم دشوارتر می‌سازد. همچنین از سوی دیگر این دسته جرایم به‌سرعت خبرساز شده و تهدیدات گرانباری ازجمله احساس ناامنی و ترس از بزه‌دیدگی را به جامعه تحمیل می‌کند. بااین‌وجود، باید اشاره داشت که جرایم سریالی در اینجا موضوعیتی ندارند و چنانچه هر جرمی از این ویژگی‌ها برخوردار باشد، می‌توان از این فن به‌منظور کشف و شناسایی آن‌ها بهره برد.

۲. در عصر نوین شاید هیچ جرمی به‌مانند جرایم سایبری را نتوان سراغ داشت که بزهکاران آن بدین شکل معادلاتِ شناسایی را برای مأمورین تحقیق پیچیده ساخته باشند. بستر سایبر به‌واسطه ویژگی‌های خاص خود، در وهله نخست شناساییِ بزهکار و در مراتبِ پسینی، کشف بزه را دشوار ساخته است. افزون بر ویژگی‌هایی که فضای سایبر به بزهکاری اعطاء کرده است، ابزارهای سنتیِ تحقیقاتی نیز در رویارویی با این جرایم به‌شدت ناکارآمد و فاقد اثربخشیِ لازم می‌باشند؛ زیرا مسلم است که با رایانه‌ای شدن صحنه جرم[2]، تجهیز کنشگران عرصهٔ بزهکاری به سلاح‌های نوین و بالطبع بهره‌برداری آنان از روش‌های ارتکاب جرمِ متناسب با آن، نمی‌توان از ابزارهایی که هیچ سنخیتی با آن ندارند، بهره جست. لذا پی‌جوئیِ جرایم سایبری مستلزم کاربست تدابیرِ روزآمد است. در این راستا، در چند سال اخیر فن ترسیم نیمرخ جنایی به‌واسطهٔ امتیازات خاصی که دارد، ذهن پژوهشگران عرصهٔ جرم‌شناسیِ فضای سایبر و مأمورین تحقیقِ واحدِ پلیسِ 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[1] 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 متخصصینِ رشته‌های گوناگون است، روند انجام تحقیقات را تاحدی به درازا می‌کشاند.

۳. با این توضیحات مشخص می‌شود که ترسیم نیمرخی از بزهکار، مستلزم نگرشی عمیق به ویژگی‌های جمعیت‌شناختی-اجتماعی و رفتاری-روانی عمومِ مرتکبین قبلی، مشاهده صحنه ارتکاب جرم و نیز نشستن بر بالینِ بزه‌دیده‌ی مستقیم و گفتگو با وی است تا با تحلیل آن‌ها بتوان به سرنخ‌هایی دست پیدا نمود که ما را در شناسایی بزهکار یاری‌رسان باشد (Matsumoto 2009: 401)؛ اما باید اشاره کرد که تمامیِ الگوهای ترسیم نیمرخ جنایی از مدل واحدی پیروی نمی‌کنند. فن ترسیم نیمرخ جنایی از دو الگوی اصلی برای طراحیِ نیمرخ جنایی بهره می‌برد: نخست؛ رویکرد استقرایی یا پایین به بالا که بر تعمیم بخشیِ ویژگی‌های جمعیت‌شناختی-اجتماعی و روانی-رفتاری محکومین سابق و نیز انگیزه‌های آنان تکیه دارد و رویکرد استنتاجی یا بالا به پایین[2] که شواهد و مدارک به‌دست‌آمده از صحنه جرم و نه ملاحظات آماری را برای تجزیه‌وتحلیل مورد خاص و سپس برای برساختِ یک نیمرخ رفتاریِ خاص (تنها برای همان پرونده تحت بررسی) کافی می‌داند. در رویکرد استقرایی، شناساییِ مرتکبینِ احتمالی در سایه‌ی دو شاخصِ اصلی؛ یعنی شناختِ رفتارِ عمومیِ 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 رفتاریِ آنان با آن مورد تطبیق داده می‌شود[3]. از میان این دو الگو، امروزه متخصصین امنیتی به‌طور فزاینده‌ای علاقه‌مند به استفاده از ویژگی‌های عمومیِ بزهکاران سایبری در چنین اقداماتی می‌باشند؛ یعنی شناساییِ خودِ 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 تجزیه‌وتحلیل 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 ارشدِ حقوق کیفری و جرم‌شناسی، پردیس فارابی دانشگاه تهران (دانشکده حقوق)، صص ۱۴۱-۱۳۳).

معنای وسیع کلمه (Lickiewicz 2011)[1]. درواقع آنچه ما آن را «نیمرخ جرم‌شناختیِ بزهکاران سایبری» نامیده‌ایم[2]. از مزایای الگوی استقرایی نسبت به الگوی استنتاجی می‌توان به این نکته اشاره کرد که در بیشتر موارد داده‌های مرتبط با صحنه جرم سایبری ــ حتی بیش از جرایم دیگر ــ شکننده، مبهم و غیرقابل‌دسترس و درنتیجه غیرقابل اعتبارند. همچنین، دسترسی دشوار به بزه‌دیده و مصاحبه با وی و حتی در صورت دسترسی، دستیابی به اطلاعات دقیق و واقعی و نه گمراه‌کننده بسیار دشوارتر است. ازاین‌رو، مدل استنتاجی حداقل در حال حاضر، کمتر مورد اقبال طراحان نیمرخ جنایی قرارگرفته است. این نوشتار، در چارچوب ترسیم نیمرخ جناییِ استقرایی گام برمی‌دارد و با تکیه بر ویژگی‌های جرم‌شناختیِ بزهکاران سایبری که از آمارها و یافته‌های پژوهشی داخلی و خارجی به‌دست‌آمده است، به تبیین و تحلیل این ویژگی‌ها و نیز انگیزه‌های جناییِ آنان می‌پردازد.

۴. اگرچه در پژوهشی دیگر پیرامون ضرورتِ انعکاسِ یافته‌های روان‌شناختی در ترسیمِ نیمرخ‌جنایی بزهکاران، به‌ویژه بزهکاران سایبری سخن گفته‌شده است (محمدکوره‌پز ۱۳۹۳)، اما نه‌تنها نویسندگان حاضر در این زمینه در ادبیات پژوهشیِ ایران موردی را ملاحظه نکردند؛ بلکه در پژوهش‌هایی که در سایر نقاط دنیا انجام‌شده نیز تحقیقات صرفاً نظری و بدون پشتوانه‌های علمی-تجربی است یا بر پایه شبیه‌سازیِ ویژگی‌های یک‌گونه از بزهکاران سایبری با همنوعانِ کلاسیک خود صورت گرفته است. در این زمینه می‌توان نیمرخ روان‌شناختی 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، بزهکاران با توجه به عامل‌ها و متغیرهایی از قبیل پیشینه مجرمانه، نوع محکومیت کیفری، سن، تجرد و تأهل، جنسیت، بی‌کاری و اشتغال، خارجی یا بومی بودن، اعتیاد یا عدم اعتیاد، میزان تحصیلات، مسکن، محله، مهاجر بودن و غیره ــ شاخص‌های خطر ــ به‌منظور احتمال خطر ارتکاب و تکرار جرم گروه‌بندی می‌شوند و نیمرخی از این بزهکاران خطرناک به‌منظور پیش‌بینی رفتار مجرمانه احتمالی‌شان ترسیم و طبقه‌بندی می‌گردد (نجفی ابرندآبادی ۱۳۸۸: ۷۲۹). درواقع، 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 درزمینهٔ کشفِ زودهنگام از جرم ارتکابی، اعمال می‌گردد. ازاین‌رو به نظر می‌رسد گرچه پیشینهٔ تکنیک نیمرخ‌سازی به سالیانی پیش از شکل‌گیری و بالندگی جرم‌شناسی نو- کیفرشناسی نو بازمی‌گردد اما نقطهٔ اوجِ به‌کارگیری این تکنیک مصادف با پیدایش آن است؛ زیرا این تکنیک، اهدافِ این الگوی سیاست جنایی را به نحو آشکاری دنبال و سامان می‌بخشد.

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

شخصیتیِ «هیجان‌طلبی[1]» و «احساس حقارت[2]» هستند، این ویژگی‌های روان‌شناختی را به تروریست‌های سایبری نیز تعمیم داده‌اند (Kirwan 2013: 202). درحالی‌که 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. ازاین‌رو، در اثر حاضر به ملاحظات روان‌شناختی بزهکاران سایبری پرداخته نشده است. بااین‌حال، خلأ پژوهش مستقلی در این زمینه به‌شدت احساس می‌شود.

۵. گفتنی است طراحی نیمرخ جنایی از بزهکاران سایبری در مقایسه با سایر بزهکاران، به دلیل ماهیتِ پیچیدهٔ جرایم سایبری، مشکلات کشف جرم و شناساییِ بزهکارانِ آن و همچنین دشواری‌های مربوط به مصاحبه و پیمایش از مجرمین، متخصصین این رشته را در برساختِ نیمرخ‌جنایی از بزهکاران سایبری، در شرایط پیچیده‌تری قرار می‌دهد. افزون بر این، رفتار مجرمان سایبری نیز به‌مانند خودِ این جرایم پویا و به‌سرعت در حال تغییر است[3]. 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 اساسِ تحقیقات جنایی قرار گیرند (Jahankhani and Al-Nemrat 2010). بااین‌حال، چنانچه این نیمرخ‌ها به‌صورت علمی و دقیق طراحی شوند، ضمن آنکه می‌توانند ما را در درکِ جامع و دقیقی از رفتار بزهکاران سایبری کمک کنند (با یک رویکرد جرم‌شناختی) از آن می‌توان به‌منظور پیش‌بینیِ رفتار احتمالیِ بزهکاران و درنتیجه شناسایی بزهکار نیز بهره‌برداری نمود (با اتخاذ رویکرد جرم‌یابی).

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

---

1. Sensation-Seeking
2. Feelings of Humiliation

۳. این پویایی و تنوع را به‌وضوح می‌توان در گونه‌های نوظهور جرایم سایبری مشاهده نمود. گونه‌های نخستین جرایم سایبری بیشتر به‌عنوان 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، به‌نوعی 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 سایبر اشاره می‌شود (بند ب)؛ زیرا در کنار این ویژگی‌ها، شناخت و طبقه‌بندیِ انگیزه‌های بزهکاران افزون بر این‌که تکمیل‌کننده ویژگی‌های مورداشاره بوده و موجبات طراحیِ نیمرخ جرم‌شناختی دقیق‌تر و شناساییِ فردِ حمله‌کننده را فراهم می‌آورد، می‌تواند در شناساییِ عوامل این برانگیختگی‌ها و درنتیجه به‌کارگیری 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»، به‌احتمال‌زیاد پاسخ‌خواهیم داد که آن‌ها برخلاف ویژگی‌های نوعیِ بزهکاران عادی، از هوش، دانش و سطح تحصیلات و نیز از تمکن مالیِ 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 بررسیِ عمده ویژگی‌های بزهکاران سایبری، سازگاریِ 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. درواقع، با دوزیستیِ انسان‌ها در فضای سایبر و دنیای خاکی، آیا بزهکاران این دو فضا از ویژگی‌های اجتماعی و جمعیت‌شناختیِ 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 سنجه با پیمایش‌های صورت پذیرفته، آنان مورد ارزیابیِ علمی قرار می‌گیرند. با توجه به محدودیت‌ها و موانعی که پیشتر اشاره شد، از یک‌سو پیمایش و مصاحبه‌های اندکی پیرامون بزهکاران سایبری انجام‌شده 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 توصیفِ تفاوت‌های جمعیت‌شناختیِ بزهکارانِ جنسیِ کلاسیک و سایبری پرداخته‌شده است که در ادامه به آن‌ها اشاره می‌شود.

۱-۱- سن

سن یک عامل جرم‌زای فردیِ گذرا و انتقالی است. این عامل در حقوق کیفری به‌منظور تمییز سن مسئولیت کیفری و در جرم‌شناسی و بزه‌دیده‌شناسی ازلحاظ تفکیک بزهکاری اطفال و بزرگ‌سالان، موردتوجه قرار می‌گیرد[۱]. از منظر جرم‌شناسی، یافته‌های تحقیقاتی نشان می‌دهند که در هر رده سنی، گونه‌ای از بزهکاری یا بزه‌دیدگی در میانِ افرادِ 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 وندالیسمِ میان‌سالان و سالمندان گزارش‌شده است[۲] یا برعکس، برخی جرایم مختص افرادی است که در طبقه سنی بالایی قرار دارند. بارزترین نمونه از چنین بزهکارانی، مجرمین یقه‌سفید هستند (قورچی‌بیگی 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 سنیِ کاربرانِ اینترنت انجام شد، نشان داد که در کشورهایی نظیر کره (۹۵ درصد)، ایالات‌متحده امریکا (۹۱ درصد)، ژاپن (۸۱ درصد) و انگلستان (۸۰ درصد) نوجوانان و جوانان ۲۴-۱۶ 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.

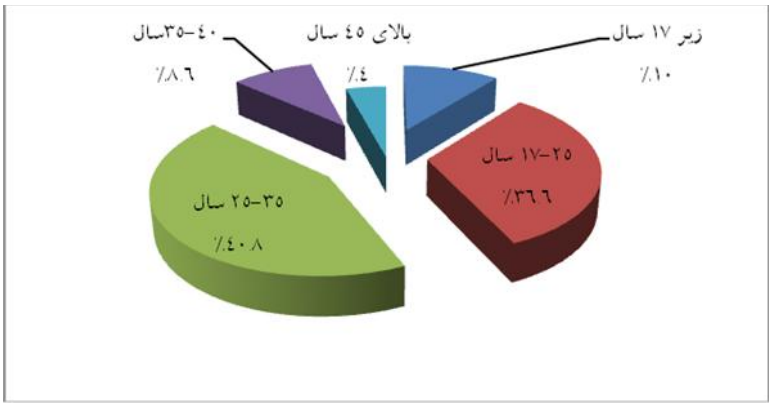
در ایران، از بررسی پرونده‌ی ۴۵ محکوم به تولید و انتشار تصاویر مستهجن مشاهده می‌شود که کمترین سن ۱۹ و بیشترین ۵۴ سال و درمجموع، میانگین سنیِ آن‌ها ۲۶/۲ است (معاونت آموزش و تحقیقات قوه قضائیه ۱۳۸۹: ۲۳۸-۲۰۹). همچنین، آمار پلیس فتا پیرامون میانگین

---

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

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

سنیِ متهمان جرایم سایبری در بازه زمانی سال ۹۰ تا تیر ۹۱ نشان می‌دهد که ۷۷/۶ درصد متهمین دارای میانگین سنیِ ۳۵-۱۷ 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 ۳۰-۲۳ سال است و هرکدام از بزهکارانِ گروه سنیِ 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 ایالات‌متحده[1]، ۳۴ درصد از مجرمین درون‌سازمانی[2] 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[3] با ۶۰ سال سن متهم به سرقت ۳ میلیون دلار، تیموتی آلن لوید[4] ۳۹ ساله متهم به بیش از ۱۰ میلیون دلار و کِوین میتنیک[5] ۳۷ ساله متهم به بیش از ۱ میلیون دلار واردشده 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 بررسیِ بخش مذکور پیرامون سارقین سایبری، مشاهده می‌شود که الگویِ معناداری در میانِ سن آنان وجود دارد. اگر سرقت کمتر از صد هزار دلار باشد، به‌احتمال‌زیاد 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 به‌احتمال‌زیاد 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 به‌استثنای 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 ارتکابی 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، نه‌تنها ارتکاب جرم سایبری برای آنان بسیار دشوار بلکه حتی گاه انجام کارهای شخصی آن‌ها با کمک سایرین صورت می‌گیرد[۱]. پس می‌توان گفت جوامعی که هرم سنیِ آن‌ها در قاعده کم‌عرض‌تر است (جوامع به‌اصطلاح پیر) نرخ جرم سایبری کمتری دارند. با پذیرش این استدلال باید گفت، دریکی دو دهه آینده بزهکاریِ 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). به‌گونه‌ای که در سال ۲۰۰۹ اداره تحقیقات فدرال امریکا گزارش داد که از ۳۰ میلیون متهم دستگیرشده، ۷۵ درصد مرد و تنها ۲۵ درصد آن‌ها زن می‌باشند و ۸۱ درصد جرایم

---

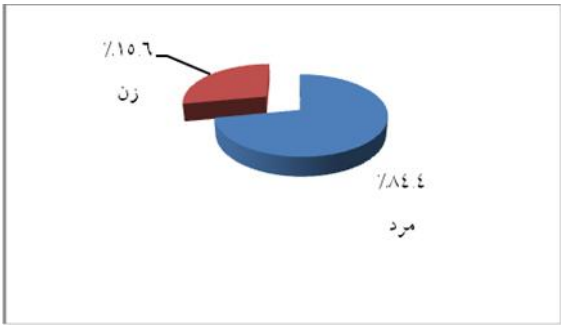
۱. مارکوس رجرز و همکاران وی نیز در دو پیمایشِ خود گزارشی (Self Report) دریافتند که در ارتباط با جرایم مرتبط بانفوذ و دسترسی غیرمجاز (هک)، افراد ۳۰-۱۷ سال بیشترین کسانی هستند که در این رفتار منحرفانه/مجرمانه سایبری مباشرت دارند.

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 (Britton 2011: 3). اطلاعات آماری زندانیان ایران نیز نشان می‌دهد که بیش از ۹۶ درصد از محکومین به حبس، مرد هستند (احمدی ۱۳۸۴: ۲۱۴).

ورای توجیهات زیست‌شناختی (کی‌نیا ۱۳۸۶: ۱۶۵-۱۵۶ و وفایی ۱۳۷۸) و جامعه‌شناختی (رستمی تبریزی ۱۳۸۸) که پیرامون بزهکاری زنان انجام‌شده است، باید گفت رویکرد پلیس و برخورد دستگاه عدالت کیفری با بزهکاران زن نیز متفاوت از مردان است و بخشی از این نابرابریِ آماری می‌تواند ناشی از نگاه مسامحه‌گرِ 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 جنسیتِ 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 انجام‌شده در تایوان نشان می‌دهد که ۹۰ درصدِ مردان در جرایم سایبری مباشرت داشته‌اند و درصد کمی از زنان آن‌هم در جرایم غیرمالی، بزهکار شناخته‌شده‌اند (Liao and Tasi 2006: 53).

باوجود مواردی که در بالا اشاره شد، در اندک پژوهش‌های انجام‌شده نیز جنسیت بزهکاران سایبری مغفول واقع‌شده و بیشترِ مطالعات به نژاد و رنگ پوست آنان معطوف است. برای نمونه تحقیقات در ایالات‌متحده نشان می‌دهند، مردانِ سفیدپوست اروپاییِ زیر ۲۶ سال،

رایج‌ترین نیمرخ مربوط به بزهکارانِ هرزه‌نگاریِ کودکان را دارا می‌باشند (Krone 2004: 5). شاید دلیل اصلیِ این پیش‌فرض که بزهکاریِ سایبری متعلق به مردان است ــ در کنار توجیهات بالا ــ پیچیدگی، فنی و تخصصی بودن جرایم سایبری باشد؛ اما به نظر می‌رسد ازآنجاکه بیشتر جرایم سایبری تخصص و مهارت زیادی را نمی‌طلبد، نرخ کمِ 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 زبانِ 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[1] بامهارت و تخصص دانشگاهیِ خود به برنامه‌نویسی و ویروس‌نگاری‌هایِ پیشرفته اقدام می‌نمودند و جز خود آن‌ها، کسی توان مقابله با آن‌ها را نداشت (Shinder 2002: 138)؛ اما امروزه با پیشرفت‌های سخت‌افزاری و نرم‌افزاریِ رایانه‌ای و نیز پیدایش اینترنت، بزهکاران سایبری به‌راحتی یک اشاره بر موشواره می‌توانند آنچه را پیشتر به‌دشواری انجام می‌شد را عملی سازند.

اما تصورِ رایجِ نادرست‌تر آن است که سطح مهارت فنیِ[2] تمامیِ بزهکاران سایبری، همگن و متجانس انگاشته شود. یافته‌های یک پژوهش نشان می‌دهد که از مجموع ۲۳۹ نفر موردمطالعه، ۲۱ درصد مهارت فنیِ پایین، ۲۲ درصد مهارت بالا، ۲۴ درصد متخصص و ۳۲ درصد توان فنی متوسط دارند (Chiesa 2009: 45). درواقع، اگرچه هنوز برخی شیوه‌های ارتکاب[3] نظیر حملات ممانعت از سرویس‌دهیِ توزیعی[4] در گستره سایبر به جهت ایمن بودن سامانه‌ها و شبکه‌ها نیازمند مهارت‌های عالیِ رایانه‌ای است، اما امروزه بیشتر جرایم سایبری با حداقل مهارت و تلاش روی می‌دهند. در این زمینه می‌توان به مهارت حداقلی ریزه‌خواران[5] اشاره نمود. حتی در حملاتی که از پیچیدگیِ 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 نرم‌افزارهای خودکار و از پیش طراحی‌شده‌ی نفوذ، نسبت به آن اقدام کند. از روش‌های جدید جبرانِ خلأ نداشتن مهارتِ لازم می‌توان به اجیر کردن نوجوانان به‌منظور طراحی حمله و برنامه‌نویسی اشاره کرد که به‌نوعی می‌توان آن را شکل جدیدی از «کودکانِ کار[1]» دانست (Jahankhani and Al-Nemrat 2010).

با توضیحات بالا می‌توان به این پرسش که «آیا سطح هوش بزهکاران سایبری نسبت به سایر بزهکاران بیشتر است؟» نیز پاسخ داد؛ زیرا این کلیشه در ذهن ما رخنه کرده که «چون هکرها (ما بزهکاران سایبری را همان هکرها می‌دانیم) دست به اعمال خارق‌العاده می‌زنند، پس توانمندی‌های ذهنی-هوشی بالا و استعدادهای ویژه‌ای دارند». درحالی‌که این تعمیم ناروا است. پس اگرچه هوش بالا یا به‌عبارتی توانایی استدلال، تجزیه‌وتحلیل و فکر منطقی، اثربخشیِ حمله را تضمین می‌کند، اما آن دسته از بزهکارانی که از نرم‌افزارهای تألیفی دیگران یا برنامه‌های نفوذِ بارگیری شده[2] بهره می‌برند، لزوماً نباید ضریب هوش[3] بالایی داشته باشند. بااین‌وجود، 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 بزهکاری 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 توسعه‌یافتگی یک کشور تلقی شود، اما ضرورتاً کاهش بزهکاری را به دنبال ندارد. حتی با لحاظ عواملی نظیر توسعه‌ی شهرنشینی، افزایش جمعیت- به‌عنوان شاخص‌های افزاینده‌ی 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، نه‌تنها بزهکاری کاهش نیافته بلکه در اَشکال و فراوانی سیر صعودی داشته است.

از سوی دیگر حتی با چشم‌پوشی از یافته‌هایی که رابطه معکوسی میان بزهکاری 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)

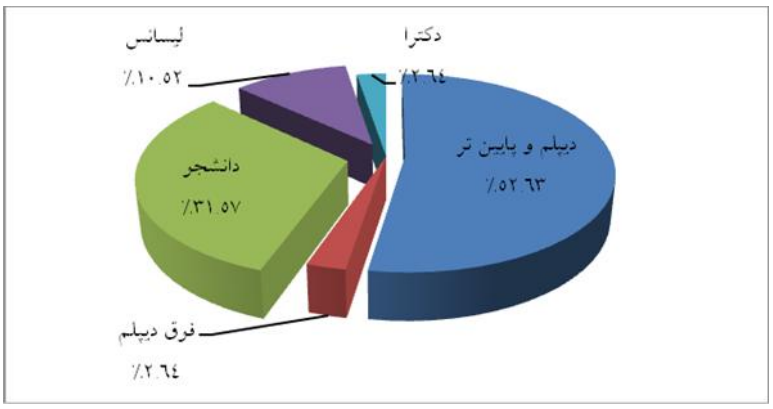
زمانیِ ۸۰ ساله اگرچه تعداد بی‌سوادها تا ۹۰ درصد کاهش‌یافته، اما از نرخ جرم کاسته نشده است. ممکن است انتقاد شود که میزان افزایش جمعیت و رشد شهرنشینی در این دوره زمانی لحاظ نشده است، اما به نظر می‌رسد حتی باوجود چنین نقیصه‌ای، نباید نرخ کاهش جرم تا این اندازه ناچیز باشد (مظلومان ۱۳۵۴). باید گفت موضوع مطالعه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

یک پیمایشِ خود گزارشی در میان دانشجویانِ 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 به‌منظور اعمال خرابکارانه و به‌دست‌آوردن رمز کارت اعتباری دیگران و غیره مباشرت داشته‌اند (Rogers, Seigfried and Tidk 2006). رجرز 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 ازآنجاکه نوجوانان و جوانان بیش از هر رده‌ی سنی دیگر در اعمال مجرمانه سایبری دخالت دارند و ازآن‌رو که بیشتر افراد در این سنین مشغول تحصیل در دانشگاه‌ها یا دانش‌آموخته می‌باشند، پس می‌توان نتیجه گرفت که افراد دانشجو یا تحصیل‌کرده بیش از اقشار دیگر می‌توانند به‌عنوان بزهکار سایبری شناخته شوند.

در پژوهشی دیگر، میزان تحصیلات در کنار سایر ویژگی‌های جمعیت‌شناختیِ 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).

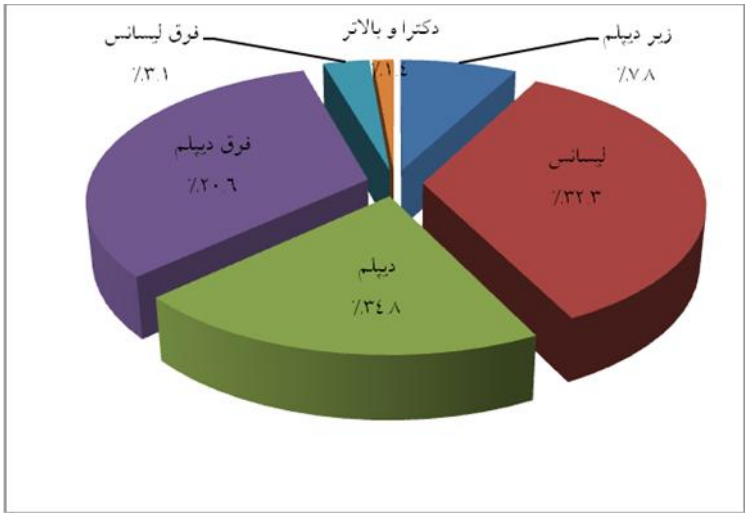
البته باملاحظه‌ی ۳۸ پرونده‌ی محکومینِ هرزه‌نگاری از مجموع ۴۵ پرونده‌ی موجود (در ۷ پرونده میزان تحصیلات محکومین ذکر نشده بود) مشخص شد که این بررسی تا حدی بامطالعه اخیر همخوانی دارد. در ۲۰ پرونده محکومین تحصیلات دیپلم و کمتر داشتند و در ۱۸ پرونده آن‌ها فوق‌دیپلم به بالا_ یک نفر فوق‌دیپلم، ۱۲ مورد دانشجو، 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 به‌دست‌آمده است (به نقل از: ابوذری، ۱۳۹۲)، به شکل قابل‌توجهی 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 آماریِ خود را تنها معطوف به دانشجویان

نمودند. البته باید اشاره کرد که جرایم موردبررسی مطالعه‌ی نخست در زمره جرایم سایبریِ محض می‌باشند و این جرایم نسبت به سایر جرایم سایبری، به دانش و مهارت بیشتری نیاز دارند. لذا بدیهی است که معمولاً افراد تحصیل‌کرده‌تر 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 تحصیل‌کردگان را شاهد هستیم.

پس به‌طورکلی می‌توان گفت وضعیت تحصیل در تمامی بزهکاران ازجمله 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 ضرب‌وجرح و برگلری محکوم‌شده‌اند، از سطح تحصیلاتیِ متفاوتی برخوردار می‌باشند (Durost 2006: 5-6). از سوی دیگر باید اذعان داشت در جرایم سایبری به دلیل آنچه در بالا آمد، اغلب افراد تحصیل‌کرده بیش از سایرین دست به ارتکاب جرم می‌زنند.

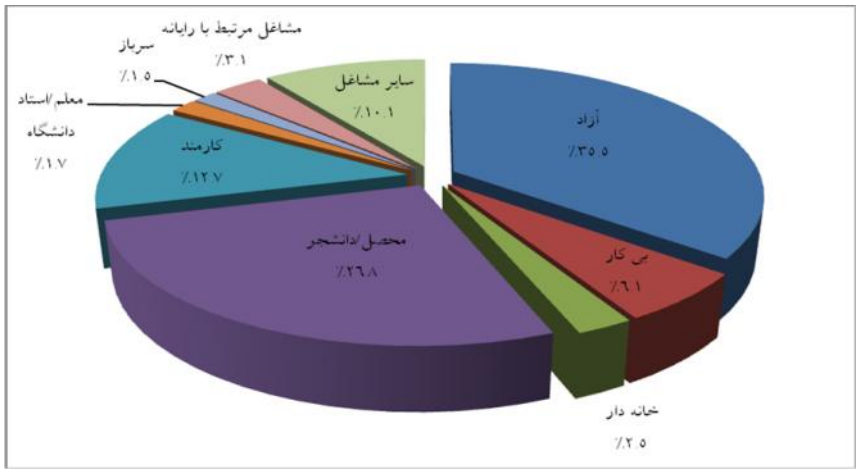
۵-۱- پیشینه خانوادگی و زمینه‌های شغلی

تصور رایج ما از خانواده‌ای که یک بزهکار سایبری/هکر در دامان آن پرورش‌یافته، خانواده‌ای محروم و سطح پایین است که پدر و مادر هیچ نظارتی بر فرزند خود ندارند، پدر و مادر از هم جداشده 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 انحرافیِ والدین، کودک در دوران رشد خود دچار اختلال می‌گردد. پس به‌طورکلی، هکرها به‌مانند بیشتر بزهکاران در دوران کودکی و نوجوانی از سوی والدین خود حمایت عاطفی و مورد مراقبت نبوده‌اند. ازاین‌رو، معمولاً هکرها به خاطر شخصیت ضداجتماعی و درون‌گرای[1] خود در مدرسه نیز دوستان زیادی ندارند. آن‌ها با فرار از تمامیِ موج‌های ناایمنِ زندگی، به ساحل امنی چون فضای مجازی رسیده‌اند؛ جایی که می‌تواند اظهارنظر کنند، قدرت ازدست‌رفته خود را بازیابند و به عبارتی به‌تمامی آنچه در دنیای خاکی از آن محروم بوده‌اند، دست یابند.

1. Introversion

اما باید اشاره کرد که همواره وضعیت این‌گونه نیست. حتی در مواردی به جهت پیوندِ عمیقی که میان والدین و فرزند وجود دارد، کودک رفتار انحرافی را از والدین می‌آموزد. برای نمونه در یک پرونده، کودکی سه‌ساله توانست تحت آموزش و تشویق پدر و مادر خود با اجرای عملیات حملات ممانعت از سرویس‌دهی[1] به داده‌های رایانه‌ای دیگر، دسترسی یابد (Chiesa, Ducci and Ciappi 2009: 93-94).

همان‌طور 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. درواقع، برخلاف آنچه تصور می‌شود، بزهکاری سایبری منصرف به افراد بی‌کار و فاقد درآمد نیست. برای نمونه طبق آمار پلیس فتا تنها ۶/۱ درصد متهمین جرایم سایبری بی‌کار هستند (به نقل از: ابوذری ۱۳۹۱) (بنگرید به شکل ۵). کما اینکه ملاحظه می‌شود حتی بعضی از حملات از سوی کسانی که در سازمان/شرکت دارای اختیارات گسترده هستند (بزهکاران درون‌سازمانی) انجام می‌شود. برای نمونه پیمایشی نشان داد که ۲۵/۱ درصد بزهکاران دانشجو، ۱۷/۵ درصد بیکار و بقیه مشغول به‌کار در سازمان‌های دولتی یا شرکت‌های خصوصی می‌باشند. شگفت‌آور اینکه حتی در چهار مورد، بزهکاران سایبری از استادان دانشگاه بودند (Liao and Tasi 2006: 54).



شکل ۵- زمینه‌های شغلی متهمین جرایم سایبری در ایران

1. Denial of Service (DoS)

۶-۱- پیشینه مجرمانه

یکی از برجسته‌ترین شاخص‌های سنجشِ خطرناکی در مطالعات جرم‌شناختی، سابقه‌دار بودن یا به عبارتی «تکرار بزهکاری» است. بررسی این عامل ازاین‌جهت 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 سلبِ‌توان 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 خریدوفروش مواد مخدر، توزیع لوح‌های فشرده هرزه‌نگاری، سرقت جزئی، قمار و غیره محکوم‌شده 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 دوِ آن‌ها، بیشتر بدون سابقه مجرمانه می‌باشند؛ اما همان‌طور که گفته شد، افراد باسابقه نیز در میان آنان ملاحظه می‌شود (Rogers 2001: 85).

درنتیجه، به‌صرف پاکیِ لوحه‌ی مجرمانه متهمین نمی‌توان بیان داشت آنان نسبت به سایرین کمتر خطرناک می‌باشند، بلکه عمل ارتکابی 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 قرارمی‌دهد به‌صرف نداشتن پیشینه مجرمانه خطرناک نیست. یا ازآنجاکه 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 منزجر 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 مفاسد اقتصادی» بسیج می‌شوند.

مجرمانه می‌تواند به‌عنوان اماره‌ای مبنی بر خطرناکیِ بزهکاران مورد لحاظ قرار گیرد، اما تنها دلیل موجود نیست.

آنچه در پژوهشِ حاضر آشکارا دیده می‌شود آن است که بزهکاری سایبری تنها از سوی یک گروه مشخص یا یک طرز فکر و باور واحد سر نمی‌زند. درواقع، همان‌طور که ما به‌هیچ‌وجه بزهکاران کلاسیک را یک کلِ متجانس و همگن نمی‌انگاریم، باید چنین رویکردی را نیز در برابر بزهکاران سایبری اتخاذ کنیم؛ بنابراین، حداقل می‌توان گفت نتایج تحقیقات تجربی انجام‌شده در این چارچوب و نیز نتایج تحقیقات میدانی مورد استناد این نوشتار، انگاره‌های برخی جرم‌شناسان درباره ویژگی‌های مجرمین سایبری را ثابت نمی‌کند.

لذا پژوهش حاضر نشان می‌دهد، گزاره‌های زیر به جهت تعمیم شاخص‌ها و ویژگی‌های عمومی به‌تمامی بزهکاران سایبری، نادرست و فاقد پشتوانه علمی-تجربی است:

- تمامی بزهکاران سایبری از ضریب هوشی بالایی برخوردارند و مهارت‌های فنی آن‌ها در سطح بسیار بالایی است؛
- تمامی بزهکاران سایبری دارای کمترین مهارت اجتماعی می‌باشند، آن‌ها افرادی گوشه‌گیر، منزوی و درون‌گرا می‌باشند[1]؛
- 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 می‌باشند؛
- تمامی بزهکاران سایبری خطرناک و همواره برای سامانه‌ها و رایانه‌ها دردسر ایجاد می‌کنند؛
- تمامی بزهکاران سایبری روابط عاطفیِ ازهم‌گسیخته‌ای با والدین خود دارند یا اغلب آن‌ها کودکانِ طلاق یا فرزندخوانده[2] می‌باشند؛

---

۱. شاید هیچ تعبیری به‌مانند «نِرد» به‌وضوح از شخصیت آن‌ها پرده برنمی‌دارد. «نرد» به کسانی گفته می‌شود 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 می‌آورند. «نردها» معمولاً از طرف اجتماعات مختلف طرد می‌شوند، در ارتباط با جنس مخالف دچار مشکل هستند، ظاهر ژولیده‌ای دارند و به‌اصطلاح افرادی «سوسول» می‌باشند که اگر کسی پیدا نشود و از نبوغشان استفاده کند، ازلحاظ مالی دچار بحران می‌شوند. در میان بزهکاران سایبری، جاسوس‌ها بیش از سایر آن‌ها، افرادی ساکن و آرام به نظر می‌رسند. آن‌ها کاملاً مراقب سخنان و نحوه نگاه خود هستند و نمی‌خواهند متفاوت به نظر برسند. لذا همیشه سعی می‌کنند با دیگران اختلاط کنند. برای به دام انداختن یک جاسوس، باید دنبال افرادی باشیم که همیشه کارهای خود را پنهان می‌کنند (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 به‌طورکلی:

- 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، به نحو 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 به سلاح 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 کاربستِ 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 ازآنجا ناشی می‌شود که ما به‌اشتباه ویژگی‌های یک دسته از بزهکاران سایبری (بخشی و نه همه بزهکاران سایبری محض) را به‌تمامی آنان قابل‌تعمیم می‌دانیم[۱].

۲- بزهکاران سایبری و کلاسیک: همسانی یا گوناگونی

پس از ارائه توضیحاتی در ارتباط با ویژگی‌های اجتماعی و جمعیت‌شناختیِ بزهکاران سایبری، پرسش کلیدی که به ذهن خطور 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، این انگاره در ارتباط با بزهکاران سایبری کمتر صدق می‌کند: زیرا با توجه به این‌که مطالعات کمتری این واقعیت را نشان داده‌اند و در این میان بیشتر رسانه‌ها ذهن عامهٔ 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 به تصویر 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 واقعیتِ بزهکاران سایبریِ ایرانی مشخص شود و اساساً در چنین مطالعاتی، تعمیم پیمایش‌های دیگر، گمراه‌کننده و ناروا است.

همان بزهکاران 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 انجام‌شده است (به‌ویژه در ارتباط با تفاوت یا شباهت بزهکاران جنسیِ برخط و بزهکاران جنسیِ برون‌خط[1])، اما پاسخ قطعی نیازمند مطالعات بیشتری است. برای نمونه در پژوهشی که در قالب یک «فرا تحلیل»[2] صورت گرفت، نشان داد که بزهکاران جنسیِ برخط به‌احتمال‌زیاد سفیدپوست و تا حدی جوان‌تر از بزهکاران جنسی برون‌خط می‌باشند (Babchishin, Hanson and Hermann 2011).

بااین‌وجود نباید پنداشت که ویژگی‌های بزهکاران سایبری و بزهکاران کلاسیک به‌طور کامل برهم منطبق و سازگار است؛ زیرا به جهت تفاوت عمیق بسترِ بی‌پیکرِ سایبر با فضای مادی، بی‌تردید ماهیت بزه و گونه‌های بزهکاران را دستخوش تغییر قرار داده است. برای نمونه گستره فضای مجازی نسبت به فضای مادی دارای اهداف مناسبِ بی‌شماری است و بالتبع این امر برانگیختگیِ مضاعف هر بزهکاری را در پی دارد. همچنین می‌توان به ویژگی‌هایی مانند ناشناختگی و مخفی ماندن هویت در فضای سایبر اشاره کرد. حتی به نظر ما ویژگیِ اخیر در ترغیب افراد از طبقات اجتماعیِ مختلف[3] و ویژگی‌های جمعیت‌شناختیِ متفاوت نسبت به بزهکاران کلاسیک، در کنشگری و بالتبع بزهکاری یا بزه‌دیدگی بسیار حائز اهمیت است. چراکه افراد در پشت سِپر ناشناختگی، اجتماعی‌تر و نسبت به ارتباطات رودررو آزادتر می‌باشند. آن‌ها به‌واسطه‌ی رشد شخصیت اجتماع‌پذیر، پرخاشگرتر می‌شوند و دیگر کم رو و خجالتی نیستند (منفرد و جلالی فراهانی ۱۳۹۱). ازاین‌رو ویژگی‌های محیطی، احتمال انحراف آن‌ها را تقویت می‌کند. همچنین، بدین لحاظ که بهره‌برداریِ سوء از بستر سایبر نیازمند حداقل مهارت و دانش فنی است، نوجوانان و جوانان - بیش از سایر گروه‌ها- باید مخاطب اصلیِ برنامه‌های کنشی و واکنشی قرار گیرند.[4]

---

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 انجام‌شده است. با تجمیع و تحلیل حجم زیادی از داده‌ها، امکان اعتماد به نتایج به‌طور قابل‌توجهی بیشتر می‌شود. به‌این‌ترتیب می‌توان گفت که یافته‌های «فرا تحلیل»، اساسی‌تر از یافته‌های مطالعاتِ پژوهشیِ منفرد هستند.

۳. برای نمونه درحالی‌که برخی پیمایش‌ها نشان می‌دهند آن‌هایی که در خانه‌های سازمانی و سایر ناحیه‌های با درآمدِ 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 فراوانیِ ارتکاب جرم سایبری را دارند درحالی‌که بیشترین فراوانی جرایم کلاسیک متعلق به گروه سنی ۳۵-۲۶ است (Rogers 2001: 86).

ب) گونه‌شناسی انگیزه‌ها

باوجود تعاریف گوناگونی که از انگیزه ارائه‌شده است،[۱] تمامیِ آن‌ها به‌گونه‌ای بر هدف نهایی و آنچه فرد را به انجام کاری سوق می‌دهد، اشاره دارند. به نظر می‌رسد انگیزه «مقصودی است که فرد به‌منظور 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 علت‌شناسیِ جرم و پیشگیری از بزهکاری بسیار حائز اهمیت است[۳]؛ زیرا جرم‌شناسان و سیاست‌گذاران همواره به دنبال آن‌اند تا از گذرِ انحراف در فرآیندِ گذارِ 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 این‌چنینی را برای آنان لحاظ کند. البته به نظر ما هیچ تأدیبی اثربخش‌تر از آموزش؛ یعنی تقویت اخلاقی و برونی‌سازی هنجارها نیست (بنگرید به: بهره‌مند، محمدکوره‌پز 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 موردنظر فاعل جرم است»، تعریف‌شده است (کی نیا ۱۳۸۶: ۸۰).

۲. به نظر می‌رسد انگیزه در حقوق کیفری و مدنی واجد یک مشخصه باشد. ازاین‌رو به نظر همان تعریف ارائه‌شده 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 تحققی یا پوزیتویستی بود. به عقیده بنیان این مکتب، انگیزه عنصری است که می‌تواند از حالت خطرناک فرد پرده بردارد (کی نیا ۱۳۸۶: ۸۱).

4. Acting Out

آسیب‌پذیر محافظت نماید (پیشگیری وضعی[1]) 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 مفهومِ حالت خطرناک و پیدایش یک سیاست جناییِ امنیت‌مدار، شاهد آن هستیم که انگیزه در گفتمان نوینِ 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 انجام‌شده 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- صرف‌نظر از انگیزه جنسی- تمام انگیزه‌ها را در این تقسیم‌بندی گنجاند.

اما چنانچه بخواهیم بر اساس گونه‌های رایج جرایم سایبری، انگیزه‌های بزهکاران سایبری را به‌گونه‌ای طبقه‌بندی کرد که با یکدیگر هم‌پوشانی نداشته باشند، آن‌ها عبارت‌اند از[2]:

۱- پاسخ به گرایش‌های درونی: کنجکاوی- لذت طلبی

یکی از اولین روانشناسانی که پیرامون ابعادِ لذت طلبیِ انسان‌ها مطالعه کرد، بیان نمود: «برخی از رفتارها به خاطر لذتِ 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. بااین‌حال نباید تصور شود که تنها با کاربستِ 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 دوْر 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 قرارگرفته است. در حال حاضر به نظر می‌رسد، ازلحاظ فراوانی، بیشتر بزهکاران که اکثراً نوجوان و جوان می‌باشند با انگیزه جنسی به ارتکاب جرم برانگیخته می‌شوند. به‌هرحال بدون پشتوانه‌ی آماریِ 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، تمامیِ سلایق را پاسخگو است و به نحو خیره‌کننده‌ای انسانِ تفریح گر 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، به‌سوی 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 به‌صورت امنیت‌سنجیِ سیستم دفاعیِ یک دولت/شرکت ظهور پیدا می‌کند. بااین‌وجود، این افراد به جهت غیر پیچیدگی حملاتشان، شناسایی آنان دشوار نیست. ازاین‌رو، در زمره مشتریان همیشگی دستگاه عدالت کیفری قرار دارند.[1] مثال‌های فوق نشان می‌دهند که ممکن است افراد با سطحِ مهارت‌های گوناگون به دنبال سرگرمی و کنجکاوی باشند. در این راستا یک هکر ۱۹ ساله‌ی سربازِ ارتشِ رژیمِ اشغالگر قدس انگیزه خود از هک را این‌گونه بیان می‌دارد:

«هک، انجام یک کار غیرقانونی و نامشروعِ 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 آموزش‌محور و یا با کاربستِ تدابیر وضعی- به‌ویژه با جاذبه‌زدایی- تا حد زیادی فراوانیِ رفتار آنان را تقلیل داد.

۲- طمع‌ورزی و کسب منافع مالی

با وابستگی فزاینده‌ی روابط تجاریِ میان مردم- دولت به ارتباطات از راه دور و شکل‌گیری دولت الکترونیک (E-Government)، جرایم مالیِ 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 نرم‌افزار و استفاده غیرمجاز از آثار ادبی و هنری دیگران، بزهکاران با موج وسیعی از اطلاعات دیجیتالیِ مالیِ کاربران رویارو شده‌اند. هزینه‌ی پایین ارتکاب جرم، کثرت بزه دیدگان و بالطبع عواید بالا نه‌تنها بزهکاران سایبری بلکه دیگران را نیز به این عرصه گسیل داشته است.[1] از رایج‌ترین جرایم که با انگیزه مالی صورت می‌گیرند می‌توان به کلاه‌برداری، سرقت اطلاعات مالی و نیز دسترسی به اطلاعات محصولات پرفروش، تقلب مالیاتی و پول‌شویی اشاره نمود.

به نظر می‌رسد افرادی که به دلیل جلب‌توجه و کسب شهرت به رفتارهای مخرب دست می‌زنند را نیز می‌توان در این دسته جا گنجاند؛ زیرا انگیزه غائیِ 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 برتری‌جوئی آن‌ها را به ارتکاب جرم برمی‌انگیزاند. ازاین‌رو می‌توان گفت که جلب‌توجه و کسب شهرت از انگیزه‌های بینابین یا مختلط محسوب می‌شوند.

۳- انتقام‌جویی

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

یکی دیگر از جرایمی که با انگیزه انتقام‌جویی روی می‌دهد، تعقیب ایذائی[2] 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، به‌منظور 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 ازدست‌داده 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 ایالات‌متحده ۶٫۷ میلیون دلار بود- که افزایش ۵ درصدی نسبت به سال ۲۰۰۷ را نشان می‌دهد- و زیان آن به کسب‌وکار به‌طور میانگین بالغبر 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 بدین‌وسیله می‌تواند به دیگران ثابت کند که هنوز از عشق دیرینش دست نکشیده است. همچنین ممکن است رابطه زناشویی ازهم‌گسیخته، 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 نقل‌مکان 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 نه‌تنها 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 جنسیِ خود به فضای سایبر سفر می‌کنند.[۱] چراکه این فضا با ناشناختگیِ 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 دربازی‌های کثیف و فرعیِ هرزه‌نگاری یافت می‌شد، قابل‌قبول می‌سازد. نگران‌کننده‌ترین موضوع در مورد تمام این اطلاعات، آن است که صنعت مذکور نه‌تنها تجارت بزرگی است، بلکه فروشِ 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 مرسومی که با انگیزه جنسی روی می‌دهند می‌توان به سیاحت‌گری جنسی[1] و کودک دوستی اشاره نمود.

بنابراین، افراد زیادی با درجات خطرناکیِ 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 جنسیِ خود را در این فضا برآورده سازند. چنانکه گروه‌های دیگری نظیر آزارگر- آزارپذیرها (Sado-Masochist)، متجاوزان به عنف سریالی و قاتلین سریالیِ جنسی ازجمله بزهکاران جنسیِ 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 پیگیریِ اهدافِ 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 مقابله‌به‌مثل 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

1. Sex Tourism

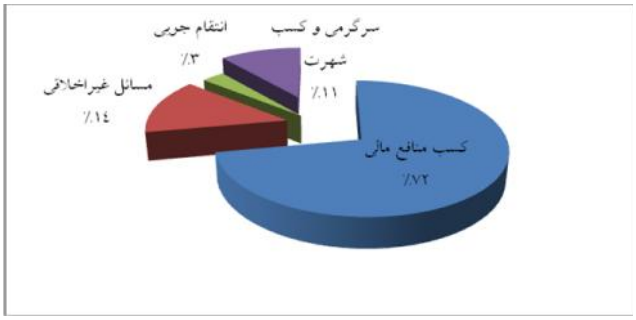
بزهکاران سایبری را تحریک به حمله به وبگاه‌های دولتی و حتی زیرساخت‌های حیاتی یک دولت کند تا به همگان ثابت کنند که در این جنگ سایبری، آن‌ها فاتح بلامنازع می‌باشند.

افزون بر این، گاه این جرایم به‌واسطه تنفر از یک گروه نژادی- جنسی یا یک اندیشه سیاسی- مذهبیِ معارض صورت می‌گیرد.[۱] برای نمونه مردان علاقه چندانی به اندیشه‌های فمینیستی ندارند و رشد این طرز فکر را به ضرر خود می‌دانند. ازاین‌رو، ممکن است به شبکه‌های اجتماعیِ مروّجین این باورها حمله کنند. باید اشاره کرد که اگرچه این جرایم به‌مانند 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 به‌مانند همتایان کلاسیک خود، طیف وسیعی از انگیزه‌ها را در سر می‌پرورانند؛ زیرا هم‌اکنون همان انگیزه‌های سنتی که همواره با بشر همراه بوده است درپوششی 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 نامقبولِ اجتماعی درصدد 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 ارائه‌شده است، اشاره دارد. این آمار از ۱۹۰۸ مورد مکشوفه از مجموع ۴۰۰۰ پرونده موجود، به‌دست‌آمده است (به نقل از: ناصرآبادی ۱۳۹۱).

---

۱. درواقع این جرایم، گونه‌ی سایبریِ 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

پس‌ازآنکه داده‌های مربوط به نیمرخ‌جناییِ محکومین پیشین گردآوری شد، باید از آن‌ها در تحلیل رویداد مجرمانه و درنهایت در طراحیِ نیمرخ‌جنایی 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، نه‌تنها این اطلاعات ارزشی ندارند بلکه می‌توانند گمراه‌کننده نیز باشند.

در مرحله تحلیل داده‌ها این مأمورینِ تحقیقِ واحد جرایم رایانه‌ای می‌باشند که بیش از هر متخصصین دیگری می‌توانند با پردازش داده‌ها، برونداد/خروجیِ (Output) مناسب و مفیدی را از آن‌ها به دست آورند؛ زیرا این امر تنها از سوی مأمورینِ تحقیقِ زبده یا کسانی که به‌اصطلاح دارای «شمِّ پلیسی»اند، برمی‌آید. در تأیید این نکته، سخنگوی واحد ملیِ جرم فناوریِ 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 حوزهٔ رایانه را انتخاب و آن‌ها را به مأموران خوبی تبدیل کنیم» (جوکز و همکاران ۱۳۸۹: ۱۶۰). بااین‌حال، در این مرحله نیز مأمورین پلیس از مشاوره با متخصصین علوم رایانه مستغنی نمی‌باشند.

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

گردآوری‌شده 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 ارتکابی، با بررسی صحنه‌ی جرم- که شامل شیوه، مکان، زمان ارتکاب، ملاحظات بزه‌دیده‌شناختی و غیره است- سرنخ‌های مهم گردآوری می‌گردند. سپس این داده‌ها با وضعیت بزهکارانِ جرایمِ مشابهِ پیشین- ویژگی‌های جمعیت‌شناختی- روانی مقایسه می‌شوند. سرانجام کارآگاهان و مأمورین تحقیق با تلفیق این دودسته اطلاعات با یکدیگر، از آن‌ها به‌منظور شناساییِ بزهکاران بهره‌برداری می‌کنند.[1] برای نمونه زمانی که فردی از اتاق‌های گپ به‌منظور تعقیب ایذایی 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 گمانه‌های که قابل‌اعتنا 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. درحالی‌که در بادیِ امر این‌طور به نظر می‌رسید که اگرچه شناخت این ویژگی‌ها تنها برای یک جرم‌شناس یا سیاست‌گذار عرصهٔ فضای سایبر بسیار اهمیت دارد، اما وجه ضرورت گردآوری آن داده‌ها در شناساییِ بزهکار احتمالی کمی دور از ذهن به نظر می‌رسید. نگاه پررنگ 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 به شمار می‌رفت. پس کمینه وجهِ تمایزِ فن نیمرخ‌جنایی 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 میزانِ اهمیت و ارزشِ «تفسیرپذیری» طبقه‌بندی و تدوین شوند؛ زیرا تمامیِ داده‌ها از ارزش و اهمیت یکسانی برخوردار نیستند؛ اما درعین‌حال مأمورین نباید داده‌های جزئی را به بهانه این‌که 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.

نتیجه‌گیری

در ارتباط با نیمرخ‌جناییِ بزهکاران سایبری باید گفت، طبقه‌بندی‌هایی که از بزهکاران سایبری ارائه‌شده است (محمدکوره‌پز ۱۳۹۳)، نشان می‌دهند که بزهکاران سایبری برخلاف تصور رایج برخی جرم‌شناسان، گروهی همگن و متجانس نیستند. به بیانی دیگر، یافته‌های پژوهش‌های جدیدتر و پژوهش حاضر، اساساً هر گزاره‌ای که ویژگیِ خاصی را به‌تمامی بزهکاران سایبری تعمیم دهد، عوامانه و فاقد پشتوانه‌ی علمی می‌دانند؛ زیرا آنان نیز به‌مانند بزهکاران کلاسیک به گونه‌های متنوعی تقسیم می‌شوند. پس نباید پنداشت که تمامیِ بزهکاران سایبری، نوجوان و جوان، مرد، یقه‌سفید، باهوش، دارای مهارت فنیِ بالا، برخوردار از تحصیلات مطلوب و به‌طورکلی «حرفه‌ای» می‌باشند بلکه در میان بزهکاران سایبری نیز هم کسانی که مبتدی‌اند و به‌راحتی شناسایی می‌شوند و هم بزهکاران حرفه‌ای که شناسایی و ردیابی آنان دشوار است، وجود دارد. البته این تصور نیز نادرست است که ویژگی‌های آنان به‌طور کامل همسان و سازگار با بزهکاران کلاسیک فرض شود؛ زیرا حداقل، تفاوت عمیق بسترِ سایبر با فضای 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. ازاین‌رو، شایسته است که سیاست‌گذاران، یک راهبرد یا سیاست جناییِ افتراقی را به‌منظور مبارزه و پیشگیری در برابر بزهکاران سایبری، اتخاذ کنند.

در کنار تمرکز بر ویژگی‌های اجتماعی- روانیِ بزهکاران که اساس این نوشتار را تشکیل داد، باید اشاره کرد که بررسیِ صحنه‌ی جرم می‌تواند به‌طور مؤثری طراحانِ نیمرخ را در رمزگشایی و تعیین بزهکارِ احتمالی کمک کند. شیوه‌ی ارتکاب، مکان و زمان حمله و ملاحظات بزه‌دیده‌شناختی از مهم‌ترین عواملی‌اند که در ذیل صحنه‌ی جرم بررسی می‌شوند. نکته بسیار مهم اینکه بررسیِ این عوامل زمانی معنا پیدا می‌کنند که طراحان نیمرخ به ویژگی‌های اجتماعی- روانیِ بزهکاران نیز نگاه پررنگی داشته باشد. کما اینکه تنها نمی‌توانند 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 فنیِ بالایی دارد یا خیر _ این دو بدین خاطر جداگانه مطرح شد که لزوماً کسی که مهارت فنیِ بالایی دارد حرفه‌ای

نیست زیرا حرفه‌ای بودنِ مرتکب بیشتر ناظر به آن است که ردّ 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 به‌منظور آشکارسازیِ روابط پیشینیِ بزهکار- بزه‌دیده، میزان تقصیر وی و به‌طورکلی سرنخ‌هایی که طراح نیمرخ را به تعیین بزهکار احتمالی استفاده نمود، موجبات پیشگیری از آسیب‌های ثانویه و حمایت از بزه دیدگان را فراهم می‌آورد.

منابع

الف) منابع فارسی

- آس، کاتیا فرانکو (۱۳۹۰)، *جهانی‌سازی و جرم*، ترجمه: یوسف بابایی و اصلی عباسی، تهران: مجد.

- 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 محمدکوره‌پز ح؛ و سلیمی ا (۱۳۹۳)، *راهبردهای وضعی پیشگیری از جرایم سایبری*، آموزه‌های حقوق کیفری (۷): ۱۷۶-۱۴۷.

- پیتارو، میشل (۱۳۹۲)، *مزاحمت سایبری: گونه‌شناسی، علت‌شناسی و بزه‌یده‌شناسی*، 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 واکنش-های جهانی تا پاسخ‌های نظام‌های کیفری ملی*، در: حقوق فناوری اطلاعات و ارتباطات (مجموعه مقالات)، گردآوری: امیرحسین جلالی فراهانی، تهران: روزنامه رسمی جمهوری اسلامی ایران.

- شمسه، 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 (مجلهٔ 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)*، ترجمهٔ 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.

- محمدکوره‌پز، 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 جرم شناختی بزهکاری رایانه‌ای»، فصلنامه مطالعات پیشگیری از جرم، (۲۵)، ۷۶-۴۷.

- منفرد م؛ و جلالی فراهانی ا (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*، قابل‌دسترسی 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

- 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 درآمدی 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 حقوقِ دانشگاه شهید بهشتی، نیم سال دوم تحصیلی، ۱۳۹۲-۱۳۹۱. قابل‌دسترسی در: www.lawtest.ir.

- نجفی ابرندآبادی، علی حسین (۱۳۹۱)، *دربارهٔ سن و علوم جنایی*، دیباچه در: مبانی پیشگیری اجتماعی رشدمدار از بزهکاری اطفال و نوجوانان. نوشتهٔ 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)، *زمینهٔ حقوق جزای عمومی*، تهران: گنج دانش.

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

- ویلیامز، ماتیو (۱۳۹۱)، *بزهکاری مجازی: بزه، انحراف و مقررات‌گذاری برخط*، ترجمه: امیرحسین جلالی‌فراهانی و محبوبه منفرد، زیر نظرِ علی حسین نجفی ابرندآبادی، تهران: میزان.

- هالدر، داراتی؛ 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 Expriences, 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*, NewYork: 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.