فصلنامه علوم خبری
سال نهم، شماره ۳۵ پاییز ۱۳۹۹
صفحات ۲۳۰-۱۹۳

La revue science de I'information
année 9 / No 35 Tombe 2020
pages: 193-230

علت شناسی ارتکاب جرایم سایبری و سازوکارهای پیشگیری از آن

امین امیریان فارسانی[۱]
راضیه عبدالصمدی
فاطمه حیدری فارسانی[۲]

چکیده

قانون جرایم رایانه‌ای سرانجام پس از فراز و نشیب‌های فراوان در سال ۱۳۸۸ تصویب و به ترتیب اجرا نهاده شد و دست به جرم انگاری رفتارهای مجرمانه که به تاسی از کنوانسیون جرایم رایانه‌ای اتخاذ شـــده بود پرداخت. این قانون به عنوان یک قانون نوین و نوپا تحلیل و بررسی حقوقی از جنبه‌ها و صور مختلف را می‌طلبید از این رو بررسی‌های کیفری از جنبه‌ها و منظرهای مختلف در خصوص جرایم رایانه‌ای از زمان تصویب تا حال حاضر صورت گرفته اســـت اما آن چه مورد کنکاش و پژوهش قرار نگرفت و از منظر پژوهشـــگران مغفول مانده بررسی علت شناسانه جرایم رایانه‌ای است. نگاه علت‌شناسانه به پدیده‌ی جنایی، بر شناخت ما از ســـبب‌های پدیدآورنده‌ی آن می‌افزاید. به ویژه، عرصـــه‌های ناشـــناخته یا نوشـــناخته‌ی اجتماعی که هنجارهای نوینی را نیز به همراه آورده‌اند. نمونه‌ی بارز قابل اشـــاره در دنیای امروز، جهان فناوری اطلاعات و ارتباطات ا ست که همانند جهان خاکی، از بزه و بزهکاری در امان نمانده اســـت. این مباحث به جرم‌شـــناســـان کمک می‌کند تا با توجه به شـــرایط و ویژگی‌های فضای سایبر، راهکارهای منا سبی را برای سالم سازی آن پیشنهاد دهند. عوامل فردی و محیطی، چه در دنیای فیزیکی و چه در دنیای ســـایبر، نقش تعیین کننده‌ای در پیـ شبرد فرایند جنایی و بزهکاری ایفا می‌کنند. برخی ویژگی‌های فردی بزهکاران رایانه‌ای به

[۱] استادیار، دانشکده حقوق و الهیات، دانشگاه شهید اشرفی اصفهانی، اصفهان (نویسنده مسئول)
amirian.amin@yahoo.com
[۲] کارشناسی ارشد حقوق جزا و جرم شناسی. aminamirian13@yahoo.com

تاریخ دریافت: ۱۳۹۹/۰۹/۲۰ تاریخ پذیرش: ۱۳۹۹/۱۲/۱۰

آن‌ها در پیشبرد اهداف شومشان کمک می‌کند. همچنین خود فضای سایبر نیز ویژگی‌ها و بسترهای جرم‌خیزی دارد که انگیزه‌های جنایی مرتکبان بالقوه را تحقق می‌بخشد.

واژگان کلیدی: جرم شـــناختی، قانون جرائم رایانه‌ای، فضـــای مجازی، جرم رایانه‌ای، بزهکار، بزه دیده

مقدمه

پیدایش فضای مجازی در چند دهه‌ی اخیر یکی از بزرگ‌ترین نمادهای تحول جهانی است. رخدادی که تأثیرات شگرف آن هر روز در ابعاد فرهنگی، اجتماعی، اقتصادی، سیاسی، امنیتی و دفاعی در عرصه‌ی ملی و بین‌المللی نمود بیشتری پیدا می‌کند. هرگونه تغییر و تحول در دنیای کنونی به دلیل پیچیدگی فعالیت‌های انسانی، خواه ناخواه آثار و پیامدهایی به همراه خواهد داشت. به گونه‌ای که با اختراع وسیله‌ای جدید، در کنار استفاده ی صحیح و مشروع از آن، همواره امکان سوءاستفاده از آن‌ها وجود دارد. در این راستا علم حقوق، به عنوان حامی عدالت و موجد توازن در جامعه انسانی، هر آنچه را که کوچک‌ترین خدشه‌ای به این توازن وارد نماید، تحت پوشش قرار داده و سعی در رفع یا پیشگیری از آثار نامطلوب آن می‌نماید. فضای سایبر، که ماحصل پیشرفت‌های علمی و صنعتی در قرون اخیر است، از این قاعده مستثنی نبوده و آثاری به صورت مثبت و منفی در زندگی بشر وارد نموده است که ضرورت مطالعه آن را انکارناپذیر می‌نمایاند

جرم رایانه‌ای جرمی است وارداتی که با ورود کامپیوتر در استفاده از اینترنت در سطح گسترده در کشور رواج پیدا کرده است ورود اینترنت به کشور از سال ۱۳۷۰ و آغاز شد و در سال ۱۳۷۲ به تکامل رسد اما در این چند سال نبود قانونی مدون باعث گردید که بسیاری از مجرمین رایانه‌ای از زیر مجازات فرار کنند و به جرائم خود ادامه دهند و استناد آن‌ها نیز به اصل برائت واصل قانونی بودن جرم و مجازات بود که استناد درستی هم بود با تصویب قانون جرائم رایانه‌ای (۱۳۸۸)، مفاهیم و جرائم تازه‌ای در حقوق کیفری ایران خلق شد که هریک نیازمند بررسی‌های دقیق و کارشناسانه می‌باشد وقتی در خصوص فناوری بحث می‌شود، نمی‌توان رایانه را نادیده گرفت. رایانه هم خود بزرگ‌ترین فناوری عصر حاضر است و هم سایر فناوری‌های نوین یا به و سیله آن و یا بر بستر آن شکل می‌گیرند البته فناوری‌ها در کنار مزایای خود می‌توانند بسترساز سوءاستفاده‌هایی نیز باشند. به خصوص اگر این فناوری، رایانه باشد، دامنه خطرهای آن افزایش می یابد. حقوق کیفری نوین، امروزه با جرائم و مجرمان رایانه‌ای باشد، دامنه خطرهای آن افزایش می یابد. حقوق کیفری نوین،

امروزه با جرائم و مجرمان رایانه‌ای طرف است. ماهیت و ویژگی این دسته از جرائم به نحوی ا سا سی با جرائم سنتی تفاوت دارد. امروزه، مجرمان رایانه‌ای در مکان‌هایی به غیر از نقاطی که آثار و نتایج اعمال آن‌ها ظاهر می‌شـــود، قرار دارند. در صـــورتی که کارایی قوانین جزایی موجود و متداول، منحصر به قلمرو خاصی است و به دلیل آنکه اجزای عنصـــر مادی کاملاً یا بعضـــاً تغییر یافته و برخی عناوین مجرمانه تازه هم به وجود آمده است، نمی‌توان مجرمان را با قوانین قبلی محاکمه کرد.

فضـــای ســـایبر یا به عبارتی فضـــای مجازی محدودیت‌های زمانی، جغرافیایی و فضایی که بشر امروز با آن در ستیز است را از بین خواهد برد. امکانات عصر مجازی در مقایســـه با عالم واقع بســـیار زیاد اســـت، به عنوان مثال، اقتصـــاد مجازی، تجارت مجازی، بانکداری مجازی، آموزش مجازی، دولت مجازی، ادارات مجازی، شـــرکت‌های مجازی، پول مجازی و خدمات و تفریحات مجازی بخشی از آن‌ها می‌باشند. با توسعه و تحول اینترنت و پیشرفت علم الکترونیک، در مقابل انقلاب عظیمی در ایجاد جرائم در سطح بین‌المللی به وجود آمده است. لذا در بیشتر کشورهای دنیا جرائم اینترنتی به‌عنوان یک معضل حاد و بسیار مهم تلقی می‌گردد و دولت‌ها درصدد پیدا نمودن راه حل‌های مختلفی در جهت جلوگیری از وقوع آن می‌باشـــند. در حال حاضـــر جرائم سایبر با اشکال مختلفی صورت می‌پذیرد که مجرمین محیط سایبر شامل هکرها، کرکرها، فریک های تلفن و انواع جرم های ممکن با نام ســـایبرکرایم آن را انجام می‌دهند.

جرم‌شناسی قانون جرایم رایانه‌ای به مطالعه عوامل ایجاد جرم در فضای مجازی و تأثیرات آن بر دنیای حقیقی و راهکار های پیشـــگیری از حدوث این‌گونه جرائم می‌باشـــد. مطالعات عینی پرونده‌های جرائم رایانه‌ای نشـــان می‌دهد ایجاد شـــخصـــیت جرائم فضای مجازی با ذهنیت عدم شناسایی و البته سهولت و گستردگی ارتکاب برخی بزه‌ها در این فضا بستر مناسبی را برای بروز خلأهای شخصیتی و روانی فراهم می سازد لذا ما بر این باور هستیم که شخصیت واقعی یک بزهکار رایانه‌ای را باید در همان شخصیت مجازی وی جستجو کرد به دیگر سخن شخصیت مجازی که بزهکار رایانه‌ای از خود ساخته است در واقع همان (خود واقعی) اوست که به دلایل مختلف

امکان بروز آن در دنیای حقیقی را نداشته است . این پژوهش با گرداوری اطلاعات با روش کتابخانه‌ای و روش تجزیه و تحلیل اطلاعات به صورت توصیفی و تحلیلی به بررسی علل مؤثر بر جرایم سایبری می‌پردازد

۱- عوامل مؤثر بر ارتکاب جرائم رایانه‌ای

۱-۱- عوامل فردی مهیاکننده‌ی بزهکاری رایانه‌ای

عوامل فردی مهیاکننده‌ی بزهکاری به عواملی گفته می‌شود که آمادگی لازم برای ارتکاب بزه را در فرد فراهم کرده و وی را برای ارتکاب رفتار مجرمانه آماده می‌کنند که به همین دلیل می‌توان از آن‌ها به عوامل توانا ساز یاد کرد. به طورکلی، این عوامل در پهنه‌ی رایانه‌ای در دو گروه انگیزه‌ها و دانش و تخصص جای می‌گیرند. در گفتار یکم، طیف گسترده انگیزه‌های فردی بزهکاری رایانه‌ای شناسایی شده‌اند. گفتار بعدی نیز به بررسی نقش دانش و تخصص در جرائم رایانه‌ای اختصاص یافته است.

۱-۱-۱- سن

سن یک عامل جرم‌زای فردی گذرا و انتقالی است. این عامل در حقوق کیفری به منظور تمییز سن مسئولیت کیفری و در جرم شناسی و بزه دیده شناسی ازلحاظ تفکیک بزهکاری اطفال و بزرگسالان، مورد توجه قرار می‌گیرد. از منظر جرم‌شناسی، یافته‌های تحقیقاتی نشان می‌دهند که در هر رده سنی، گونه‌ای از بزهکاری یا بزه دیدگی در میانِ افراد آن طبقه وجود دارد. برای نمونه در دوران طفولیت، کودکان ممکن است بزه دیده‌ی جرایمی چون تکدیگری (در این موارد فرد بزهکار - بزه دیده است)، ترک نفقه، آدم ربایی و غیره شوند. چنانکه وندالیسم یا خرابکاری در بین نوجوانان و جوانان شایع‌ترین جرم است و موارد معدودی از وندالیسمِ میانسالان و سالمندان گزارش شده است یا برعکس، برخی جرائم مختص افرادی است که در طبقه سنی بالایی قرار دارند. بارزترین نمونه از چنین بزهکارانی، مجرمین یقه سفید هستند (قورچی بیگی، ۱۳۹۲، ص۳۲)؛ اما به‌عنوان یک قاعده کلی باید گفت که میان بزهکاری و سن (حداقل در فراوانی) رابطه‌ی معکوسی وجود دارد؛ به گونه‌ای که با افزایش سن، بزهکاری کاهش می‌یابد.

بررسی ۱۶۵ پرونده جرم رایانه‌ای در تایوان نیز نشان می‌دهد که بیشترین جرائم 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 جرائم را مرتکب شده‌اند (Liao and Tasi 2006: 54).

البته نباید پنداشت که کل جرائم رایانه‌ای را نوجوانان و جوانان مرتکب می شوند. بر اساس اعلام بخش جرائم رایانه‌ای و مالکیت معنوی وزارت دادگستری ایالات متحده[3]، ۳۴ درصد از مجرمین درون سازمانی[4] 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[5] با ۶۰ سال سن متهم به سرقت 3 میلیون دلار، تیموتی آلن لوید[6] ۳۹ ساله متهم به بیش از ۱۰ میلیون دلار و کوین میتنیک[7] ۳۷ ساله متهم به بیش از ۱ میلیون دلار وارد شده است (Nykodym, Taylor and Vilela 2005).

همچنین با توجه به بررسیِ بخش مذکور پیرامون سارقین سایبری، مشاهده می‌شود که الگوی معناداری در میانِ سن آنان وجود دارد. اگر سرقت کمتر از صد هزار دلار باشد، به احتمال زیاد مهاجم ۲۰ تا ۲۵ ساله است و هنوز در رده پایین سلسله‌مراتب سازمان قرار دارد.

اگر ارزش جرم بین صد هزار تا یک میلیون دلار باشد، مرتکب جرم به احتمال زیاد بین ۲۵ تا ۳۵ سال و مرد است و چنانچه جرم بیش از یک میلیون دلار باشد، مهاجم بالای ۳۵ سال سن داشته و جزو کادر مدیریتی است (Nykodym, Taylor and Vilela 2005). بنابراین به استثنای برخی جرائم (تروریست‌های سایبری، جاسوس‌های رایانه‌ای و نفوذ کارمندان که یا از متخصصین امنیت شبکه

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

هستند یا بدین منظور شیوه‌های ارتکاب را به طور 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 میان سال و سالمند، نه‌تنها ارتکاب جرم رایانه‌ای برای آنان بسیار دشوار بلکه حتی گاه انجام کارهای شخصی آن‌ها با کمک سایرین صورت می‌گیرد[۸]. پس می‌توان گفت جوامعی که هرم سنیِ آن‌ها در قاعده کم‌عرض‌تر است (جوامع به‌اصطلاح پیر) نرخ جرم رایانه‌ای کمتری دارند. با پذیرش این استدلال باید گفت، دریکی دو دهه آینده بزهکاری افراد میانسال نیز شایع‌تر خواهد بود.

۲-۱-۱- 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 جرائم فاصله‌ی ارقام بزهکاری مردان با زنان زیاد است (رستمی تبریزی ۱۳۸۸). به گونه‌ای که در سال ۲۰۰۹ اداره تحقیقات فدرال امریکا گزارش داد که از ۳۰ میلیون متهم دستگیرشده، ۷۵ درصد مرد و تنها ۲۵ در صد آن‌ها زن می‌باشند و ۸۱ در صد جرائم 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، ص ۲۱۴).

ورای توجیهات زیست شناختی (کی نیا ۱۳۸۶: ۱۶۵-۱۵۶ و وفایی ۱۳۷۸) و جامعه شناختی (رستمی تبریزی ۱۳۸۸) که پیرامون بزهکاری زنان انجام شده است، باید گفت رویکرد پلیس و برخورد دستگاه عدالت کیفری با بزهکاران زن نیز متفاوت

---

۸ مارکوس رجرز و همکاران وی نیز در دو پیمایشِ خود گزارشی (Self Report) دریافتند که در ارتباط با جرائم مرتبط بانفوذ و دسترسی غیرمجاز (هک)، افراد 30-17 سال بیشترین کسانی هستند که در این رفتار منحرفانه /مجرمانه رایانه ای مباشرت دارند.

از مردان اســت و بخشــی از این نابرابری آماری می‌تواند ناشــی از نگاه مســامحه‌گرِ دستگاه عدالت کیفری به جنسیت زنان باشد.

وضــعیت بالا تا حد زیادی در ارتباط با جرائم رایانه‌ای نیز صــادق اســت. برخی پژوهش‌ها بیانگر وجود رابطه‌ی مســتقیم میان جنســیت کاربران و میزان مراجعه به سایت‌های هرزه نگاری است. بر اساس یافته‌های پژوهشی با عنوان «مواجهه با تصاویر هرزه نگارانه در اینترنت میان کودکان و بزرگسالان»، ۸۲ درصد سایت‌های هرزه‌نگاری را مردان جوان و تنها ۵ درصــد از آن‌ها را زنان تشــکیل می‌دهند (نگهی ۱۳۹۱). از بررسی ۴۵ محکوم هرزه نگاری که در بالا اشاره شد نیز ۸۴/۴ درصد مجرمان مردان و ۱۵/۶ درصد را زنان تشکیل داده‌اند

۳-۱-۱- 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 برنامه نویسی و نیز به طور تخصصی از امنیت رایانه‌ها و سامانه‌ها آشنایی دارند. شاید بتوان این دیدگاه را در ارتباط با جرائم رایانه‌ای که در دهه های گذشــته روی می‌داد، با اغماض پذیریم. زمانی که دانش‌آموختگان دانشگاه ام.آی.تی[9] بامهارت و تخصص دانشگاهیِ خود به برنامه‌نویسی و ویروس نگاری‌های پیشــرفته اقدام می‌نمودند و جز خود آن‌ها، کســی توان مقابله با آن‌ها را نداشت (Shinder 2002: 138)؛ اما امروزه با پیشرفت‌های سخت‌افزاری و نرم‌افزاری رایانه‌ای و نیز پیدایش اینترنت، بزهکاران رایانه‌ای به‌راحتی یک اشــاره بر موشواره می‌توانند آنچه را پیش‌تر به‌دشواری انجام می‌شد را عملی سازند.

اما تصــورِ رایجِ نادرســت‌تر آن اســت که ســطح مهارت فنی[10] تمامیِ بزهکاران سایبری، همگن و متجانس انگاشته شود. یافته‌های یک پژوهش نشان می‌دهد که از مجموع ۲۳۹ نفر مورد مطالعه،۲۱ درصــد مهارت فنیِ پایین، ۲۲ درصــد مهارت بالا، ۲۴ در صد متخصص و ۳۲ در صد توان فنی متوسط دارند (Chiesa 2009: 45).

9 Massachusetts Institute of Technology (MIT)
10 Technical Skills

درواقع، اگرچه هنوز برخی شیوه‌های ارتکاب[11] نظیر حملات ممانعت از سرویس‌دهی توزیعی[12] در گستره سایبر به جهت ایمن بودن سامانه‌ها و شبکه‌ها نیازمند مهارت‌های عالیِ رایانه‌ای است، اما امروزه بیشتر جرائم رایانه‌ای با[13] حداقل مهارت و تلاش روی می‌دهند. در این زمینه می‌توان به مهارت حداقلی ریزه خواران اشاره نمود. حتی در حملاتی که از پیچیدگیِ زیادی برخوردارند، افراد می‌توانند با مشورت پیرامون مشکل خود در شبکه اجتماعی هکرها یا با خرید نرم افزارهای خودکار و از پیش طراحی شده‌ی نفوذ، نسبت به آن اقدام کند. از روش‌های جدید جبرانِ خلأ ندا شتن مهارت لازم می‌توان به اجیر کردن نوجوانان به‌منظور طراحی حمله و برنامه‌نویسی اشاره کرد که به نوعی می‌توان آن را شکل جدیدی از «کودکانِ کار[14]» دانست (Jahankhani and Al-Nemrat 2010).

با توضیحات بالا می‌توان به این پرسش که «آیا سطح هوش بزهکاران رایانه‌ای نسبت به سایر بزهکاران بیشتر است؟» نیز پاسخ داد؛ زیرا این کلیشه در ذهن ما رخنه کرده که «چون هکرها (ما بزهکاران رایانه‌ای 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 به عبارتی توانایی استدلال، تجزیه‌وتحلیل و فکر منطقی، اثربخشیِ حمله را تضمین می‌کند، اما آن دسته از بزهکارانی که از نرم‌افزارهای تألیفی دیگران یا برنامه‌های نفوذ بارگیری شد[15] بهره می‌برند، لزوماً نباید ضریب هوش[16] بالایی داشته باشند. بااین‌وجود، پاسخ شفاف‌تر به این پرسش نیازمند ارزیابی‌های دقیق‌تر و مطالعات بیشتری است.

۴-۱-۱- سطح تحصیلات

---

1 Modus Operandi
2 Distributed Denial of Service (DDoS)
3 Script Kiddies
4 Child Labor
5 Download
6 Intelligence Quotient (IQ)

مطالعات گوناگون نشـان می‌دهد که رابطه معکوسـی میان سـطح تحصـیلات 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 فرضـیه حتمی و غیرقابل رد نیسـت؛ زیرا اگرچه سـطح سـواد یک جامعه می‌تواند شـاخصـی برای توسـعه‌یافتگی یک کشـور تلقی شـود، اما ضـرورتاً کاهش بزهکاری را به دنبال ندارد. حتی با لحاظ عواملی نظیر توسـعه‌ی شـهرنشـینی، 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 سـطح سـواد جوامع، نه‌تنها بزهکاری کاهش نیافته بلکه در اَشـکال 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 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 نقیصـه‌ای، نباید نرخ کاهش جرم تا این اندازه ناچیز باشـد (مظلومان، ۱۳۵۴، ص۳۵). باید گفت موضـوع مطالعه اکثر این پژوهش‌ها جرائم خشـن یا مبتنی بر زور می‌باشند. لذا حداقل دستاورد این یافته‌ها آن است که سطح سواد با بزهکاری خشن رابطه معکوس دارد و نمی‌توان آن را به‌تمامی اَشکال جرائم تسری داد.

یک پیمایشِ خود گزارشی در میان دانشجویانِ سال اول تا سال چهارم در کانادا نشـان داد که ۸۸ درصـد شـرکت کنندگان در رفتارهای مجرمانه‌ی رایانه‌ای نظیر اسـتفاده از رمز عبور دیگران بدون اجازه آن‌ها، تغییر و جسـتجو در فایل‌های دیگران بدون اجازه آن‌ها، اسـتفاده از ویروس‌های تألیفی یا ویروس نگاری به‌منظور اعمال خرابکارانه و به دسـت آوردن رمز کارت اعتباری دیگران و غیره مباشـرت داشـته‌اند (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 رایانه‌ای دخالت دارند و ازآن‌رو که بیشتر افراد در این سنین مشغول تحصیل در دانشگاه‌ها یا دانش آموخته می‌باشند، پس می‌توان نتیجه گرفت که افراد دانشجو یا تحصیل کرده بیش از اقشار دیگر می‌توانند به‌عنوان بزهکار رایانه‌ای شناخته شوند.

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

البته با ملاحظه‌ی 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).

شاید دلیل اصلی این مشابهت، عدم لحاظ شرایط محدودکننده در جامعه آماری باشد؛ چراکه در مطالعه‌ی نخست، پژوهشگران جامعه آماری خود را تنها معطوف به دانشجویان نمودند. البته باید اشاره کرد که جرائم مورد بررسی مطالعه‌ی نخست در زمره جرائم رایانه‌ای محض می‌باشند و این جرائم نسبت به سایر جرائم سایبری، به دانش و مهارت بیشتری نیاز دارند. لذا بدیهی است که معمولاً افراد تحصیل‌کرده‌تر این جرائم را مرتکب می شوند. 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 رایانه‌ای نیز همگن نیست. برای نمونه پژوهشی که پنج سال به طول انجامید، نشان می‌دهد بزهکاران رایانه‌ای به مانند سایر بزهکارانی که به سایر جرائم نظیر ضرب‌وجرح و برگلری محکوم شده‌اند، از سطح تحصیلاتیِ متفاوتی برخوردار می‌باشند (Durost 2006: 5-6). از سوی دیگر باید اذعان داشت در جرائم رایانه‌ای به دلیل آنچه در بالا آمد، اغلب افراد تحصیل کرده بیش از سایرین دست به ارتکاب جرم می‌زنند.

۵-۱-۱- پیشینه خانوادگی و زمینه‌های شغلی

تصور رایج ما از خانواده‌ای که یک بزهکار رایانه‌ای هکر در دامان آن پرورش یافته، خانواده‌ای محروم و سطح پایین است که پدر و مادر هیچ نظارتی بر فرزند خود ندارند، پدر و مادر از هم جدا شده یا طلاق گرفته‌اند یا به دلیل مشکلات روانی یا رفتاری به طور مداوم در حال مشاجره با یکدیگر می‌باشند. گاه فرزند مدت طولانی از آغوش پر مهر یکی از والدین محروم می‌شود و یا به جهت الکل بارگی و دیگر رفتارهای انحرافیِ والدین، کودک در دوران رشد خود دچار اختلال می‌گردد. پس به طورکلی، هکرها به مانند بیشتر بزهکاران در دوران کودکی و نوجوانی از سوی والدین خود حمایت عاطفی و مورد مراقبت نبوده‌اند. از این رو، معمولاً هکرها به خاطر شخصیت ضد اجتماعی و درون‌گرای[۱۷] 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 از دست رفته خود را بازیابند و به عبارتی به‌تمامی آنچه در دنیای خاکی از آن محروم بوده‌اند، دست یابند.

اما باید اشاره کرد که همواره وضعیت این گونه نیست. حتی در مواردی به جهت پیوند عمیقی که میان والدین و فرزند وجود دارد، کودک رفتار انحرافی را از والدین می‌آموزد. برای نمونه در یک پرونده، کودکی سه‌ساله توانست تحت آموزش و تشویق

---

17. Introversion

پدر و مادر خود با اجرای عملیات حملات ممانعت از سرویس‌دهی[۱۸] به داده‌های رایانه‌ای دیگر، دسترسی یابد (Chiesa, Ducci and Ciappi 2009: 93-94).

همانطور که در بالا اشاره شد بزهکاران رایانه‌ای ممکن است از هر قشری باشند و محصور کردن آن‌ها به افرادی خاص، نادرست است. وضعیت اشتغال بزهکاران رایانه‌ای نیز از این حال خارج نیست. درواقع، برخلاف آنچه تصور می شود، بزهکاری رایانه‌ای منصرف به افراد بی کار و فاقد درآمد نیست. برای نمونه طبق آمار پلیس فتا تنها ۶/۱ درصد متهمین جرائم رایانه‌ای 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 در صد بیکار و بقیه مشغول به کار در سازمان‌های دولتی یا شرکت‌های خصوصی می‌باشند. شگفت‌آور اینکه حتی در چهار مورد، بزهکاران رایانه‌ای از استادان دانشگاه بودند (Liao and Tasi 2006: 54).

۶-۱-۱- پیشینه مجرمانه

یکی از برجسته‌ترین شاخص‌های سنجشِ خطرناکی در مطالعات جرم شناختی، سابقه‌دار بودن یا به عبارتی «تکرار بزهکاری» است. بررسی این عامل ازاین‌جهت مهم است که می‌تواند اساس سیاست گذاری‌های 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 سلبِ توان 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 جرائم خیابانی برعکس بزهکاران یقه سفید اغلب دارای سابقه مجرمانه هستند. از طرف دیگر، پژوهشی پیرامون جرائم یقه سفید نشان داد که هیچ‌یک از افراد تحت بررسی پیش‌تر دست به ارتکاب جرم نزده‌اند (قورچیبیگی ۱۳۹۲)؛ اما آیا به واقع گروه اخیر خطرناک‌تر هستند؟

---

18 Denial of Service (DoS)

مطالعه‌ای که پیرامون بزهکاران رایانه‌ای 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 هرزه نگاری، سرقت جزئی، قمار و غیره محکوم‌شده بودند (Liao and Tasi 2006: 54). در مطالعه دیگری که به مقایسه ویژگی‌های جمعیت شناختی-اجتماعی بزهکاران رایانه‌ای 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

۲-۱- عوامل محیطی مهیاکننده‌ی بزهکاری رایانه‌ای

فضای سایبر، به ویژه اینترنت به‌عنوان جلوه بارز جامعه‌ی اطلاعاتی، در کنار شرایط ایده آلی که برای تبادل اطلاعات و انجام امور تجاری، اقتصادی و آموزشی فراهم آورده، ویژگی‌های محیطی منحصر به فردی دارد که سوءاستفاده‌های فعالان این عرصه را نیز به همراه داشته است. کما اینکه برخی ویژگی‌های این فضا موجبات بزه دیدگی افراد آسیب‌پذیرتر را فراهم می‌کند. در این مبحث، آن دسته از ویژگی‌های شاخص این فضا که نقش تعیین کننده‌ای در پیشبرد اهداف جنایی بزهکاران بالقوه دارند، بررسی می‌شوند. در رابطه با ویژگی‌های محیطی مهیاکننده‌ی بزهکاری رایانه‌ای، از یک‌سو می‌توان به مجازی‌انگاری فضای سایبر و به‌تبع آن امکان به‌کارگیری هویت‌های دروغین و چندگانه و از سوی دیگر، دسترس‌پذیری آسان‌تر آماج‌های مجرمانه که از یکجانشینی همه‌ی امور خرد و کلان زندگی اجتماعی در فضای سایبر ناشی می‌شود، اشاره کرد.

۱-۲-۱- مجازی انگاری فضای سایبر

از همان بدو پیدایش فضای سایبر، حتی از زبان پدیدآورندگان آن به گوش می‌رسید که این فضا ماهیت مجازی دارد و در واقع آن را در برابر دنیای فیزیکی قرار

می‌دادند که از آن به‌عنوان دنیای واقعی نام می‌بردند. همین امر باعث شـــده فعالان این فضـــا با تلقی مجازی بودن آن ســـعی کنند آنچه را که در رؤیاها و تخیلات خود جســـتجو می‌کردند در این فضـــا پیاده کنند. منطق پردازی‌هایی مانند اینا «فقط حرفه!»، یک شگرد زبانی خنثی سازی است که تقریباً دستاورد فرعی ماهیت ناپایدار اینترنت و وابســـتگی متنی آن برای برقراری ارتباطات به شـــمار می‌آید. ممکن اســـت مرتکب، احساس گناه را در خود از بین ببرد و وجود بزه دیده را با منطق پردازی‌هایی مانند «آن‌ها واقعاً اینجا نیستند» و «این کارها واقعی نیست»، نادیده بگیرد.

آن دسته از افرادی که تصمیم می‌گیرند تا خطر آزار دادن دیگران در اجتماع‌های برخط را بپذیرند، می‌توانند برای خود، فاصـــله‌ی مکانی با طرف‌های گفتگویشـــان را یادآور شـــوند و به همین ترتیب، خود را از پاســـخگویی و خودکنترلی برهانند. این در حالی است که با توجه به میزان گمنامی اعطا شده به مرتکب، امکان تلافی از سوی طرف مقابل ناچیز است. بیشتر کاربران شبکه‌ای پندارشان از فضای سایبر فقط یک سری تصاویر و اعداد و ارقام است که در نمایشگر دیده می‌شوند، غافل از اینکه همه‌ی فعل و انفعالاتی که انجام می‌شود، کاملاً اثر و بازتاب واقعی دارند و در زندگی فیزیکی آن‌ها اثر مستقیم می‌گذارد. این وضعیت به معضل دیگری تحت عنوان بی‌هنجاری یا خلأ هنجاری[۱۹] نیز منجر می‌شـــود. ممکن اســـت اعضـــای اجتماع برخط حس کنند که حفظ ارزش‌های اجتماع مجازی و احترام به مقررات آن تأثیری در زندگی واقعی آن‌ها نداشـــته و این وضـــعیت ناپایدار به آن‌ها آمادگی ذهنی می‌دهد تا «تعطیلات اخلاقی»[۲۰] داشـــته باشـــند و باورهایشـــان در برابر هنجارها، ارزش‌ها و مقررات اجتماعی برخط سست شود

مجازی انگاشتن فضای سایبر به‌نوبه‌ی خود پیامد ناگوار دیگری را برای جامعه‌ی اطلاعاتی و البته دســـتاوردهایی برای اعضـــای بداندیش آن به همراه داشـــته اســـت. از جمله‌ی مهم‌ترین پیامدهای قابل ذکر، گمنام انگاری رایانه‌ای اســـت؛ به این معنا که عضـــو جامعه‌ی اطلاعاتی با پوشـــیده و پنهان داشـــتن هویت واقعی خود از گذر

19 Anomie
20 Moral Holiday

به کارگیری هویت دروغین یا ربودن هویت دیگران، می‌کوشد انگیزه‌های جنایی خویش را تحقق بخشد. در تعریف واژگانی، منظور از گمنامی یا ناشناختگی هویت به‌طور ساده «بدون نام بودن» یا «نام دروغین داشتن» است (کابای، ۱۹۹۸: ۷). در زبان عرفی، گمنام به شخصی اطلاق می‌شود که هویت معتبری نداشته باشد یا هویت وی قابل احراز و انتساب به وی نباشد. گمنامی ارتباط تنگاتنگ و مستقیمی با مفهوم «معرفی»[۲۱] و «تأیید»[۲۲] دارد. معرفی فرایندی است که در پی آن فرد با ارائه‌ی اطلاعات شخصی، خودش را به دیگران می‌شناساند و انتظار دارد به‌عنوان عضوی از اجتماع تأیید و پذیرفته شود. هرچه میزان پذیرش افراد اجتماع گسترش یابد، گمنامی کمرنگ‌تر خواهد شد. (بینام، ۲۰۰۴: ۱۱). به دیگر سخن، پذیرش اجتماعی افراد برای خارج شدنشان از گمنامی کافی است و تأیید آن صرفاً برای اعطای حقوق تکالیف قانونی و اجتماعی است. پس، «هویت فردی»[۲۳] پنداشت نسبتاً پایدار فرد از کیستی چیستی خود، در ارتباط با افراد و سایر گروه‌هاست که از طریق تعاملات اجتماعی با دیگران در فرایند اجتماعی شدن تکوین می‌یابد (ذکایی و خطیبی، ۱۳۸۵: ۱۶۷).

حال در دنیای سایبر، هنگامی‌که ما برای برقراری تعاملات اجتماعی، ارتباطات الکترونیکی را به خدمت می‌گیریم، هویت دقیقا به چه معناست؟ یکی از تفاوت‌های بارز شناسایی هویت در دنیای فیزیکی و رایانه‌ای این است که در دنیای فیزیکی، هویت افراد یا بر پایه‌ی روابط چهره به چهره و بر اساس شخصیت ظاهری و رفتاری فرد از سوی دیگران پذیرفته می‌شود و یا بر پایه‌ی سوابق و اطلاعات ثبت‌شده‌ی رسمی تعریف می‌شود، حال آن که در فضای سایبر به دلیل حذف ماهیت فیزیکی و مکانی موجود در دنیای خاکی، اصل بر گمنام ماندن هویت است و هویت همان چیزی است که خود فرد اعلام می‌کند که به دلیل نبود ارتباط رو در رو و حضور فیزیکی، هرلحظه باید خود را ثابت کند. رایانامه، تارنما، وبلاگ و به‌طور پیشرفته‌تر،

21 Identification
22 Authentication
23 Self-identify

امضای دیجیتال[24] شناسه‌هایی هستند که افراد برای اثبات هویت‌شان در دنیای رایانه‌ای به کار می‌گیرند.

با این حال، ناشناس ماندن هویت جزء لاینفک فضای سایبر است که انجام همه‌ی فعالیت های را یا نه‌ای و بالأخص شبکه‌ای در خلوت[25] امکان پذیر می‌سازد. پنهان سازی یا جعل هویت، که یکی از پیش شرط‌های سوءاستفاده‌های موفقیت‌آمیز تلقی می شود و به سختی در دنیای فیزیکی امکان‌پذیر است، در فضای سایبر، تقریباً به آسانی از عهده‌ی هرکسی ساخته است. همین ویژگی باعث می‌شود شخص به سرعت و بدون مشاهده کسی یا حتی بهتر از آن، بی‌آنکه کسی بتواند به حریمش متعرض شود، هر کاری که می‌خواهد انجام دهد. شرایط روانی خلوت، عدمِ احساس خطر نسبت به آسیب دیدن شخصیت اجتماعی به علت عدمِ حضور در جامعه و ویژگی ناشناسی، یک حس تحریک، غلیان احساسی و فقدان مسئولیت منجر به ولنگاری در شخص پدید می‌آورد که موجب کاهش محدودیت‌های درونی و فقدان علقه‌های اجتماعی یا «خودارجمندی» می‌شود (حسنی، ۱۳۸۸: ۱۷۵).

حضور در فضای مجازی همراه با ویژگی‌های خاص آن، مانند گمنامی و حذف نشانه‌های فیزیکی به کاربر اجازه می‌دهد چهره یا شخصیتی کاملاً متفاوت از دنیای فیزیکی بروز دهد. کاربران به همان دلایلی که در بالا بیان شد، در دنیای بیرون به آسانی تمایلات نفسانی و مجرمانه‌شان را بروز نمی‌دهند و می‌کوشند نزد همگان به‌عنوان یک چهره معتبر و واجد احترام شناخته شوند. اما زمانی که در خلوت خود پای رایانه می‌نشینند و به دنیای شبکه‌ها وارد می‌شوند، انواع تمایلات مجرمانه در آن‌ها بیدار می شود. فضای سایبر این امکان را فراهم آورده که در خصوصی‌ترین و ایمن‌ترین مکان، زمینه‌های ارتکاب شدیدترین جرائم فراهم شود. برای نمونه می‌توان به شخصی اشاره کرد که مربی برجسته‌ی آموزشگاهی بوده و در طول زندگی‌اش هیچ خطایی از او سر نزده، اما از آنجا که توانسته در فضای سایبر با یک شخصیت متفاوت ظاهر شود و به‌زعم خود شخصیت واقعی‌اش را از دیدگان افراد بپوشاند، تمایلات

---

24 Digital Sign
25 Privacy

آزارگری یا آزاربینی جنسی‌اش بیدار شده و تا آنجا پیش رفته که در دنیای فیزیکی منجر به مرگش شده است (جلالی فراهانی: ۱۳۸۴: ۷۱).

در تحقیقات تجربی جرم شناختی نیز ثابت شده که میزان رفتار مجرمانه‌ی انسان‌ها در فضای سایبر، به مراتب بالاتر از میزان چنین رفتارهایی در دنیای واقعی است. در یک تحقیق تجربی در دانشگاه لستر انگلستان نشان داده شد که در خوشبینانه‌ترین حالت، ۳۰ درصد کاربران اینترنتی که با قصد انجام کارهای قانونی وارد یک سایت شده‌اند، در مواجهه با آماج‌های غیرقانونی مرتکب جرم می شوند. اگر آن دسته از افرادی هک صرفاً برای ارتکاب جرم در این فضا وارد می شوند را هم به این آمار بیفزاییم، نتایج وحشتناک و غیرقابل باوری به دست می‌آید. جرم‌شناسان در بیان علل این تفاوت فاحش دلایل مختلفی بیان می‌کنند هک عمدتاً مبتنی بر «گمنامی» و نیز «رهاپنداری یا ولنگاری» است. امروزه کار با اینترنت دقتای چنین ویژگی های روانی و فیزیکی را به‌صورت تحریک آمیزی فراهم می‌کند. مجرمان و خرابکاران رایانه‌ای برای ارتکاب رفتارهای متجاوزانه در نترنت، ای عمدتاً از القاب، شناسه‌های به سرقت رفته و آدرس‌های IP تقلبی یا عاریتی و دیگر ابزارهای متقلبانه استفاده می‌کنند. آن‌ها به دلیل ندیدن فوری آثار و نتایج رفتار تجاوزکارانه‌شان راحت‌تر مرتکب جرم می‌شوند (حسنی، ۱۳۸۸: ۱۷۶).

با این حال، باید یادآور شد که این ویژگی به خودی خود ناپسند به شمار نمی‌آید. حتی در دنیای فیزیکی نیز گمنامی لزوماً به‌عنوان یک مؤلفه‌ی محرک ارتکاب جرم محسوب نمی‌شود. در دنیای فیزیکی اصل بر ناپسند بودن گمنامی است، مگر در جایی که قانون‌گذار در مقام استثنا مجاز شمرده باشد. برای نمونه، در برخی مواقع، افراد بنا بر موقعیت‌های شغلی اجازه می‌یابند نام‌های مستعار به کار ببرند یا در بحث حمایت از شاهدان، یکی از اصول دادرسی منصفانه که در برخی از کنوانسیون‌های بین‌المللی نیز به آن اشاره شده است، ناشناخته ماندن شاهدان برای حمایت هرچه بیشتر از آن‌هاست. اهمیت گمنامی گاه به حدی است که نقطه‌ی مقابل آن به‌عنوان یک سازوکار سزاده و ترهیبی به کار می‌رود. مجازات «تشهیر» از جمله مجازات‌های پذیرفته شده در نظام کیفری اسلام است که به معنای معرفی مجرم به افراد جامعه و

اعلان جرم او به همگان است که در جدیدترین نمونه‌ی آن می‌توان به قانون «تشهیر نام مفسدان اقتصادی» مصوب ۱۳۸۵ اشاره کرد.

به همین ترتیب، در دنیای سایبر نیز نمی‌توان به موضوع گمنامی صرفاً نگاه انتقادی و غیرقابل پذیرش داشت. اگر از نگاه بزه دیدگان بالقوه به گمنامی در دنیای سایبر بنگریم، ناشناس ماندن هویت موجب می‌شود آن‌ها هنگام قرار گرفتن در محیط‌های پرخطر، کمتر در معرض سوءاستفاده‌های احتمالی قرار بگیرند. همانگونه که در دنیای فیزیکی برخی از افراد بنا بر شرایط و دلایلی اجازه پیدا می‌کنند که هویت خود را برملا نکنند و از مزیت گمنامی برخوردار باشند، در دنیای سایبر نیز گمنامی برای عده‌ای ضروری انگاشته می شود. بر همین اساس در برخی از کدهای رفتاری که برای حمایت از برخی گروه‌های آسیب‌پذیر و در معرض خطر مانند زنان و کودکان پیش‌بینی شده، توصیه شده است که از به‌کارگیری شناسه‌هایی که دربردارنده‌ی اطلاعاتی درباره‌ی هویت واقعی‌شان است، خودداری کنند و نام و نام خانوادگی‌شان را در رایانامه یا نام‌های کاربری‌شان بکار نبرند

۲-۲-۱- دسترس‌پذیری آماج‌های گوناگون رایانه‌ای

در دنیای فیزیکی، آماج‌های جنایی معمولاً در نقطه‌های جداگانه‌ای متمرکز و از هم تفکیک شده‌اند. برای نمونه، برای سرقت از هر بانکی به دلیل موقعیت مکانی خاص و جداگانه‌ی آن، بزهکار شیوه‌ی خاصی را تعریف می‌کند یا کلاه برداری از یک مؤسسه آموزشی آماج جداگانه‌ای محسوب می شود. قاعدتاً بزهکار برای هدف قرار دادن هریک از اختیارات به منظور جلب منفعت برای خود یا دیگری، جرائم گمرکی، جرائم مالیاتی، قاچاق کالا و ارز و به طور کلی جرم علیه حقوق مالی دولت، به دستور دادگاه صادرکننده رأی قطعی، خلاصه متن حکم شامل مشخصات فرد، سمت یا عنوان، جرائم ارتکابی و نوع و میزان مجازات محکوم علیه به هزینه وی در یکی از روزنامه‌های کثیرالانتشار و عنداللزوم یکی از روزنامه‌های محلی منتشر و در اختیار سایر رسانه‌های عمومی گذاشته می‌شود. مشروط به آنکه ارزش عواید حاصل از جرم ارتکابی یکصد میلیون ریال یا بیشتر از آن باشد.

این آماج‌ها، یک شـــیوه ارتکاب[۲۶] خاص طراحی خواهد کرد و نمی‌تواند با یک روش به همه‌ی این آماج‌ها دسترسی داشته باشد.

در دنیای ســـایبر این معادله دگرگون شـــده اســـت. مجرمان همه‌ی آنچه را می‌خواستند، اکنون در یکجا می‌بینند: امنیت ملی، اموال عمومی و خصوصی، حیثیت و حتی در مواردی جان افراد تبدلی به ارقامِ صـــفر و یک شـــده و در تمام جهان در د سترس دیگران قرار گرفته ا ست (ح سنی، ۱۳۸۸: ۱۷۳). پس از گذ شت یک سوم قرن، بشر با پیشرفت‌های فنی و فناورانه‌ی پدیدهای نوظهور شگفت‌زده شد. پیدایش و گســترش رایانه‌های شــخصــی و برقراری ارتباطات ســریع دیجیتالی، تلفیق فناوری اطلا عات (ای تی) با فـناوری ارتـبا طات (ای ســـی تی) رونق تلفن های همراه، شبکه‌های رایانه‌ای پرسرعت و صنعت محتوای دیجیتالی، اینترنت و خدمات وب، همه و همه م ستقیماً «کارکردهای رایانه‌ای» و آبـشاری از اطلاعات را در د سترس کاربران قرار داده‌اند.

هنگامی‌که در دهه‌ی ۱۹۸۰ ایده‌ی جامعه‌ی اطلاعاتی شکل گرفت، اندیـشه‌ی در دســترس قرار دادن اطلاعات درباره‌ی امور اداری و جاری کشــور یا به عبارت کلی‌تر خدمات عمومی،[۲۷] به یکی از محورها و ارکان اصـــلی جامعه‌ی اطلاعاتی تبدیل شـــد. امروزه افراد بدون مراجعه به نهادهای دولتی یا خصــوصــی و پشــت ســر گذاشــتن مشکلات بسیار، می‌توانند از طریق سامانه‌های رایانه‌ای و اتصال به سایت‌های مربوط، در یک بستر واحد، همه‌ی امور و نیازمندی‌های اجتماعی‌شان را برآورده سازند.

با پدیداری دولت‌های الکترونیکی[۲۸] و پایگاه‌های متمرکز داده‌های شـــخصـــی، این فناوری به شــکلی گســترش یافته که تمام داده‌های یک شــخص از لحظه‌ی تولد تا مرگ، در فـضای سایبر، ثبت و قابل د سترس می شود (همان). واژه‌هایی مانند دولت

---

26 Modus Operandi
27 Public Services
28 E-government

دیجیتالی،[29] دولت الکترونیکی، دولت برخط[30] دولت مجازی[31] به کار می‌روند تا میزان و پیچیدگی به کارگیری فناوری های ارتباطاتی و اطلاعاتی در دولت و فرایندهای راهبردی نشان داده شود.

پس، با یکجانشینی همه‌ی امور در دنیای سایبر، آرمان‌شهری برای بزهکاران رایانه‌ای فراهم آمده تا در یک محیط واحد به هر نوع آماج مجرمانه‌ای دسترسی داشته باشند. در جهان خاکی، امور گوناگون، مکان‌های ویژه‌ی خود را دارند و هیچ‌گاه امور اداری، آموزشی، سرگرمی، تجاری، اقتصادی، پولی و بانکی و فرهنگی در یک مکان گرد هم نمی‌آیند و برای همه‌ی آن ها یک ابزار یا روش کاربری پیش‌بینی نمی‌شود، نه به این دلیل که چنین اراده‌ای وجود ندارد، بلکه این کار امکان‌پذیر نیست. اما در جهان سایبر، به لطف ویژگی مجازی سازی امور جاری در دنیای خاکی، همه چیز در کنار یکدیگر قرار گرفته‌اند و جالب‌تر آن که تنها با در اختیار داشتن یک ابزار و کارکردهای رایانه‌ای تقریباً مشابه، امور همگی بسامان می‌شود. این دسترس‌پذیری، نقطه‌ی مقابل زبان زدی است که می‌گوید: «تخم‌مرغ‌هایت را در یک سبد نگذار». در پروژه‌ی «کارت هوشمند چندمنظوره‌ی ملی» در سال ۱۳۸۳، مقامات دولتی با توجه به تکالیف قانون برنامه‌ی چهارم توسعه‌ی کشور مبنی بر به‌کارگیری فناوری اطلاعات و ارتباطات برای بهبود کمی و کیفی ارائه‌ی خدمات به شهروندان و فراهم ساختن زمینه‌های اجرای قانون تجارت الکترونیکی به فکر تدوین سند کارت هوشمند چند منظوره‌ی ملی افتادند. هدف از به‌کارگیری چنین کارتی به‌عنوان یکی از زیرساخت‌های اطلاعاتی در کنار مراکز داده و شبکه‌های ارتباطی برای ارائه‌ی خدمات الکترونیکی یک پارچه، این بود که یکی از ضرورت‌ها و الزامات پیاده‌سازی طرح دولت الکترونیک تحقق یابد و جایگزین انواع کارت‌های هوشمند، مانند کارت سوخت، کارت‌های اعتباری بانک‌ها، کارت‌های هوشمند اداری، کارت‌های تلفن، کارت‌های هوشمند دانشجویی و... شود و در واقع همه این کارت‌ها در کارت هوشمند

29. Digital Government
30. Online Government
31. Virtual Government

ملی ادغام شـــود تا بدین ترتیب مردم از انبوه کارت‌هایی که این روزها هر ســـازمانی درصدد طراحی و ترویج آن است، خلاصی یابند.

این وضـــعیت، شـــرایط ایده آلی را برای مرتکبان بالقوه فراهم می‌کند تا در یک محیط به همه‌ی آماج‌های مجرمانه‌شـان دسـترسـی داشـته باشـند. چنانچه دارنده‌ی کارت آن را گم کند، بزهکار تنها با دا شتن یک نرم‌افزار مربوط به شکستن رمز عبور می‌تواند به تمام اطلاعات و دارایی‌های الکترونیکی شـخص دسـت یابد. این وضـعیت موجب آ سیب‌پذیری صاحب کارت از جنبه‌های گوناگون می شود و د ست‌آویزی برای یابنده خواهد بود تا با دسترسی به طیف گسترده‌ای از اطلاعات و دارایی‌های ارزشمند شخص، با انگیزه‌های گوناگون اعم از مالی، انتقام‌جویی یا سرگرمی از فرد سوءاستفاده کند.

با این حال، دسـترس‌پذیری سـریع و آسـان به انواع اطلاعات و خدمات در دنیای سایبر، به خودی خود زیان‌بار تلقی نمی شود. این ویژگی هنگامی یک عامل محیطی مهیاکننده‌ی بزهکاری به شمار می‌آید و فضای سایبر را به یک مدینه‌ی فا ضله برای بزهکاران تبدیل می‌کند که بدون پیش‌بینی تدابیر امنیتی مربوط به حفاظت از داده‌ها و کاربران، همه‌ی امور خرد و کلان زندگی‌مان را به این دنیا منتقل کنیم، بی‌آنکه با پیش‌بینی تدابیری مانند ام ضاهای الکترونیکی و دیگر ا شکال کدگذاری‌ها و م سدود کردن داده‌ها، حفاظت هرچه بیشـتر دارایی‌هایمان را در دنیای سـایبر تضـمین کرده باشیم.

درحالی‌که فناوری‌های اطلاعات و ارتباطات امکان ایجاد اقتصـــادهای جهانی و شـبکه‌های دانشـی مشـروع و انواع فعالیت‌های بهره‌ورانه‌تر را فراهم می‌آورند، به روی تاریک‌تر نیز اجازه می‌دهند تا کاربری نامشـــروع از شـــبکه‌های اطلاعات را نظاره‌گر باشند. بزهکاری رایانه‌ای، جلوه‌ی تاریک فضایی است که از آن به‌عنوان خانه‌ی جدید ذهن یاد شده است. گروه‌های جنایتکار سازمان‌یافته که پیش‌تر در سطح ملی فعالیت می‌کردند، اکنون می‌توانند شـــبکه‌های جهانی را برای گســـترش ســـوداگری‌های نامشـــروعشـــان به کار گیرند. فناوری اطلاعات به گروه‌های جنایتکار امکان داده تا با ســـایر بزهکاران در ســـراســـر جهان به‌منظور قاچاق کارآمدتر کالاهای غیرقانونی و به

شکل گمنام با یکدیگر بر هم کنش داشته باشند و بزه دیدگان بالقوه را با یک کلیک شناسایی کنند.

۳-۱- پیشگیری از جرایم رایانه‌ای و مصادیق آن

امروزه فناوری اطلاعات باعث شـــده که انســـان امروزی در دنیای جدیدی به نام فضای سایبر قرار دارد که ویژگی‌های آن از دنیای فیزیکی متمایز است، و گسترش رو به رشد فضای سایبر با توجه به ناشناخته بودن بسیاری از اجزای آن برای عامه مردم به عاملی برای افزایش فرصت‌های جنایی بدل گشته است این ویژگی توسط مجرمان سایبری مورد سوء استفاده قرار گرفته و سبب شکل‌گیری جرایم سایبری شده است. همواره پیشـگیری و ارائه راهکارهای غیر کیفری مؤثر و سـودمند از مبارزه و مجازات اســت بی تردید مؤثرترین راهکار پیشـگیری از وقوع جرایم سـایبری اطلاع رسـانی صحیح و ارائه برنامه‌های متنوع آموزشی و تربیتی و نهادهای متولی این امر است که بتوانند به اتخاذ راهکارهای منطقی و واقع گرایانه اقدام کنند. لذا به بررســـی انواع پیشگیری در خصوص جرایم سایبری پرداخته می‌شود

۱-۳-۱- پیشگیری کیفری از جرائم رایانه‌ای

در هر مکتب و منطقی این امر پذیرفته شـده اسـت که همواره پیشـگیری بهتر از درمان و مقدم بر آن است. برخورد با جرائم و مجازات عامل جرم در واقع نوعی درمان و تسکین آلام مجنی علیه و خسارات وارده بر جامعه است. عرف نیز بر این امر قائل اســـت که علاج واقعه را قبل از وقوع باید کرد. احتراز روحی و روانی آدمی از وقوع خطرات احتمالی بیانگر آن است که «اصل تقدم پیشگیری بر درمان» ریشه در فطرت و سرشت آدمی دارد. در قرآن نیز ذکر کردن تقوی به عنوان یکی از موارد ضروری و مورد تأکید قرآن به عنوان راهی برای پیشگیری از وقوع جرم تلقی می‌شود.

امروزه با وجود هزینه های بالای برخورد با مجرمان و مجازات آن ها - چه هزینه های زندان، اعم از امکانات نیروی انســـانی مورد نیاز، مکان آن و ... و چه هزینه‌های تعقیب و مورد پیگرد قرار دادن مجرمان - شـــاید چندین برابر هزینه‌ای باشد که برای پیشگیری از وقوع جرم می‌شود. آن چه که بیشتر جالب توجه است این که حتی بعد از برخورد با مجرمان و مجازات آن‌ها با وجود هزینه‌های بســـیار زیاد،

غالب اوقات نه تنها نتیجه مطلوب بدست نمی‌آید بلکه به دلیل اجرای نادرست مجازات و فضای جرم‌زای زندان نتیجه این همه هزینه وارد کردن فرد متهم و یا مجرم در بین مجرمان سابقه‌دار و در نتیجه تعدد و تکرار جرم می‌گردد. در حالی که اگر از همان اول از وقوع جرم پیشگیری می‌شد این نتایج منفی را در پی نداشت.

گاهی اوقات برچسب زنی به فردی که مجرم نیست آمادگی بیشتری را برای ارتکاب جرم بعد از ورود دوباره فرد به جامعه در او ایجاد می‌کند؛ زیرا با این برچسب‌ها این فرد همه آنچه را که داشته از دست داده و بازگشت دوباره او به جامعه کار بسیار مشکلی خواهد بود؛ چرا که اقدامات اصلاحی و تأمینی و تربیتی همیشه نتیجه مطلوب خود را ندارد. پس این همه هزینه می‌شود؛ اما اصلاح و بازپروری؛ غیرقطعی خواهد بود. پس پیشگیری آسان‌تر از اصلاح یا مجازات است. پیشگیری از وقوع جرم باعث سالم ماندن فضای اجتماعی و فرهنگی جامعه و تأمین امنیت آن می‌شود و نقش سازنده‌تری را ایفا می‌کند. ارتکاب هر جرم، آثار و تبعات زیانباری را برای مجرم و جامعه در برداشته و لطمات زیادی را هم بر شخص مجرم و هم بر اعضای جامعه وارد می‌کند و مجازات هر چند که بتواند مجرم را متنبه سازد و جنبه ارعاب و عبرت پذیری داشته باشد؛ و به هیچ وجه نمی‌تواند آثار زیان‌بار آن را جبران کند و فرصت‌ها و حرمت‌های از دست رفته را باز یابد و مجرم و جامعه را به جایگاه قبل از وقوع جرم بازگرداند. این امر حتی در مورد مجنی علیه هم می‌تواند صادق باشد.

ما در برابر ارتکاب یک جرم دو دسته و حتی سه دسته قربانی داریم. یک قربانی، جامعه است که به لحاظ اجتماعی، ذهنی، امنیتی و اقتصادی لطمه می‌خورد و قربانی دیگر شخص مجنی علیه است که به طور اخص و ملموس مورد جرم واقع می شود و قربانی مستقیم جرم است. دسته سوم قربانیان، بستگان، آشنایان و به خصوص خانواده جانی یا مجرم هستند که بنا بر جایگاه مشخص مجرم به آن‌ها نیز خسارات مادی و معنوی وارد می‌گردد. چه شخص مجنی علیه و چه خانواده جانی یا مجرم در اثر ارتکاب جرم خساراتی را متحمل می‌شوند که شاید به لحاظ مالی جبران شود لیکن به لحاظ روحی و معنوی خیلی بعید است که به حالت ماقبل جرم برگشته و جبران گردد. اعمال مجازات در بسیاری از موارد هر چند که تنبیه مجرمان و عبرت

دیگران را در پی دارد ولی خود، عامل وقوع و پیدایش جرائم دیگری اســت که گاهی جرائم ناشـــی از اعمال مجازات به مراتب از جرائم اولیه مجرم خطرناک‌تر و زیان‌بارتر است.

۲-۳-۱- پیشگیری قضایی از جرائم رایانه‌ای در ایران

از آنجا که بیش از چند ســـال از ورود فناوری اطلاعات و ارتباطات نوین به کشـورمان نمی‌گذرد، بالطبع مسـائل جنبی مربوط به آن نیز به تازگی مطرح شـده و نمی‌توان انتظار داشـت که همانند کشـورهای پیشـرو در این حوزه، اقدامات وسـیعی انجام شـده باشـد. البته باید به این نکته نیز توجه داشـت که بحث راجع به این نوع فناوری با دیگر فناوری‌های جدیدی که وارد کشـور می‌شـود، تا حدود زیادی متفاوت اســـت. همان‌طور که پیش از این بیان شـــد، فضـــای تبادل اطلاعات، از چنان انعطاف‌پذیری‌ای برخوردار است که تقریباً می‌توان گفت در تمامی عرصه‌ها وارد شده و آن‌ها را متحول کرده اســـت. از طرف دیگر، قابلیت‌ها و امکاناتی که در اختیار نوع بشر قرار می‌دهد، چنان وسیع و گسترده است که روزبه‌روز بهره‌برداری از آن وسیع‌تر می‌شـــود و چهره های جدیدی به خود می‌گیرد. بنابراین، بدیهی اســـت که سیاست‌گذاران و تصمیم‌گیران جامعه ما باید به فکر چاره‌ای اساسی باشند.[۳۲] طبق آمارهای رسمی، تنها بیش از ده میلیون نفر از شبکه اینترنت استفاده می‌کنند که اگر بهره برداران از تلفن های همراه، تجارت و بانکداری الکترونیک و بســـیاری دیگر از سیستم‌ها و دستگاه‌هایی که با دنیای دیجیتال سروکار دارند را به این رقم بیفزاییم، حداقل نیمی از جمعیت کشورمان را دربر خواهد گرفت.

البته باید خاطرنشـان کرد که تاکنون در حوزه‌های مختلف، اقداماتی قانونی جهت برخورد با برخی سـوءاسـتفاده‌های مورد نظر به عمل آمده اسـت. به عنوان مثال، در اردیبهشت ۱۳۷۹، قانون اصلاح قانون مطبوعات به تصویب رسید و مطابق تبصره ۳

---

[۳۲] در میزان توجه و اهمیت دادن جامعه ما به این حوزه همین بس که در طی ســـال جاری (۱۳۸۳) چندین همایش ملی و بین‌المللی در زمینه های بررســـی ابعاد حقوقی فناوری اطلاعات و ارتباطات، دولت الکترونیک، تجارت الکترونیک، پول الکترونیک و بانکداری الکترونیک برگزار شده است.

ماده یک این قانون، کلیه نشریات الکترونیک مشمول این ماده قرار گرفتند که بدین ترتیب همه مسئولیت‌های کیفری، حقوقی و اجرائی این قانون نسبت به ناشران الکترونیک نیز قابل اعمال خواهد بود. هرچند باید اذعان داشت که به لحاظ فقدان تعریف مشخصی از نشر الکترونیک و ناشران الکترونیک و همچنین از آنجا که موضوع اولیه این قانون نشریات فیزیکی است، اجرای آن نسبت به نشریاتی که در قالب حامل‌های داده (نظیر لوح‌های فشرده) یا در فضای تبادل اطلاعات منتشر می‌شوند با ابهاماتی مواجه است.

همچنین، در آبان ۱۳۷۹ قانون حمایت از حقوق پدیدآورندگان نرم افزارهای رایانه‌ای در راستای قانون حمایت از حقوق مؤلفان، مصنفان و پدیدآورندگان مصوب ۱۳۴۸ در ۱۷ ماده به تصویب رسید که در ماده ۱۳ آن برای ناقضان حقوق مزبور ضمانت اجرای کیفری پیش بینی شده است. هرچند باید اظهار داشت، که اجرای این قانون نیز به خاطر بروز یک سری ایرادهای آئین نامه‌ای که ریشه در خود قانون داشت، تا مدتی در هاله‌ای از ابهام بود.

اما در بهمن ۱۳۸۲، قانون تجارت الکترونیک که در قالب طرح به مجلس شورای اسلامی ارائه شده بود، در ۸۱ ماده به تصویب رسید که باب چهارم آن از مواد ۶۷ تا ۷۷ تحت عنوان جرائم و مجازات‌ها صراحتاً به تحمیل ضمانت اجرای کیفری به متخلفین این قانون پرداخته است. این باب به طور کلی شامل چهار مبحث است: مبحث اول که در ماده ۶۷ آمده است، به کلاه‌برداری کامپیوتری و مبحث دوم در ماده ۶۸ به جعل کامپیوتری اشاره دارد. مبحث سوم که به نقض حقوق انحصاری در بستر مبادلات الکترونیک پرداخته است خود شامل دو فصل است. فصل اول که مواد ۶۹ و ۷۰ به آن اختصاص یافته‌اند، با اشاره به مواد این قانون، تخلفات مربوطه را جرم‌انگاری کرده است. فصل دوم نیز که تحت عنوان حمایت از «داده پیام‌های شخصی/ حمایت از داده» است، در مواد ۷۱، ۷۲ و ۷۳ منعکس شده است. مبحث چهارم این باب که تحت عنوان نقض حفاظت از «داده پیام» در بستر مبادلات الکترونیک است، خود شامل چهار فصل است: فصل اول که راجع به نقض حق مؤلف است، در ماده ۷۴ منعکس شده است. فصل دوم هم که ماده ۷۵ به آن اختصاص دارد

راجع به نقض اسرار تجاری است. فصل سوم با عنوان نقض علائم تجاری در ماده ۷۶ آمده است و فصل چهارم نیز که ماده ۷۷ به آن اختصاص دارد، معلوم نیست از لحاظ عنوان و محتوا چه سنخیتی با سه فصل فوق دارد؛ چرا که به طور کلی تکلیف سایر جرائم، آئین دادرسی و مقررات مربوط به صلاحیت جزائی و روش‌های همکاری بین‌المللی قضائی جزائی مرتبط با بستر تبادلات الکترونیک را روشن می‌کند (جلالی فراهانی، ۱۳۸۳: ۹۹-۹۴).

جدی‌ترین اقدامی که تاکنون در قلمرو جرائم حوزه فناوری اطلاعات انجام شده، تهیه قانون مبارزه با جرائم رایانه‌ای توسط قوه قضاییه است که اولین سند نسبتاً جمع در زمینه پیشگیری کیفری از جرائم این حوزه به شمار می‌رود.

این قانون شامل سه بخش در قالب ۵۶ ماده است که بخش اول آن به جرائم و مجازات‌ها می‌پردازد. این بخش شامل هشت فصل است. فصل اول آن که راجع به جرائم علیه محرمانگی داده‌ها و سیستم‌های رایانه‌ای و مخابراتی است، خود شامل سه مبحث می شود. مبحث اول راجع به دسترسی غیرمجاز، مبحث دوم راجع به شنود غیرمجاز و مبحث سوم راجع به جاسوسی رایانه‌ای است. فصل دوم نیز که به جرائم علیه صحت و تمامیت داده‌ها و سیستم‌های رایانه‌ای و مخابراتی اختصاص دارد، خود شامل دو مبحث است. مبحث اول جعل رایانه‌ای و مبحث دوم تخریب و اخلال در داده‌ها یا سیستم‌های رایانه‌ای و مخابراتی را به خود اختصاص می‌دهد. فصل سوم نیز به کلاه‌برداری و سرقت مرتبط با رایانه اختصاص دارد و در فصل چهارم جرائم علیه عفت و اخلاق عمومی بیان شده است و در فصل پنجم هتک حیثیت و نشر اکاذیب آمده است. هم چنین در فصل ششم مسئولیت کیفری اشخاص و در فصل هفتم در قالب یک ماده که در سه بند و یک تبصره تشریح شده سایر جرائم را مطرح می‌کند و فصل هشتم هم به تشدید مجازات‌ها می‌پردازد.

بخش دوم که آیین دادرسی جرائم رایانه‌ای را مطرح می‌کند، خود شامل سه فصل است. فصل اول راجع به صلاحیت است و فصل دوم که تحت عنوان جمع آوری ادله الکترونیک می‌باشد، شامل پنج مبحث است. مبحث اول به نگهداری داده‌ها، مبحث دوم به حفظ فوری داده‌های رایانه‌ای ذخیره شده، مبحث سوم به ارائه داده‌ها و مبحث

چهارم به تفتیش و توقیف داده‌ها و سیستم‌های رایانه‌ای و مخابراتی و در نهایت مبحث پنجم به شنود محتوای ارتباطات رایانه‌ای اشاره شده است. و فصل سوم این بخش هم به استنادپذیری ادله الکترونیکی می‌پردازد و در نهایت امر بخش سوم این قانون در قالب سایر مقررات به معاضدت بین‌المللی اشاره می‌کند.

علاوه بر قوانین ذکر شده باید به آئین دفاتر خدمات اینترنت[۳۳] نیز اشاره کرد که ماده ۷ و تبصره‌های آن ابتدا به مواردی اشاره دارد که تولید و عرضه آن توسط شبکه‌های انتقال اطلاعات رایانه‌ای ممنوع می‌باشد و سپس به مجازات تخطی از این قانون که لغو پروانه است اشاره می‌کند و در نهایت بخشنامه پلیس فتا به کافی‌نت‌ها نیز در قلمرو قوانین مورد بحث جای می‌گیرد زیرا در صورت تخلف از مفاد این اطلاعیه، طبق تبصره‌های ۱ تا ۳ ماده ۷ آیین نامه دفاتر خدمات اینترنت (کافی نت) و نیز سایر قوانین و دستورالعمل‌های مرتبط، اقدامات لازم انتظامی و معرفی متخلفین به مراجع قضایی صورت خواهد گرفت.

۳-۳-۱- پیشگیری انتظامی از جرائم سایبری

بدون تردید، سیستم کلان پیشگیری و مبارزه با جرم که از سوی پلیس اتخاذ می شود - چه در محیط فیزیکی و چه در فضای مجازی- یکسان است و پلیس در پیشگیری از وقوع جرائم سایبری، همان جایگاه خود را خواهد داشت. در واقع، اقدامات پلیس در جهت پیشگیری از وقوع این جرائم، چیزی جز مبارزه وضعی و سیاست عام این نهاد در مقابله با سایر جرائم نیست. اما در هر حال، آنچه باعث تفاوت در این حوزه می شود، ویژگی‌های منحصر به فرد جرائم رایانه‌ای است که شیوه‌های اجرایی خاص خود را به منظور تحقق این سیاست عام طلب می‌کند (آیکاو، ۱۳۸۳، ۱۵۱).

در حقیقت، علی رغم سیاست‌های عام و مشترک موجود در پیشگیری از سایر جرائم، به دلیل وجود تفاوت های ماهوی میان محیط فیزیکی و فضای مجازی، روش‌های پیشگیری از جرائم رایانه‌ای نیز متفاوت خواهد شد. برای مثال صحنه جرائم ارتکابی در محیط فیزیکی، به طور معمول، متمرکز بوده و پراکندگی جغرافیایی

33afenet

نخواهد داشت اما در جرائم سایبری، پراکندگی جغرافیایی صحنه جرم بسیار زیاد و معمولاً دور از هم و در محدوده مرزی کشورهای مختلف است.

در محیط فیزیکی، حضور پلیس در جامعه، عاملی در پیشگیری از جرم محسوب می‌شود. شکل و ترکیب اتومبیل پلیس و مأموران ملبس به لباس پلیس، تهدیدی برای مجرمان بالقوه به شمار می‌رود. به بیان دیگر، حضور پلیس در جامعه را می‌توان نوعی تهدید ضمنی برای مجرمان تلقی کرد. بدون تردید، حضور فیزیکی پلیس در مواردی که جرائم رایانه‌ای با ورود کاربران غیرمجاز به یک سایت رایانه‌ای صورت می‌پذیرد، نقش مؤثری در پیشگیری از این جرائم خواهد داشت (آیکاو، ۱۳۸۳، ۱۶۹). اما آیا هنگامی که جرائم مزبور توسط خطوط ارتباطی و از طریق شبکه اینترنت و بدون نفوذ فیزیکی در سایت رایانه‌ای ارتکاب می‌یابد، می‌توان اقدامات پیشگیرانه را در این فضای مجازی تصور کرد و آن را محقق دانست؟ به نظر می‌رسد در چنین فضایی نیز می‌توان حضور داشت و با گشت‌زنی و مراقبت، مجرمان بالقوه را تهدید کرد. به منظور انجام این امر، ابزارها و روش‌های خاصی مورد نیاز است که آشنایی با آن‌ها برای مأموران گشت شبکه‌های رایانه‌ای واحد مبارزه با جرائم رایانه‌ای سازمان‌های پلیس لازم و ضروری است.

گشت‌زنی و مراقبت یک مظنون در فضای مجازی کار چندان آسانی نیست و هیچ سازمان پلیسی - هرچند قدرتمند - به تنهایی قادر به انجام آن نیست؛ بلکه لازمه این کار، همیاری چندبخشی دولتی و غیردولتی است. در این مرحله از کار است که وجود تعامل و همکاری مناسب میان شرکت‌های مخابراتی ارائه خدمات و پلیس، اهمیت ویژه خود را نشان می‌دهد. امروزه نرم افزارهای قدرتمندی در اختیار پلیس وجود دارد که شبیه سیستم‌های دزدگیر عمل کرده و پلیس یا مسئول امنیتی را از هرگونه تهدید قریب‌الوقوع به منظور انجام عملیات مجرمانه در فضای مجازی مطلع می‌کند و امکان پیشگیری از این جرائم را به پلیس خواهد داد. به علاوه، این نرم افزارها، آن دسته از کاربران مجازی را شناسایی می‌کند که با عدم رعایت مقررات مربوط به طبقه‌بندی، قصد دسترسی به اطلاعات غیرمجاز را دارند. همچنین این نرم افزارها مشخصات لازم از این افراد را در اختیار پلیس می‌گذارد. بسیاری از سیستم‌ها

نیز، اطلاعات مربوط به تلاش‌های موفق یا ناموفق افراد در ورود به سیستم را ثبت می‌کنند. همچنین امکان شناسایی افراد غیرمجاز که به طور مکرر، رمز عبور نادرست را توسط صفحه کلید تایپ کرده‌اند، نیز وجود دارد. البته چنانچه کاربر غیرمجاز، اطلاعات لازم برای ورود به سیستم را داشته باشد، می‌تواند با نفوذ در رایانه به فایل‌های حاوی رمز عبور دست یابد. درنتیجه تمهیدات فوق بی‌ثمر خواهد بود.

یکی دیگر از شیوه‌های پی شگیری از جرم که سال‌ها ست به طور معمول تو سط نیروی انتظامی صورت می‌گیرد، آموزش همگانی و شناسایی و ارائه آموزش‌های خاص به اشخاص و سازمان‌هایی است که احتمال می‌رود در معرض جرائم رایانه‌ای قرار گیرند. در واقع، به‌کارگیری این شیوه، به همان اندازه که در پیشگیری از جرائم ارتکابی در محیط فیزیکی مؤثر است، در فضای مجازی نیز از تأثیر قابل توجهی برخوردار خواهد بود (رضوی،۱۷۲-۱۷۰). بدون تردید، در راستای تحقق نقش مؤثر پلیس در پی شگیری از جرائم سایبری، ا ستفاده از نیروهای متخ صص پلیس در این حوزه و شیوه‌های تحقیق و بررسی توسط این نیروها، از اهمیت فوق‌العاده‌ای برخوردار است. لذا آشنایی با تشکیلات پلیس فتا در ایران که مهم‌ترین سازمان پلیسی در زمینه مبارزه با جرائم رایانه‌ای می‌باشد خالی از لطف نیست.

نتیجه‌گیری

اگرچه وجود قانون کیفری برای تمیز هنجارها و ناهنجاری‌ها و سازماندهی و تأمین نظم و امنیت جامعه و تعیین الگوی رفتار قانونی شهروندان برای هر جامعه‌ای ضروری و حیاتی است، با این حال برای ایجاد یک جامعه سالم و قانونمند و تأمین و تضمین حقوق و آزادی‌های اساسی شهروندان تنها از سازوکار جرم‌انگاری نمی‌توان بهره برد و پیامدهای مترتب بر جرم‌انگاری و هزینه‌های جبران ناپذیر آن را نادیده گرفت.

اگر در فرایند تصمیم‌گیری راجع به جرم دانستن یک رفتار، مشخص گردد که آن رفتار بر اساس اصول و مبانی نظری، داخل در صلاحیت قضایی جامعه و مربوط به اقتدار حکومت است؛ به عبارت دیگر دولت مجاز به مداخله در آن قلمرو است و نیز ثابت گردد که استفاده از سایر ابزارهای دارای اجبار کمتر و غیر سرکوبگر مانند کنترل‌های اجتماعی غیررسمی برای پیشگیری و کاهش و کنترل رفتار مورد نظر موفقیت آمیز و مناسب و مؤثر نیست، این امر به تنهایی برای جرم دانستن عمل کفایت نمی‌کند؛ بلکه در اینجا باید به پیامدهای عملی جرم‌انگاری نیز توجه نموده و هزینه‌ها (مضار) و فواید (منافع) آن را مورد ارزیابی قرار دهیم. به نحوی که هرگونه بی‌توجهی به کارکردهای جرم‌انگاری می‌تواند آثار و پیامدهای منفی زیادی را به دنبال داشته باشد.

قانونگذار کیفری از جرم‌انگاری یک رفتار اهداف خاصی را دنبال می‌کند لکن هنگامی که این جرم‌انگاری بدون معیار و ضابطه صورت گیرد نه‌تنها این اهداف محقق نمی‌شود بلکه چهره دستگاه عدالت کیفری مخدوش می‌گردد. بنابراین برای جرم شمردن یک رفتار ضروری است اصول و قواعد حقوق کیفری و اقتضائات خاص یک جرم کاملاً رعایت شود در واقع جرم‌انگاری رفتار کاربران فضای سایبر باید به عنوان آخرین حربه نگریسته شود. «احترام به حریم خصوصی و رعایت موازین حقوق بشری» مقوله مهم دیگری است که برای جرم شمردن یک رفتار در محیط سایبر باید کاملاً مورد توجه قرار بگیرد. به جهت ویژگی‌های خاص بزه‌های رایانه‌ای «تناسب بین جرم و مجازات» و فردی کردن مجازات ضرورتی مضاعف دارد. همچنین با توجه به

نوین بودن جرائم رایانه‌ای جرم‌انگاری بدون عنایت به ابزار و وسایل موجودِ دستگاه عدالت کیفری از مرحله شناسایی جرم تا تعقیب و دستگیری مجرم و در نهایت اعمال مجازات، موجب ناکامی در عمل و لطمه به اقتدار حقوق کیفری می‌شود. برخی از ویژگی‌های جرائم سایبری که از یک سو بر ضرورت رعایت دقت و ضابطه در جرم‌انگاری می‌افزاید و از سوی دیگر اقتضائات خاصی را در امر جرم‌انگاری موجب می شود عبارتند از: سن و جنس مجرمان، فرامرزی بودن جرم، گستردگی خسارت و بزه دیده این جرائم، پیشرفت سریع و به‌روز این فناوری و انگیزه و روحیه خاص مجرمان سایبر.

پژوهش در باره‌ی بزهکاری را یا نه‌ای به ما امکان می‌دهد تا چگونگی و چرایی به‌کارگیری فناوری‌های رایانه‌ای توسط بزهکاران را در رفتارهای بزهکاران‌شان درک کنیم. یک بزهکار، برای ارتکاب جرائم رایانه‌ای از یک‌سو بر فرصت‌هایی که فضای سایبر به‌عنوان یک جهان نوپدید پیش روی وی نهاده، تکیه می‌کند و از رهگذر مجازی انگاشتن این فضا و هرچه در آن است، واقعیت‌ها و ارزش‌های اجتماعی آن را نادیده گرفته و به لطف گمنامی اعطا شده در این فضا یا بهره‌گیری از ابزارهای پنهان‌نگاری و رمزنگاری، در مقایسه با جهان خاکی بسیار آسان‌تر و کم هزینه‌تر مرتکب جرم می‌شود. همچنین، وابستگی روزافزون انسان امروزی به فناوری‌های اطلاعاتی و ارتباطاتی و انتقال همه‌ی امور اداری، آموزشی، سرگرمی، تجاری، اقتصادی، پولی و بانکی و فرهنگی به این فضا، موجب پیدایش طیف گسترده‌ای از آماج‌های گوناگون شده و آرمان‌شهری برای بزهکاران فراهم آمده است.

شناسایی ماهیت و ویژگی‌های جرم برانگیز فضای سایبر در کنار شناخت عوامل فردی کنش‌گران این فضا به ویژه بزهکاران، به پیش‌بینی تدابیر پیشگیرانه‌ی اثربخش‌تر و کاربردی‌تر کمک خواهد کرد. این تدابیر که نوعا جلوه‌ی فناورانه یا اصطلاحا وضعیتی دارند، به‌نوبه‌ی خود می‌توانند حساسیت‌ها و پیامدهایی را برانگیزند و به اعضای جامعه‌ی اطلاعاتی تحمیل کنند؛ پس شناخت درست و واقع بینانه‌ی آن‌ها می‌تواند فرصت‌ها و فناوری‌های جنایی رایانه‌ای را با اثربخشی بیشتری برچیند و کم‌ترین محدودیت‌ها و آزردگی‌ها به دیگران تحمیل شود. به‌کارگیری تدبیرهایی

مانند اقسام نظارت‌های الکترونیکی، پالایه‌ها، اقسام مؤیدها (مانند مؤیدهای سنی یا حرفه‌ای) همگی در گرو شناخت عوامل فردی و محیطی بزهکاری رایانه‌ای است که در این نوشتار به‌طور اجمالی شرح آن آمد و در نوشتارهای بعدی نقش آفرینی آن‌ها با نگاه تخصصی‌تر دنبال خواهد شد.

کیفرگزینی مهم‌ترین و شاخص‌ترین قسمت رویه قضایی در رویارویی با پدیده‌های مجرمانه است. در واقع رویه قضایی در امور کیفری بیشتر از هر چیزی تابع کیفرگزینی است. دلیل این امر این است که قانون‌گذار در راستای واقعی و فردی کردن پرونده‌های کیفری، اختیارات عدیده‌ای به قضات می‌دهد تا لزوماً در پی تعیین کیفر قانونی نباشند و با توجه به این اختیارات، کیفری را تعیین کنند که نه تنها اهداف حقوق کیفری را مدنظر داشته باشد، بلکه متناسب با جرم ارتکابی و البته مرتکب آن باشد. این اختیارات عدیده مایه اصلی رویه قضایی می‌شود که خود هویت مستقلی پیدا می‌کند و جدا از منابع اصلی حقوق کیفری و به ویژه قانون قابل تحلیل و ارزیابی است.

جرائم سایبری طیفی جدید از جرائم است که به جهت تبلور فضایی جدید به نام محیط تبادل اطلاعات یا محیط سایبر شکل گرفته‌اند. ویژگی‌های این قبیل جرائم از منظر بستر جرم، موضوع مورد حمایت، مرتکب و مانند اینها سبب شده است تا رویه قضایی به ویژه در زمینه کیفر گزینی، متفاوت از دیگر جرائم به نظر برسد. اینکه پس از گذشت کمتر از یک دهه از تصویب قوانین مرتبط با نقض هنجارهای رایانه‌ای و سایبری و به طور ویژه قانون جرائم رایانه‌ای مصوب خرداد ۱۳۸۸، رویه قضایی مشخصی با محوریت کیفر گزینی در ایران شکل گرفته است یا خیر، منوط به درک رویکردهای گوناگون در تعیین قضایی کیفر برای مجرمان سایبری از یک سو و لحاظ رویه قضایی ایران دست کم به شیوه استقرای ناقص از سوی دیگر است. هر چند عدم بررسی رویه قضایی ایران و تحلیل همه یا بیشتر آرای قضایی به عنوان یک آسیب جدی در ادبیات حقوقی ایران به شمار می‌رود، ولی دلایل عدم بررسی آن به جهات مختلف مانند عدم انتشار همه آرای کیفری، عدم ارتباط تنگاتنگ دستگاه قضایی و دانشگاه‌ها و در نتیجه عدم تبادل فراگیر اندیش‌ها و نیز دگرگونی‌های عدیده قوانین

کیفری که مجالی برای شکل‌گیری رویه قضایی مستمر و محکم باقی نمی‌گذارد، تا اندازه‌های قابل توجیه است. با این حال بررسی رویه قضایی به ویژه از منظر کیفر گزینی باید به عنوان یک راهکار اساسی در رویارویی علمی و درست با جرائم و به طور ویژه جرائم سایبری لحاظ شود. بر این اساس چالش اصلی این نوشتار در اتخاذ رویکرد مناسب در کیفرگزینی در قبال جرائم سایبری است.

منابع

۱. ابوذری م.. جرم شناسی جرائم سایبری، پایان نامه کارشناسی ارشد دانشکده حقوق و علوم سیاسی دانشگاه تهران. ۱۳۸۸
۲. حسنی ج.. معیارهای جرم‌انگاری موارد نقض حریم دادههای شخصی در فضای سایبر، چاپ نخست، مجموعه مقالات حقوق فناوری اطلاعات و ارتباطات (نکوداشت مرحوم استاد محمدحسن دزیانی)، تهران، روزنامهی رسمی کشور. ۱۳۸۸
۳. حسنی ج.. معیارهای جرمانگاری موارد نقض حریم دادههای شخصی در فضای سایبر، مجموعه مقالات حقوق فناوری اطلاعات، معاونت حقوقی و قضایی قوۀ قضائیه. ۱۳۸۹
۴. حیدری ع.. ده قانون مورد نیاز شبکه، نشریه دبیرخانه انفورماتیک کشور، سال چهاردهم، شماره ۱۳۸۹۷۲
۵. خرم‌آبادی ع.. سابقه‌ی پیدایش، تعریف و طبقه‌بندی جرائم رایانه‌ای، مجموعه مقالات همایش بررسی ابعاد حقوقی فناوری اطلاعات، تهران، کمیته مبارزه با جرائم رایانه‌ای، مرکز مطالعات راهبردی و توسعه قضایی. ۱۳۸۴
۶. رضوی ، محمد ، ، جرایم سایبری و نقش پلیس در پیشگیری از این جرایم و کشف آن‌ها، نشریه پژوهش دانش انتظامی ۱۳۹۰
۷. غلامی ح.. تکرار جرم به عنوان حرفه مجرمانه، فصلنامه حقوق (مجله‌ی دانشکده حقوق و علوم سیاسی سابق)، ۱۳۸۲
۸. فضلی م.. تخریب و اخلال در داده‌ها و سیستم‌های رایانه‌ای، مجموعه مقالات همایش جنبه‌های حقوقی فناوری اطلاعات، قم، انتشارات سلسبیل، چاپ اول۱۳۸۳
۹. قورچیبیگی م. ، تحلیل و بررسی جرم شناختی جرائم یقه‌سفیدها، رساله دوره دکتری، دانشگاه تهران، دانشکده حقوق و علوم سیاسی، حقوق کیفری و جرم‌شناسی. ۱۳۹۲
۱۰. کاظمی ق.. ردیابی، ضبط و مصادره عواید مالی ناشی از فساد در چهارچوب عدالت کیفری یا خارج از آن، مجله حقوقی دادگستری، شماره ۶۱، ۱۳۸۶
۱۱. کی نیا م.. مبانی جرم‌شناسی، جلد اول، تهران: انتشارات دانشگاه تهران. ۱۳۸۶
۱۲. گرکی م.. جرائم سایبری راهنمایی برای کشورهای در حال توسعه، ترجمه: مرتضی اکبری، تهران، ۱۳۸۹
۱۳. مظلومان ر. ۱۳۵۳، نقش تحصیل در کمیت و کیفیت جرم، نشریه کاوه (مونیخ)،

۱۴. معاونت آموزش و تحقیقات قوه ق ضائیه.. م سائل ق ضایی هرزه نگاری در محیط سایبر، تهران: راه نوین. ۱۳۸۹
۱۵. ملکیان ا.. اصـــول مهندســـی اینترنت، تهران، انتشـــارات علمی فرهنگی نص، چاپ دهم۱۳۹۳
۱۶. نجفی ابرندآبادی ع.. بزهکاری و جرم‌شـناسـی سـایبری، تعالی حقوق، دادگسـتری کل استان خوزستان. سال ۱۳۸۸

1. Abe David Lowell, and Kathrync Arnold, Corporate Crime after 2000: A New Law Enforcment Challenge, American Criminal Law review, volume 40. 2003, p:221
2. Ahmad Kamal. 2005. The Law of Cyberspace. An Invitation to the Table of Negotiations, Published by United Nations Institute for Training and Research, p:194
3. Alder, Freda & Muller, Gerhard & Laufer, William. 1996. the criminal justice: the core, U.S.A. Mc Graw.
4. 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.
5. Brenner, Susan, Toward a Criminal Law for Cyberspace: Distributed Security, university of Dayton School of law,p:55
6. Britton, Dana M. 2011. the Gender of Crime, New York: Rowman & Littlefield Publishers.
7. Carey, Peter, Media Law, sweet&Maxwell, Second Edition, London, 1999, p:176
8. 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.
9. 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.
10. Cisco System Inc. v Greoffrey Osowski and Wilson Tang, see: www.usdoj.gov/criminal/cybercrime/cccases.html 5. Smith, R. 2004. Criminal Forfeiture and Restriction-of-Use orders in sentencing high tech offenders, in
11. Cisco System Inc. v Greoffrey Osowski and Wilson Tang, see: www.usdoj.gov/criminal/cybercrime/cccases.html 5. Smith, R. 2004. Criminal Forfeiture and Restriction-of-Use orders in sentencing high tech offenders, in
12. Criminal Behavior. International Journal of Information Science and Forensics Handbook, Rockland: Syngress Publishing Forensics Process. Computers & Security. 22(4), 292-298
13. Currani. John F. 2007. Internet Crime Victimization: Sentencing, Mississipi Law Journal, Vol.76.
14. Cyber crime and. 2010. Debarati Halder and K. Jaishankar in press, Victimization of Women: Laws, Rights, and Regulations. Hershey, PA, USA:
15. Cyberstalking: Harassment in the Internet Age and Bocij, 2004. Paul.
16. Cyberterrorism-the usw of the Internet for terrorist Purposes, Council of Europe, Decsmber 2007, p:304
17. Durost, Shane. 2005. Profiling a Hacker, Capstone Project, available at: ciag.umfk.maine.edu/Shane%20Durost.pdf.
18. Erbschloe, Michael. 2001. Information Warfare: How to Survive Cyber Attacks, NewYork: McGraw Hill.
19. Examination of Cyber-Council of Europe – cybercrime. 1990. Recommendation No. 89, Strasbourg, the translation of the High Council of Informatics, Management and Planning Organization of Iran, 1376.
20. Explanatory Notes to Counter-Terrorism Act 2008
21. Faiza, Patel, Crime without frontiers, Journal of international Law and Policy, 22 N.Y.U

22. Goldschmidt, Orly Turgeman. 2011. Identity Construction among Hackers, In: Jaishankar, K. (Ed), Cyber Criminology: Exploring Internet Criminal Behavior. Boca Raton: CRC Press.
23. Graner, Brayan A. 2004. black, s Law Divtionary, Eight Edition, Thomason. www.unesco.org/webworld-screen/cons-index.html
24. Jahankhani, Hamid and Al-Nemrat, Ameer. 2010. Examination of CyberCriminal Behavior. International Journal of Information Science and Management (Special Issue), 41-48.
25. Global Society, Vol. 17, No. 1.
26. Kirwan, Gráinne and Power, Andrew. 2013. Cybercrime: the Psychology of Online Offenders. New York: Cambridge University Press.
27. 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