مطالعات علوم سیاسی، حقوق و فقه

دوره ۳، شماره ۱/۳، بهار ۱۳۹۶

صفحات ۱۳۶- ۱۲۶

Online ISSN: ٢٤٧٦-٤٤٦٩

Print ISSN: ٢٥٣٨-٢٠٣٩

www.irijournals.com

بررسی انگیزه‌های اصلی بزه کاران در فضای سایبری

جلال شیرمحمدی

کارشناس ارشد حقوق جزا و جرم‌شناسی، دانشگاه آزاد اسلامی، واحد اردبیل

چکیده

فناوری اطلاعات و ارتباطات، همراه با امتیازات بی‌نظیر خود، گستره وسیعی از فرصت‌های مجرمانه را نیز فراهم آورده است. این وضعیت موجب «عمومی شدن بزه» در فضای مجازی شده است؛ به‌گونه‌ای که علاوه بر افراد باانگیزه مجرمانه محض، بسیاری از کاربران فضای سایبر نیز به رفتارهای بزهکارانه می‌پردازند. این انگیزه‌ها و اهداف گاهی در راستا هنجارهای جامعه است و گاهی محل مناسب برای انواع نابهنجاری‌ها و جرائم می باشددر این راستا این پژوهش که به مطالعه موضوع به شیوه توصیفی- تحلیلی می‌پردازد، انگیزه‌های بزه کاران را در پنج مؤلفه پاسخ به گرایش‌های درونی: کنجکاوی- لذت طلبی؛ طمع‌ورزی و کسب منافع مالی؛ انتقام‌جویی؛ انگیزه جنسی و باورهای ایدئولوژیک موردبحث قرار می‌دهد.

واژه‌های کلیدی: انگیزه جرم، فضای سایبری، بزهکاران فضای سایبری، شبکه‌های اجتماعی.

۱- مقدمه

در عصر حاضر گستردگی فضای اینترنت، شکل جدیدی از تعاملات اجتماعی را تحت عنوان شبکه‌های اجتماعی مجازی ایجاد کرده است. فناوری نسل سوم علاوه بر اینکه توانست نتایج و اثرات مفیدی همچون تسریع امور، تعاملات مجازی سریع و ورای مرزهای جغرافیایی و ... را بر زندگی بشری به‌جای بگذارد، از سوی دیگر توانست خالق جرائمی باشد، با شیوه ارتکاب آسان، سودآوری کلان، خطرپذیری پایین و ردیابی مشکل. نتیجه به‌طور کامل معلوم است، فضای مجازی مهم‌ترین فضای مجرمانه قرن ۲۱ است (رحیمی، ۱۳۹۳).

یکی از چالش‌های اساسی مأمورین اجرای قانون، دشواریِ کشف جرائم سایبری است. در این جرائم، برخلاف تمامی جرائم، جرم دربستری رها و درِ پوشش ناشناختگی و گمنامیِ نسبی بزهکاران انجام می‌شود لذا پی‌جویی جرائم سایبری مستلزم کاربستِ تدابیر روزآمد می‌باشد و می‌توان با استفاده از شگرد نیمرخِ سازی جنایی با نگرشی عمیق به ویژگی‌های جمعیت شناختی- اجتماعی و رفتاری- روانیِ عموم مرتکبین قبلی، مشاهده صحنه ارتکاب جرم و نیز نشستن مستقیم برِ بالین بزه دیده و گفتگو با وی درصدد برآمد تا از ِ گذر تحلیل این داده‌ها بتوان به سرنخ‌هایی دست‌یافت که افسران تحقیق را در شناسایی بزهکار یاری‌رسان باشد (ماتسو متو، ۲۰۰۹, ۴۰۱). عوامل فردی همچون انگیزه‌های گوناگون و میزان دانش و تخصص فرد در کنار عوامل محیطی نظیر غیرواقعی پنداشتن محیط سایبر، امکان گمنامی هویت بی‌هنجاری سایبری و وجود فرصت‌های کلی مجرمانه از مهم‌ترین عوامل تأثیرگذار در ارتکاب جرم در محیط سایبر می‌باشد. روشن است که این عوامل درواقع بیان‌کننده جنبه‌های تاریک محیط سایبر می‌باشند که نقش انکارناپذیری در ارتکاب جرائم گوناگون سایبری دارد. (چابک پور، ۱۳۹۳)

مرتکبین جرائم رایانه‌ای از خصوصیات و روحیات خاصی برخوردارند. بر طبق تحقیقاتی که انجام‌شده است مجرمین رایانه‌ای اکثراً درون‌گرا هستند (شیرزاد، ۱۳۸۸، ۹۲). مجرمان رایانه‌ای اکثراً از طبقات تحصیل‌کرده هستند و نکته اینجاست که این دسته از افراد در ارتکاب سایر انواع جرائم اصلاً موفق نیستند. از این جهات، تعقیب و دستگیری این مجرمان دشوارتر است. از سوی دیگر، علم کیفر شناسی اقتضا دارد که به خاطر موقعیت اجتماعی خاص این‌گونه مجرمان برخورد متفاوت و عموماً ملایم‌تری با آن‌ها صورت گیرد (منفرد، ۱۳۹۱). انگیزه این دسته از مجرمان هم عموماً باانگیزه مجرمان جرائم عادی تفاوت دارد. عموم انگیزه این دسته از مجرمان غیر از سود و منفعت شخصی خودشان است. برخی از این مرتکبین درصدد نشان دادن مهارت خود هستند و برخی دیگر صرفاً برای سرگرمی این کار را انجام می‌دهند. در برخی از این مرتکبان حتی انگیزه‌های بشردوستانه هم وجود دارد. برخی دیگر از مرتکبین، اصولاً با محدودیت مشکل‌دارند و نمی‌توانند با محدودیت دسترسی خود به برخی اطلاعات کنار بیایند. نکته دیگری که ازلحاظ رفتارشناسی این مجرمین باید بدان توجه کرد این است که عموم این مجرمان جوان یا حتی نوجوان هستند (شیرزاد، ۱۳۸۸، ۹۲) همچنین محمود زاده ۱۳۹۱ در تحقیق خود نشان داد که بیشترین میزان ارتباط میان انگیزه انتقام‌جویی و جرم هتک حرمت و حیثیت است. همچنین رابطه میان انگیزه ترویج بی‌بندوباری و جرم علیه عفت و اخلاق عمومی زیاد بود.

همچنین با توجه به آنکه گسترش شبکه‌های اجتماعی مجازی باعث به هم خوردن مناسبات و روابط اجتماعی افراد شده است. ازجمله ویژگی‌های اساسی این شبکه‌های اجتماعی مجازی گمنامی، ویژگی‌های انعطاف‌پذیری هویت، عدم وجود نیروهای کنترل و قدرت متمرکز و آزادی بی‌حدوحصر می‌باشد. این شبکه فرصت‌های جدید را برای افراد خلق می‌کند که می‌توانند باانگیزه‌ها و اهداف متفاوت از آن استفاده کند؛ این انگیزه‌ها و اهداف گاهی در راستا هنجارهای جامعه است و گاهی محل مناسب برای انواع نابهنجاری‌ها و جرائم می‌باشد و بر همین اساس شناخت انگیزه‌های کاربران شبکه‌های اجتماعی از نوع جرم ارتکابی ضروری می‌نماید (محمود زاده، ۱۳۹۱). در این راستا هدف اصلی این تحقیق مطالعه بررسی انگیزه‌های اصلی بزه کاران در فضای سایبری است. بر اساس نتایج کوره‌پز،۱۳۹۳ طبقه‌بندی‌هایی که از بزهکاران سایبری ارائه‌شده است نشان می‌دهند که بزهکاران سایبری برخلاف تصور رایج برخی جرم‌شناسان، گروهی همگن و متجانس نیستند. به بیانی دیگر، اساساً هر گزاره‌ای که ویژگیِ خاصی را به‌تمامی بزهکاران سایبری تعمیم دهد، عوامانه و فاقد پشتوانه 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 و انگیزه‌های متفاوتی نیز دارند، وجود دارد.

۲- ادبیات تحقیق

۲-۱- انگیزه‌های بزه‌کاران سایبری

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) باوجود تعاریف گوناگونی که از انگیزه ارائه‌شده است، 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. 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 (کاتوزیان ۱۳۸۶، ۱۴۲)

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، ۸۰) اگرچه در حقوق کیفری جز در موارد استثنائی به انگیزه توجه نمی‌شود، اما برعکس این عنصر در علت شناسیِ جرم و پیشگیری از بزهکاری بسیار حائز اهمیت است زیرا جرم‌شناسان و سیاست‌گذاران همواره به دنبال آن‌اند تا از گذرِ انحراف در فرآیند گذارِ اندیشه به عمل (پویایی یا دینامیک جنایی) زمینه تحقق فرصت‌های ارتکاب جرم را خنثی سازند و از آماج آسیب‌پذیر محافظت نماید (پیشگیری وضعی) یا در پیشگیری اجتماعی به‌ویژه پیشگیری رشد مدار با از بین بردن انگیزه‌های مجرمانه، فرد را از ارتکاب جرم در آینده بازدارند (منفرد و جلالی فراهانی، ۱۳۹۱).

در حال حاضر نیز با تحول در مفهومِ حالت خطرناک و پیدایش یک سیاست جناییِ امنیت مدار، شاهد آن هستیم که انگیزه در گفتمان نوینِ سیاست‌گذاری جنایی همچنان کانون توجه است (نجفی ابرندآبادی، ۱۳۹۲؛ ۲۳-۲۷)؛ اما افزون بر آنچه در بالا بدان اشاره شد، در 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 انگیزه خود را یکی از چهار مورد زیر بیان کرده‌اند. انتقام‌جویی، مالی، شهرت و کنجکاوی (راجر، ۲۰۱۰؛ ۲۲۱).

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 باانگیزه جنسی به ارتکاب جرم برانگیخته می‌شوند. به‌هرحال بدون پشتوانه آماری قطعی، سخن گفتن از این فراوانی دشوار است 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 جرائم سایبری، انگیزه‌های بزهکاران سایبری را به‌گونه‌ای طبقه‌بندی کرد که با یکدیگر همپوشانی نداشته باشند، آن‌ها عبارت‌اند از:

۱. پاسخ به گرایش‌های درونی: کنجکاوی- لذت طلبی

یکی از اولین روانشناسانی که پیرامون ابعاد لذت طلبیِ انسان‌ها مطالعه کرد، بیان نمود: برخی از رفتارها به خاطر لذت حاصل از انجام آن‌ها، صورت می‌گیرند (کستری، ۲۰۱۰، ۲۲)؛ بنابراین انسان‌ها همواره سعی دارند در فعالیت‌هایی مباشرت کنند که بتواند حس لذت طلبی و 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 امنیت سنجیِ 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. بر اساس آمار سازمان ملی جوانان، بیش از ۴۴ درصد کاربران ایرانی باهدف تفریح و سرگرمی وارد فضای مجازی می‌شوند (حاجیلی، ۱۳۸۸، ۱۲۸). مثال‌های فوق نشان می‌دهند که ممکن است افراد با سطحِ مهارت‌های گوناگون به دنبال سرگرمی و کنجکاوی باشند. در این راستا یک هکر ۱۹ ساله سربازِ ارتشِ اسرائیلی 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 (گلدسمیدت، ۲۰۱۱، ۴۵).

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 رنج می‌برند، نسبت به سایرین می‌توان با برنامه‌های آموزش محور و یا با کاربست تدابیر وضعی- به‌ویژه با جاذبه زدایی- تا حد زیادی فراوانیِ رفتار آنان را تقلیل داد.

۲. طمع‌ورزی و کسب منافع مالی

با وابستگی فزاینده روابط تجاری میان مردم- دولت به ارتباطات از راه دور و شکل‌گیری دولت الکترونیک جرائم مالیِ سایبری وارد مرحله نوینی شده است؛ 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. هزینه پایین ارتکاب جرم، کثرت بزه دیدگان و بالطبع عواید بالا نه‌تنها بزهکاران سایبری بلکه دیگران را نیز به این عرصه گسیل داشته است. در سال ۲۰۰۸، ٪۷۸ درصد 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 قراردادند و این بخش نیز اکثر شناسه/هویت‌ها را به سبب رخنه در داده‌ها ازدست‌داده بود. به همین منوال، در سال ۲۰۰۸، ۱۲ درصد 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 (جهان خانی و نمرات، ۲۰۱۱ :۸۵) در همین زمینه، مدیرکل طرح و برنامه سازمان قضایی نیروهای مسلح کل کشور بیان می‌دارد که ۸۱ درصد از جرائم سایبری باانگیزه مالی رخ می‌دهند. از رایج‌ترین جرائم که باانگیزه 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 درصد از جرائمی که سامانه‌ها و رایانه‌های یک سازمان/شرکت را هدف قرار می‌دهند، از سوی کارمندانِ خودی صورت می‌گیرند (تیلور و همکاران، ۲۰۰۵). یکی دیگر از جرائمی که باانگیزه انتقام‌جویی روی می‌دهد، تعقیب ایذائی است. تعقیب ایذائی رفتاری است که فرد با استفاده از ارتباطات از راه دور به آزار و اذیت دیگری می‌پردازد. (پیتارو:۱۳۹۲) انگیزه اصلی بزهکاران از تعقیب بزه دیده 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 سوءاستفاده گر یا حتی شوهر سابق را به انتقام از زن خود تحریک کند (هالدر و جیشنکار،۱۳۹۳). مثال زیر نمونه 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 (هالدر و جیشنکار،۱۳۹۳). مزاحمت سایبری و تجاوز به عنف سایبری از دیگر جرائمی است که می‌تواند باانگیزه 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 بزه دیده 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. 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.

فضای سایبری 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 متخلفانه محتوای 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،۲۸۵:۱۳۸۸) افزون بر هرزه‌نگاری، از دیگر جرائم مرسومی که باانگیزه جنسی روی می‌دهند می‌توان به سیاحت‌گری جنسی 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 چرخه بزهکاری مباشرت دارند تا بتوانند نیازهای جنسیِ خود را در این فضا برآورده سازند. چنانکه گروه‌های دیگری نظیر آزارگر- آزار پذیر 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 پیگیری اهداف جنسی به‌عنوان انگیزه ثانویه آنان، تلقی شود.

۵. باورهای ایدئولوژیک

اگرچه به نظر برخی نویسندگان، انگیزه سیاسی هیچ‌گاه انگیزه ابتدایی و اولیه نیست (راجرز ۲۰۱۰) 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 می‌تواند (الادین، ۲۰۱۳) 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 جرائم به‌واسطه تنفر از یک گروه نژادی- جنسی یا یک اندیشه سیاسی- مذهبیِ معارض صورت می‌گیرد. درواقع این جرائم، گونه سایبری جرائم مبتنی بر نفرت[1] 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 انگیزه مشددِ لحاظ نشده است.

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 مروجین این باورها حمله کنند. باید اشاره کرد که اگرچه این جرائم به‌مانند جرائم کلاسیک اغلب همراه با خشونت می‌باشند، اما برخلاف نظر برخی نویسندگان (منفرد، ۱۳۹۱) باید گفت انگیزه اولیه 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.

.شکل زیر 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).

شکل زیر انگیزه مجرمین سایبری در ایران پس‌ازآنکه داده‌های مربوط به نیمرخ جناییِ محکومین پیشین گردآوری شد، باید از آن‌ها در تحلیل رویداد مجرمانه و درنهایت در طراحیِ 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، نه‌تنها این اطلاعات ارزشی ندارند بلکه می‌توانند گمراه‌کننده نیز باشند. در مرحله تحلیل داده‌ها این مأمورینِ تحقیقِ واحد جرائم رایانه‌ای می‌باشند که بیش از هر متخصصین دیگری می‌توانند با پردازش داده‌ها، برونداد/خروجی مناسب و مفیدی را از آن‌ها به دست آورند؛ زیرا این امر تنها از سوی مأمورینِ تحقیقِ زبده یا کسانی که به‌اصطلاح دارای شمِّ پلیسی‌اند، برمی‌آید. در تأیید این نکته، سخنگوی واحد ملیِ جرم فناوری پیشرفته انگلستان بیان می‌دارد: این کار نسبتاً راحتی است که مأموران خوبی انتخاب و به آن‌ها در امور فناوری‌های رایانه 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) بااین‌حال، در این مرحله نیز مأمورین پلیس از مشاوره با متخصصین علوم رایانه مستغنی نمی‌باشند.

[1] Hate Crime

در مرحله تحلیل داده‌ها، افزون بر نگرشی عمیق به نیمرخ‌های بزهکارانِ بزه‌های مشابه، مأمورین تحقیق باید به بررسی و تحلیل داده‌ها و رفتارهای مرتکب درصحنه جرم نیز توجه ویژه‌ای داشته باشند؛ زیرا اگرچه گونه‌های مختلفی از نیمرخ سازی 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 صحنه جرم که شامل شیوه، مکان، زمان ارتکاب، ملاحظات بزه دیده شناختی و غیره است- سرنخ‌های مهم گردآوری می‌گردند. سپس این داده‌ها با وضعیت بزهکارانِ جرائم مشابه پیشین- ویژگی‌های جمعیت شناختی- روانی مقایسه می‌شوند. سرانجام کارآگاهان و مأمورین تحقیق با تلفیق این دودسته اطلاعات با یکدیگر، از آن‌ها به‌منظور شناساییِ بزهکاران بهره‌برداری می‌کنند.

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 مهم‌اند، از تحلیل خود کنار گذارند؛ زیرا گاه همین ملاحظات جزئی می‌توانند مفید واقع شوند. دیگر تدابیر و اقداماتی که مأمورین تحقیقِ جرائم سایبری مکلف به رعایت آن می‌باشند تا حد زیادی به‌مانند دیگر جرائم است که به جهت پرهیز از اطاله کلام از آن صرف‌نظر می‌شود.

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 بزه دیده شناختی که از صحنه جرم به دست می‌آیند، توجه به این امر که در موارد پیشینی این دسته بزهکاران چه ویژگی‌های جمعیت شناختی - 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 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 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 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 جرائم کلاسیک و سایبری، توجه به صحنه جرم و داده‌های مرتبط با آن، یک اقدام ابتدایی و ضروری به شمار می‌رفت. پس کمینه وجه تمایزِ فن نیمرخ جنایی با دیگر روش‌های تحقیقی، در گنجاندن چنین ویژگی‌هایی در اقدامات تحقیقی است.

۲-۲- تدابیر پیشگیرانه

در عصر نوین اطلاعات، نیاز جوامع انسانی به رایانه و اینترنت افزایش‌یافته است. در این راستا با افزایش فراگیر شدن استفاده از رایانه جرائم مربوط به آن نیز افزایش‌یافته است این موضوع به افراد فرصت‌طلب و تبهکار اجازه می‌دهد تا مقاصد شوم خود را در فضای سایبری که به دلیل نامحدود بودن و احتمال کم ردگیری آن‌ها، دنبال کنند. از همین رو حقوقدانان و جرم شناسان می‌بایست تمام تلاش خود را به کار بگیرند تا بتوانند با افزایش آگاهی در رابطه با مسائل حقوقی فضای سایبر به قانون‌گذاران کشورها و جوامع بین‌المللی کمک کرده تا به امنیت این دنیای مجازی کمک کنند. همچنین 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. از دیرباز کاربست تدابیر پیشگیرانه با موانع و محدودیت‌های متعدّدی مواجه بوده است. این چالش‌ها در فضای سایبر نیز وجود دارند و با توجه به ماهیت این فضا، برخی از چالش‌های پیشین

پیشگیری موقعیت مدار در فضای سایبر تحقق می‌یابند و برخی دیگر غیرقابل تحقق‌اند و همچنین، دسته‌ای از چالش‌های نوین در این فضا ایجاد گردیده‌اند. در بحث تحقق سالم‌سازی فضای مجازی و علی‌الخصوص شبکه‌های اجتماعی مجازی که خود مفهومی چندبعدی است و اصولاً به معنای عاری سازی فضای سایبر از لوث ناهنجاری‌های منحرفانه و مجرمانه تعریف می‌شود، باید به ابعاد مختلف مسئله نظر داشت. بخشی از اقدامات به‌منظور تأکید بر جنبه‌های مثبت کاربری از این فناوری نوین بر روی «ساماندهی» متمرکز می‌شوند؛ تا درنهایت منافع حاصل از توسعه این فناوری از معایب آن پیشی گرفته و زمینه ارتکاب ناهنجاری‌ها را به حداقل برساند. بااین‌حال، نباید رکن «سزادهی» را برای آن دسته از افرادی که تدابیر پیشگیرانه بر آن‌ها تأثیرگذار نبوده فراموش کرد. هرچند به دلیل ملاحظات جدی ناظر به این تدابیر، به‌ویژه در پرتوی موازین حقوق بشری و همچنین هزینه سنگینی که در اثر پیگرد عاملان جرائم ارتکابی در فضای سایبر بر دولت‌ها تحمیل می‌شود، تأکید و اولویت اصلی باید بر روی تدابیر پیشگیرانه باشد.

۶- بحث و نتیجه‌گیری

نتیجه 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.

در تمام مراحل کاربست تدابیر پیشگیرانه، همواره باید پایبندی به موازین حقوق بشری مدنظر قرار گیرد وسعی در رعایت توازن میان منافع افراد و جامعه شود. ویژگی‌های موجود در محیط سایبر همچون حذف بعد مکان، سرعت ارتکاب جرم در این فضا، عدم حضور فیزیکی مرتکب جرم و ناشناختگی بزه و بزهکار و مواردی ازاین‌دست نیز پیشگیری از جرائم سایبری را با مشکلات فراوانی مواجه می‌نمایند. از طرفی دیگر، اقدامات خنثی‌کننده مجرمین سایبری، تدابیر فنی موقعیت مدار را در مقام عمل با نارسایی‌های متعددی مواجه کرده است. با توجه به این مباحث می‌توان گفت که کارایی تدابیر موقعیت مدار در فضای سایبر نسبی می‌باشد و در کنار این تدابیر باید از تدابیر پیشگیرانه اجتماعی و کیفری استفاده گردد.

منابع

۶. پیتارو، میشل (۱۳۹۲)، مزاحمت سایبری: گونه شناسی، علت شناسی و بزه یده شناسی، ترجمه: لمیاء رستمی تبریزی، سودابه رضوانی و مرضیه السادات آقا میرسلیم، در: دایرۀ المعارف علوم جنایی (مجموعه مقاله‌های تازه‌های علوم جنایی)، کتاب دوم، زیر نظر: علی حسین نجفی ابرندآبادی، تهران: میزان.

۷. جوکز، یونی. ۱۳۸۹. جرم و اینترنت، مرتضی حاجعلی فرد، اصحاب حبیب زاده، سونا احمدی، رسول نجارباغسیاه. نشر دانشگاه علوم انتظامی. تهران.

۸. چابک پور، مهدی. ۱۳۹۳. نقش محیط سایبر در وقوع جرائم. پایان‌نامه کارشناسی ارشد، دانشگاه آزاد اسلامی - دانشگاه آزاد اسلامی واحد تهران مرکزی، دانشکده حقوق و علوم سیاسی.

۹. حاجیلی، محمود (۱۳۸۸)، وضعیت فناوری ارتباطات در حوزه جوانان، تهران: دبیرخانه شورای عالی اطلاع رسانی.

۱۰. رحیمی، زهره. ۱۳۹۳. سیاست جنایی ایران در قبال جرائم و تخلفات شبکه‌های اجتماعی مجازی. پایان نامه کارشناسی ارشد، دانشگاه فردوسی مشهد - دانشکده علوم اقتصادی.

۱۱. زینالی، امیرحمزه (۱۳۸۸)، حمایت کیفری از کودکان در برابر هرزه نگاری 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.

۱۲. شیرزاد، کامران. ۱۳۸۸. جرائم رایانه‌ای از دیدگاه حقوق جزای ایارن و حقوق بین الملل، چاپ اول، تهران. نشر بهینه فراگیر.

۱۳. کاتوزیان، ناصر (۱۳۸۶)، حقوق مدنی (اعمال حقوقی، قرارداد ایقاع)، دوره مقدماتی، تهران: انتشارات سهامی انتشار.

۱۴. کی‌نیا، مهدی (۱۳۸۶)، مبانی جرم‌شناسی، جلد اول، تهران: انتشارات دانشگاه تهران.

۱۵. محمدکوره پز، حسین (۱۳۹۳)، نیمرخ جنایی بزهکاران سایبری، پایان نامه دوره کارشناسی ارشد، پردیس فارابی دانشگاه تهران، دانشکده حقوق، حقوق کیفری و جرم‌شناسی.

۱۶. محمودزاده، سودابه، ۱۳۹۱. مطالعه جامعه شناختی انگیزه افراد و نوع جرم ارتکابی در شبکه اجتماعی فیس بوک (با بررسی پرونده‌های تشکیل شده در دادگاه جرائم سایبری). پایان‌نامه. کارشناسی ارشد. دانشگاه الزهرا.

۱۷. منفرد، محبوبه (۱۳۹۱)، «بررسی جرم شناختی بزهکاری رایانه‌ای»، فصلنامه مطالعات پیشگیری از جرم، (۲۵)،۷۶-۴۷.

۱۸. منفرد، محبوبه؛ جلالی فراهانی، امیرحسین (۱۳۹۱)، «کدهای رفتاری و پیشگیری از بزهکاری»، پژوهشنامه حقوق کیفری. (۶): ۱۳۴-۱۰۵.

۱۹. منفرد، محبوبه. ۱۳۹۱. پیشگیری از جرائم رایانه‌ای از گذر کدهای رفتاری رایانه‌ای. پایان‌نامه کارشناسی ارشد. موسسه آموزش عالی غیرانتفاعی و غیردولتی شهید اشرفی.

۲۰. ناصرآبادی، سید پاشا (۱۳۹۱)، سخنرانی در: سمینار آموزشی پیشگیری از سرقت اطلاعات رایانهای.

۲۱. 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.

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

۲۳. هالدر، دباراتی؛ جیشنکار، جی (۱۳۹۳)، جرم رایانه‌ای و بزه دیدگی زنان: قانون‌ها، حق‌ها و مقرره‌ها، ترجمه: مهرداد رایجیان اصلی، حسین محمدکوره پز و احسان سلیمی، تهران: مجد.

24. Goldschmidt, Orly Turgeman (2011). Identity Construction among Hackers, In: Jaishankar, K. (Ed), Cyber Criminology: Exploring Internet Crimes and Criminal Behavior. Boca Raton: CRC Press.
25. 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.

26. 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.
27. Matsumoto, David. (2009). the Cambridge Dictionary of Psychology, New York: Cambridge University Press.
28. Nykodym, Nick, Taylor, Robert and Vilela, Julia (2005). Criminal profiling and insider cyber crime. Computer Law & Security Report, (21), 261-267.
29. 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.
30. 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.
31. Shinder, Debra Littlejohn. (2002). Scene of the Cybercrime: Computer Forensics Handbook, Rockland: Syngress Publishing.

مطالعات علوم سیاسی، حقوق و فقه

دوره ۳، شماره ۱/۳، بهار ۱۳۹۶، صفحات ۱۳۶- ۱۲۶

Examining Main Motivations of Criminals in Cyberspace

Jalal Shirmohammadi

MA Criminal Law and Criminology, Islamic Azad University, Ardabil

Abstract

With its unique advantages, information and communication technology has also provided a wide range of criminal opportunities. This situation caused a "public crime" in cyberspace, so that in addition to individuals with pure criminal motives, many of cyberspace users also engage in delinquent behaviors. The motives and objectives are sometimes in direction with norms of the society and sometimes, a perfect place for all types of aberrations and crimes. In this regard, the present research, which studies the issue in a descriptive-analytical method, discusses motivations of criminals using five components: responding to internal trends; curiosity-pleasure; greed and gaining financial interests; revenge; sexual motives and ideological beliefs.

Keywords: Motivations of Crime, Cyberspace, Cyberspace Criminals, Social Networks