فصلنامهٔ پژوهش‌های اطلاعاتی و جنایی، سال سیزدهم
شمارهٔ سوم، پاییز ۱۳۹۷

عوامل مؤثر بر ارتکاب جرم در فضای مجازی از دیدگاه قضات دادسرای جرائم رایانه‌ای تهران[1]

تاریخ دریافت: ۹۷/۰۲/۳۰ تاریخ پذیرش: ۹۷/۰۶/۲۸

از صفحهٔ ۹ تا ۳۶

زهرا جاه بین[2]، افسانه مظفری[3]، نوروز هاشم زهی[4]، سید محمد دادگران[5]

چکیده

دنیای سایبر با ویژگی‌های منحصربه‌فرد خود در کنار دنیای کنونی، توجه هنجارشکنان را جلب کرده است. این فضای رها شده که هر لحظه بر گسترهٔ آن افزوده می‌شود، فرصت بسیار مناسبی را برای مرتکبان جرم و مجموعه چالش‌هایی را برای مراجع قضایی و انتظامی که سعی در کنترل این پدیده دارند، ایجاد کرده است. مقالهٔ حاضر بخشی از یک تحقیق کیفی با روش تحلیل تم است. در راستای نیل به هدف اصلی پژوهش، شناسایی عوامل مؤثر بر ارتکاب جرم در فضای مجازی، با ۱۶ نفر از قضات (بازپرسان و دادیاران) دادسرای جرائم رایانه‌ای تهران که به روش نمونه‌گیری هدفمند انتخاب شده بودند، مصاحبهٔ نیمه ساختاریافته صورت گرفت. هر مصاحبه، ضبط و سپس کلمه به کلمه پیاده‌سازی شد. مصاحبه‌های انجام شده به روش نظام بندی کلارک و برون، مورد تجزیه و تحلیل قرار گرفتند. کدهای استخراج شده یا مستقیماً در صحبت‌های مصاحبه شوندگان بیان شده بود یا کدهای تلویحی بودند که توسط پژوهشگر از متن مصاحبه‌ها استخراج شدند. براساس نتایج این مطالعه، علل ارتکاب جرم در فضای مجازی در ۴ تم اصلی (عوامل مرتبط با بزهکار، عوامل مرتبط با بزه‌دیده، عوامل مرتبط با فضای مجازی، عوامل مرتبط با فضای فیزیکی) احصاء شد. از دیدگاه قضات، عوامل مرتبط با فضای مجازی همچون گمنامی و سهل‌الوصول بودن، فراگیر بودن، جذابیت‌های فضای مجازی، از مهم‌ترین دلایل ارتکاب جرائم سایبری بودند.

کلید واژه‌ها: ارتکاب جرم، فضای مجازی، جرائم رایانه‌ای، قضات، تهران.

استناد: جاه‌بین، زهرا؛ مظفری، افسانه؛ هاشم‌زهی، نوروز و دادگران، سید محمد (پاییز ۱۳۹۷). عوامل مؤثر بر ارتکاب جرم در فضای مجازی از دیدگاه قضات دادسرای جرائم رایانه‌ای تهران. *فصلنامهٔ پژوهش‌های اطلاعاتی و جنایی*، ۱۳(۵۱)، صص ۳۶-۹.

---

۱. برگرفته از رسالهٔ دکترای دانشگاه آزاد اسلامی واحد علوم تحقیقات تهران با موضوع «عوامل مؤثر بر ارتکاب جرم در فضای مجازی».

۲. دانشجوی دکترای ارتباطات اجتماعی دانشگاه آزاد اسلامی واحد علوم تحقیقات تهران، jahbin1394@gmail.com

۳. استادیار گروه ارتباطات اجتماعی دانشگاه آزاد اسلامی واحد علوم تحقیقات تهران، نویسندهٔ مسئول:
dr.afsaneh.mozaffari@gmail.com

۴. استادیار گروه علوم اجتماعی دانشگاه آزاد اسلامی واحد تهران شرق، no- hashemzehi@yahoo.com

۵. استادیار گروه ارتباطات اجتماعی دانشگاه آزاد اسلامی واحد تهران مرکزی، mohamad_dadgaran@yahoo.com

مقدمه

رشد فزایندهٔ فناوری‌های اطلاعاتی و ارتباطی با آنکه براساس برخی ویژگی‌های بی‌مانند خود، نویدبخش حیات بهتر با ویژگی‌هایی همچون توزیع عادلانه‌تر منابع، کم‌رنگ کردن مرزهای طبقاتی، جغرافیایی، برخورداری مادی و پیشینهٔ خانوادگی بوده‌اند، اما در پی خود، انواع جدیدی از ناهنجاری‌ها، آسیب‌ها و جرائمی را امکان‌پذیر ساخته‌اند که می‌توان از آن‌ها به «نامطلوبیت فناورانه» تعبیر کرد. این پیامدها شاید پیش‌بینی نشده و ناخواسته، متولیان، دانشوران و پژوهشگران را با وضعیت ویژه‌ای مواجه کرده است که طی آن نظارت، کنترل، برخورد و پیشگیری از آن‌ها صرفاً با نگاهی تک جهانی و بدون ملاحظهٔ خصایص فضای مجازی یا دوم، نه تنها میسر نیست؛ بلکه ممکن است اثرات ناخوشایندی را نیز در پی داشته باشد (عاملی و حسنی، ۱۳۹۱، ص۲۶).

به دنبال گسترش و بسط فضای مجازی و افزایش دسترسی به آن، میل و اشتیاق و تنوع استفاده از آن نیز افزایش یافته است. این تمایل که با سرعت قابل‌توجهی در حال افزایش است، اگرچه زمینهٔ مشارکت جوامع را در فرآیند اقتصاد داده‌پردازی فراهم می‌سازد؛ اما در عین حال، شرایط و بستر مساعدی نیز برای ظهور پدیده‌های نوین بزهکاری به وجود آورده است. جرائم ارتکابی در فضای سایبری، یکی از این پدیده‌های نوین تلقی می‌شود (خداقلی، ۱۳۸۳، ص۱۸). در حال حاضر، جرائم و تهدیدهای سایبری، به عنوان یکی از دغدغه‌های بزرگ هزارهٔ سوم میلادی، آیندهٔ اجرای قوانین را در بسیاری از کشورهای جهان به مخاطره انداخته است. کشورهای توسعه‌یافته، برای مبارزه با این جرائم، پیشقدم شده و قوانینی تدوین کرده‌اند که بسیاری از آن‌ها، از اسناد بین‌المللی سرچشمه می‌گیرند. این اسناد، راهکارهای مناسبی پیش روی قانونگذاران کشورها قرار داده‌اند (راسخی، ۱۳۹۳، ص۲۰۳).

مشخص کردن دلیل جرم و انگیزه‌های مجرمان و اینکه آیا جرم برخاسته از سرکشی، درماندگی یا اعتراض برای عدالت‌خواهی است، هرگز کار آسانی نیست. تنوع انگیزه‌ها و مقاصد جرم به‌اندازهٔ تنوع افرادی است که مرتکب جرم می‌شوند (آنجلیز، ۱۳۸۳، ص۳). هرچند ناهنجاری‌ها و جرم، موضوعات فراگیر جامعه‌شناسی و آسیب‌شناسی اجتماعی محسوب می‌شود، ولی پیچیدگی عوامل مؤثر در این پدیده باعث شده است تا هر حوزهٔ علمی از دیدگاه خود به آن توجه کند. روان‌شناسان و روان‌پزشکان از دیدگاه روان‌شناختی، حقوق‌دانان از دیدگاه جرم‌شناسی و مسائل کیفری، پزشکان و

زیست‌شناسان از دیدگاه عوامل مؤثر زیستی و جامعه‌شناسان از دیدگاه آسیب‌شناسی اجتماعی به بررسی عوامل این پدیده می‌پردازند؛ اما فهم ناهنجاری‌ها و جرائم در جهان دو فضایی شدهٔ جدید، مستلزم نگاهی بین‌رشته‌ای و در عین حال، درکی دوفضایی است. طبق اعلام گروه آمار مرکز مطالعات راهبردی قوهٔ قضائیه در سال ۱۳۹۶ طی شش ماههٔ اول سال، تعداد پرونده‌های ثبت شدهٔ جرائم سایبری در کل کشور ۱۰۶۰۹ بود که بیش‌ترین تعداد پرونده‌ها مربوط به استان تهران با ۳۰۵۰ پرونده در رتبهٔ اول و استان خراسان رضوی با ثبت ۱۱۰۹ پرونده در رتبهٔ دوم جرائم سایبری قرار گرفته‌اند.

در ادامه، به پژوهش‌هایی که در ارتباط با موضوع تحقیق حاضر انجام پذیرفته شده است، اشاره می‌شود. پژوهشی با عنوان «مطالعهٔ جامعه‌شناختی انگیزهٔ افراد و نوع جرم ارتکابی در شبکهٔ اجتماعی فیس بوک» توسط سودابه محمودزاده (۱۳۹۱) انجام شده است. هدف اصلی این تحقیق مطالعهٔ جامعه‌شناختی انگیزه‌های افراد و نوع جرم ارتکابی در فضای سایبر و شبکهٔ اجتماعی مجازی فیس بوک با بررسی پرونده‌های تشکیل شده در دادگاه جرائم سایبری است. نظریهٔ مورد استفاده در این پژوهش برای بررسی انگیزه‌های فردی در نوع جرم ارتکابی، تئوری خنثی‌سازی سایکزو و ماتزا و برای بررسی انگیزه‌های اجتماعی افراد، تئوری خرده‌فرهنگ بزهکاری کوهن و تئوری مرتون دربارهٔ آنومی است که به توصیف ارتباط بین انگیزه‌های فردی و اجتماعی با نوع جرم ارتکابی افراد پرداخته شده و از میان همهٔ فرضیه‌ها، بیش‌ترین میزان ارتباط، میان انگیزهٔ انتقام‌جویی و جرم هتک حرمت و حیثیت است. همچنین، رابطهٔ میان انگیزهٔ ترویج بی‌بندوباری و جرم علیه عفت و اخلاق عمومی نیز بیشتر از سایر فرضیه‌ها است. میان جنسیت شاکی و جنسیت متهم نیز ارتباط وجود دارد.

مارکوم[1] (۲۰۰۸) با مرور مطالعات انجام شده، بیش‌ترین تعداد آسیب‌های اخلاقی اینترنت را آزار جنسی، قرار گرفتن ناخواسته در معرض محتواهای هرزه نگاری و فریب می‌داند. او با انجام پیمایشی روی ۲۶۷۳ نفر از دانشجویان مقطع کارشناسی، به آسیب‌شناسی آن‌ها در روابط مجازی پرداخت. از پاسخگویان سؤالاتی در مورد رفتارهای برخط آن‌ها پرسیده و از آن‌ها خواسته شد در صورت داشتن تجارب قربانی شدن در روابط اینترنتی، این واقعه را شرح دهند. نتایج پژوهش وی نشان داد کسانی که بیشتر در

1.Marcum

محیط‌های مجازی چت می‌کنند، احتمال بیشتری دارد که قربانی سوءاستفاده‌های مجازی و غیرمجازی شوند. همچنین، چترهای حمایتی حکومتی برای محافظت از نوجوانان در برابر قربانی شدن در اینترنت کارا نبوده‌اند (عاملی، ۱۳۹۰، ص۱۴۳).

رنون[1] (۲۰۰۶) به ویژگی گمنامی در اینترنت و نقش آن در گرایش زنان به برساختن هویت‌های جایگزین در اینترنت توجه می‌کند. رنون اینترنت را «ماسک متنی»[2] می‌نامد و معتقد است این ماسک متنی به زنان کمک می‌کند تا ابعاد جدیدی از خود را آشکار کنند. او کار کیفی خود را بر پنج زن بیست تا چهل ساله متمرکز کرد و نشان داد که مشارکت‌کنندگان تلاش داشتند تا از چت روم‌ها به عنوان ابزاری برای تخلیهٔ عاطفی و جنسی استفاده کنند (عاملی، ۱۳۹۰، ص۱۴۲).

مک فارلان و بوسیچ[3] (۲۰۰۵) مطالعات جامعی دربارهٔ مجرمان سایبری و قربانیان به پایان رسانده‌اند. از این دست داده‌ها، چهار نوع مشخص از مجرمان سایبری ظهور کرده‌اند که شامل مجرم سایبری انتقامی، مجرم سایبری آرام، مجرم سایبری صمیمی و مجرم سایبری جمعی است. به گفتهٔ مک فارلان و بوسیچ، مجرم سایبری انتقامی، شخص بدخواهی است که قربانیان را بیش از دیگر قربانیان در سه گروه تهدید و ایذا کرده‌اند. مجرمان این گروه از شماری تاکتیک‌های مغرضانه نظیر بد افزارها، هک کردن، اشباع ایمیلی و سرقت هویت برای ایذای قربانیان خود استفاده می‌کنند. فقط مجرمان سایبری انتقامی، از میان مجرمان چهار گروه، برای دسترسی به رایانهٔ قربانی و خرابکاری از ویروس‌های مخرب تروی استفاده کرده‌اند. مجرمان این گروه، مهارت و خبرگی فراوانی در رایانه داشتند و نشانه‌هایی از بیماری روانی از محتوای پیام‌های عجیب و غریب اخلال‌گرایانه به قربانیان نمایان بود. مجرم سایبری آرام، قربانی خود را به شیوه‌ای موقرانه و متوازن و خونسرد، هدف قرار می‌دهد؛ هدف اولیه، پدیدآوردن تنش و اضطراب مداوم در قربانی از طریق رفتارهای تهدیدآمیز است. هدف اول مجرم سایبری صمیمی، برقراری رابطه با قربانی براساس شیفتگی و مشغلهٔ ذهنی است. اعضای این گروه بسیار متنوع‌اند؛ به صورتی که برخی از آن‌ها زمانی شخصاً با قربانی رابطه داشتند و شیفتهٔ قربانی‌اند. همان‌گونه که از نام مجرمان سایبری جمعی برمی‌آید، شامل دو یا چند فرد است که در

1.Ranon
2.Textual Mask
3.McFarlane and Bosic

تعقیب یک قربانی‌اند. مهارت‌های رایانه‌ای این گروه در مقایسه با مهارت‌های سه نوع دیگر بسیار بالاست (کی جایشانکار[1]، ۱۳۹۴، صص۱۹۵-۱۹۶).

برخی معتقدند اگرچه فضای سایبری چالش‌های جدیدی را پدید آورده است، اما مکانیسم‌های زیرین ارتکاب جرم در فضای مجازی همانند جهان واقعی است. این دسته از محققان، جرائم نوظهور سایبری را با استفاده از نظریه‌های سنتی تبیین کرده‌اند و در این میان، نظریهٔ خودکنترلی، نظریهٔ یادگیری اجتماعی و نظریهٔ سبک زندگی- فعالیت‌های روتین بیش‌ترین سهم را داشته‌اند. برخی دیگر نیز به تدوین نظریه‌های جدید یا بازنویسی نظریه‌های قدیمی اعتقاد دارند؛ چراکه تصور می‌کنند جرائم سایبری، نوع جدیدی از جرائم هستند (بولدن و نالا[2]، ۲۰۱۴، صص۱و۵). این دو دیدگاه منجر به تعاریف مختلفی از جرائم سایبری شده است. از میان تعاریف متعدد ارائه شده از جرائم سایبری، به نظر می‌رسد که تعریف به کار رفته توسط مک گوئیر[3] و داولینگ[4]، تعریفی کامل و جامع باشد. آن‌ها جرائم سایبری را به عنوان مفهومی چتری[5] تعریف می‌کنند که دو نوع فعالیت مجرمانهٔ کاملاً متمایز ولی مربوط به هم را پوشش می‌دهد: جرائم وابسته به فضای سایبری و جرائم ممکن شده توسط فضای سایبری (مک گوئیر و داولینگ[6]، ۲۰۱۳، ص۶). حاصل این تعاریف و دسته‌بندی‌های متنوع، مجموعه‌ای از نظریه‌ها برای تبیین جرائم سایبری فراهم ساخته که در ادامه به آن‌ها پرداخته خواهد شد.

الف) نظریهٔ یادگیری اجتماعی: در علوم اجتماعی، روان‌شناسی، جرم‌شناسی و حتی در علوم تربیتی، نظریه‌های گوناگونی به منظور علت شناسیِ بزهکاری مطرح شده‌اند. پیرامون خودِ یادگیری نیز نظریه‌های مختلفی مطرح شده است. در این چارچوب، می‌توان به نظریهٔ «قوانین تقلید[7]» گابریل تارد، نظریهٔ «شرطی شدن کلاسیک[8]» و حتی به رویکرد رفتارنگرِ «اسکینر[9]» و شرطی شدنِ عامل[10] اشاره کرد. نقطهٔ مشترک هریک از این نظریه‌ها آن است که چنانچه رفتار آدمی با پاداش روبرو شود، تقویت و چنانچه تنبیه و سرزنش شود، تضعیف می‌شود.

1. K. Jaishankar
2. Bolden and Nalla
3. McGuire McGuire
4. Dowling
5. Umbrella term
6. McGuire and Dowling
7. Imitation
8. Classical Conditioning
9. Skinner
10. Operant Conditioning

- **نظریهٔ یادگیری اجتماعیِ بندورا:** آلبرت بندورا با طرد دیدگاه‌های رفتارنگر معتقد است، در این نظریه‌ها عوامل انگیزشیِ درونی و عوامل شناختیِ انسان نادیده گرفته شده است و به نوعی، خواهانِ بازگشتِ توجه به فرآیندهای درونیِ انسان است. از دید نظریه‌پردازان یادگیری اجتماعی، نظریهٔ شرطی شدن کلاسیک و شرطی شدن عامل، تنها قسمتی از رفتار و تکامل انسان را در برمی‌گیرد، در حالی که رفتارهای دیگری نیز وجود دارند که نه از راه نظام تنبیه – پاداش، بلکه از راه مشاهده آموخته می‌شود (ثنایی، ۱۳۶۸، ص۱۳). این یادگیریِ مشاهده‌ای ممکن است از طریق خانواده، خرده‌فرهنگ‌های غالب یا نمادهای فرهنگی مانند تلویزیون، ارتباطاتِ برخط[1]، کتاب و غیره صورت گیرد (دادستان، ۱۳۸۹، ص۸۹). بنابراین، رفتار بهنجار و ناهنجار افراد از طریق ارتباط با دیگران و مشاهدهٔ رفتار آن‌ها بر مبنای الگوی شناختیِ تشویق - تنبیه آموخته می‌شود. یکی دیگر از مفاهیم کلیدی در نظریهٔ بندورا، انگیزه است. او انگیزه را دارای سه جنبه می‌داند؛ «تقویتِ برونی[2]»، شبیه مفهوم تقویت در نظریهٔ اسکینر است که اشاره به محرک‌های موجود در محیط دارد. «تقویتِ جانشینی[3]»، براساس مشاهدهٔ تقویت یا تضعیف رفتار افراد دیگر به دست می‌آید و «خود تقویتی[4]»، با احساس غرور، رضایت یا دستیابی به هنجارهای رفتاری خاص هر فرد مطابقت دارد (دادستان، ۱۳۸۹، ص۸۸). بنابراین، به اعتقاد بندورا تقویت، عامل اصلیِ موفقیت در یادگیری مشاهده‌ای است. پس اگر شخص آن عمل را موفقیت‌آمیز مشاهده و ارزیابی کند، تقلید و در غیر این صورت، نامحتمل است که آن رفتار الگوبرداری شود.

- **تحلیلِ انحطاط اخلاق سایبری در پرتو نظریهٔ یادگیریِ اجتماعی:** بی‌شک، بزهکاران سایبری به مانند سایر انسان‌ها بیشتر با افراد هم‌فکرِ خود تعامل دارند. در دنیای سایبر، بخش بزرگی از این معاشرت‌ها از طریق ارتباطات رایانه محور[5] صورت می‌گیرد. الگوهای یادگیری نیز از این طریق در افراد نهادینه می‌شود؛ زیرا به همان اندازه که در فضای مادی معاشرت‌های رودررو اهمیت دارد، برای بزهکاران سایبری ارتباطات غیرحضوری مهم تلقی می‌شود. آن‌ها به واسطهٔ این معاشرت‌ها، تکنیک‌ها و شگردهای مجرمانه، انگیزه، طرز فکر و

1. Online
2. External Reinforcement
3. Vicarious Reinforcement
4. Self Reinforcement
5. Computer-Mediated Communication (CMC)

توجیهاتی را که از ارتکاب نوع خاصی از عمل مجرمانه طرفداری می‌کند، مـی‌آموزنـد. در اینجا ذکر این نکته ضروری است که تصور عموم مردم آن است که هکرها و به‌طـور کلـی بزهکاران سایبری، از روابط عمومی سطح پـایین و حـداقل مهـارت اجتمـاعی برخـوردار هستند. در پاسخ باید بیان داشت که این تصورِ نادرست، ناشی از آن است که میزان مهارت افراد در ارتباط با دیگران تنها با معیار ارتباطات چهره به چهره سنجیده می‌شود؛ در حالی که چنانچه ارتباطات رایانه محور در تعریفِ جدید خود، از مهارت‌های اجتماعیِ طرفینی در نظر گرفته شود، آن تصور کلیشه‌ای کنار گذاشته خواهد شد (راجرز[1]، ۲۰۱۰، ص۲۲۴). از طرفی، آن‌ها در اتاق‌های گپ و شبکه‌های اجتماعی، افرادی بذله‌گو، فعال و دارای روابـط اجتماعی بسیار قوی هستند؛ در نتیجه کاربرانِ زیادی با آن‌ها دوست هسـتند. افـزون بـر این، همان‌طور که برخی نویسندگان اشاره کرده‌اند، «وضعیت تأهل[2]» می‌تواند شاخصـی برای میزان مهارت اجتماعی افراد باشد که این شاخص در بزهکاران سایبری به انـدازه‌ای است که کارآمدیِ اجتماعی آن‌ها را تأیید کند (دوراست[3]، ۲۰۰۵، ص۶).

ب) نظریهٔ رهایی اخلاقی: اگرچه این نظریه از دید صاحب‌نظران رشتهٔ جرم‌شناسی پنهان مانده است، اما می‌تواند به عنوان یکی از بهترین نظریه‌ها در علت شناسیِ رفتار بزهکـاران بکار رود.

– **تبیین عمومیِ نظریه:** این نظریه به نقش فرآیند موجه سازیِ رفتار منحرفانـه از سـوی بزهکاران اشاره دارد.[4] بندورا بر این باور بود که افراد ممکن است در بعضی شرایط نسبت به اصول اخلاقی بی‌اعتنا باشند. این نظریه بیانگر آن است افراد با اسـتفاده از فنـون مختلـف روان‌شناختی، به دنبالِ رهایی از عذاب وجدان و زدودن سرزنش عمومی از خـود هسـتند (مارش، ملویله، مورگان، نوریس و والکینگتن[5]، ۱۳۸۹، ص۱۴۴). بر طبق این نظریه، عموم

1.Rogers
2.Marital Status
3.Durost

۴. این نظریه شباهت زیادی با نظریهٔ فنون خنثی‌سازی ماتزا دارد؛ اما فرق عمدهٔ این دو رهیافت _ افزون بر این تفاوت که نظریهٔ بندورا برخلاف نظریهٔ ماتزا به تکنیک‌های روان‌شناختی می‌پردازد تا جامعه‌شناختی _ در آن است کـه در نظریهٔ ماتزا بزهکاران می‌دانند عملِ ناهنجار و ناسازگاری انجام داده‌اند و چنانچه توسط جامعه مؤاخذه می‌شـوند، سرِ پشیمانی تکان خواهند داد (صدیق سروستانی، ۱۳۸۶، ص۶۵)، اما در چارچوب نظریهٔ رهـایی از اخـلاق، فـرد تمـامیِ مکانیسم‌های خود، کنترلی خود را از دست داده است و حتی در صورت دستگیری همچنان منکر ناهنجار بودن عملِ خود می‌شود، پس به نوعی این افراد دارای شخصیت خوددوست دار (نارسیسم) هستند. بنابراین، اصلاح و بازسازگاری افراد دستهٔ دوم بسیار سخت‌تر است؛ زیرا «کسی که خوابیده است را می‌توان بیدار کرد، اما کسی که خودش را به خواب زده، هرگز!».

5. Marsh, Melville, Morgan, Norris and Walkington

افراد تمایل دارند تا از رفتارهایی که به معیارهای اخلاقیِ آن‌ها آسیب می‌زند، اجتناب کنند. چنانچه فرد این استانداردها را رعایت نکند، خود را محکوم و سرزنش می‌کند. این امر نشان می‌دهد که استانداردهای اخلاقی تا چه اندازه در تنظیم بخشیِ رفتار انسان مؤثر است. با این حال، این استانداردهای اخلاقی از «فاعلیت اخلاقی»[1] به دست می‌آیند و در مکانیسم‌های «خود نظم‌دهنده»[2] متجلی می‌شوند. مکانیسم خود نظم‌دهنده شامل سه زیرشاخهٔ اصلی یعنی خود نظارتی[3]، قضاوت[4] و خودواکنشی[5] است که به جهت اهمیت مکانیسم خود نظم‌دهنده، تنها به آن پرداخته می‌شود (راجرز، ۲۰۱۰، ص۲۲۵). تا زمانی که معیارهای اخلاقی در فرد نهادینه نشده باشند، سیستمِ خود نظم‌دهنده به درستی عمل نمی‌کند. به نظر بندورا ممکن است اخلاق درونیِ فرد در کنترلِ اعمالِ منحرفانه به یکی از دلایل زیر با شکست مواجه شود. در واقع، فرد به منظور آنکه بتواند خود را از قیود اخلاقی رها سازند، ممکن است به این توجیه‌ها متوسل شود: توجیه اخلاقی (مقایسهٔ آرام‌بخش)؛ نادیده یا ناچیز انگاشتن نتایج عمل؛ «انسانیت زدایی»[6] از بزه‌دیدگان (نسبت دادن سرزنش) و جابه‌جایی مسئولیت (بندورا، آلبرت، باربارانلیا، کلادیو، کپرارا، گیان و پاستورلیا[7]، ۱۹۹۶، ص۳۶۵). به نوعی در هریک از این تکنیک‌ها، فرد به دنبال آن است که با عملیات خودفریبی از احساس گناه و سرزنش درونی که از رفتارهای خلاف معیارهای اخلاقی ناشی می‌شود، رهایی یابد.

- **بزهکاری سایبری و رهاییِ اخلاقی:** همان‌طور که در بالا اشاره شد، افراد در شرایط عادی هیچگاه دست به اعمالی نمی‌زنند که باعث سرزنش و نکوهش آن‌ها شود؛ اما اگر در شرایطی، فرد آگاهانه یا ناآگاهانه توانست رفتار نادرستِ خود را توجیه کند، ارتکاب رفتار منحرفانه از جانب وی محتمل می‌شود. معمولاً بزهکاران سایبری، به منظور رهایی از این فشار درونی و برونی ممکن است عمل خود را یک ضرورتِ اجتماعی معرفی کنند. آن‌ها ممکن است با لبخند بیان کنند: «اگر ما نباشیم هیچ امنیتی وجود ندارد» و در این پوشش، رفتارهای خطرناک خود را توجیه می‌سازند. آن‌ها معتقدند «دولت یا شرکت‌ها،

1.Moral Agency
2.Self-Regulatory
3.Self-Monitoring
4.Judgment
5.Self-Reaction
6.Dehumanization
7.Bandura, Albert, Barbaranelli, Claudio, Caprara, Gian & Pastorelli

قربانیِ اعمال خود هستند؛ چراکه نباید تدابیر دفاعی امنیتی به‌گونه‌ای باشد که ما به راحتی بتوانیم به آن‌ها نفوذ کنیم». همچنین ممکن است کسانی که داستان‌های شهوانی یا فیلم‌های مستهجنِ خود را به اشتراک می‌گذارند، بیان کنند: «صرفاً دارم تجربه‌هام را انتقال می‌دم تا افراد فلان کار رو نکنن یا با انجام فلان کار از رابطهٔ جنسی خود بیش‌ترین لذت رو ببرن». از دیگر توجیهات متداول آن‌ها این است که چرا دولت‌ها باید مانع از جریان «آزاد اطلاعات[1]» باشند. آن‌ها در این زمینه ممکن است بگویند: «ما باید به منظور برچیدن این موانع گام برداریم و به همنوعان خود کمک کنیم» (فوتینگر و زیگلر[2]، ۲۰۰۵، ص۸).

روش‌شناسی تحقیق

در این تحقیق از روش کیفی تحلیل تم استفاده شده است. تحلیل تم روشی برای تعیین، تحلیل و بیان الگوهای (تم‌ها) موجود درون داده‌ها است. این روش، داده‌ها را سازمان‌دهی و در قالب جزئیات توصیف می‌کند؛ اما می‌تواند از این فراتر رفته و جنبه‌های مختلف موضوع پژوهش را نیز تفسیر کند (توماس[3]، ۲۰۰۳، ص۳۲). تم انتزاعی‌ترین سطح داده‌هاست که شکل گرفتن و انتخاب آن‌ها بستگی زیادی به ساختارهای تحقیق دارد (ریان[4]، ۲۰۰۳، ص۲۴). دلیل انتخاب روش تحلیل تم در تحقیق حاضر این بود که هدف تحقیق، شناسایی ایده‌هایی اولیه و عمیق برای توسعهٔ الگوهایی نظری برای تحقیقات تجربی آتی در حوزهٔ علل ارتکاب جرائم سایبری، براساس یافته‌های کیفی بوده است. اندرسون یک فرآیند پانزده مرحله‌ای را برای تحلیل تم ارائه می‌دهد (اندرسون[5]، ۲۰۰۷، ص۴۵). کلارک و براون[6] نیز فرآیند شش مرحله‌ای بدین منظور سامان داده‌اند که در این تحقیق از این رویکرد استفاده شده است.

مرحلهٔ اول- آشنایی با داده‌ها: برای اینکه محقق با عمق و گسترهٔ محتوایی داده‌ها آشنا شود، لازم است که خود را در آن‌ها تا اندازه‌ای غوطه‌ور سازد. غوطه‌ور شدن در داده‌ها معمولاً شامل بازخوانی مکرر داده‌ها به صورت فعال (جستجوی معانی و الگوها) است.

1.Freedom of Information
2.Pöttinger and Ziegler
3.Thomas
4.Ryan
5.Anderson
6.Clark and Brown

مرحلهٔ دوم- ایجاد کدهای اولیه: مرحلهٔ دوم زمانی شروع می‌شود که محقق داده‌ها را خوانده و با آن‌ها آشنایی پیدا کرده است. این مرحله شامل ایجاد کدهای اولیه از داده‌ها است. کدها یک ویژگی داده‌ها را معرفی می‌کنند که به نظر تحلیل‌گر جالب می‌رسد. داده‌های کدگذاری شده از واحدهای تحلیل (تم‌ها) متفاوت هستند. کدگذاری را می‌توان به صورت دستی یا از طریق برنامه‌های نرم‌افزاری انجام داد. در این مرحله، ۴۷۰ کد اولیه از مصاحبه‌ها احصاء شد.

مرحلهٔ سوم- جستجوی کدهای گزینشی: این مرحله شامل دسته‌بندی کدهای مختلف در قالب کدهای گزینشی و مرتب کردن همهٔ خلاصهٔ داده‌های کدگذاری شده است. در واقع محقق، تحلیل کدهای خود را شروع کرده و در نظر می‌گیرد که چگونه کدهای مختلف می‌توانند برای ایجاد یک تم کلی ترکیب شوند. در این مرحله، ۹۰ کد گزینشی توسط محققان به دست آمد و کدهای ناقص یا نامرتبط و همچنین کدهای تکراری کنار گذاشته شد تا به این تعداد کد گزینشی دست یافتند.

مرحلهٔ چهارم- شکل‌گیری تم‌های فرعی: مرحلهٔ چهارم زمانی شروع می‌شود که محقق مجموعه‌ای از تم‌ها را ایجاد کرده و آن‌ها را مورد بازبینی قرار می‌دهد. این مرحله شامل بازبینی در سطح خلاصه‌های کدگذاری شده است. در مرحلهٔ دوم، اعتبار تم‌های فرعی در رابطه با مجموعه داده‌ها در نظر گرفته می‌شود. در این مرحله، محققان به ۱۹ تم فرعی دست پیدا کردند.

مرحلهٔ پنجم- تعریف و نام‌گذاری تم‌های اصلی: مرحلهٔ پنجم زمانی شروع می‌شود که یک تصویر رضایت‌بخش از تم‌ها وجود داشته باشد. محقق در این مرحله، تم‌های اصلی را که برای تحقیق ارائه کرده، تعریف کرده و مورد بازیابی مجدد قرار می‌دهد، سپس داده‌های داخل آن‌ها را تحلیل می‌کند. به وسیلهٔ تعریف و بازبینی کردن، ماهیت آن چیزی که یک تم در مورد آن بحث می‌کند، مشخص شده و تعیین می‌شود که هر تم اصلی کدام جنبه از داده‌ها را در خود دارد. در این مرحله، محققان در نهایت پس از رفت و برگشت در میان تم‌های فرعی به چهار تم اصلی دست یافتند. در زیر، ۱۹ تم فرعی که تم‌های اصلی از آن‌ها استخراج شده، آورده شده است.

جدول ۱ – تم‌های فرعی و شکل‌دهی به تم‌های اصلی

ردیف	تم‌های فرعی	تم‌های اصلی
۱	گمنامی	عوامل مرتبط با فضای مجازی
۲	حس ایمن بودن	
۳	سهل‌الوصول بودن	
۴	فراگیر بودن	
۵	جذابیت‌های فضای مجازی	
۶	خود افشاگری اطلاعات	
۷	سرعت فوق‌العاده	
۸	برتری سود نسبت به هزینه	
۹	ویژگی فردی بزهکار	عوامل مرتبط با بزهکار
۱۰	ویژگی شخصیتی بزهکار	
۱۱	عدم آگاهی بزهکار از مسائل حقوقی	
۱۲	میزان دینداری بزهکار	
۱۳	ویژگی فردی بزه‌دیده	عوامل مرتبط با بزه‌دیده
۱۴	ویژگی شخصیتی بزه‌دیده	
۱۵	عدم آگاهی بزه‌دیده	
۱۶	میزان دینداری بزه‌دیده	
۱۷	میزان سواد رسانه‌ای بزه‌دیده	
۱۸	مسائل مرتبط با قانون	عوامل مرتبط با فضای فیزیکی
۱۹	ضعف در عملکرد سازمان‌ها و نهادها	

مرحلهٔ ششم- تهیهٔ گزارش: مرحلهٔ ششم زمانی شروع می‌شود که محقق مجموعه از تم‌های اصلی که کاملاً انتزاعی و منطبق با ساختارهای زمینه‌ای تحقیق در اختیار داشته باشد. این مرحله شامل تحلیل پایانی و نگارش گزارش است.

مشارکت‌کنندگان در تحقیق حاضر، ۱۶ نفر از قضات (باز پرسان و دادیاران) دادسرای جرائم رایانه‌ای (۹ نفر مرد و ۷ نفر زن) بودند که به روش هدفمند (نمونه‌گیری نظری)، با روش ارجاع زنجیره‌ای (روش گلوله برفی) انتخاب شدند. نمونه‌گیری نظری نوعی نمونه‌گیری هدفمند است که پژوهشگر را در خلق یا کشف نظریه یا مفاهیمی که ارتباط نظری آن‌ها با نظریهٔ در حال تکوین اثبات شده است، یاری می‌کند. در نمونه‌گیری نظری از رویدادها نمونه‌گیری می‌شود، نه لزوماً از افراد. اگر به سراغ افراد رفته می‌شود، با هدف کاوش رویدادها است؛ رویدادهایی که نشانگر تم‌های گوناگون مرتبط با پدیدهٔ مورد بررسی پژوهش هستند. ابزار مورد استفاده در این تحقیق مصاحبه‌های عمیق و نیمه ساختاریافته بود. قبل از انجام مصاحبه‌ها، به شکل حضوری یا تلفنی در مورد امکان انجام مصاحبه و زمان انجام آن هماهنگی شد. نهایتاً در زمان تعیین شده و در محل کار قضات، مصاحبه‌ها انجام شد. در ابتدای مصاحبه، به‌طور کلی هدف پژوهش ذکر شد و تأکید شد

که از مصاحبه‌ها تنها برای مقاصد پژوهشی استفاده خواهد شد و هویت افراد به هیچ وجه در گزارش‌های تحقیق و مقالات منتشر شده، مشخص نخواهد شد. با توجه به سؤال‌های تحقیق، سؤال‌های زیر در مصاحبه به عنوان سؤال‌های اصلی در نظر گرفته شد و با توجه به ماهیت نیمه ساختاریافته آن، سؤال‌های دیگری نیز با توجه به پاسخ‌ها و به منظور روشن‌تر شدن مفهوم پاسخ‌های ارائه شده طرح شد. برای ضبط صدای مصاحبه، کسب اجازه شد و در صورت مخالفت با ضبط صدای مصاحبه، صرفاً از نظرها یادداشت برداشته شد. در پایان هر جلسهٔ مصاحبه نیز از مصاحبه شدگان درخواست شد که چنانچه مطلب دیگری برای طرح دارند، اضافه کنند.

- ویژگی‌های فردی و شخصیتی بزهکار و بزه‌دیده چه تأثیری در ارتکاب جرائم سایبری دارد؟
- ویژگی‌های فضای مجازی چه تأثیری در ارتکاب جرائم سایبری دارد؟
- سواد رسانه‌ای چه تأثیری در ارتکاب جرائم سایبری دارد؟
- دینداری چه تأثیری در ارتکاب جرائم سایبری دارد؟

مدت زمان مصاحبه با قضات در مجموع ۸ ساعت و ۴۷ دقیقه بود. مصاحبه‌های انجام شده به روش نظام‌بندی که کلارک و برون (۲۰۰۶) توسعه داده‌اند و شرح آن در بالا گذشت، مورد تجزیه و تحلیل قرار گرفتند. لازم به ذکر است که کدهای استخراج شده یا مستقیماً در صحبت‌های مصاحبه شوندگان بیان شده بود یا کدهای تلویحی بودند که توسط پژوهشگر از متن مصاحبه‌ها استخراج شدند. برای اطمینان از روایی و پایایی داده‌ها به معیارهای خاص پژوهش کیفی، بررسی‌های لازم شامل مقبولیت و قابلیت تأیید صورت گرفته است (رضوی زاده و محمد پور، ۱۳۸۹، ص۴۸). جهت افزایش مقبولیت از روش‌های بازنگری توسط شرکت‌کنندگان استفاده شد و برای رسیدن به آن، محقق علاوه بر بازگرداندن گفتار و پنداشت‌ها در طول انجام مصاحبه توسط مصاحبه‌گران و تأیید یا اصلاح آن توسط آن‌ها، متن کامل تایپی و دست‌نویس، چهار مصاحبهٔ اول همراه با کدهای سطح اول به افرادی که از آن‌ها مصاحبه به عمل آمده بود، جهت تأیید یا اصلاح برگردانده شد که همگی مورد تأیید قرار گرفته و نکته‌های پیشنهادی آن‌ها در نظر گرفته شد. برای قابلیت تأیید، در مرحلهٔ پایانی، طبقات به دست آمده به سه نفر از مشارکت‌کنندگان اولیه به منظور بازبینی و تأیید برگردانده شد و نیز متن کامل سه مصاحبهٔ اولیه پیاده شده مجدداً توسط فرد متخصص دیگری کدگذاری شد و ضریب

اعتماد و پایایی سنجیده شد. با توجه به اینکه بالای ۸۰ درصد از کدگذاری‌ها مشترک بود، لذا این مقوله‌ها دارای قابلیت اعتماد هستند.

یافته‌های تحقیق

پس از انجام مصاحبه‌های عمیق و نیمه ساختاریافته با ۱۶ نفر از قضات (بازپرسان و دادیاران)، تمام کدهای موجود در مصاحبه‌ها که به نظر می‌رسید ارتباط مستقیم با موضوع تحقیق دارد، استخراج شد. پس از انجام فرآیند تحلیل تم، در نهایت محققان به چهار تم اصلی دست یافت که از جمله این تم‌ها، عنصر عوامل مرتبط با فضای مجازی یا «ویژگی‌های فضای مجازی» است که از دیدگاه قضات، عامل مهمی برای ارتکاب جرم سایبری محسوب شده است. این تم‌ها به شرح زیر انتزاع شد:

نمودار ۱ – چهار تم اصلی مؤثر بر ارتکاب جرم در فضای مجازی

۱- عوامل مرتبط با بزهکار: با بررسی متون مصاحبه، مضمون‌های فرعی عوامل مرتبط با بزهکار (ویژگی‌های فردی، ویژگی‌های شخصیتی، عدم آگاهی از مسائل حقوقی و میزان دینداری) شناسایی شد.

۱-۱- ویژگی‌های فردی

- **جنسیت:** «اگر بخواهیم تقسیم کنیم، جرائم علیه اموال به‌طور خاص شامل کلاهبرداری یا سرقت در این جرائم اکثراً از طریق مردان اتفاق می افته» {دادیار،۶.۵۳}؛ «خب ما الآن توی جرائم مالی بیشتر متهم‌ها، مردان هستند چه اونایی که هک می‌کنند و چه اونایی که پای دستگاه Atm حساب را خالی می‌کنند، مرد هستند؛ ولی از خانم‌ها برای پولشویی استفاده میشه، کارت‌های بانکی که خریداری میشه از خانم‌ها حالا با

پوششی که دارند برای خرید ارز برای خرید دلار برای خرید سکه برای مراجعه به دستگاه Atm از خانم‌ها بیشتر در این زمینه استفاده میشه» {بازپرس،۱۶.۵۵}.

- **سن:** «بیشتر مجرمان معمولاً در سنین ۲۰ تا ۳۰ سال هستند» { دادیار، ۲.۷۱ }؛ «اکثر کسانی که مرتکب جرم می‌شوند توی سنین پایین هستند؛ زیر ۳۰ سال. معمولاً بین ۲۰ تا ۲۵ سال هستند» { دادیار،۱۴.۵۴}.

- **تحصیلات:** «ما دو نوع جرم داریم؛ یه نوع جرم داریم که ذاتاً رایانه‌ای هست مثل هک. دسترسی غیرمجاز یعنی موضوع‌اش فضای مجازیه، ولی جرائم دیگه‌ای که رایانه وسیلهٔ ارتکاب جرمه مثلاً توهین از طریق رایانه، کلاهبرداری از طریق رایانه. این‌ها را میتونیم بگیم که مرتکبان از تحصیلات بالایی برخوردار نیستند. همون مرتکبانی هستند که توی فضای واقعی وجود دارند، ولی حداقل اش اینه که این ابزار را باید در دسترس داشته باشن؛ یعنی سواد ابتدایی داشته باشند. ولی در مورد جرم هک و کلاهبرداری حتماً باید به لحاظ فنی اشراف و تسلط داشته باشه هک و کلاهبرداری کار هر کسی نیست» {دادیار،۶.۵۳}.

- **بیکاری:** «شما در نظر بگیرید جوانان بیکارند. همش سرشون توی گوشی هست. خب دور و برمون جوان داریم توی خانواده هامون. میان چهار تا عکس به اون میفرستن دو تا فحش به اون میدن و این میشه سرآغاز یک سری داستان‌های اون جوری ...» {دادیار، ۱۴.۵۴}؛ «بیکاری جوان‌ها و استفاده زیاد و چرخیدن زیاد توی فضای مجازی یکی از عوامل ارتکاب می تونه باشه» {دادیار، ۵.۶۶}.

۱-۲- ویژگی‌های شخصیتی

- **باهوش در جرائم اقتصادی:** «کلاهبرداری‌های اینترنتی، دسترسی‌های غیرمجاز، اینها یک سری افرادی هستند که از یک سری دانش خاصی برخوردار هستند یا هک‌هایی که انجام می‌دهند افراد باهوشی هستند» {بازپرس، ۱۵.۵۶}؛ «جرمی مثل هک یا دسترسی غیرمجاز، افرادی که باهوش هستند توسط این افراد اتفاق میافته» {دادیار، ۷.۶۷}.

- **خودنمایی:** «ممکنه در جرائم سنتی یکی فقیر باشه بره دزدی یا سرقت کنه، ولی در فضای مجازی بعضی‌ها ممکنه یه خانواده پولداری هم داشته باشه، ولی حالا همین جوری برای اینکه خودش را نشون بده، بره سازمان سنجش را هک کنه، بانک را هک کنه، همین جوری. مثلاً میخواد خودش را به اثبات برسوند ...» {دادیار، ۹.۵۹}؛ «برخی از جرائم مثلاً دسترسی غیرمجاز و هک و غیره یک مقدار میشه گفت سوءنیت از اشخاص

نیست؛ بحث کنجکاویه، طرف میخواد خودش را به رخ بکشد. در این فضا حتی برخی برنامه‌ها در تلویزیون هم اینها را به عنوان نخبه معرفی می‌کنند. همهٔ اینها باعث می‌شوند که به این سمت بیایند» {دادیار، ۱۰.۶۱}.

- **انتقام‌جویی:** «یه علل روانی هم هست به نظر من. افرادی هستند که با مشکلات روانی انتقام‌جویی می‌کنند در اینترنت، عکس‌های دیگران را پخش می‌کنند به دلیل عقده‌هایی که دارند» {دادیار، ۷.۶۷}؛ «... انتقام در فضای مجازی از مهم‌ترین علل ارتکاب جرائم سایبری است» {دادیار، ۱۳.۶۵}.

- **کنجکاوی و علاقه به تجربه کردن جرم:** «خیلی وقت‌ها هم اون طور که ما در پرونده‌ها می‌بینیم فقر نیست، یه کنجاویه یا ابراز قدرت که مثلاً من تونستم دسترسی پیدا کنم به حساب فلان کس» {دادیار، ۱۲.۶۵}؛ «ویژگی‌های شخصیتی مجرمان و حس کنجکاوی در فضای مجازی از مهم‌ترین علل ارتکاب جرائم سایبری است» {دادیار، ۱۳.۶۵}؛ «... بعضی‌ها می‌خوان تجربه‌ای داشته باشند، مثلاً میگن اگر در تلگرام چهار تا فحش بدیم مگه چه اتفاقی می افته ...» {دادیار، ۱۴.۵۴}.

۱-۳- عدم آگاهی از اطلاعات حقوقی: «ما به عنوان کاربر نمی دونیم که وقتی می‌آییم توی این فضا چه چیزهایی را باید رعایت کنیم چه چیزهایی جرم هست؛ برای مثال در حالت عادی تصویر مستهجن نشان دادن جرم نیست، کما اینکه در قانون ما نگهداری تصاویر مبتذل جرم نیست؛ یعنی اگر من در کیفم ده تا عکس مستهجن داشته باشم جرم نیست، اگر به یه طریقی از کیفم در بیارم بیرون در جلوی دید شما قرار بگیره، به نوعی عمداً و عامدانه باشد، بازم جرم نیست؛ ولی اینو وقتی برای شما بفرستم جرم هست. خب نمی دونند افراد اینها رو، وقتی در غالب انتشار و ارسال باشد، جرم است» {دادیار، ۱۴.۵۴}؛ «... افراد متشخص میایند و چون سواد حقوقی ندارند، میگه من نمی‌دونستم که این مسئله جرمه» {دادیار، ۱۲.۶۵}.

۱-۴- میزان دینداری: «توی فضای فیزیکی همین روبروشدن با مردم، حیائی که هست همین عامل بازدارنده است؛ توی فضای مجازی اینجوری نیست. اگر بحث اخلاق و دین نباشه خدا را در نظر نگیره فکر میکنه هر کاری میتونه انجام بده، کسی هم نیست که جلوش را بخواد بگیره. فضای واقعی اگر دعوایی بشه حالا بقیه دخالت می‌کنند جلوش را می‌گیرند، ولی توی این فضا کسی نیست که جلوش را بگیره» {دادیار، ۱۰.۶۱}؛ «کسی که واقعاً معتقد قلبی باشد اصلاً مرتکب جرائم سایبری نمیشه؛ چون مرتکبان ما یا

علیه اموالش که مؤمن هیچ‌وقت نظر به مال مردم نداره. حتی شبهه دارش هم نمی پـذیره یا ناظر به ناموس و آبروی مردم است که از نظر مؤمن اگر فرد آبروی شخصی را ببره انگار خونش را ریختی، انگار کشتی‌اش. به نظر من مؤمن قلبی یک عامل بازدارنـده قـوی داره که بخواد مرتکب جرائم در کل و علی‌الخصوص سایبری که جـرائم سـایبری یـا مـال یـا آبروی مردم را هدف قرار می‌ده که همه اینها در دین ما امری ناپسـند اسـت» {دادیـار، ۱۴.۵۴}.

۲- عوامل مرتبط با بزه‌دیده: با بررسی متون مصـاحبه، مضـمون‌هـای فرعـی عوامـل مرتبط با بزه‌دیده (ویژگی‌های فردی، ویژگی‌های شخصیتی، عدم آگاهی، میزان دینداری، میزان سواد رسانه‌ای) شناسایی شد.

۲-۱- ویژگی‌های فردی

- **جنسیت:** «اگر بخواهیم رقم سیاه را هم در نظر بگیرم اصطلاحاً اینکـه بـه‌طـور واقـع، میزان جرائم در بطن جامعه وجود دارد فکر می‌کنم جرائم در بین زنان و مردان یکسـان است؛ منتها توی دادسرا بیشتر شکایت از جانب خانم‌ها مطرح میشه. به خـاطر اینکـه از نظر جنسی بیشتر در معرض هستند به خصوص در کیس های اخلاقی» {دادیار، ۶۶ }؛ «... زنان اغلب به عنوان مجنی علیه در پرونده‌های رایانه‌ای ظهور پیدا می‌کنند» {دادیار، ۶۵}.

- **تحصیلات:** «... مثلاً جرائم کلاهبرداری‌های کارت به کارت که در قرعه‌کشی مردم را به پای دستگاه خودپرداز می‌کشانند؛ ما پزشک داشتیم که رفته پای دستگاه خـودپرداز یـا خود وکیل‌ها بودند که بزه‌دیده واقع شدند، نادرند؛ ولی خب باسواد بودنشون باعث میشه که کمتر بزه دیده بشوند» {دادیار، ۷.۶۷}.

- **بیکاری:** «الآن شما اگر بستریابی بکنید علت بیشتر جرائم، بیکـاری افـراد هسـت چـه خانم‌ها و چه آقایـان در دام افتـادن. اونیکـه مجـرم حرفـه‌ای هسـت، طعمـه هاشـون را شناسایی می‌کنند، اونایی که طعمه و مجنی علیه فضای مجازی هستند بیش‌ترین عامل اش بیکاریه» {بازپرس، ۱۶.۵۵}.

۲-۲- ویژگی‌های شخصیتی

- **ساده‌لوحی:** «یه سری افراد داریم زودباورند؛ خیلی ببخشید ساده‌لوح هسـتند. در ایـن جور افراد زمینهٔ ارتکاب جرم بالاتر است. افرادی که تیزترند هر چیزی را کنکاش می‌کنند تا به واقعیت اش برسند بدونند آیا واقعاً این مطلب و موضـوعی کـه اومـده صـحت داره،

نداره؟ از کجا اومده؟ یه سری از افراد را داریم هر مطلبی که میاد مـی‌پذیرنـد» {دادیـار، ۵۴}.

- **سهل‌انگاری:** «تـوی خیلـی از پرونـده‌هـا مـی‌بینـیم کـه ریشـهٔ اصـلی ارتکـاب جـرم سهل‌انگاری شخص بزه‌دیده و کم آگاهی است. از این منظر که در سایتی ثبـت‌نـام کنـد وجهی را پرداخت کند به صورت آنلاین. بر اثر سهل‌انگاری، آگاهی کم چه‌بسا مورد حملهٔ فیشینگ قرار بگیرد و بالطبع وقتـی کـه بـه عنـوان مثـال، اطلاعـاتش از طریـق مجـرم کپی‌برداری می‌شود ...» {دادیار، ۲.۷۱}.

- **خودنمایی زنان:** «الآن در خانم‌هـا خـود نمـایی بـروز و ظهـورش بیشـتر پیـدا کـرده؛ تصاویری از خودشون در پروفایل‌ها چه تو اینتسا و تلگـرام مـی‌گذارنـد و اون تصـاویر در دسترس دیگران قرار می‌گیرد و مورد سوء استفاده قرار می‌گیرد و نهایتاً منجر به شکایت میشه در حالی که ریشه‌یابی می‌کنی، خودشون مقصرند، خودشـون بـر علیـه خودشـون اقدام کردند، اون تصویر اون فیلم یا مطلب را که نباید توی فضای مجازی قرار می‌دادنـد، قرار دادند و در نهایت منجر شده کـه طعمـهٔ قـرار بگیرنـد و مجنـی علیـه واقـع بشـن» {بازپرس، ۱۶.۵۵}.

۲-۳- میزان دینداری: «... کسی که رعایت می‌کند حجابش را. نتیجتاً این میشـه کـه عکسشو نمیزاره روی پروفایلش. نتیجه این میشه کـه کسـی از عکسـش سـوء اسـتفاده نمی‌کنه» {دادیـار، ۵.۶۶}. «افـراد متـدین کمتـر عکـس‌هاشـون را انتشـار مـی‌دهنـد، حواسشون هست به این چیزها؛ ولی افرادی که آزادترند خیلی راحـت عکـس‌هاشـون را میزارند و بعد که این اتفاق می افته میرن شکایت می‌کنند» {دادیار، ۷.۶۷}.

۲-۴- میزان سـواد رسـانه‌ای: «یـه اصـل کلـی هسـت کـه معمـولاً فـرد مجـرم از نقطه‌ضعف‌های بزه‌دیده استفاده می‌کنه و الآن مثلاً در بحث هک فرد بزهکـار یـه سـری بدافزار را برای مخاطبش ارسال می کنه، خـب اگـر طـرفش وارد باشـه اون فایـل را بـاز نمی‌کنه و اجازه دسترسی‌ها را به اون نمیده. مطلبی که هست معمولاً اینها میان متهمان توی فضای مجـازی میشـه گفـت سـورپرایزهایی را مـی‌دهنـد یـا یـه وعـده‌هـای پـوچ ترغیب‌کننده در غالب اینکه اگر فایل را باز کنی عکس و فیلم فلان هنرمنـد مشـهور یـا امثال این یا در غالب استخدام در فلان شرکت را وعده می‌دهند یا دانلود رایگان فایلی را که طرف ترغیب بشه فایل را باز کنه. بـاز کـردن فایـل همانـا و در دادم افتـادن همانـا» {بازپرس، ۱۶.۵۵}؛ «خیلی از افراد نمی دونند که چی دارن کلیک می‌کنند یا مثلاً هک

شدند متوجه نشدند اطلاعاتشون در اختیار خیلی‌ها قرار گرفته یا بعضی‌ها حتی وقتی گوشی اپل می‌خرند اپل آیدی شون را یکی دیگه براشون فعال می‌کنه و اینها آگاهی ندارند که برن رمزشو عوض بکنند و بعد طرف از اطلاعات تمام گوشی استفاده می کنه؛ بعد متوجه می‌شوند» {دادیار، ۷.۶۷}.

۲-۵- عدم آگاهی: «... جرائمی که بحث اخلاقی هست، بحث انتشار فیلم‌های خصوصی هست، ناشی از عدم اطلاع مردم است که اعتماد می‌کنند و عکس‌ها و فیلم‌ها را در اختیار می‌گذارند یا اینکه اجازهٔ دسترسی افراد را به گالری تلگرام می‌دهند...» {بازپرس، ۱۵.۵۶}؛ «اینکه که مردم ما در اثر ناآگاهی یا اثر هر چیزی که توی ذهنشونه خودشون را در معرض جرم قرار می‌دهند؛ مثلاً عکس‌های مختلف و زیبا از عروس‌ها یا یه خانم عکس‌هایی با آرایش مختلف خودشو بزاره توی پروفایلش. خود بزه‌دیده هم به نظر من می تونه یکی از عوامل باشه... » {دادیار، ۷.۶۷}.

۳- عوامل مرتبط با فضای مجازی: طبق تجربه‌های بیان شده توسط قضات، این تم یا مضمون اصلی یعنی عوامل مرتبط با فضای مجازی از عوامل تعیین کنندهٔ ارتکاب جرم در فضای مجازی است. مضمون‌های فرعی آن شامل گمنامی، حس ایمن بودن، سهل‌الوصول بودن، فراگیر بودن، جذابیت، خودافشاگری اطلاعات، سرعت فوق‌العادهٔ ارتکاب جرائم و برتری سود نسبت به هزینه در ارتکاب جرائم بود.

۳-۱- گمنامی در فضای مجازی: «فضای مجازی خاصیتی داره که اهل فن میگن که ۹۴ درصد این فضا بهش فضای تاریک میگن؛ یعنی فضای ناشناخته، یعنی فرد توی این فضا میتونه مرتکب جرم بشه و شناخته نشن» {دادیار، ۶.۵۳}؛ «ویژگی که فضای مجازی داره این هست که شخص خودش را میتونه نامشخص نشون بده. هویت‌اش را معلوم نکنه، الآن شما راحت می‌تونید یک صفحهٔ اینستاگرام بسازید یا ایمیل مجهول و هزاران تبلیغ مالی بکنید و میتونید با vpn کشورهای همسایه، هزاران میلیارد تومان پول را جابه‌جا کنید و قابل شناسایی نباشید» {دادیار، ۱.۷۰}.

۳-۲- حس ایمن بودن فضای مجازی: «... فضای مجازی یک فضایی است که مجموعه عواملی درگیر این فضا می‌شوند که حس ایمن را پیدا می‌کنند که از ارتکاب این جرائم شناسایی نمی‌شوند یا حداقل شناسایی آن‌ها کمی سخت‌تر از جرائمی هست که در فضای واقعی و عادی رخ می‌دهد؛ به عنوان مثال هکر وارد سیستم رایانه‌ای می‌شود با هویت نامعلومی دسترسی غیرمجاز پیدا می‌کند، سرقت می‌کند و مورد تخریب قرار

می‌دهد، هکر در واقع ناشناخته است و این یقین را دارد تا بخواد از طریق سیستم و مجموعهٔ قضایی مورد شناسایی قرار بگیرد، حداقل یک زمانبندی وجود دارد... » {دادیار، ۲.۶۸}.

۳-۳- سهل‌الوصول بودن فضای مجازی: «مردم به راحتی و سهولت در سریع‌ترین زمان به بسیاری از اطلاعات و بسیاری از چیزهایی که مد نظرشون هست دسترسی پیدا کنند و این ویژگی سریع دسترسی به اطلاعات و با توجه به اینکه اپراتورها خدماتشون را قیمت هاش را پایین آورده بسته‌هایی که ارائه می‌دهند بسته‌های ارزونی هست، مردم تشویق می‌شوند به خرید بسته‌های اینترنت و دسترسی پیدا کردن به اطلاعات روز تو هر زمینه‌ای هرکسی بسته به علاقه خودش و این اشتیاق و عدم اطلاع باعث ارتکاب جرم خواسته و ناخواسته بشوند» {بازپرس، ۱۶.۵۵}؛ «یکی از عواملی که الآن خیلی‌ها به فضای مجازی روی آوردند، آسان بودن دسترسی به آن و ارزان بودن آن. تقریباً میشه گفت رایگانه و تبادل اطلاعات در سریع‌ترین زمانه و از کل دنیا می تونید اطلاعات را بگیرید» {بازپرس، ۸.۵۱}.

۳-۴- فراگیر بودن فضای مجازی: «فراگیر بودن این فضا، چون الآن خیلی از مردم ایران، نه‌تنها ایران کشورهای دیگر هم از این فضا در همهٔ امور استفاده می کنن. چه در امور شخصی و همه چیز» {دادیار، ۲.۷۱}؛ «این فضا فضای بی‌نهایت است، شما محدودیت و قالبی نمی تونید براش در نظر بگیرید» {دادیار، ۱۲.۶۵}.

۳-۵- جذابیت‌های فضای مجازی: «فضای مجازی جذابیت داره» {بازپرس، ۱۶.۵۵}؛ «با توجه به موضوعات پرونده‌هایی که داشتم و ارباب‌رجوع‌هایی که داشتم به خاطر جذابیت‌هایی که فضای مجازی داره افراد جذبش میشن». {دادیار، ۱۱.۶۷}

۳-۶- خودافشاگری اطلاعات در فضای مجازی: «خود افشاگری اطلاعات در فضای مجازی و عدم دانش اطلاعات فنی و حفاظتی جهت نگهداری رمز عبور در جرائم کلاهبرداری رایانه‌ای و انتشار اسرار خصوصی شاکی می‌تواند از مهم‌ترین علل ارتکاب جرائم باشد» {دادیار، ۱۳.۶۵}.

۳-۷- سرعت فوق‌العادهٔ ارتکاب جرائم در فضای مجازی: «یکی از ویژگی‌هاش، نشر لحظه‌ای و حداکثری است که توی فضای مجازیه؛ این هم خیلی مؤثره. مثلاً نشر اکاذیب الان دیگه خیلی از فضای فیزیکی استفاده نمی کنه؛ چون میدونه که توی فضای رایانه‌ای هرچی که بزاره سریع از اون کپی می‌گیرند و توی گروه یا کانال همه می‌بینند، این

ویژگی‌اش به نظرم میتونه» {دادیار، ۵.۶۶}.

۳-۸- برتری سود نسبت به هزینه در ارتکاب جرائم مجازی: «... ما از نظر حقوق اقتصادی می تونیم بگیم بزهکار حقوق کاست بنفیت[1] ارتکاب جرم را در ابتدا در نظر می‌گیرد؛ هزینه ارتکاب جرم براش چقدر هست؟ و در کنارش چقدر منفعتی را می‌برد؟ توی فضای مجازی فردی که بزهکار است با هزینه و فایده‌ای که در ذهنش و منطق عقلایی‌اش در نظر می‌گیرد، به این نتیجه می‌رسد که با توجه به اینکه امکان شناسایی آن سخت‌تر است، پس مزایای ارتکاب جرم برای اون در این فضا بهتر میسر است تا اینکه بخواد از طریق فضای واقعی مرتکب فضای واقعی بشود» {دادیار، ۳.۶۸}.

۴- عوامل مرتبط با فضای فیزیکی: مضمون‌های فرعی عوامل مرتبط با فضای فیزیکی (مسائل مرتبط با قانون، ضعف در عملکرد سازمان‌ها و نهادها) شناسایی شد.

۴-۱- مسائل مرتبط به قانون

- **خلأ قانونی:** «قانون و قانون‌گذار رسالت اصلی‌اش این هست که مفاهیم و جرائمی که در این حوزه است را به‌طور اخص مورد قانون‌گذاری قرار بدهد. الآن مثلاً ما در توهین در فضای مجازی مادهٔ قانونی توی جرائم رایانه‌ای نداریم، بلکه به قانون تعزیرات قانون مجازات بخش مجازات استناد می‌کنیم، در حالی که می‌توانست قانون‌گذار قانون جرائم رایانه‌ای را به‌طور خاص و اخص موضوع توهین در فضای مجازی را مورد قانون‌گذاری قرار بگیرد یا حتی از نظر من یک سری شفاف‌سازی‌هایی در هر یک از مواد خیلی مؤثر هست، حداقل برای کسی که به عنوان قاضی می‌خواهد استنباط حقوقی از مواد قانونی داشته باشه با صراحت قانون‌گذار و عدم ابهام واژگانی که در تصفیهٔ مواد استفاده می‌شود خیلی مؤثر است این موضوع» {دادیار، ۳.۶۸}.

- **به‌روز نشدن قوانین:** «... قوانین باید به‌روز بشه؛ هم‌زمان با جرائمی که داره پیش میاد خودشو به روز کنه. ما متأسفانه عادت نداریم قوانینمون را به‌روز کنیم. لازمه که نمایندگان مجلس قوانین را به روز کنند، قوانین از سال ۱۳۱۰ اجرا میشه. آدم‌هایی که با این پرونده‌ها سروکار دارند اونها باید کمک کنند تا بروز بشه» {دادیار، ۱۲.۶۵}.

- **متناسب نبودن جرم و مجازات:** «بخشی از جرائم ما برمی گرده به مصوبات مجلس ... برای مثال کلاهبرداری سنتی ما یه ماده قانونی داریم که مجلس تصویب کرد؛ شورای

1.CAST Benefit

نگهبان اختلاف کرد و نهایتاً این موضوع به تشخیص مصلحت نظام رفت. در تشخیص مصلحت نظام ما قانونی داریم قانون تشدید مجازات مرتکبین ارتشاء، اختلاس و کلاهبرداری، اونجا اومده گفته که فردی که مرتکب کلاهبرداری میشه یک تا هفت سال زندان. خب اگر این ماده قانون را در قوه قضائیه بخواهیم برای کلاهبردارها پیاده کنیم کسی که هزار تومان کلاهبرداری کرده از حیث مجازات حبس اش یک تا هفت سال زندان است؛ کسی که صدها میلیون تومان کلاهبرداری هم کرده باشه باز یک تا هفت سال زندان داره؛ بنابراین قاضی مخیره که یک تا هفت سال زندان را برای فرد مرتکب در نظر بگیرد. خب این نشون میده که این قانون، قانون کارشناسی شده‌ای نبوده. قانون باید همه ابعاد را ببینه، همه ظرفیت‌ها و همه رفتارها را ببینه و بعد به صورت قانون اجرا بشه» {بازپرس، ۸.۵۱}.

۴-۲- ضعف در عملکرد سازمان‌ها و نهادها

- **آموزش عملی بزهکاری در صدا و سیما:** «صداوسیما خیلی راحت در فلان قرعه‌کشی همراه اول میگه شرکت کنید؛ واقعاً این همه جرمی که به وجود اومده از صداوسیماست دیگه. برنامه میزاره بعد از توی برنامه زنگ می‌زنند؛ این‌ها همه تعلیماتی که می‌دهند و مردم را ترغیب می‌کنند» {دادیار، ۱۱.۷۰}.

- **عدم انطباق برنامه‌های صداوسیما با موازین قانونی و حقوقی:** «... شبکهٔ خبر برنامه‌ای را گذاشته در خصوص فضای مجازی که با مردم مصاحبه می‌کنند که جعل هویت جرمه. بعد مردم هم میگن نمی دونیم آره جرمه. کجا جرمه؟ جرم نیست جعل هویت در فضای مجازی جرم نیست. ما جعل داده و جعل عناوین داریم، ولی جعل هویت نداریم...» {دادیار، ۱۲.۶۵}.

- **عدم کنترل و نظارت:** «در خیلی از موارد چون تحریم‌ایم، چون سرورها ایران نیست، محدودیت‌های فنی داریم که متأسفانه چون نمی دونیم اونور قضیه چه اتفاقی افتاده، IPهایی که استفاده میشه vpn هست و غیرقابل ردیابی هست؛ این‌ها واقعاً نشان‌دهندهٔ اینه که بستر لازم فراهم نشده، بعد ما اومدیم این امکانات را به مردم دادیم، بدون اینکه بیاییم بستر نظارتی را فراهم کنیم؛ قشنگ کلی امکانات کلان را دادیم بدون اینکه نظارتی وجود داشته باشه» {دادیار، ۱۲.۶۵}.

- **عدم همکاری سازمان‌های بین‌المللی:** «... ضمن اینکه کشورهای دیگر در بحث نیابت قضایی واقعاً همکاری نمی‌کنند؛ حتی چین که ما این همه بازارمون به کالای چینی باز

هست، جرائمی که از اون کشور به وقوع می‌پیوندد، ما وقتی نیابت می‌دهیم برای شناسایی متهم، نیابت بدون اقدام بر می‌گردد. میتونم بگم کشورهایی که با ما تو این زمینه معاضدت دارند انگشت‌شمارند؛ در تعاملات جهانی می طلبه که توی این زمینه کار بشه» {دادیار، ۶.۵۳}.

- **عدم دسترسی مراجع انتظامی و قضایی به data base و شناسایی سرورها و آی‌پی‌ها:** «مشکل اصلی که داریم اینه که ما اکثر اپلیکیشن ها و نرم‌افزارهایی که وسیلهٔ ارتکاب جرم میشه، دیتا بیس‌اش در ایران نیست، ما نمی‌تونیم به دیتا بیس این نرم‌افزارها دسترسی پیدا کنیم و همین عدم دسترسی به این دیتا بیس‌ها باعث شده که خیلی از متهمین به این امید که شناخته نمی‌شوند بیان مرتکب بشن» {دادیار، ۶.۵۳}.

- **ضعف شرکت‌های خدمات ارتباطی (ایرانسل و همراه اول) و بانک‌ها:** «شرکت‌های خدمات ارتباطی و بانک‌ها در زمان ارائه خدمت احراز هویت نمی‌کنند...» {دادیار، ۶.۵۳}؛ «جرائم اقتصادی به خاطر ضعف سیستم بانکی است و حساب‌های افراد خالی میشه و بانک هیچ مسئولیتی نداره» {بازپرس، ۱۵.۵۶}؛ «این شرکت‌های همراه اول و ایرانسل همشون مقصرن، این بانک‌ها خیلی راحت افتتاح حساب می‌کنند با مدرک یکی دیگه. اصلاً توجه نمی‌کنند...» {دادیار، ۷.۶۷}.

- **ضعف اطلاع‌رسانی:** «ارگان‌هایی می‌توانند اطلاع‌رسانی کنند که کار به دادگستری نکشه؛ دادگستری داره منفجر میشه از پرونده. دادسرای ما را اگر با دو سال پیش مقایسه کنید، واردهٔ من چندین برابر شده، خیلی زیاد شده» {دادیار، ۱۴.۵۴}؛ «اگر صداوسیمای ما بیاد در خصوص آفت‌های فضای مجازی و فرصت‌های فضای مجازی اطلاع‌رسانی دقیق و کارشناسی شده انجام بده، قطعاً در رفتارهای کاربران ما بسیار مؤثر است؛ هم در رفتارهای مجرمانه و هم در رفتارهای به سمت تعالی و خدمات‌رسانی» {بازپرس، ۸.۵۱}.

بحث و نتیجه‌گیری

افزایش میزان بروز اتفاقات در دنیای مجازی و نگرانی جامعهٔ جهانی از تهدیدهای آیندهٔ جهان در خصوص میزان ارتکاب جرائم سایبری و تبعات و آثار منفی و مخرب فرهنگی این محیط، همچنین مداقه در شناخت علل و عوامل شکل‌گیری جرائم سایبری و شکل‌دهی تدابیر واکنشی متناسب با خصوصیات این فضا، از دلایل و اهمیت تدوین این مقاله محسوب می‌شود. لذا این نوشته، با نگاه بین‌رشته‌ای به دنبال شناخت و بررسی عوامل

مؤثر بر ارتکاب جرم در فضای مجازی از دیدگاه قضات دادسرای جرائم رایانه‌ای تهران به روش کیفی بود.

بیش‌ترین عاملی که قضات به آن اشاره کردند ویژگی‌های فضای مجازی بود. اساساً برخی از علل اساسی ارتکاب جرم در فضای مجازی، مربوط به مختصات و زیرساخت‌های سخت‌افزاری و نرم‌افزاری فضای مجازی است؛ ویژگی‌هایی همچون گمنامی، دیجیتالی بودن، مبتنی بر زمان مجازی بودن، جهانی بودن، سرعت، فراگیری، سیالیّت، تشدید شدگی، متکثر بودن و درنهایت همه جا حاضر بودن، خود به خود فضایی را ایجاد می‌کند که اثرات اولیه و ثانویهٔ آسیب در جهان دوفضایی را تشدید و تقویت می‌کند. گمنامی و ناشناختگی از اصول حاکم بر جرائم جهان مجازی است. نامرئی بودن این امر را به افراد می‌دهد که به هرکجا می‌خواهند، سرک بکشند و کارهایی انجام دهند که در دنیای واقعی انجام نمی‌دهند. فضای مجازی علاوه بر ابزار قوی برای ارتکاب جرم، فرصت‌های ارتکاب را نیز افزایش می‌دهد. فضای سایبر، بسیاری از امور خرد و کلان اجتماعی را در امن‌ترین، خلوت‌ترین و راحت‌ترین موقعیت، در مقابل دیدگان افراد قرار می‌دهد. این فرصت مغتنم در کنار دیگر شرایط مهیا، حتی کسانی که متعهد به رعایت هنجارهای اجتماعی هستند را وسوسه می‌کند تا روحیات پلیدشان را بروز دهند. لذا به عقیدهٔ عده‌ای، این فضا مصداق بارز بهشت امن هنجارشکنان است. سایبر یک فضای سیال است که هیچ‌گونه حدومرزی را نمی‌شناسد و از مرزهای جغرافیایی واقعی در آن خبری نیست. طبیعی است که مجرمان با تأسی از این نقطه‌ضعف‌ها، فرصت ارتکاب جرائم بیشتر و انتخاب‌های کلان‌تری نیز دارند.

از ویژگی‌های دیگر این فضا براساس نظرات قضات، سهل‌الوصول بودن و سرعت ارتکاب جرائم است. مجرمان سنتی اغلب در فرآیند گذار از اندیشه به عمل و ارتکاب یک جرم تام، زمان و فاصلهٔ زیادی را طی می‌کردند. شاید یکی از عوامل کندی وقوع پدیدهٔ بزهکارانه در جهان واقعی، بعد مکانی میان سه ضلع بزهکاری یعنی بزهکار، آماج بزه و مکان ارتکاب بزه است. حال‌اینکه، ساختار فضای مجازی به‌گونه‌ای است که در آن قرابت مکانی میان سه عنصر فوق ضرورتی ندارد. لذا امروزه به مدد فناوری‌های نوین، مرتکب اغلب با یک کلیک می‌تواند به عرصهٔ ارتکاب جرم راه پیدا کند، مثلاً در ارتکاب جرم کلاهبرداری دیگر به عوامل و ارکان خاص این جرم در دنیای فیزیکی از جمله مانورهای خاص متقلبانه و تعاملات رو در روی افراد با هم نیازی نیست؛ چراکه سایبر امکان بردن

اموال دیگری را به‌سادگی فشردن تنها چند کلید و انجام عملیاتی پیش پا افتاده ممکن ساخته است. در فضای سایبر، پایبندی کم‌تری به محدودیت‌های زمانی و مکانی دیده می‌شود. این وضعیت اساساً به رشد چشم‌گیر فناوری اطلاعات و ارتباطات الکترونیکی مربوط می‌شود. جوامع شبکه‌ای این امکان را فراهم آورده‌اند تا زمان و مکان محو شوند. یک تراکنش متقلبانه می‌تواند از هزاران مایل و در کسر هزارم ثانیه ارتکاب یابد و در عین حال، یک آزارگر می‌تواند بزه‌دیدهٔ خویش را از فاصلهٔ بسیار دور و به صورت زنده، آماج گفتار تمسخرآمیز خویش قرار دهد.

مهم‌ترین خصیصهٔ فضای سایبر، فراگیری یا به عبارت بهتر، فرامرزی بودن است. شبکه‌های پیشین به صورت محلی یا حداکثر منطقه‌ای قابل بهره‌برداری بودند؛ اما به مدد سیستم‌های بی‌سیم و با سیم، نظیر شبکه‌های ماهواره‌ای یا خطوط فیبر نوری، این امکان فراهم شده است. ویژگی‌های فضای مجازی همچون گمنامی در اینترنت با مطالعات رنون (۲۰۰۶) نیز مطابقت دارد. بزهکاران تلاش می‌کنند تا از ویژگی‌های فضای مجازی به عنوان ابزاری برای تخلیهٔ عاطفی و جنسی و غیره استفاده کنند. اما در سوی دیگر می‌توان از عللی نام برد که به زیرساخت و مختصات فضای مجازی ارتباط ندارد و به تجربهٔ کاربران و در حقیقت، تجربهٔ زیستی افراد باز می‌گردد. کاربران (بزه‌دیده و بزهکار)، عوامل اصلی تحرکات اطلاعاتی، فکری و خلاقانه در فضای مجازی هستند. گرایش‌ها و تجربه‌های زیستی فکری بزهکار و بزه‌دیده به شدت بر فضای مجازی اثرگذار است. جنس، سن، بدبینی، خودپسندی، خودخواهی، نفرت، کینه، جنون ثروت، جنون اخلاقی، انتقام، اعتقادات یا گرایشات خاص از عوامل فردی است که با توجه به وضعیت زیستی – روانی فرد، وی را متمایل به انجام یک رفتار خلاف هنجار می‌کند؛ به عنوان مثال، آنچه در خصوص سن و مرتکبان جرائم سایبری به عنوان یکی از علل فردی قابل‌توجه است، وقوع جرائم مالی معمولاً در سنین بالا و جرائم علیه عفت و اخلاق عمومی در سنین پایین است. خودنمایی و سرگرمی از دیگر علل فردی جرائم سایبری است که طی آن در اکثر موارد اشخاص صرفاً جهت نشان دادن توانایی و استعداد خود مرتکب این جرائم می‌شوند؛ به‌گونه‌ای که هک کردن یک سایت یا دسترسی به داده‌های دیگری و مختل کردن یک سیستم را امری مطلوب و افتخارآمیز تلقی می‌کنند.

دین، مذهب و اعتقاد به ارزش‌های تعیین شدهٔ جامعه از ابزارهای بسیار مهم سیاست جنایی یک جامعه در مبارزه یا پیشگیری از جرم محسوب می‌شود تا جایی که در فضای

سایبر، اعتقاد به ارزش‌های دینی، ناخودآگاه فرد را از ارتکاب جرائم سایبری به خصوص در زمینهٔ محتویات مبتذل و مستهجن بازخواهد داشت. علاوه بر این موارد، سطح تحصیلات و آگاهی در عین اینکه آثار مثبتی به همراه دارد، خود نیز می‌تواند از عوامل اصلی ارتکاب جرائم سایبری محسوب شود. نقش و تأثیر بزه‌دیده در ارتکاب جرائم سایبری انکارناپذیر است. فردی که از ایمیل خود به شکل صحیح خارج نمی‌شود یا عکس‌ها و فیلم‌های خود را در تلگرام، اینستاگرام و غیره قرار می‌دهد یا دستگاه رایانه یا گوشی هوشمند خود را جهت تعمیر به افراد غیرمطمئن می‌سپارد، همگی از جمله اقدامات خطرساز و ریسکی محسوب می‌شود که می‌تواند فرد را به عنوان یک طعمه در اختیار افراد سودجو قرار دهد. لذا عدم آگاهی افراد از تدابیر امنیتی و نداشتن تفکر انتقادی و سواد رسانه‌ای می‌تواند منجر به قربانی شدن آن‌ها شود. از سوی دیگر، شرایط محیطی (عوامل مرتبط با فضای فیزیکی) ممکن است، منشأ ظهور نوستالژی‌هایی شود که رفتار تشدید شده‌ای را در محیط مجازی به وجود آورد. عدم تصویب قوانین مناسب فضای مجازی، متناسب نبودن جرم و مجازات، ضعف در عملکرد برخی از سازمان‌ها همچون فقدان ابزارهای نظارتی، زمینه‌های ارتکاب جرم در فضای مجازی را برای فرصت‌طلبان امکان‌پذیر می‌کند. مجرمان در فضای سایبر به معنای واقعی کلمه، از آزادی عمل و آزادی اراده برخوردارند؛ چراکه هیچ قدرت تحکیم کننده و هیچ نیرو و اهرم بازدارنده‌ای وجود ندارد. دنیای جدید، موقعیتی را به وجود آورده که افراد فارغ از هرگونه نظارت و کنترل در خلوت خود در مقابل رایانه قرار بگیرند و به راحتی وارد فضای افسارگسیخته‌ای شوند که اثری از عوامل دولتی و جامعهٔ محدودکنندهٔ آزادی نیست؛ این فضا مالک خصوصی و دولتی ندارد، تابع آیین‌نامهٔ جهانی نیست و هیچ قانون‌گذار عمومی در آن وجود ندارد. با گسترش حوزهٔ فناوری اطلاعات در تمامی شئون زندگی انسان‌ها اسناد و مدارک ناشی از کارکردهای این فناوری، برای اثبات دعاوی راجع به آن هیچ جایگاهی ندارد؛ زیرا به آسانی می‌توان در آن‌ها دستکاری یا آن را جعل کرد یا آن‌ها را با استفاده از دانش فنی مناسب پنهان کرد. به علاوه برخی ادلهٔ قانونی که همواره در سایر جرائم از وسایل مهم اثبات تلقی می‌شوند، کارآمد نخواهد بود. قانون جرائم رایانه‌ای مصوب سال ۸۸ جوابگوی جرائم نوظهور نیست؛ چون بعضاً برخی از قضات اذعان داشتند که با عناوینی روبرو می‌شوند که تاکنون جرم‌انگاری نشده‌اند و نمی‌دانند که جزء عناوین مجرمانه هستند یا نه. در خصوص پیشگیری، تعقیب و کشف جرائم سایبری، همکاری

متقابلی از ناحیهٔ کشورها به چشم نمی‌خورد. همچنین، مکانیسم قانونی مشترکی که تشریک مساعی بین‌الملل را تجویز کند وجود ندارد.

پیشنهادها: با توجه به یافته‌های این مطالعه، می‌توان موارد زیر را به عنوان پیشنهاد در راستای پیشگیری و کنترل جرائم سایبری ارائه داد:

- نهادینه کردن فرهنگ استفاده از فضای سایبر؛
- اهمیت بیشتر به رشد تفکر انتقادی و ارتقای امکانات در خصوص آموزش‌های سواد رسانه‌ای؛
- جرم‌انگاری و تعیین واکنش‌های تأدیبی و کیفری متناسب با جرائم رایانه‌ای؛
- مهیا کردن مکانیسم‌های پیشگیری رشد مدار در محیط آموزشی و تحصیلی برای مقابله با آثار نامطلوب فضای مجازی؛
- تبلیغات گسترده در خصوص چگونگی استفاده از فضای مجازی؛ برای مثال، اطلاعیه‌های پلیس فتا در مورد استفاده صحیح از کارت‌های بانکی عضو شتاب تأثیر شگرف در کاهش بزه‌دیدگی ناشی از این نوع کلاهبرداری به دنبال داشت؛
- تهیهٔ آمار و ارقام جرائم سایبری ارتکابی و در اختیار عموم قرار گرفتن این اطلاعات با حفظ حریم خصوصی افراد جهت آگاه‌سازی افراد جامعه از تهدیدها؛
- تهیه و تولید فیلم‌هایی با محتوای جرائم سایبری در رسانه‌ها؛
- فرهنگ‌سازی و آموزش مفهوم دینی امر به معروف و نهی از منکر؛
- تشویق مؤسسه‌های مالی، بانک‌ها و شرکت‌ها برای به‌کارگیری تدابیر امنیتی مناسب با توجه به قابلیت خطرپذیری و نفوذ مجرمان به سیستم‌های رایانه‌ای؛
- تدوین قوانین و مقررات سخت برای شرکت‌های ایرانسل، همراه اول و بانک‌ها در زمان احراز هویت افراد؛
- تأمین نیازمندهای پلیس سایبری در راستای تجهیز مراکز تخصصی و از بین بردن موانع خریدهای خارجی جهت دسترسی به دیتا بیس‌ها؛
- برگزاری نشست‌های علمی با حضور اساتید و دانشجویان در رابطه با تأثیر شبکه‌های اجتماعی مجازی بر هویت دینی؛
- آینده‌نگری و آینده‌پژوهی در حوزهٔ جرائم نوظهور.

سپاسگزاری

با تشکر فراوان از ریاست محترم مرکز مطالعات راهبردی قوۀ قضائیه که حمایت معنوی در اجرای پژوهش داشتند. قضات محترم دادسرای جرائم رایانه‌ای که همکاری بسیار خوبی برای انجام مصاحبه داشتند و نیز تشکر ویژه از مساعدت و تلاش‌های سرکار خانم قنبری کارشناس آن دادسرا و قدردانی از سرکار خانم میرزایی به عنوان دستیار علمی پژوهش.

منابع

منابع فارسی

- آنجلیز، جینا دی (۱۳۸۳). *جرائم سایبر* (سعید حافظی و عبدالصمد خرم آبادی، مترجمان). تهران: شورای عالی توسعۀ قضایی، دبیرخانۀ شورای عالی اطلاع‌رسانی (چاپ اول).
- ثنایی، باقر (۱۳۶۸). نظریۀ یادگیری اجتماعی. *فصلنامۀ تعلیم و تربیت* (آموزش و پرورش). (۲۰)، صص۱۱-۲۱. بازیابی از: http://yon.ir/gRUSN
- جایشانکار، کی (۱۳۹۴). *جرم‌شناسی سایبری* (مهدی مقیمی، مترجم). تهران: انتشارات دانشگاه علوم انتظامی امین (چاپ اول).
- خداقلی، زهرا (۱۳۸۳). *جرائم کامپیوتری*. تهران: آریان (چاپ اول).
- دادستان، پریرخ (۱۳۸۹). *روان‌شناسی جنایی*. تهران: سازمان مطالعات و تدوین کتب علوم انسانی دانشگاه‌ها (سمت) (چاپ هفتم).
- راسخی، افشین (پاییز ۱۳۹۳). جرائم و تهدیدهای سایبری و نقش پلیس در توسعۀ امنیت نرم در محیط سایبر. *فصلنامۀ مطالعات حفاظت و امنیت انتظامی*. ۹ (۳۲)، صص۲۰۱-۲۵۲. بازیابی از: http://yon.ir/dTH4x
- رضوی زاده، ندا و محمدپور، احمد (تابستان و پاییز ۱۳۸۹). برساخت تفسیری تجربۀ زیستۀ خیران مدرسه‌ساز. *فصلنامۀ راهبرد فرهنگ*. ۳ (۱۰ و ۱۱)، صص۴۱ – ۶۶. بازیابی از: http://www.sccr.ir/UserFiles/Rahbord/10/2.pdf
- عاملی، سید سعیدرضا (۱۳۹۰). *رویکرد دو فضایی به آسیب‌ها، جرائم، قوانین و سیاست‌های فضای مجازی*. تهران: انتشارات امیرکبیر (چاپ اول).

- عاملی، سید سعیدرضا و حسنی، حسن (بهار ۱۳۹۱). دوفضایی شدن آسیب‌ها و ناهنجاری‌های فضای مجازی؛ مطالعهٔ تطبیقی سیاست‌گذاری‌های بین‌المللی. *فصلنامهٔ تحقیقات فرهنگی*. ۵ (۱)، صص ۱-۳۰. بازیابی از: http://www.sid.ir/FileServer/JF/47213911701

- مارش، یان؛ ملویله، گینور؛ مورگان، کیت؛ نوریس، گارت و والکینگتن، زئو (۱۳۸۹). *نظریه‌های جرم* (حمیدرضا ملک محمدی، مترجم). تهران: میزان (چاپ اول).

- محمود زاده، سودابه (۱۳۹۱). *مطالعهٔ جامعه‌شناختی انگیزهٔ افراد و نوع جرم ارتکابی در شبکهٔ اجتماعی فیس بوک*. پایان‌نامهٔ کارشناسی ارشد. دانشکدهٔ اقتصاد و حسابداری دانشگاه الزهراء.

منابع انگلیسی

- Anderson, Rosemarie (2007). Thematic content analysis (TCA) descriptive presentation of qualitative data, sage publication.

-Bandura, Albert, Barbaranelli, Claudio, Caprara, Gian Vittorio and Pastorelli, Concetta (1996). Mechanisms of Moral Disengagement in the Exercise of Moral Agency. Journal of Personality and Social Psychology, Vol. 71, No. 2.

-Bolden, M. and Nalla, M. (2014). Theorizing Cybercrime: Applying Routine Activities Theory, CJ 801. Retrieved from: http://yon.ir/bcgep

-Durost, Shane (2005). Profiling a Hacker, Capstone Project. Retrieved from: http://yon.ir/NEzCW

-Fötinger, Christian S. and Ziegler, Wolfgang (2005). Understanding a Hacker's Mind A psychological Insight into the Hijacking of Identities, University Krems. Retrieved from: http://yon.ir/b7Q3C

-McGuire M. and Dowling S. (2013). Cyber Crime: A Review of the Evidence, Home Office Research Report 75. Retrieved from: http://yon.ir/ogsf5

-Thomas David r. (2003), A general inductive approach for qualitative data analysis, university of Auckland, new Zealand.

-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 Publications Ltd.

-Ryan Gery w. (2003). techniques to identify themes, sage publication,university of Florida.