Journal of
Modern Jurisprudence and Law
Homepage: http://www.jaml.ir

تبیین جرم‌شناختی بزه‌دیدگی زنان در فضای مجازی با تأکید بر بزه‌های جنسی در نظام کیفری ایران

سارا محمد رضائی
کارشناسی ارشد حقوق جزا و جرم شناسی دانشگاه آزاد اسلامی(نویسنده مسئول)

دکتر سینا کیانی
استادیار حقوق جزا و جرم شناسی دانشگاه آزاد اسلامی

فصلنامه علمی فقه و حقوق نوین

Print ISSN: 2717- 1469
Online ISSN: 2717 – 1477

ISC.SID.NOORMAGZ.MAGIRAN
GOOGLESCHOLAR.ENSANI
www.jaml .ir

سال پنجم، شماره ۱۹،
صفحات ۳۷-۱

چکیده

«فضای مجازی» مانند هر وسیله‌ای که قابلیت استفاده مطلوب یا مضر را دارد، دارای ویژگی‌های مثبت و منفی است، به‌این‌ترتیب به‌وجودآمدن جرایم فضای مجازی نیز یکی از معایب این پدیده است که در حوزه‌ی مطالعه حقوق کیفری قرار می‌گیرد. همان‌طور که در فضای واقعی زنان بزه‌دیده خاص جرایم جنسی هستند. در فضای مجازی نیز زنان بیش از دیگر افراد در معرض بزه‌دیدگی جنسی قرار می‌گیرند که این بزه‌دیدگی در گستره بزه‌های گوناگون نوظهور انجام می‌پذیرد؛ لذا توجه ویژه‌ای را در حوزه‌ی مطالعات حقوق کیفری و بالاخص بزه‌دیده‌شناسی می‌طلبد تا در این زمینه پیشگیری‌هایی نیز انجام شود. باتوجه‌به مطالب پیش‌گفته در این تحقیق نیز که با روش تحقیق تحلیلی - توصیفی و بامطالعه کتابخانه‌ای بزه‌دیدگی زنان در فضای مجازی با تأکید بر بزه‌های جنسی سعی می‌شود؛ راهکارهای پیشگیری از بزه‌دیدگی زنان در فضای مجازی ارائه شود. نتایج نشان داد که به نظر می‌رسد باتوجه‌به مطالعات انجام شده دولت به معنای اعم آن نتوانسته است به‌صورت تخصصی در خصوص جرایم رایانه‌ای با محوریت بزه‌دیدگی زنان جرم‌انگاری‌هایی انجام دهد اگرچه در سال‌های اخیر با جرم‌انگاری‌های کلی در این زمینه ورود کرده است؛ اما محوریت بیشتر اقدامات دولتی جرایم مالی بوده است. آنچه که در حوزه‌ی ی پیشگیری بزه‌دیدگی زنان بیشتر اهمیت دارد اقدام به پیشگیری وضعی در این زمینه است؛ چرا که در این نوع پیشگیری می‌توان اقدامات پیشگیرانه را بر اساس ویژگی‌های فضای مجازی اعمال نمود، همچنین به دلیل وضعیت خاص زنان به‌خصوص در سنین پایین اقدامات پیشگیرانه رشد مدار ضرورت دارد.

واژگان کلیدی: بزه‌دیده، زنان، فضای مجازی، بزه‌دیدگی جنسی، حقوق کیفری

طبقه‌بندی JEL: فقه – حقوق – جزا و جرم شناسی – حقوق بین الملل – حقوق خصوصی

Journal of
Modern Jurisprudence and Law
Homepage: http://www.jaml.ir

Scientific Journal of Modern Jurisprudence and Law

Print ISSN: 2717- 1469
Online ISSN: 2717 - 1477

Profile in ISC,SID, Noormags, Magiran, Ensani, GoogleScholar
www.jaml .ir

fifth year, Issue 19

Pages 1-37

Criminological explanation of women's victimization in cyberspace with emphasis on sexual crimes in the Iranian penal system

Sara Mohammad Rezaei — Master's degree in Criminal Law and Criminology, Islamic Azad University (Corresponding author)

Dr. Sina Kiani — Assistant Professor of Criminal Law and Criminology, Islamic Azad University

Abstract

"Cyberspace" like any tool that can be used for good or harm has positive and negative characteristics, so the emergence of cyberspace crimes is also one of the disadvantages of this phenomenon, which is included in the field of criminal law studies. Just as in real space, women are the victims of sexual crimes. In cyberspace, women are more exposed to sexual victimization than other people, and this victimization occurs in a wide range of emerging crimes; therefore, it requires special attention in the field of criminal law studies, especially victimology, so that prevention can be done in this field. Considering the aforementioned materials in this research, which uses the analytical-descriptive research method and library study, attempts to investigate the victimization of women in cyberspace with an emphasis on sexual crimes; Strategies for preventing women's victimization in cyberspace should be presented. The results showed that, according to the studies conducted, the government in its broad sense has not been able to specifically criminalize computer crimes centered on women's victimization, although in recent years it has entered this field with general criminalizations; however, the focus of most government actions has been on financial crimes. What is most important in the field of preventing women's victimization is taking situational prevention in this field; because in this type of prevention, preventive measures can be applied based on the characteristics of cyberspace, and also, due to the special situation of women, especially at a young age, development-oriented preventive measures are necessary.

Keywords: Victim, Women, Cyberspace, Sexual Victimization, Criminal Law

JEL Classification: Jurisprudence - Law - Criminal and Criminology - International Law - Private Law

مقدمه

برآمد

گسترش استفاده از اینترنت و فضای مجازی در تعاملات روزمره منجر به ایجاد تغییر در زندگی روزمره افراد به‌ویژه قشر جوان شده است. جاذبه‌های این فضا منجر شده افراد ساعات زیادی از روز خود را در این فضا گذرانده و تعاملات در این فضا را جایگزین تعاملات با اعضای خانواده و همسالان خود کنند؛ دراین‌بین باتوجه‌به شکل‌گیری شکل نوین ارتباطات جرایم خاصی شکل‌گرفته است که یک‌سوی آن بزهکار و سوی دیگر آن بزه‌دیده است.[1] بزه‌دیده‌شناسی بدون هیچ بحث و تردیدی شاخه‌ای از جرم‌شناسی به شمار می‌رود، بزه‌دیده‌شناسی به هر مسئله‌ای که مربوط به بزه‌دیده باشد توجه می‌کند: شخصیت بزه‌دیده، ویژگی‌های زیست‌شناختی، روان‌شناختی و اخلاقی او، مشخصه‌های اجتماعی - فرهنگی‌اش، روابطش با مجرم و بالاخره مشارکتش در وقوع جرم از طرف دیگر مندلسون با توسعه مفهوم بزه‌دیده؛ بزه‌دیده‌شناسی را به کیفری که فقط بزه‌دیدگان جرایم کیفری را مدنظر قرار دارد و بزه‌دیده‌شناسی عمومی که به‌تمامی بزه‌دیدگان (آسیب‌دیدگان) مانند بزه‌دیدگان حوادث، بزه‌دیدگان جامعه، بزه‌دیدگان دولت و نهادهای وابسته می‌پردازد تقسیم کرده است، بزه‌دیده‌شناسی به انواعی تقسیم شده است: بزه‌دیده‌شناسی اولیه: به مطالعه ویژگی‌ها و نقش بزه‌دیده در تکوین جرم و نیز رابطه قربانی جرم با مجرم می‌پردازد و در حقیقت بزه‌دیده‌شناسی اولیه شاخه‌ای از جرم‌شناسی علت‌شناسانه است که در آن نقش بزه‌دیده در وقوع جرم و به‌عنوان یکی از علل و عوامل ارتکاب جرم از سوی بزهکار بررسی و در کنار سایر علل و عوامل جرم‌زا قرار می‌گیرد و در مقابل بزه‌دیده‌شناسی پیشگیرانه به‌عنوان شاخه‌ای از جرم‌شناسی پیشگیرانه شیوه‌های پیشگیری از بزه‌دیدگی را بررسی و مطالعه می‌کند.

بزه‌دیده‌شناسی ثانویه: این نوع از بزه‌دیده‌شناسی در اثر تحول و توسعه بزه‌دیده‌شناسی اولیه به وجود آمده است که دغدغه آن، بهتر ساختن سرنوشت بزه‌دیده با ارائه کمک، حمایت‌های مادی و معنوی و جبران خسارت‌های وی است و انواع مختلف از حمایت‌ها را در شرایط گوناگون نسبت به بزه‌دیدگان پیشنهاد می‌کند.[2]

به دلیل تفاوت‌های جنسیتی و جامعه‌شناختی، زنان، از جایگاه ویژه‌ای در مطالعات بزه‌دیده شناختی برخوردارند که امروزه با مطرح‌شدن فضای سایبری و به‌وجودآمدن بزه‌دیدگی زنان در پی آن، مطالعه‌ی این پدیده ضروری به نظر می‌رسد؛ در این حوزه‌ی نکته‌ای که حائز اهمیت است بزه‌دیدگی زنان ناشی از بزه‌های جنسی است که دامنه‌ای از جرایم مهم را در بر می‌گیرد، در این تحقیق با مطالعه‌ی بزه‌دیدگی زنان از نگاه جرم‌شناسی در فضای مجازی به بزه‌دیدگی زنان ناشی از جرایم جنسی در فضای مجازی توجه ویژه‌ای داریم.

۱. مفاهیم

۱.۱. بزه‌دیده

عنصر اصلی در پژوهش حاضر «بزه‌دیده» است، در طول تکوین اندیشه‌های حقوق کیفری نخست توجه و مطالعه معطوف به «بزه» بود سپس اندیشمندان حقوق کیفری «بزهکار» را محور مباحث و پژوهش‌های خود قرار دادند، باگذشت زمان اندیشمندان متوجه حلقه گمشده مطالعات خود یعنی «بزه‌دیده» شدند، به‌این‌ترتیب با گسترش مطالعات حول محور بزه‌دیده این مفهوم به طور دقیق‌تر

[1] مینولی، د. (۱۳۹۵). مهندسی اینترنت و اینترانت. (ترجمه او مهابادی). انتشارات آذرخش، چاپ دوم. ص ۷۲

[2] زندی، م. (۱۳۹۹)، تحقیقات مقدماتی در جرایم سایبری. انتشارات جنگل چاپ اول. ص۱۵۵

شناسایی شد و بستگی به نگرش اندیشمندان به حوزه‌های مختلف نیز تقسیم گشت.[1]

۱.۱.۱.تعریف بزه‌دیدگی و بزه‌دیده

برای مطالعه‌ای با محوریت بزه‌دیده و بزه‌دیدگی نخست باید تعریفی از این مفاهیم ارائه نمود تا منظور نگارنده در کاربرد آن‌ها عیان شود.

الف: تعریف بزه‌دیدگی: «بزه‌دیدگی، عمل قربانی‌کردن مجرمانه را بزه‌دیدگی می‌گویند.» عمل مجرمانه‌ای که شخص قربانی آن می‌گردد؛ می‌تواند قتل، سرقت، تجاوز به عنف و بسیاری از جرایم دیگر باشد، فردی هم که قربانی چنین عمل مجرمانه‌ای قرار می‌گیرد ممکن است زن، مرد، پیر یا جوان باشد به عبارتی، همان‌گونه که جرایم متنوع هستند بزه‌دیدگان هم متنوع و گوناگون‌اند.

ب: تعریف بزه‌دیده: بزه‌دیده را می‌توان معادل واژه‌ی «قربانی از جرم» دانست که از کلمه‌ی ***Victim*** گرفته شده است. برخی گفته‌اند: «بزه‌دیده، شخصی مستقل یا متعلق به یک مجموعه است که متحمل آثار دردناک برخی عوامل شده که این عوامل دارای ریشه‌های مختلف فیزیکی، روانی، اقتصادی، سیاسی، اجتماعی و همچنین طبیعی هستند. در این تعریف، بزه‌دیده، مفهوم وسیعی داشته و معادل واژه‌ی قربانی قرار می‌گیرد.»[2] آنچه که از عبارت بزه‌دیده معلوم است (بزه+دیده) نشانگر تصدیق معادل انگاری قربانی از جرم است. [3]

۲.۱.۱. انواع بزه‌دیده

بزه‌دیده را می‌توان فراخور گرایش تحقیق به اقسام متفاوتی طبقه‌بندی کرد آنچه که در این تحقیق به‌عنوان طبقه‌بندی ذکر می‌شود، تقسیم‌بندی‌ای است که مرتبط با بزه‌دیدگی زنان در فضای مجازی است. از کسانی که در حوزه‌ی طبقه‌بندی بزه‌دیدگان بسیار فعالیت کرده‌اند؛ «لوپز» است که بزه‌دیده را از نظر جنسیت یا خصایص ظاهری و شخصیتی و... تقسیم‌بندی کرده است.[4] اما آنچه که بیش از همه نظر جرم شناسانی نظیر (مندلسون و هیندلانگ) را به خود جلب کرده بود نقش و مسئولیت بزه‌دیده در فرایند بزه‌دیدگی بود.

ازاین‌جهت می‌توان بزه‌دیده را این‌چنین طبقه‌بندی نمود:

۱.۲.۱.۱. بزه‌دیدگان ایده‌آل (واقعی)

بزه‌دیده واقع‌شدن بسته به جرایم مختلف، متفاوت است، آنچه که توجه بزه‌دیده شناسان را بیشتر به خود جلب کرده است. دسته‌ای از بزه‌دیدگان هستند که نقش فعالی در فرایند بزه‌دیدگی ایفا نکرده‌اند و به‌اصطلاح ناخواسته بزه‌دیده جرم شده‌اند؛ به همین جهت این دسته از بزه‌دیدگان را بزه‌دیدگان بی‌گناه یا ایده‌آل نام‌گرفته‌اند. این بخش از افراد بدون هیچ آگاهی بزه‌دیده جرم واقع شده‌اند که عوامل متعدد در بزه‌دیدگی آنان نقش داشته است. یکی از این عوامل داشتن شرایط خاص فردی (سفیه بودن، صغیر بودن، کهولت سن، زن بودن و.) است که منجر به بزه‌دیدگی افراد شده

[1] پاک‌نهاد، ا سدره نشین، ا. (۱۳۹۰). بررسی قانون جرایم رایانه‌ای از دیدگاه موازین حقوق کیفری فناوری اطلاعات، فصلنامه علمی‌ترویجی کارآگاه. دفتر تحقیقات کاربردی پلیس آگاهی ناجا. شماره ۱۷. ص ۱۴

[2] باستانی، بهزاد. (۱۳۸۹). جرایم کامپیوتری و اینترنتی، جلوهای نوین از بزهکاری، انتشارات بهنامی. چاپ دوم. ص ۴۴

[3] نیا فیلی، ز. (۱۳۷۹) بزه‌دیده و بزه‌دیده‌شناسی. ترجمه روح الدین کرد، علیوند و احمد محمدی. تهران: مجمع علمی و فرهنگی مجد، ص ۷۵.

[4] صلاحی، ج. (۱۳۹۳) کلیات جرم‌شناسی و تئوری‌های جدید. چاپ اول. انتشارات مجد. ص ۴

یا آن را تسهیل کرده است، لذا به این جهت که این افراد در بزه‌دیدگی خود نقش فعالی نداشته‌اند توجه ویژه‌ای را می‌طلبند.[1]

این تقسیم‌بندی بزه‌دیدگان که بر اساس نقش بزه‌دیده در فرایند بزه‌دیدگی است؛ در فضای مجازی نیز مشهود است. فارغ از شرایط زیستی و عوامل فردی و... می‌توان گفت: برخی از افراد بدون اینکه خواسته خودشان باشد یا رفتار تحریک‌آمیزی از آن‌ها سرزده باشد بزه‌دیده جرایم فضای مجازی واقع می‌شوند. می‌توان گفت که این افراد قربانی به معنای اخص کلمه هستند و در مسیر عمل مجرمانه‌ای قرار گرفته‌اند و قربانی جرم شده‌اند. در فضای مجازی این قسم از بزه‌دیدگان افرادی هستند که تدابیر حفاظتی و امنیتی را کاملاً رعایت می‌کنند، اعمال خطرناکی ندارند، اما بااین‌وجود قربانی رفتار مجرمانه واقع می‌شوند، برای مثال فردی که بر روی رایانه خود نرم‌افزار حفاظتی به روزی را نصب‌کرده و در دام تبلیغات بلندپروازانه نیفتاده است؛ بزه‌دیده جرم سایبری واقع شود که در این موارد مهارت خاص بزهکار در عبور از نرم‌افزارهای امنیتی و ایرادات موجود در برخی از سیستم‌عامل‌ها و یا نرم‌افزارهای امنیتی منجر به بزه‌دیدگی می‌شود.[2] البته این استفاده تنها به سایت‌ها و نرم‌افزارهایی محدود می‌شود که براساس قوانین بین‌المللی به وجود آمده‌اند، چراکه استفاده از سایت‌هایی که بر خلاف قوانین کشورها مطالبی را در سراسر جهان منتشر می‌کنند و نیز بدافزارها و نرم‌افزارهای غیرقانونی که به‌تبع یک نوع خطر آفرینی بالقوه دارند؛ مشمول این موارد نمی‌شود و مراجعه به آنها در زمره رفتارهای پرخطر سایبری محسوب می‌شود. با این تفاسیر بزه‌دیده‌ی واقعی سایبری شخصی است که از هرگونه رفتار خطرآفرین خودداری کرده و سطحی از امنیت را برای سیستم رایانه‌ای خود فراهم کرده است که به‌نوعی با میزان کار و استفاده وی از اینترنت متناسب است.[3]

۲.۲.۱.۱. بزه‌دیدگان مقصر یا سرزنش‌پذیر

این دسته از بزه‌دیدگان برخلاف گروه اول که هیچ تأثیری در وقوع جرم نداشتند، به نحوی در تحقق جرم علیه خودشان نقش دارند. در نظر رایجیان اصلی (۱۳۸۶) بزه‌دیدگان سرزنش‌پذیر به دو روش کلی زمینه بزه‌دیدگی خویش را فراهم می‌کنند. برخی از بزه‌دیدگان زمینه‌های ارتکاب جرم از سوی بزهکار را بر خویش فراهم می‌کنند و به نحوی محرک بزهکار برای ارتکاب جرم هستند، از جمله می‌توان به رفتار یا گفتار تحریک‌آمیز بزه‌دیده اشاره کرد که با انجام این کارها به‌گونه‌ای مجرم را به ارتکاب جرم تشویق می‌کنند. دراین‌رابطه می‌توان به نقش اثرگذار و شتاب‌دهنده بزه‌دیده اشاره کرد. در مقابل این دسته از بزه‌دیدگان که به نحوی خود زمینه تحریک و تشویق بزهکار را به ارتکاب جرم فراهم می‌کنند، دسته دیگری از بزه‌دیدگان هستند که به واسطه ویژگی‌های خاص خود سبب تقویت انگیزه مجرمانه در بزهکار می‌شوند. از مهم‌ترین موارد این ویژگی‌ها در نظر «اسپارکس» می‌توان به آسیب‌پذیربودن، فرصت، جذابیت، تسهیل، تأثیرگذاری و مصونیت اشاره نمود. [4]

---

[1] شیرزاد، ک. (۱۳۹۷). جرایم رایانه‌ای از دیدگاه حقوق جزای ایران و حقوق بین‌الملل، انتشارات بهینه فراگیر. چاپ اول. ص۳۰

[2] جوان جعفری، ع. شاهیده، ف. (۱۳۹۲). رفتار و گفتار تحریک‌آمیز بزه‌دیده در قوانین و مقررات کیفری و رویه قضایی ایران - مجله آموزه‌های حقوق کیفری. دانشگاه علوم اسلامی رضوی .

[3] زکوی، م. (۱۳۹۰). بزه‌دیدگان خاص در پرتو بزه‌دیده‌شناسی حمایتی، انتشارات مجد. ص۱۱۷

[4] در تحقیقی که از سوی ویلیام (۱۳۸۶) صورت‌گرفته است اسپارکس اصطلاح «آسیب پا پریا» را در چند احتمال بررسی می‌کند. اولین احتمال اشاره به بزه‌دیدگان ایده‌آل دارد که هیچ‌گونه تقصیری در تحقق جرم علیه خویش ندارند، این افراد در معرض جرم و بزه‌دیدگی قرار می‌گیرند نه به‌خاطر اینکه فعالیت محرکی انجام داده‌اند؛ بلکه به‌خاطر شرایط خاص جسمی و روحی، ضعف، پیری یا جوانی است که مستعد بزه‌دیدگی می‌شود. از جمله

دسته‌بندی‌های صورت‌گرفته از سوی «اسپارکس»[1] به‌نوعی نشانگر تقصیر و مسئولیت بزه‌دیده است. در واقع به‌نوعی اسپارکس این پیام را می‌دهد که همه مردم باید با ماندن در خانه‌ها و یا نگهداری از اموالشان در جای مناسب (حرز)، به نحوی خود و اموالشان را از دید مرتکبین احتمالی دور کنند تا بتوانند از موقعیت‌های خطرناک رهایی یابند. حال اگر امکان انجام این اقدامات را ندارند، این دسته از بزه‌دیدگان احتمالی باید با بیرون رفتن دسته‌جمعی با رفتن به خیابان‌های نورانی و تقویت امنیت اموال، خود و اموالشان را محافظت کنند، ایده‌های دیگری نیز همچون تغییر روش و سبک زندگی به‌منظور کاهش ارتکاب جرایم نسبت به بزه‌دیدگان احتمالی از سوی دولت‌ها پیشنهاد شده است.

باتوجه‌به کلیات مطرح شده، باید گفت به نحوی شاهد این نوع تقسیم‌بندی در خصوص بزه‌دیدگان سایبری نیز هستیم. این دسته از بزه‌دیدگان سرزنش‌پذیر به‌صورت آگاهانه یا ناآگاهانه و یا با بی‌احتیاطی زمینه بزه‌دیدگی خویش را در فضای سایبر فراهم می‌کنند. در واقع می‌توان گفت، در فضای سایبر، کاربران عموماً در سطوح پایینی از آگاهی‌های نرم‌افزاری و به‌تبع امنیتی قرار دارند و غالباً از روی ناآگاهی مرتکب رفتارهای پرخطری می‌شوند که آنها را در معرض بزه‌دیدگی قرار می‌دهد، در مواردی نیز شاهد سهل‌انگاری کاربران فضای مجازی هستیم.[2]

این دسته از بزه‌دیدگان باتوجه‌به میزان تقصیرشان به دودسته کلی تقسیم می‌شوند که در ادامه به بررسی هر یک از آنها می‌پردازیم:

الف: بزه‌دیدگان با کمینه تقصیر:

همان‌گونه که مطرح شد میزان آگاهی کاربران در بزه‌دیدگی آنان نقش تعیین‌کننده‌ای دارد، در نظر مندلسون نیز آگاهی یا ناآگاهی قربانیان می‌تواند عامل مؤثری در وقوع جرم و تحقق بزه‌دیدگی افراد تأثیرگذاری در نظر اسپارکس به طور ویژه‌ای مرتبط با خشونت‌های بین افراد و تجاوز جنسی است. خصوصاً زمانی که مرتکب و جزء داده یکدیگر را می‌شناسند و غالباً خیلی به هم نزدیک هستند. به‌عنوان‌مثال او درباره همسری می‌نویسد که شوهر خود را هنگام خوابیدن می‌کشد؛ زیرا او را مکرراً کتک می‌زده است.

«لوپز»، به این دسته از بزه‌دیدگان تحت عنوان بزه‌دیدگان با کمینه تقصیر اشاره کرده است.[3]

۱. بزه‌دیدگان آگاه: این دسته از بزه‌دیدگان با اینکه می‌دانند رفتارشان پرخطر است و در اثر آن چه عواقب خطرناکی محقق خواهد شد، باز هم مرتکب آن رفتار می‌شوند که

آسیب‌پذیری‌هایی که خارج از اراده و کنترل فرد است می‌توان به شرایط اقتصادی و محیط زندگی فرد و یا عضویت در گروه اجتماعی ضعیف مانند اقلیت‌های نژادی، زنان با کودکان اشاره کرد.

[1] ۱.«فرصت»، در دو سطح قابل‌طرح است. اولین آن مربوط به قابل‌دسترس بودن است، در حالتی که مالک، مال خود را در حرز مناسب قرار داده و از آن محافظت می‌کند و با زمانی که جزء مالک مالی نیست عملاً سرقت قابل‌تحقق نیست. دومین سطح درارتباط‌با تغییرات روش زندگی قابل‌طرح است. زمانی که شیوه زندگی تغییر کرده و زنان ساعاتی از روز را همچون مردان در خارج از منزل مشغول کار هستند، احتمال سرقت از منازل افزایش می‌یابد. ۲. «جذابیت» اشاره به این نکته دارد که چه‌قدر یک شی با فرد می‌تواند برای مرتکب خاصی جذاب و اغواگر باشد. در واقع به نحوی مرتکب انتخاب عقلانی انجام می‌دهد و خطرات حاصل از با دست آوردن یک کالا را با سود احتمالی آن می سجاد و در مواردی که خطر دستگیری پایین و سود احتمالی بیشتر باشد، قاعدتاً جذابیت آن کالا بیشتر خواهد بود. اسپارکس معتقد است، اهداف جذاب از لحاظ دسترسی راحت‌تر به آن‌ها و هم از جهت سود محتمل، بیشتر در مناطق مرکزی شهر متمرکزند و لذا جای تعجب نیست که چنین مناطقی دارای نرخ جرم بالاتری هستند. ۳.«تسهیل» اشاره به این دارد که آیا بزه‌دیده موقعیت خطرناک ویژه‌ای را به‌صورت عمدی، مسامحه‌آمیز یا به طور ناآگاهانه به وجود آورده است؟ برای مثال، کوتاهی در نصب قفل ایمنی با زنگ خطر در منطقه‌ای که دارای نرخ بالای سرقت از منزل است. این نوعی بسط‌دادن خطرناک در جابه‌جایی تقصیر از مرتکب به بزه‌دیده است.

[2] زکوی، همان منبع پیشین

[3] رایجیان اصلی، م، (۱۳۸۴) بزه‌دیده‌شناسی حمایتی، چاپ اول، نشر دادگستر، ص ۵۲.

در نتیجه منجر به تحقق جرم و بزه‌دیدگی خود می‌شوند، در فضای سایبر نیز ما شاهد این دسته از بزه‌دیدگان هستیم، به‌عنوان‌مثال در بسیاری از موارد، سیستم‌های امنیتی موجود، برخی سایت‌ها را به‌عنوان سایتی‌های خطرناک و آسیب‌رسان معرفی می‌کنند و از فرد می‌خواهند وارد آن سایت به‌خصوص نشود. [۱] در برخی موارد اجرای نرم‌افزارهای به خصوصی که با نام‌های متداول کرک[۲] پچ[۳] یا کی جن[۴] برای استفاده‌کردن نرم‌افزارهای غیررایگان به کار می‌روند، نیز همین هشدارها را برای کاربر از سوی سیستم حفاظتی‌اش به همراه دارد. [۵] درصورتی‌که کاربر به این هشدارها بی‌توجهی کند و به آن سایت خاص وارد شود یا نرم‌افزار مذکور را اجرا کند، بزه‌دیدگی احتمالی ناشی از آن در واقع مستقیماً ناشی از عملکرد خود شخص است. خیلی از کاربران نیز از این قانون آگاهی دارند و می‌دانند که نباید روی هر لینک یا فایلی کلیک کنند و یا هر لینک ضمیمه ایمیل‌های ناآشنا را باز کنند، اما بااین‌وجود از روی کنجکاوی و با اطمینان خاطر از اینکه بزه‌دیدگی رخ نخواهد داد، اقدام به کلیک روی فایل مربوطه می‌کنند. در نتیجه این دسته از کاربران باوجود آگاهی از خطرناکی اعمال خود باز هم آن رفتار را انجام می‌دهند.[۶] دراین‌رابطه بزه‌دیده در عین آگاهی خویش زمینه بزه‌دیدگی‌اش را فراهم کرده است. به بیان دیگر ازآنجاکه بحث دررابطه‌با نقش بزه‌دیده در وقوع جرایم سایبری است، مشاهده می‌کنیم که در مواردی آگاهی بزه‌دیدگان زمینه را برای بزه‌دیدگی آنان فراهم می‌کند و در پی آن شرایط برای وقوع جرایم سایبری فراهم می‌شود.

۲. بزه‌دیدگان ناآگاه: فضای سایبر، فضایی جدید و مدرن است و کار با این فضا نیاز به آگاهی و دانش رایانه‌ای دارد، در نتیجه کاربران در هر سطح دانش و تخصصی که باشند؛ در جهان امروز نمی‌توانند خود را نسبت به فضای سایبر بی‌علاقه و بی‌تفاوت نشان دهند؛ فراگیری دانش رایانه‌ای یک لزوم برای تمامی کاربران است. اما متأسفانه بسیاری از کاربران فضای سایبر فاقد دانش کافی برای ورود به این جهان مجازی هستند، در نتیجه به علت فقدان آگاهی، ناخواسته موجبات تحقق جرم و بزه‌دیدگی خویش را فراهم می‌کنند. این دسته از افراد مستقیماً موجب تحریک بزهکار و تحقق جرم علیه خویش نشده‌اند، اما در اثر ناآگاهی‌شان زمینه وقوع جرایم سایبری و بزه‌دیدگی خود را فراهم کرده‌اند. این افراد هم قربانی نادانی خود و هم قربانی رفتار مجرمانه بزهکار شده‌اند که در این میان بی‌اطلاعی و رفتار پرخطرشان بیشترین تأثیر را در بزه‌دیدگی‌شان داشته است، به تعبیری «بزه‌دیدگی آنها منشأ دوگانه دارد که تا حدود بسیاری، رفتار پرخطرشان موجب تحقق و

---

[۱] در مثال دیگر می‌توان به قانون، «روی هر لینکی کلیک کن» اشاره کرد. خیلی از کاربران از این قانون پیروی می‌کنند. این‌گونه افراد به هر سایتی که وارد می‌شوند روی لینک‌ها و فایل‌های آن کلیک می‌کنند، هر ایمیلی که برایشان فرستاده می‌شود بازکرده و روی لینک‌های ضمیمه آن کلیک می‌کنند. این قانون از سوی نفوذگران برای تحریک کاربران جهت کلیک بر روی فایل‌های آلوده در فضای سایبر رواج پیدا کرده است.

[۲] .Crack شرکت‌های ارائه‌دهنده نرم‌افزار جهت ارائه نرم‌افزار با بازی از کاربران تقاضای پول می‌کنند. اما کاربران زیادی هستند که حاضر به پرداخت پول برای آن بازی یا نرم‌افزار نیستند. در نتیجه اقدام به کرک کردن آن نرم‌افزار با بازی می‌کنند. این اقدام منجر می‌شود تا آن نرم‌افزار با بازی بدون هیچ‌گونه محدودیتی همانند فایل اصلی در اختیار کاربران قرار بگیرد.

[۳] .Path": در لغت به معنای وصله‌کردن با سرهم کردن است. اما در لغت‌نامه برنامه‌نویسی مجموعه کدهایی است که موجب ارتقای نرم‌افزار و ازبین‌بردن خطای موجود می‌شود. (پایگاه اطلاع‌رسانی تبیان. ۱۳۶۱)

[۴] **Key Gen.** برنامه کی جن برنامه‌هایی هستند که به روش‌های مختلف نرم‌افزارهای رسمی ثبت و فعال شده است و لذا به کاربر امکان استفاده کامل و نامحدود از نرم‌افزار را می‌دهد (پایگاه اطلاع‌رسانی تبیان - ۱۳۹۱).

[۵] زررخ و مالمیر، (۱۳۸۹)، پیشگیری از بزه‌دیدگی سایبری، فصلنامه علمی - ترویجی مطالعات پیشگیری از جرم ص ۶۵

[۶] جوان جعفری، ع. شاهیده، ف. (۱۳۹۲). رفتار و گفتار تحریک‌آمیز بزه‌دیده در قوانین و مقررات کیفری و رویه قضایی ایران - مجله آموزه‌های حقوق کیفری. دانشگاه علوم اسلامی رضوی.

تشدید، رفتار مجرمانه نسبت به ایشان شده است.» و به تعبیر دیگری، بی‌توجهی افراد در فعالیت‌های روزمره خود در فضای سایبر که ناشی از یکنواختی فعالیت‌های روزانه و امن تلقی کردن آنها به‌واسطه‌ی تکرارهای بسیار است و نیز ناآشنایی آنها با توانمندی‌ها و به‌تبع خطرهای فضای سایبر موجب بزه‌دیدگی آنها در این فضا می‌شود»[1]

ب- بزه‌دیدگان با بیشینه تقصیر

در دسته دوم، لوپز به تقسیم‌بندی دیگری از مندلسون اشاره می‌کند، ازآنجاکه در چه تقصیر برخی از قربانیان بالاست، لوپز آنان را در دسته بزه‌دیدگان با بیشینه تقصیر قرار می‌دهد. در این نوع تقسیم‌بندی بی‌احتیاطی و سهل‌انگاری عاملی برای درنظرگرفتن بیشترین میزان تقصیر تلقی می‌شود. از طرفی حس طمع‌ورزی و حرص ورزیدن برخی از کاربران نیز زمینه بزه‌دیدگی آنان را فراهم می‌کند که در ادامه به آن اشاره خواهد شد.

۱. بزه‌دیده بی‌احتیاط: بزه‌دیده بی‌احتیاط، فردی است که مراتب احتیاط را رعایت نکرده و توجه و دقت کافی را هنگام کار با رایانه و در فضای سایبر مدنظر قرار نمی‌دهد. در واقع در این دسته از افراد، بی‌احتیاطی و یا حتی سهل‌انگاری‌شان منجر به بزه‌دیدگی آنان می‌شود. از جمله این افراد می‌توان به اشخاصی اشاره کرد که اطلاعات شخصی از جمله رمز عبور، شماره ملی و... خود را در هر سایتی که اطلاعاتشان را درخواست می‌کند می‌نویسند و یا افرادی که شرایط لازم برای داشتن رمز عبور قوی و ایمن را رعایت نکرده و خود منجر به بزه‌دیدگی‌شان می‌شوند. برخی از کاربران نیز نسبت به الزامات امنیتی سیستمشان بی‌توجهی و با سهل‌انگاری می‌کنند، برای مثال از نرم‌افزارهای آنتی‌ویروس مناسب و به‌روز استفاده نمی‌کنند. فیلم و آهنگ را از سایت‌هایی که امنیت درستی ندارند به‌صورت رایگان دانلود می‌کنند. هنگام خروج از پست الکترونیکی‌شان گزینه ***sign out***را انتخاب نمی‌کنند و مواردی از این نوع... در تمامی این مصادیق و مواردی مشابه شاهد بی‌احتیاطی و با سهل‌انگاری کاربران هستیم، بی‌احتیاطی که در خیلی از موارد خواسته یا ناخواسته منجر به ایجاد سهمی برای کاربران در وقوع جرایم سایبری می‌شود. به عبارتی این بی‌احتیاطی زمینه را برای بزه‌دیدگی کاربران فراهم می‌کند و منجر به ایجاد مسئولیتی برای کاربران می‌شود.[2]

۲. بزه‌دیده طماع[3] و در نهایت منظور از بزه‌دیدگان طماع افراد حریص و طمع‌کاری است که به خیال دستیابی به پول بیشتر، شارژ بیشتر و یا دستیابی به تسهیلات فوق‌العاده فریب تبلیغات دروغین و آگهی‌های وسوسه‌انگیز را خورده و به‌راحتی مدارک و یا اطلاعات حساس و محرمانه خود از قبیل شماره ملی، شماره کارت، رمز عبور و... را به‌راحتی در اختیار بیگانگان قرار می‌دهند. در واقع این دسته کاربران طماع تصور می‌کنند؛ تمامی تبلیغات، آگهی‌ها و پیام‌های مبنی بر برنده‌شدن در قرعه‌کشی، اعطای شارژ ویژه و.... حقیقت داشته به‌راحتی فریب می‌خورند، در این دسته از بزه‌دیدگان حرص و طمع زمینه بزه‌دیدگی آنان را فراهم کرده است

[1] زررخ و مالمیر، (۱۳۸۹)، پیشگیری از بزه‌دیدگی سایبری، فصلنامه علمی - ترویجی مطالعات پیشگیری از جرم ص ۶۷

[2] عالی‌پور، ح (۱۳۹۶). مجموعه مقاله‌های همایش بررسی جنبه‌های حقوقی فناوری اطلاعات معاونت حقوقی و توسعه قضایی قوه قضائیه. مرکز مطالعات توسعه قضایی، انتشارات سلسبیل. چاپ اول. ص ۷۷

[3] در خصوص این دسته از کاربران تقسیم بنیادی روشنی از سوی مندلسون صورت نگرفته است، اما وقتی مصادیق و پرونده‌های واقعی را بررسی می‌کنیم در خیلی از موارد نمونه‌های عینی از حس طمع‌ورزی را می‌بینیم که به دلیل عدم کنترل آن، شرایط برای بزه‌دیدگی کاربران فراهم شده است. ما نیز باتوجه‌به مصادیق موجود، تقسیم بنیادی چند یادی را تحت عنوان «بزه‌دیده طماع» در زیر مجموعه بزه‌دیدگان با بیشینه تقصیر اضافه کردیم.

۲.۱. فضای مجازی و فضای سایبری

۱.۲.۱. مفهوم فضای مجازی

در زبان فارسی مفهوم دقیق و کاملاً پذیرفته شده‌ای از اصطلاح «سایبر» وجود ندارد. برخی از حقوق‌دانان و صاحب‌نظران معتقدند که مفهوم سایبر در سطح بین‌المللی بسط پیدا کرده و رواج عام یافته است؛ لذا این واژه تبدیل به یک لغت بین‌المللی شده است. آنان معتقدند که ترجمه این لغت یا یافتن معادل برای آن ممکن است دایره شمول و مفهوم آن را محدود کند؛ لذا توصیه می‌کنند که همانند واژه‌ی «تلفن» که در سطح بین‌المللی مفهوم یکسانی دارد و در همه نقاط جهان به یک معنا و لفظ مشترک بکار می‌رود، واژه‌ی «سایبر» نیز باید با یک‌لفظ مشترک بین‌المللی استعمال شود. [۱] بااین‌وجود، در زبان فارسی، لغت «سایبر» را معادل واژه‌ی «مجاز» و لغت «اسپیس» را معادل واژه‌ی «فضا» ترجمه کرده‌اند و ترکیب «سایبر اسپیس» [۲] را معادل «فضای مجازی» دانسته‌اند. در همین معنا، ترکیبات دیگری مانند: «جامعه مجازی» یا «شهروند مجازی» و «فروشگاه‌های مجازی و..» امثال آنها مطرح می‌شود. همه این ترکیبات در فضای مجازی مطرح می‌شوند. [۳] همچنین در برخی از اسناد رسمی، ترکیب «فضای تولید و تبادل اطلاعات» با شکل اختصاری «فتا» به‌عنوان معادل مفهومی «سایبر اسپیس» مطرح شده است. [۴]

باتوجه‌به مطالب اخیرالذکر، می‌توان نتیجه گرفت که منظور از «فضای مجازی» یا همان «فضای سایبری» عبارت است از: فضایی که ما از طریق فن آوری مبتنی بر رایانه وارد آن می‌شویم. این فضا از زمان روشن‌کردن رایانه در مقابل ما قرار می‌گیرد و ما با اعمال هرگونه دستوری نسبت به رایانه، عملیاتی را در فضای مزبور انجام می‌دهیم و در واقع، در فضای سایبر فعالیت می‌کنیم. [۵]

مفهوم فضای سایبر و به طور عام‌تر «فضای تبادل اطلاعات» است. حدود دو دهه از به‌کارگیری این اصطلاح در حوزه‌ی فناوری اطلاعات و ارتباطات نوین می‌گذرد؛ ولی همچنان میان صاحب‌نظران اختلاف‌های بنیادینی مشاهده می‌شود، به‌گونه‌ای که هنوز در مورد واقعی یا مجازی بودن آن اختلاف‌نظر اساسی وجود دارد. بااین‌حال، تعریف ساده و مورد قبولی که می‌توان از آن ارائه داد عبارت است از: «فضای واقعی و محسوس میان سیستم‌های رایانه‌ای که داده‌های دیجیتال در آن در جریان هستند.» [۶] جرائم سایبری چنانچه گذشت در فضای سایبر و به کمک فناوری‌های نوین اطلاعات و ارتباطات ارتکاب می‌یابد.

۲.۲.۱. ویژگی‌های جرایم فضای مجازی

برای جرائم سایبری سه ویژگی اصلی می‌توان شمرد:

۱) انعطاف‌پذیری عناصر تشکیل‌دهنده‌ی جرم در زمان و مکان

---

[۱] . برومند باستانی (۱۳۹۳) جرائم رایانه‌ای و اینترنتی، تهران، انتشارات بهنامی، ص۵۴

[۲] Cyberspace

[۳] معاونت آموزش و تحقیقات قوه قضائیه (۱۳۹۲) مسائل قضایی هرزه‌نگاری در محیط سایبر، تهران، انتشارات راه نوین، ص ۷.

[۴] وزارت ارتباطات و فن آوری اطلاعات: سند راهبردی امنیت تولید و تبادل اطلاعات

[۵] داوود صادقیان: کالبدشناسی جرائم سایبری در ایران، روزنامه اطلاعات، ۱۳۹۱، ص ۱۱.

[۶] پاک‌نهاد، ا سدره نشین، ا. (۱۳۹۰). بررسی قانون جرایم رایانه‌ای از دیدگاه موازین حقوق کیفری فناوری اطلاعات، فصلنامه علمی‌ترویجی کارآگاه. دفتر تحقیقات کاربردی پلیس آگاهی ناجا. شماره ۱۷. ص ۱۵

۲) آسانی، گمنام و ناشناس ماندن نسبی مرتکبان در فضای شبکه‌ای که در واقع شناسایی آنان و محل ارتکاب جرم را دشوار می‌نماید.
۳) جهانی بودن گستره‌ی ارتکاب بزه که به بزهکاران اجازه می‌دهد؛ بتوانند جرم را بدون حضور در محل حضور بزه‌دیده یا آماج و از اقصی‌نقاط جهان مرتکب شوند.[۱]

یکی از مشکلات جامعه بشری امروز در دست‌گرفتن ابتکار عمل‌های سایبری از سوی هنجارشکنان است که روزبه‌روز بر وسعت آن افزوده می‌شود. هنجارشکنان پیش از آنکه متناسب با شرایط خاص و متمایز فضای سایبر هنجارهای لازم وضع و نهادینه شود به این فضا دست یافته‌اند و رها شده‌اند. از سوی دیگر، هنجارهای موضوعه در دنیای فیزیکی کارایی و اثربخشی لازم در دنیای سایبر را ندارند. پس امکان نقض این هنجارها فراهم است، بدون آنکه دغدغه ناشی از گرفتاری در بند ضمانت اجراهای کیفری و غیرکیفری وجود داشته باشد.

۱.۲.۲.۱.نامحدودبودن فضای مجازی

فضای مجازی از لحاظ محدوده و مکان، با فضای حقیقی و واقعی کاملاً متفاوت است. در فضای واقعی وقتی که در یک محیط حقیقی قرار داریم با یک سری افراد مشخص و در یک محدوده‌ی معین سروکار داریم، اما فضای مجازی محیطی بدون حدومرز قلمداد می‌گردد. این ویژگی مثبت که امکان استفاده شایسته از محیط سایبر را در جهت آسان‌کردن فعالیت‌ها فراهم می‌سازد، در صورت استفاده می نادرست می‌تواند آثار منفی بر جای گذارد. این ویژگی فضای سایبر فرصت‌های زیادی را به مجرمان برای تغییردادن یا پنهان نمودن هویتشان می‌دهد. این نامحدودبودن، این پرسش را مطرح می‌سازد که آیا قلمرو و حوزه‌های فضایی جدید و سازگار یافته می‌توانند در برابر این مجموعه می منحرف دوام آورند؟[۲]

۲.۲.۲.۱. دسترسی آسان و سریع

از دیگر ویژگی‌های فضای مجازی که کاملاً منحصربه‌فرد است، همان دسترسی آسان و سریع این فضا است. به‌طوری‌که هر یک از افراد جامعه می‌توانند با استفاده‌ی از یک رایانه‌ی شخصی و یا حضوریافتن در یک کافی‌نت از تمامی امکانات و مزیت‌های مربوط به این فضا فارغ از هیچ‌گونه محدودیتی استفاده کنند. اگر فردی بخواهد از یک موضوع علمی تحقیق به عمل آورد، در فضای فیزیکی و واقعی نیاز دارد که حداقل به یک کتابخانه یا کتاب‌فروشی مراجعه کرده و اطلاعات موردنیاز خویش را استخراج کند. اما برای به‌دست‌آوردن همین اطلاعات در فضای مجازی کافی است که با استفاده از یک رایانه به اینترنت متصل شده، تا دریایی از اطلاعات را به فاصله‌ی یک‌چشم به‌هم‌زدن دریافت نماییم[۳] این سهولت و دسترسی سریع به اطلاعات و محتواها، فضای مجازی را به یک محیط پرجاذبه و منحصربه‌فرد تبدیل ساخته است. اما اگر چنان چه از این فضا استفاده می نامطلوبی شود، ممکن است آثار مخرب و جبران‌ناپذیری در پی داشته باشد. آثار نامطلوبی اعم از شکل‌گیری جرایم یا انحرافات اخلاقی به‌ویژه در قشر کم‌سن‌وسال به بار آورد. برای مثال: می‌توان به قضیه‌ی شبکه‌های رایانه‌ای تلرنت و دیتاپک اشاره کرد. استفاده‌کنندگان از این دو شبکه ظرف مدت یک هفته شکایت‌هایی به مسئولان شبکه تسلیم کردند و معترض شدند که افرادی به‌صورت غیرمجاز به سیستم آن‌ها دست‌یافته و مشکلاتی ایجاد کرده‌اند. چون استفاده الکترونیکی یاد شده وضع فراملی یافت

[۱] میتنیک، ک. سیمون، و. (۱۳۹۰). آموزش مقابله با مهندسی اجتماعی در هک. انتشارات طاهریان چاپ اول. ص ۷۸

[۲] وراوبی، ا، مؤمنی پور، ح، (۱۳۹۰) جرایم سایبری: از علت‌شناسی تا پیشگیری، ص ۵

[۳] مینولی، د. (۱۳۹۵). مهندسی اینترنت و اینترانت. (ترجمه او مهابادی). انتشارات آذرخش، چاپ دوم. ص ۸۳

پلیس کانادا به همکاری پلیس آمریکا از طریق خطوط الکترونیکی شبکه چهار نوجوان را در نیویورک دستگیر کردند. [1]

۳.۲.۲.۱. پیچیدگی و تخصصی بودن:

منظور از تخصصی بودن فضای مجازی وجود توانایی و قابلیت ورود به این فضا نیست، چراکه یک شخص کاملاً عادی با سطح سواد بسیار پایین قادر است با در اختیار داشتن یک رایانه‌ی شخصی در منزل خود، وارد فضای مجازی شود و منظور ما از این امر، صرف ورود به این فضا نیست. برنامه‌ریزی‌های رایانه‌ای تخصصی، تشخیص اقدامات آسیب‌زا در فضای مجازی، نحوه‌ی استفاده‌ای ایمن از این فضا، نحوه می شناسایی و مقابله با منحرفین سایبری، تأثیر فضای سایبر بر فرهنگ و جامعه و بسیاری از امور اساسی و کلیدی در این راستا باید بر آن را اشراف کامل داشت و نیازمند وجود تخصصی مناسب با پیچیدگی این فضا هستیم.

۳.۲.۱. انواع جرایم فضای مجازی

به‌رغم آنکه قانون جرائم رایانه‌ای، تا حدود قابل‌توجهی زمینه را برای مقابله با بزهکاری و بزه‌دیدگی سایبری فراهم کرده است.

دو مسئله قابل‌توجه، روند مبارزه با بزهکاران سایبری را کند می‌نماید. نخست اینکه، هر روزشمار جدیدی از بزه‌های سایبری کشف می‌شود که در قوانین مربوطه، جرم‌انگاری نشده‌اند. بدین ترتیب، بزهکاران سایبری همواره چند قدم از قانون‌گذاران و مجریان قانون جلوتر هستند. ازآن‌گذشته، مقابله با بزهکاران این جرائم، نیازمند تخصص بسیار بالای دستگاه‌های رسیدگی‌کننده است.

مجرمین سایبری، بر خلاف بزهکاران سنتی، عموماً در شمار افرادی هستند که از ضریب هوشی بالایی برخوردارند. قابل‌درک است که مبارزه با یک جیب بر، به‌مراتب راحت‌تر از مقابله با یک کلاهبردار رایانه‌ای است که از دانش و ذکاوت بالایی بهره می‌برد. اما گاهی جرائم تنها ماهیت مالی و اقتصادی را در بر نمی‌گیرد؛ چراکه فناوری‌های اطلاعاتی، انقلابی را ایجاد کرده که دیگر رؤیاپردازی‌های کنترل امورات زندگی بشر به دست هوش مصنوعی دورازذهن نیست. انقلاب اطلاعاتی و ارتباطی؛ شرکت‌ها و حتی دولت‌ها را مجاب کرده تا مهم‌ترین اسرار خود را در حافظه رایانه‌ها و سیستم‌های اداری پیشرفته بسپارند؛ به همین علت وابستگی افزایش جرائم علیه سیستم‌های پردازش داده طی دهه اخیر در بسیاری از کشورها خطری برای شرکت‌ها و دولت‌ها محسوب می‌شود؛ لذا در سطح ملی و بین‌المللی دغدغه‌هایی در مورد تهدید جدید «جرائم رایانه‌ای» موردتوجه قرار گرفته است. [2]

۱.۳.۲.۱. کلاهبرداری رایانه‌ای[3]

هر کس به طور غیرمجاز از سامانه‌های رایانه‌ای یا مخابراتی با ارتکاب اعمالی، همچون واردکردن، تغییر، محو، ایجاد یا متوقف کردن داده‌ها یا مختل کردن سامانه‌ها وجه، مال یا منفعتی را برای خود یا دیگری تحصیل کند؛ کلاهبردار رایانه‌ای محسوب می‌شود. به‌عنوان‌مثال، ممکن است بزهکار با مختل کردن فعالیت سایت یک بانک و در نتیجه ربودن اطلاعات کاربرانی که در حال انجام عملیات در آن سایت هستند، اقدام به ربودن اطلاعات آنها نموده و بدین‌طریق، حساب‌های آنها را خالی نماید. همچنین، ممکن است کلاهبردار رایانه‌ای، صفحه‌ای متقلبانه مشابه با یک سایت معتبر را

[1] وراویی، پیشین، ص ۶.
[2] فضلی، مهدی (۱۳۸۹)، مسؤولیت کیفری در فضای سایبر. چاپ نخست. تهران: انتشارات خرسندی
[3] ماده (۱۳): هر کس به طور غیرمجاز سامانه‌های رایانه‌ای یا مخابراتی با ارتکاب اعمالی از قبیل واردکردن، تغییر، محو، ایجاد یا متوقف کردن داده‌ها یا مختل کردن سیستم وجه یا مال یا منفعت یا خدمات یا امتیازات مالی برای خود یا دیگری تحصیل کند علاوه بر رد مال به صاحب آن به حبس از یک تا پنج سال یا جزای نقدی از بیست تا یک صد میلیون ریال یا هر دو مجازات محکوم خواهد شد.

ساخته و اطلاعات کسانی که به‌اشتباه رمز ورود خود را در این صفحه متقلبانه وارد می‌کنند؛ ربوده و سپس اقدام به سوءاستفاده از این اطلاعات نماید. کلاهبرداری رایانه‌ای از دسته جرائم اصلی سوءاستفاده‌های رایانه‌ای در باب جرائم اقتصادی رایانه‌ای است. دارایی‌های عینی غیرملموس در قالب داده‌های رایانه‌ای مانند وجوه سپرده یا ساعات کاری، معمول‌ترین راه‌های کلاهبرداری کامپیوتری را تشکیل می‌دهند. در تجارت مدرن (تجارت الکترونیک) نقل‌وانتقال پول و نقد و خریدوفروش کالای تجاری، به‌سرعت جای خود را به انتقال سپرده‌ها از طریق سیستم‌های کامپیوتری می‌دهد که در نتیجه امکانات بسیاری را برای سوءاستفاده فراهم می‌آورد. در ادامه به چند نمونه از سوءاستفاده رایانه‌ای در باب کلاهبرداری اشاره می‌شود:

الف) سوءاستفاده از شبکه تلفنی

ب) سوءاستفاده از صندوق‌های پرداخت

ج) سوءاستفاده از کارت‌های پلاستیکی (اعتباری)[1]

۲.۳.۲.۱. جعل رایانه‌ای

تغییر متقلبانه داده‌های رایانه‌ای به‌نحوی‌که فرد بتواند از این داده‌ها استفاده نماید؛ مصداقی از جعل رایانه‌ای است. به‌عنوان‌مثال، کارمند بانک ممکن است با دسترسی به شبکه حساب‌های بانکی، اقدام به دست‌کاری متقلبانه صورت‌حساب‌ها نماید. البته دایره شمول جعل رایانه‌ای تنها محدود به مؤسسات مالی و شرکت‌ها نیست. ممکن است یک دانشجو از طریق هک نمودن سایت استاد خود، اقدام به دست‌کاری اطلاعات آموزشی یا تغییر متقلبانه نمره‌های خود یا دیگران نماید. همچنین، تغییر در داده‌های موجود در کارت‌های حافظه نیز از جمله مصداق‌های جعل رایانه‌ای هستند. به‌عنوان‌مثال، مرتکب با ربودن فلش مموری فرد دیگر، اقدام به تغییر متقلبانه داده‌های موجود در آن می‌نماید. واردکردن، تغییر، محو یا موقوف سازی داده‌های رایانه‌ای یا برنامه‌های رایانه‌ای یا دیگر مداخلات در زمینه داده‌پردازی از طریق یا تحت شرایطی که در قوانین ملی تشریح شده است، متشکله جرم جعل است اگر به‌خاطر هدف‌های مرسوم، چنین جرمی ارتکاب یافته باشد. اصولاً جعل برخلاف کلاهبرداری رایانه‌ای، به‌منظور ایراد خسارت به اموال و تحصیل امتیاز مالی ارتکاب نمی‌یابد لیکن در اسناد به کار می‌رود. ایجاد خسارت (تغییر، تخریب) در داده‌ها و یا برنامه‌های کامپیوتری که این نوع فعالیت مجرمانه شامل دست‌یابی مستقیم یا مخفیانه غیرمجاز به سیستم‌ها و برنامه‌های رایانه‌ای با استفاده از برنامه‌های جعلی به نام ویروس، کرم، یا بمب‌های منطقی به‌منظور ایجاد خسارت از طریق پاک‌کردن داده‌ها.

۳.۳.۲.۱. سابوتاژ اصلاح، موقوف سازی و یا پاک‌کردن غیرمجاز داده‌ها

با عملیات رایانه‌ای به‌منظور مختل ساختن عملکرد عادی سیستم، آشکارا فعالیت مجرمانه به‌حساب می‌آید و به آن سابوتاژ رایانه‌ای می‌گویند. عناصر متشکله جرم سابوتاژ رایانه‌ای عبارت است از: ۱- ابزار و راه‌ها ۲- هدف نفوذکردن رایانه‌ای خدشه زننده‌ها: این نوع عمل مجرمانه شامل دسترسی‌های غیرمجاز به رایانه‌ها و نفوذ به سیستم‌های رایانه‌ای می‌شود که دارای انگیزه‌های گوناگونی است که مهم‌ترین آنها که قصد کنجکاوی، تفریح و تفنن بوده اصولاً به‌قصد آسیب‌رساندن و بهره‌برداری مالی انجام نمی‌گیرد و از نظر سنی بیشتر خدشه زنندگان جوانان و رده سنی ۱۵ تا ۲۴ قرار دارند.

[1] شیرزاد، ک. (۱۳۹۷). جرایم رایانه‌ای از دیدگاه حقوق جزای ایران و حقوق بین‌الملل، انتشارات بهینه فراگیر. چاپ اول. ص۳۲

۴.۳.۲.۱. استراق سمع غیرمجاز و تکثیر غیرمجاز

بنا به تعریفی که ارائه شده استراق سمع عبارت است از: «استراق سمع یا قطع که بدون حق و توسط ابزارهای تکنیکی بر روی ارتباطات، (وارده یا خارجه) در حدود یک سیستم با شبکه رایانه‌ای انجام شود» سرقت و تکثیر غیرمجاز برنامه‌های رایانه‌ای حمایت شده تکثیر و توزیع یا انتشار همگانی و بدون داشتن مجوز یک برنامه رایانه‌ای که تحت حمایت قانون است.

۵.۳.۲.۱. پورنوگرافی غیرمجاز رایانه‌ای[۱]

تعریف لغوی آن عبارت است: هرگونه نوشته، فیلم، تصاویر و مطالب مربوط به امور جنسی که فاقد هر گونه ارزش ادبی، هنری، سیاسی و علمی است و اعمال مجرمانه در پورنوگرافی عبارت است از اینکه: «شخصی از ابزار سمعی و بصری یا وسایلی که حاوی این‌گونه تصاویر و عکس‌های هرزه باشد را بفروشد، پخش کند یا چنین وسایل را در معرض نمایش گذارد یا کودکان و جوانان را به شرکت در این نمایش یا پورنوگرافی اغوا یا تشویق نماید.» [۲] قمار، پورنوگرافی و دیگر جرائم علیه اخلاق: باوجود غیرقانونی بودن قمار، کازینوهای آنلاین به طور وسیعی توسعه یافتند و در تعدادی از حوزه‌های قضایی، اینترنت برای پخش و توزیع مواد و دخانیات و مشروبات الکلی باوجود ممنوعیت، استفاده می‌شود.[۳]

۶.۳.۲.۱. جرائم چندرسانه‌ای

این نوع جرم که با جرائم نسل سوم رایانه و اینترنت وابسته است؛ اصولاً در محیط مجازی قابل‌تحقق است جرم چندرسانه‌ای شامل هر گونه فعالیت ممنوعه قانونی و یا اخلاقی در ارتباط با سوءاستفاده از تکنولوژی ارتباطات و رسانه است که به طور عمده مرتکبان ناشناس به طور اجتماعی در فضای ناشناخته دست به اعمال خود می‌زنند. [۴]

۷.۳.۲.۱. جرایم علیه عفت و اخلاق عمومی

یکی از مصداق‌های قابل‌توجه جرائم رایانه‌ای، جرائم علیه اخلاق عمومی یا همان هرزه‌نگاری رایانه‌ای است. باید توجه داشت که هرزه‌نگاری رایانه‌ای، امروزه در جهان مبدل به یک تجارت پرسود شده و همین مسئله نیز موجب گرایش بیشتر بزهکاران به ارتکاب این جرائم شده است. در حال حاضر، باندهای فراملی و سازمان‌یافته‌ای از هرزه‌نگاری رایانه‌ای وجود دارند که از طریق انتشار محتواهای غیراخلاقی درآمدهای سرشاری را کسب می‌کنند. متأسفانه، اغلب کودکان و نوجوانان به‌عنوان اقشار آسیب‌پذیر و نیازمند حمایت قربانی این جرائم هستند. قابل‌درک است که برای یک کودک قربانی این قبیل جرائم بودن، آثار مخرب شخصیتی به دنبال خواهد داشت. لزوم مبارزه به این جرائم به‌ویژه از آن روست که ابعاد تأثیرات این هرزه‌نگاری بسیار گسترده است. چنان‌که، ممکن است عکس تهیه شده از یک کودک قربانی جرائم غیراخلاقی، تنها در چند ثانیه در معرض مشاهده تمام کاربران اینترنت در سراسر جهان قرار گیرد. همچنین، برخلاف جرائم سنتی که امکان امحای آثار آنها حداقل در برخی موارد وجود دارد، در هرزه‌نگاری رایانه‌ای تا ابد آثار جرم باقی خواهد ماند و این تداوم

---

[۱] جلالی فراهانی، امیرحسین باقری اصل، رضا (۱۳۸۶). پیشگیری اجتماعی از جرائم و انحرافات سایبری مجله مجلس و پژوهش شماره ۱۲۴، ص ۵۵

[۲] دزبانی، م.ح. (۱۳۹۳) مقدمه‌ای بر ماهیت و تقسیم‌بندی تئوریک جرائم کامپیوتری (سایبری)، خبرنامه انفورماتیک، شماره ۱۸۷ ص:۱۵

[۳] مینولی، د. (۱۳۹۵). مهندسی اینترنت و اینترانت. (ترجمه او مهابادی). انتشارات آذرخش، چاپ دوم. ص۸۹

[۴] حسن‌بیگی، ا. (۱۳۹۳) آسیب‌شناسی شبکه جهانی اطلاع‌رسانی اینترنت و ارائه راهبردهای مناسب جهت مقابله با تهدیدها از دیدگاه امنیت ملی با تأکید بر جنبه‌های حقوقی و فنی، پایان‌نامه دکتری، دانشگاه عالی دفاع ملی ص:۵۶

آثار به منزله قربانی شدن هر روزه فرد خواهد بود.[1] قانون جرائم رایانه‌ای هم به علت اهمیت این قبیل جرائم، اقدام به‌مواجهه با مرتکبان آنها نموده است. بر همین اساس، تهیه و انتشار فیلم‌ها و تصاویر مستهجن از افراد در شمار مصادیق مجرمانه قرار دارد.[2]

۸.۳.۲.۱.سایر جرائم سایبری

جرائم سایبر فعالیت‌هایی هستند که در آن‌ها رایانه‌ها، تلفن‌ها و تجهیزات خانگی و سایر امکانات تکنولوژیک برای اهداف نامشروعی چون کلاهبرداری، سرقت، خرابکاری الکترونیکی، تجاوز به حقوق مالکیت افراد، سوءاستفاده جنسی از زنان و کودکان و شکستن و واردشدن به سیستم‌های کامپیوتری و شبکه‌ها مورداستفاده قرار می‌گیرد.[3]

در منابع موجود، انواع جرائم سایبر موردتوجه عبارت‌اند از:

۱) هک و فعالیت‌های مرتبط با آن: هک دسترسی‌پذیری بدون اجازه به سیستم‌های کامپیوتری، برنامه‌ها و اطلاعات و باز کردن فایل‌ها برای صدمه واردکردن است.
۲) ویروس و دیگر برنامه‌های خرابکارانه: ویروس‌ها و انواع کدهای مخرب بسیار آسیب‌زا هستند. یک ویروس خطرناک می‌تواند فایل‌ها را پاک کند و یا به سیستم‌ها آسیب دائمی برساند.
۳) ورود به حریم خصوصی: به معنای ورود عمدی به حوزه‌ی مالکیت دیگری بدون اجازه مالک یا استفاده‌کننده اصلی است. در فضای مجازی هیچ‌گونه ورود فیزیکی به حوزه‌ی خصوصی افراد صورت نمی‌گیرد، بلکه اطلاعات را می‌توان از طریق دیدن صفحه مانیتور کامپیوتر به دست آورد.
۴) کمین‌کردن، اذیت‌کردن و سخنان تنفرانگیز گفتن: کمین‌کردن و اذیت‌کردن، فعالیت‌های بدخواهانه هستند که بر ضد اشخاص خاص برای بدنامی و رسوایی‌شان انجام می‌شود. سایبر تروریسم: سایبر تروریسم به‌عنوان جرم، تحریکات سیاسی و حمله علیه اطلاعات، سیستم‌های کامپیوتری برنامه‌های کامپیوتری و اطلاعات تعریف می‌شود.[4]

۳.۱. بزه جنسی

بزه جنسی به دلیل وسعت شمول موارد و تأثیر منفی آنچه در فرد بزه‌دیده و چه در جامعه موردتوجه دانشمندان حقوق کیفری است، به همین دلیل بررسی مفهوم بزه جنسی و آثار آن ضروری می‌نماید.

۱.۳.۱. تعریف بزه جنسی

«جرم جنسی» به طیف وسیعی از رفتارهای جنسی غیراجتماعی اطلاق می‌شود که در قوانین هر کشوری جرم‌انگاری شده و برای آن مجازات تعیین گردیده است و همین مسئله وجه تمایز آن از خشونت‌های جنسی با خشونت‌های مبتنی بر جنسیت است. جرم جنسی به اشکال متعددی واقع می‌شود و تنها محدود به مقاربت‌های فاقد رضایت بزه‌دیده نمی‌شود؛ بلکه شامل هر گونه رفتار جنسی غیرقانونی از لمس تا تجاوز را در بر می‌گیرد. آنچه که برای ارائه تعریف از جرم تجاوز به عنف اهمیت دارد تمایز میان

[1] رضوی، م. صادقی، ر. (۱۳۹۹). اینترنت. انتشارات ستایش. چاپ اول. ص ۱۹۹

[2] امینی، محمد (۱۳۹۴) طبقه‌بندی و آسیب شناسی جرائم رایانه‌ای، تشربه علوم انتظام، ش ۳، ج ۶، ص:۱۲

[3] رمضان نرگسی، ر. (۱۳۸۴) تجاوز و بزه‌دیدگی زنان، فصلنامه کتاب زنان، شماره ۲۰. ص۱۱۸

[4] زندی، م. (۱۳۹۹)، تحقیقات مقدماتی در جرایم سایبری. انتشارات جنگل چاپ اول. ص ۱۸۷

اشکال مختلف جرم جنسی و تمایز میان جرم جنسی و خشونت جنسی است. میان واژه‌های تجاوز جنسی به عنف، [1] خشونت جنسی، [2] تعرضات جنسی[3] و آزار جنسی[4] و که گاهی اوقات به‌جای یکدیگر استفاده می‌شوند؛ تفاوت‌های زیادی وجود دارد. علاوه بر این معانی واژه‌ها بر حسب زمان، مکان و فرهنگ هر مملکتی متفاوت است.[5] همچنین تعاریف حقوقی از انواع خاص خشونت جنسی ممکن است متفاوت از تعاریف پزشکی یا جامعه‌شناختی آن باشد؛ لذا بسیار مهم است که متخصصان و پزشکان مربوطه از تعاریف حقوقی این جرم آگاه باشند.

۱.۱.۳.۱. خشونت جنسی

«خشونت جنسی» به معنای ارتکاب هر عمل جنسی، شروع به ارتکاب این فعل، پیشنهاد به برقراری یک رابطه جنسی (البته بدون رضایت فرد)، قاچاق جنسیتی زنان و...[6] است. استفاده از تهدید به ایراد صدمه و آسیب با استفاده از اجبار فیزیکی و صرف‌نظر از ارتباط مرتکب و بزه‌دیده و مکان وقوع جرم از عناصر این مفهوم هستند. بر اساس این تعریف طیف وسیعی از رفتارها از تجاوز جنسی با استفاده از اسلحه گرفته تا تجاوز با تهدید به اخراج از کار (اجازه کاذب) در این تعریف می‌گنجد. این اجازه کاذب می‌تواند به اشکال مختلف به دست آید به‌عنوان‌مثال تهدید به خشونت جسمی، تهدید به لغو و کسر منافع شغلی، تحمیل فشار روانی، اخاذی و... که در واقع رضایت و توافق در چنین موقعیت‌هایی حاصل نشده است. رضایت افرادی که ناتوان از درک موقعیت خود در حین تجاوز هستند؛ مانند افرادی که مواد مخدر یا الکل مصرف کرده‌اند یا افراد ناتوان ذهنی، نیز مخدوش است و تجاوز به آنها مصادیق خشونت جنسی است.[7]

خشونت جنسی به اشکال مختلف و متفاوتی از سایر جرائم واقع می‌شود. یک فرد می‌تواند به‌وسیله یک نفر یا به‌صورت جمعی مورد تجاوز قرار گیرد. تجاوز ممکن است با نقشه قبلی یا به‌صورت اتفاقی، در محل زندگی بزه‌دیده یا خانه مرتکب، محل کار، زندان، ماشین، خیابان و... واقع شود. مرتکب می‌تواند آشنا، دوست، غریبه، اعضای خانواده، زندانی هم بند، فقیر، ثروتمند، دانشگاهی و تحصیل‌کرده یا بی‌سواد، مذهبی یا غیرمذهبی و... باشد.[8] مرتکب ممکن است در یک موقعیت مهم و قابل‌احترام و اعتماد باشد مثل معلم یا افسر پلیس. ارتکاب این جرم در موقعیت‌هایی نظیر جنگ به‌عنوان ابزاری برای تضعیف روحیه دشمن استفاده می‌شود تجاوز و شکنجه جنسی، اجبار به ازدواج با سربازان دشمن از مصادیق استفاده ابزاری از این جرم است. بردگی جنسی، آزار جنسی، قاچاق زنان باهدف اجبار به فاحشگی، اجبار به حاملگی، اجبار به عقیم کردن، اجبار به سقط‌جنین، اجبار به ازدواج، معیوب‌سازی جنسی از جمله اشکال دیگر خشونت جنسی هستند. گاهی برخی مجرمان برای تسهیل تجاوز جنسی مواد مخدر، الکل و... مصرف می‌کنند. به زنی که مواد مخدر خورانده شود خیلی راحت‌تر تحت کنترل در می‌آید

---

[1] **Rape**

[2] **Sexual violence**

[3] **Sexual assault**

[4] **Sexual abus**

[5] زکوی، م. (۱۳۹۰). بزه‌دیدگان خاص در پرتو بزه‌دیده‌شناسی حمایتی، انتشارات مجد. ص ۷۹

[6] دهخدا، ع.ا. (۱۳۸۸) لغت‌نامه، دانشگاه تهران، انتشارات دانشکده ادبیات. ص۷۸۱

[7] صلاحی، ج. (۱۳۹۳) کلیات جرم‌شناسی و تئوری‌های جدید. چاپ اول. انتشارات مجد. ص ۴۳

[8] رضوی، م. صادقی، ر. (۱۳۹۹). اینترنت. انتشارات ستایش. چاپ اول. ص ۹۲

تاحدی‌که اجبار فیزیکی نیاز نیست؛ زیرا این مواد فرد را ناتوان و بی حس و در برخی موارد ناهوشیار می‌سازد. باملاحظه انواع خشونت جنسی به تفاوت آن با سایر اشکال جرم جنسی پی می‌بریم. به‌عبارت‌دیگر هر چند خشونت جنسی مفهومی است بسیار گسترده که شامل جرائم جنسی نیز می‌شود؛ ولی بسیاری از خشونت‌های جنسی جرم‌انگاری نشده‌اند و همین مسئله آنها را از جرائم جنسی متمایز می‌سازد.

۲.۱.۳.۱. تعرضات جنسی

در این نوع جرم فردی از قدرت و کنترل خود برای سیطره و تسلط بر دیگری استفاده می‌کند. تعرض جنسی شامل هر رفتار جنسی یا فعل تهدیدآمیز، خشونت‌بار و اجباری نسبت به فردی که رضایت ندارد یا قادر به رضایت‌دادن نیست، است. هرگونه تماس جنسی بدون رضایت فرد، اجبار به مقاربت دهانی، چشم‌چرانی، عریان‌گرایی، رشوه‌دادن برای برقراری رابطه جنسی و... از جمله مصادیق این جرم هستند. البته عمل ارتکابی زمانی عنوان تعرض جنسی به خود می‌گیرد که رابطه جنسی رابطه‌ای غیر از دخول باشد. آزار جنسی این جرم وقتی واقع می‌شود که یک فرد در موقعیتی از قدرت و برتری قرار دارد به‌طوری‌که طرف مقابل به واسطه اعتماد و احترامی که برای وی قائل است مرتکب چنین جرمی شود. این جرم ممکن است بین یک کودک و کودک بزرگ‌تر یا بزرگسال، یک فرد ناتوان و یک پرستار، یک بیمار و پزشک، فروشنده و مشتری واقع شود.

۳.۱.۳.۱. تجاوز جنسی به عنف

از نظر لغوی، «تجاوز» به معنای ظلم و تعدی[۱] است، در لغت‌نامه دهخدا، یکی از معانی این مفهوم، تخطی، تعدی، بیرون‌شدن از حد، حق و عدل است. [۲] تعریف اصطلاحی تجاوز به عنف نوعی رفتار خشن و تحقیرآمیز است که از طریق اعمال جنسی و برای ابراز قدرت و خشم صورت رد، در چنین مواردی، رابطه جنسی به‌ندرت موضوع اصلی است و در اکثر موارد مسائل جنسی در خدمت نیازهای غیرجنسی در می‌آیند. از نظر حقوقی تجاوز جنسی به عنف عبارت است از اجبار جسمی و فیزیکی با هر اجبار دردآور دیگری به مقاربت از مهبل یا مقعد با استفاده از یک شی، یا هر قسمت از بدن. در واقع این مفهوم به معنای تجاوز جنسی و رابطه جنسی به معنای بسیار خاص آن (دخول) است. موضوع موردبحث در این پژوهش، تجاوز جنسی به عنف است که به‌اختصار از آن به تجاوز به عنف یاد شده است. بزه‌دیده در این مفهوم می‌تواند هم مرد باشد وهم زن، هر چند برخی از مردان و پسران جوان، توسط مردان دیگر مورد تجاوز واقع می‌شوند، اما زنان، قربانیان اصلی تجاوزات جنسی هستند و درصد تجاوز به مردان نسبت به زنان بسیار ناچیز است. [۳]

۲.بزه‌دیدگی زنان در فضای مجازی از منظر جرم‌شناختی

۱.۲. فرایند بزه‌دیدگی

ارتکاب عمل مجرمانه که محور اصلی مطالعات جرم‌شناسی است، تنها نقض قانون و هنجار اجتماعی نیست؛ بلکه مشابه دیگر رفتارهای انسانی اصولاً باید هدفمند بوده و ناشی از وجود قدرت انتخاب باشد، به عبارتی می‌توان گفت غالباً عملکردی اختیاری است و انسان دست به یک سلسله انتخاب‌های استراتژیک عقلانی می‌زند. براین‌اساس نظریات مختلفی از سوی جرم‌شناسان مطرح گردید که دارای نوعی جهت‌گیری جامعه‌شناختی، زیست‌شناختی بود.

[۱] دهخدا، ع.ا. (۱۳۸۸) لغت‌نامه، دانشگاه تهران، انتشارات دانشکده ادبیات. ص ۹۱۱۹

[۲] دهخدا، ع.ا. (۱۳۸۸) لغت‌نامه، دانشگاه تهران، انتشارات دانشکده ادبیات

[۳] رمضان نرگسی، رضا، تجاوز و بزه‌دیدگی زنان، فصلنامه کتاب زنان، شماره ۱۳۸۲۰۲۲

برخلاف نظریه‌های جرم‌شناختی که توجه کمی به عوامل موقعیتی تعیین‌کننده جرم را داشتند، هدف اصلی این نظریه‌ها همچون نظریه مدل انتخاب عقلانی، شیوه زندگی، به بررسی فرایندهای اجتماعی و رخدادهای روان‌شناختی به‌عنوان دلایل وقوع جرم و فرایند عقلانی تصمیم‌گیری و انتخاب در بزهکاران است. [1]

۱.۱.۲. بزه‌دیدگان فاقد تأثیر در بزه‌دیدگی

تجربه بزه‌دیدگی در جرائم گوناگون با هم متفاوت است. به عبارتی می‌توان گفت برخی از بزه‌دیدگان در فرایند وقوع جرم از جایگاه بالاترین برخوردارند و حتی تجربه بزه‌دیدگی‌شان را باید جدی‌تر گرفت. این دسته از بزه‌دیدگان که در تحقق جرم هیچ نقشی نداشته‌اند و ناخواسته قربانی جرم شده‌اند را بزه‌دیدگان بی‌گناه می‌نامند و از آنها به بزه‌دیدگان ایده‌آل نیز یاد شده است، این دسته از بزه‌دیدگان بدون هیچ‌گونه انگیزه قبلی و حتی علم، نسبت به اینکه ممکن است قربانی جرم قرار بگیرند، قربانی می‌شوند و این خود می‌تواند ناشی از عوامل گوناگونی باشد. عواملی تحت شرایط ویژه‌ای چون سن (صغر و سالمندی)؛ وضعیت اجتماعی (مهاجران)، شغل و غیره که به‌نوعی استعداد خاص و آمادگی لازم برای بزه‌دیده شدن را در فرد ایجاد می‌کند و گروه دیگر از عوامل که استعداد ذاتی برای بزه‌دیدگی را در فرد ایجاد می‌کنند که اصطلاحاً به آن بزه‌دیدگان مادرزاد می‌گویند. [2]

استعداد بزه‌دیدگی تحت‌تأثیر شرایط ویژه سالمندان و به‌ویژه زنان سالمند و کودکان نمایانگر بزه‌دیده ایده‌آل هستند، کسانی که ناتوان و آسیب‌پذیر و بی‌گناه بوده و شایسته و نیازمند کمک و مراقبت هستند. در بزه‌دیدگی کودکان، اصولاً جرائم غیرعمدی و مالی مستثنی هستند و بیشتر سوءرفتارهای عمدی و بی‌توجهی‌های غیرمتعارف موردتوجه است. به عبارتی طفولیت به‌خصوص در طبقات فقیر با رفتارهای بد، بهره‌برداری و سوءاستفاده جنسی همراه است. حتی بزه‌دیدگی‌های غیرمستقیم علیه کودکان بیشتر اتفاق می‌افتد؛ چرا که آنها ممکن است شاهد وقوع جرمی به‌وسیله یکی از اعضای خانواده علیه دیگری باشند یا شاهد جرمی باشند که توسط غریبه‌ها علیه اعضای خانواده ارتکاب می‌یابد؛ حتی اگر این جرائم را هم مشاهده نکنند باز می‌توانند تحت‌تأثیر عوارض جرائم ارتکابی قرار بگیرند؛ مثلاً از وقوع سرقت از منزل تأثیر بپذیرند. این جرائم به‌عنوان جرم مستقل علیه کودکان در نظر گرفته نمی‌شود ولی می‌تواند آثار منفی روی کودکان داشته باشد. کهولت نیز خطر کشته‌شدن و موضوع سرقت قرارگرفتن را چندبرابر می‌کند. به‌عنوان‌مثال در جرم کیف زنی بیشتر قربانیان را سالمندان تشکیل می‌دهند که این دسته باتوجه‌به وضعیت فیزیکی و اجتماعی خود قربانی جرم شده‌اند و خود در آن هیچ نقشی نداشته‌اند.[3]

عامل دیگری که می‌توان مطرح کرد، شغل است. در هر پیشه‌ای مقدار خطر قربانی زایی وجود دارد. برخی شغل‌ها خطر بزه‌دیدگی بالاتری نسبت به بقیه دارند و قابل فرض است که محیط کار، یک محیط مناسب برای جرم فراهم می‌کند؛ چرا که محل کار کمتر امن بوده و مکان‌های عمومی و نیمه عمومی بیشتری دارد. به‌عبارت‌دیگر اشکال مختلف بزه‌دیدگی یکی از مخاطرات شغلی محسوب می‌شود که افراد شاغل در بخش‌های مختلف ممکن است به آن دچار شوند. مثلاً کارکنان بانک‌ها را خطرات سرقت بانک تهدید می‌کند، همچنین خطر سرقت در کمین داروخانه‌داران و افرادی که در سوپرمارکت‌ها کار می‌کنند است. خطر گروگان گرفته‌شدن در

[1] رایجیان اصلی، مهرداد (۱۳۹۰)، بزه‌دیده‌شناسی حمایتی، چاپ دوم، تهران: انتشارات دادگستر، ص: ۵۹

[2] . نجفی ابرندآبادی، علی حسین، هاشم بیگی، حمید (۱۳۸۷)، دانشنامه جرم‌شناسی، انتشارات دانشگاه شهید بهشتی، تهران

[3] شیرزاد، ک. (۱۳۹۷). جرایم رایانه‌ای از دیدگاه حقوق جزای ایران و حقوق بین‌الملل، انتشارات بهینه فراگیر. چاپ اول. ص ۶۲

کمین افرادی همچون دیپلمات‌های خارجی است و خلبانان هواپیماها را خطر هواپیماربایی و یا حتی انفجار هواپیما تهدید می‌کند. افرادی همچون پلیس، زندانیان که شغل آنها اقتضا می‌کند تا با بزهکاران در گیر باشند مستعد و دارای زمینه بزه‌دیدگی‌های جدی هستند. حتی آن دسته از افرادی که در کارهای غیرقانونی شرکت دارند خیلی بیشتر از افراد عادی مستعد بزه‌دیدگی هستند.

علاوه بر این، مباحث اقلیت‌ها (نژادی و قومی و دینی) نیز نقش بسزایی در بزه‌دیدگی افراد دارند. نقطه پیوند بزه‌دیدگی اقلیت‌ها جرم‌های برخاسته از نفرت هستند که در برخی از کشورها برای آن دسته جرم‌ها که به دلیل نژاد، قومیت، مذهب یا خاستگاه ملی بزه‌دیده برانگیخته می‌شوند، بکار برده می‌شود. به‌عنوان‌مثال در این زمینه نتایج پژوهش‌ها در آمریکا نشان داده است که هر دو اقلیت آسیایی و سیاهان آفریقایی بیش از سفیدها از بزه‌دیدگی رنج می‌برند. این در حالی است که میزان بزه‌دیدگی سیاهان بیش از آسیایی‌هاست. [1] موارد بیان شده نشان می‌دهد که در بسیاری از موارد بزه‌دیدگان بدون آنکه نقشی در ارتکاب جرم داشته باشند قربانی آن می‌شوند. افزودن بر عوامل یادشده این احتمال نیز وجود دارد که برخی از این دسته از بزه‌دیدگان در گروه بزه‌دیدگان اتفاقی قرار بگیرند که بر حسب اتفاق در مسیر بزهکار قرار گرفته و جرم نسبت به آنها به وقوع پیوسته است.

۲.۱.۲. بزه‌دیدگان مؤثردر بزه‌دیدگی

در بزه‌دیدگی باتوجه‌به مطالب پیش‌گفته در خصوص بزه‌دیدگان واقعی که هیچ نقشی در ارتکاب بزه علیه خویش نداشتند مطرح شد، در این قسمت به بررسی بزه‌دیدگانی که در تحقق جرم علیه خویش نقش داشته‌اند پرداخته می‌شود. این دسته از بزه‌دیدگان به طرق مختلف در ارتکاب جرم علیه خویش و نیز بزه‌دیده واقع‌شدن خویش نقش ایفا می‌کنند. به عبارتی این افراد به دو روش کلی زمینه‌های بزه‌دیده شدن خود را فراهم می‌کنند.

۱. بزه‌دیدگی به واسطه نقش بزه‌دیده (ویژگی‌های بالفعل) برخی بزه‌دیدگان به‌گونه‌ای عمل می‌کنند که زمینه‌های ارتکاب جرم از سوی بزهکار را بر خویش فراهم می‌سازند و در واقع با عمل خود قصد ارتکاب جرم را در بزهکار ایجاد می‌کنند. از جمله این موارد می‌توان به رفتار یا گفتار تحریک‌آمیز از سوی بزه‌دیده اشاره کرد. در این حالات قربانی جرم در واقع با بیان کلمات و یا انجام کارهایی بزهکار را نسبت به انجام جرم تشویق می‌نماید. هر چند که بزه‌دیده به شخصه چنین نتیجه‌ای را از فعل خویش انتظار نداشته باشد. این‌گونه موارد درواقع اغلب ایجادکننده انگیزه بزهکاری در فرد مجرم هستند و او را به‌سوی ارتکاب عمل مجرمانه سوق می‌دهد، لذا در این موارد است که حتی قانون‌گذار گفتار و یا رفتار بزه‌دیده را از علل مؤثر در میزان مسئولیت مرتکب جرم دانسته است.

۲. بزه‌دیدگی به واسطه ویژگی بزه‌دیده (ویژگی‌های بالقوه) در این فرض بزه‌دیده به واسطه ویژگی‌های خاص خود سبب تقویت انگیزه مجرمانه در بزهکار می‌شود. از مهم‌ترین موارد این ویژگی‌ها می‌توان به هم‌جواری [2] یا

[1] برنارد، توماس (۱۳۸۰)، جرم‌شناسی تطری (گذری بر نظریه‌های جرم‌شناسی)، مترجم علی شجاعی، سمت، تهران. ص:۹۱

[2] هم‌جواری یا نزدیک بودن: هنگامی که افراد از نظر فیزیکی و مادی به یکدیگر نزدیک می‌شوند امکان بروز اختلافات میان آنها بیشتر شده و در نتیجه امکان تحقق جرم نیز بیشتر می‌شود. این همان دیدگاهی است که طراحان مکتب شیکاگو از آن بهره جستند و اگر چه بیشتر در جرم‌شناسی محیط‌مدار استفاده شده است؛ اما در خصوص بزه‌دیدگان نیز کاربرد دارد؛ چرا که نزدیکی فیزیکی افراد منجر به افزایش روابط و به‌تبع، منجر به افزایش تنش‌ها و در نهایت بزه‌دیدگی یکی از طرفین خواهد شد. البته این ویژگی در جرائم جنسی بسیار حائز اهمیت است.

نزدیک بودن، جاذب بودن قربانی، [1] قابلیت وصول و دسترسی و... اشاره نمود. [2]

۳. بزه‌دیدگی جنسی زنان و راهکارهای پیشگیرانه از آن در فضای مجازی

۱.۳. بزه‌دیدگی جنسی زنان در فضای مجازی

بزه‌دیدگی جنسی زنان در فضای مجازی شامل طیف وسیعی از جرایم است که بررسی هر یک از آنها به‌صورت جداگانه ضروری است.

۱.۱.۳. هرزه‌نگاری زنان در فضای سایبر

تعریف لغوی «هرزه‌نگاری» (پورنوگرافی) عبارت است از: «هرگونه نوشته، فیلم، تصاویر و مطالب مربوط به امور جنسی که فاقد هر گونه ارزش ادبی، هنری، سیاسی و علمی بوده با قصد در معرض دید قراردادن امور جنسی انجام می‌گیرد.»

باتوجه‌به این تعریف رفتار بزهکارانه در هرزه‌نگاری را می‌توان این‌گونه تعریف کرد که شخصی ابزار سمعی و بصری با وسایلی که حاوی این‌گونه تصاویر و عکس‌های هرزه باشد را بفروشد، پخش کند با چنین وسایلی را در معرض نمایش گذارد و افراد را به شرکت در این نمایش یا پورنوگرافی اغوا یا تشویق نماید. در فضای مجازی نیز همانند فضای واقعی جنسیت نقش فعالی در بزه‌دیدگی جنسی دارد این نقش فعال برآیند شیوه متفاوت زندگی زنان و مردان و همچنین نقش گزینی آنان در جامعه است. هرزه‌نگاری زنان از جمله جرائمی است که به واسطه خصوصیات خاص زنانه که هم شامل ویژگی‌های جسمی و تحریک‌آمیز می‌گردد و هم ویژگی‌های روحی نظیر مهربان و شکننده بودن اغلب زنان، موجب بزه‌دیدگی زنان در فضای سایبر می‌گردد. [3]

به‌این‌ترتیب زنانی که به‌قصد غیر از هرزه‌نگاری اقدام به ارتباط با افراد در فضای مجازی می‌کنند؛ در معرض هرزه‌نگاری قرار می‌گیرند. در این دسته از جرایم که با محوریت ارتباط و هرزه‌نگاری جنسی انجام می‌گیرد بزهکار کسی است که مطابق امیال غریزی خود که ویژگی‌های فضای مجازی باعث تصحیح ابراز آن است، مرتکب جرم شود؛ بنابراین نقش جبر در ارتکاب این دسته از جرایم بسیار کم‌رنگ است چرا گه حتی جبرگرایی متعادل که به‌موجب آن، ارتکاب جرم مرتبط بامحتوا از جمله هرزه‌نگاری زنان کمتر تحت‌تأثیر اراده آزاد یا اختیار بوده و باوجود این که اراده آزاد نفی

[1] جاذب بودن قربانی: جذاب بودن در حالات مختلفی قابل‌طرح است و می‌تواند از دیدگاه‌های مختلفی موردبحث قرار گیرد. در جرائم جنسی ظاهر قربانی و نوع پوشش او و حتی لحن سخن‌گفتنش می‌تواند از موارد جذابیت قلمداد شود. در جرائم مالی میزان ثروت و مکنت بزه‌دیده علت اصلی جذابیت اوست. البته برخی موارد هستند که میان تمام بزه‌دیدگان در جرائم مختلف مشترک است مثل ضعف قربانی کاملاً معقول است که مجرمین به دنبال افرادی هستند که توان مقابله با آنها را نداشته باشند و بهتر بتوانند به خواست خود برسند. قابلیت وصول و دسترسی: در بسیاری موارد سهل‌الوصول بودن بزه‌دیده نقش عمده در گرایش بزهکار به ارتکاب جرم دارد. خصوصیات شخصی، خانوادگی، شغلی و فعالیت‌ها و رفتارهای بزه‌دیدگان سبب می‌شود خود را اهداف سهل‌الوصول برای تحقق جرم بنمایانند. به‌عنوان‌مثال در عمده موارد، خانه‌ها هنگامی مورد ورود غیرمجاز به‌قصد سرقت قرار می‌گیرند که هیچ‌کس در آنها نیست و یا افرادی که در مسیرهای تاریک و خلوت تردد می‌کنند گزینه مناسبی را در اختیار بزهکاران قرار می‌دهند.

[2] ۱ .انتشار محتوای حاوی تحریک، ترغیب، با دعوت به اعمال خشونت‌آمیز و خودکشی، (ماده ۱۵ قانون جر) ۲. تبلیغ و ترویج مصرف مواد مخدر، مواد روان گردان و سیگار. (ماده ۳ قانون جامع کنترل و مبارزه ملی با دخانیات ۱۳۸۵) ۳- باز انتشار و ارتباط (لینک) به محتوای مجرمانه تارنماها و نشانی‌های اینترنتی مسدود شده، نشریات توقیف شده و رسانه‌های وابسته به گروه‌ها و جریانات منحرف و غیرقانونی ۴ .تشویق تحریک و تسهیل ارتکاب جرائمی که دارای جنبه عمومی هستند از قبیل اخلال در نظم، تخریب اموال عمومی، ارتشاء، اختلاس، کلاهبرداری قاچاق مواد مخدر، قاچاق مشروبات الکلی و غیره. (ماده ۴۳ ق.م.) ۵ - تبلیغ و ترویج اسراف و تبذیر. (بند ۳ ماده ۶ ق.م)

[3] صلاحی، ج. (۱۳۹۳) کلیات جرم‌شناسی و تئوری‌های جدید. چاپ اول. انتشارات مجد. ص ۴۷

نمی‌شود، به‌طورجدی از عواملی همچون شرایط حاکم بر جامعه، تأثیر امیال و غریزه‌های حیوانی، وجود محیطی عاری از نظارت و کنترل و... متأثر بوده است؛ بنابراین در اعمال خلاف قانون و اخلاق مرتبط بامحتوا- به‌ویژه اعمال مرتبط با جنسیت - مرتکب یک فرد سود انگار و حسابگر نیست، بلکه اراده وی عموماً تحت‌تأثیر عوامل درونی و بیرونی است.

منطبق با تعاریفی که در دکترین ارائه شده است هرزه‌نگاری زنان در فضای مجازی را می‌توان این‌گونه تعریف کرد: تولید، انتشار با معامله محتویاتی با مضمون نمایش اندام جنسی زنان با نمایش آمیزش با عمل جنسی صریح میان انسان با انسان با حیوان از طریق سیستم‌های رایانه‌ای با مخابراتی با این محتویات اعم از تصویر با صدا است که ممکن است به طور مشترک با فردی تولید با منتشر شوند که مراد از اندام جنسی زنانه، اندام‌های برجسته در زنان است که مرد فاقد آن است. هرزه‌نگاری کلاسیک که درگذشته وجود داشته است با به‌وجودآمدن فضای مجازی، اینترنت و شبکه‌های اجتماعی روی تازه‌ای به خود دیده است چرا که خصوصیات فضای مجازی باعث گردیده است که محتوای جنسی به‌سرعت گسترش یابد و در برخی از موارد عمومیتی یابد که فراتر از انتظار باشد (به‌عنوان‌مثال در کشور خودمان انتشار تصاویر پورنوگرافی بازیگر سابق تلویزیون که به‌صورت وسیعی گسترش یافت).

اهمیت این جرم در زمانی برای ما آشکار می‌شود که بدانیم علاوه بر بزه‌دیدگی زنی که تصاویر وی پخش شده است بزه‌دیده‌ی ثانی و ثالث نیز وجود دارد که باید به آنها نیز توجه نمود برای مثال زنی که تصاویر وی به نمایش گذاشته شده است و یا در سطح وسیعی پخش شده است می‌تواند دارای همسری باشد که به‌عنوان بزه‌دیده نخستین شناخته نمی‌شود؛ ولی عدم توجه به وی در سیستم عدالت کیفری می‌تواند هزینه‌های جبران‌ناپذیری مانند انتقام شخصی را به بار بیاورد. همچنین باید به تأثیری که در جامعه بر اثر این تصاویر هرزه ایجاد می‌شود نیز توجه کرد. برای مثال: بسیاری از پژوهشگران، تبلیغ آزادانه زنان روسپی و هرزه‌نگاری در شبکه‌های ماهواره‌ای و اینترنتی را عمده‌ترین عامل تجاوز به حقوق جنسی زنان می‌دانند که تمایلی به دیدن با اجرای محتوای آن‌ها، تحت‌فشار شریک جنسی خود، ندارند. خردکردن شخصیت زن در فیلم‌های مبتذل، آمادگی روسپیان برای نمایش زننده‌ترین اعمال، استفاده از مانکن‌ها برای تبلیغات تلویزیونی با تأکید بر زیبایی و جنسیت، عادی جلوه‌دادن خشونت‌بارترین روابط جنسی، روابط جنسی گروهی که مصداق بارز خشونت علیه زنان به شمار می‌آید و صدها مورد دیگر، نمونه‌هایی بارز از آموزش خشونت جنسی به شمار می‌آید که علاوه بر شبکه‌های ماهواره‌ای و اینترنتی، در تلویزیون سراسری و مطبوعات بسیاری از کشورهای جهان عادی شده است.[1]

به‌طورکلی رسانه‌ها از دو جهت عامل خشونت جنسی علیه زنان به شمار می‌روند که منحصر به آن‌ها است. نخست، تبدیل زن به کالا از طریق استفاده تبلیغاتی از زیبایی زن در پیام‌های بازرگانی و نمایش روابط خصوصی جنسی از انواع مختلف آن به‌عنوان صحنه طبیعی از فیلم‌ها، تئاترها و مستندها. دوم، طبیعی جلوه‌دادن تعرض جنسی بدون وجود رابطه قانونی میان طرفین. ۲

ماهیت اینترنت به‌گونه‌ای است که می‌تواند باعث پیشرفت بسیاری در زمینه‌های مختلف شود؛ اما خصوصیات اینترنت در عرصه کیفری می‌تواند صدمات جبران‌ناپذیری را به بزه‌دیده و جامعه وارد آورد. خصوصیات فضای مجازی باعث شده است که زنان که قدرت حضور

[1] جوان جعفری، ع. (۱۳۹۹) جرایم سایبر و رویکرد افتراقی با نگاهی به قانون مجازات اسلامی بخش جرایم رایانه‌ای. مجله دانش و توسعه علمی - پژوهشی. سال هفدهم. شماره ۳۴

کمتر و مشارکت کمتری در جامعه واقعی داشته‌اند جبران شده و در این فضا مشارکت فعالی در تهیه اطلاعات و انتشار آن داشته باشند چرا که موانع فضای واقعی در فضای مجازی وجود ندارد؛ اما از طرفی به واسطه جرایم خاصی که علیه زنان بیشتر اتفاق می‌افتد فضای مجازی تهدیدی علیه آنها محسوب می‌شود.

۲.۱.۳. قاچاق اینترنتی زنان

علی‌رغم برچیده‌شدن نظام برده‌داری در قرن ۱۸ و ۱۹ میلادی در جهان این پدیده در قالب قاچاق انسان ادامه دارد، لذا بهره‌کشی و استفاده ابزاری از کودکان و زنان نه‌تنها در دوره الغای برده‌داری کمتر نشده؛ بلکه دامنه آن نیز گسترش‌یافته است که با پیشرفت‌های علمی جدید نه‌تنها بهره‌کشی هدف اصلی از ارتکاب این جرم است؛ بلکه فروش اعضای آنان نیز مدنظر قرار گرفته است که از برده‌داری نوین در عصر حاضر سخن به میان می‌آید. در این میان قاچاق زنان و دختران توسط نهادهای سازمان‌دهی شده در نقاط مختلف جهان بحث‌برانگیز شده است. افراد سازمان‌دهی شده زنان و دختران را که به دنبال کار و درآمد هستند به این بهانه فریب داده و به‌صورت برده و اسیر توسط راه‌های دریایی به مقاصد خود می‌رسانند. [۱]

باتوجه‌به گستردگی و اهمیت این موضوع در ادامه با بررسی مفهوم قاچاق به رابطه قاچاق زنان و فضای مجازی و بالاخص اینترنت می‌پردازیم.

۱.۲.۱.۳. مفهوم قاچاق و قاچاق زنان

در معنای لغوی «قاچاق» برگرفته از واژه‌ی ترکی «قاچماق» به معنای گریزاندن، فرار و ترک وطن است.[۲]

قاچاق در معنای آن را می‌توان این‌گونه تعریف نمود: «انتقال پنهانی یک چیز از یک نقطه‌به‌نقطه دیگر که همان‌گونه که می‌تواند به شکل‌های مختلف و تمهیدات پنهان‌سازی متنوع صورت گیرد، می‌تواند گونه‌های مختلفی داشته باشد». به‌عبارت‌دیگر بر اساس نوع چیزی که به‌صورت پنهانی از مکانی به مکان دیگر منتقل می‌شود می‌توان از قاچاق مواد مخدر، قاچاق انسان، قاچاق اسلحه، قاچاق مواد هسته‌ای، قاچاق اعضای بدن و... سخن به میان آورد. اما بدون توجه به نوع کالایی که جابه‌جا می‌شود همه آن‌ها را می‌توان تحت عنوان کلی قاچاق قرار داد.[۳]

در مورد قاچاق اشخاص دو مفهوم از اسناد بین‌المللی برداشت می‌شود که بازگردان آن به فارسی به‌درستی انجام نگرفته است. آن دو مفهوم «*Trafficking*» و «*smuggling*» است. به بیان ساده می‌توان گفت که «*smuggling*»اشاره به انتقال غیرقانونی مهاجران به مقاصد موردنظرشان جهت تحصیل منافع مادی است درحالی‌که «*Trafficking*»به‌نوعی همان عمل انتقال انسان‌ها است با این تفاوت که موضوع این انتقال قربانیانی هستند که به‌منظور نگهداری در شرایط شبیه بردگی با فحشای اجباری انتقال داده می‌شوند. به‌عبارت‌دیگر، واژه‌ی نخست اشاره به حالتی دارد که قاچاقچیان به‌زور و با فریب اشخاصی را به‌ویژه زنان و کودکان را برای مقاصد سودآور مختلف قاچاق می‌کنند و واژه‌ی دوم اشاره به حالتی دارد که گروه‌های بزهکار داوطلبان مهاجرت غیرقانونی را با گرفتن هزینه صرفاً به مقصدهای موردنظر آنان می‌رسانند در نهایت

[۱] عالی‌پور، ح (۱۳۹۶). مجموعه مقاله‌های همایش بررسی جنبه‌های حقوقی فناوری اطلاعات معاونت حقوقی و توسعه قضایی قوه قضائیه. مرکز مطالعات توسعه قضایی، انتشارات سلسبیل. چاپ اول. ص ۸۱

[۲] حبیب‌زاده و همکاران، ۱۳۸۸، ص ۱۰۳

[۳] معظمی، ۱۳۸۶، ص ۹۹

پس از رساندن به مقصد نیز آنها را با ترفندهایی استثمار می‌کنند.[۱]

برخی از منابع ۲ از آمار، سالانه میان ۷۰۰ هزار تا دو میلیون زن در سطح جهان که موضوع قاچاق قرار می‌گیرند سخن به میان آورده‌اند.

به طور خلاصه می‌توان گفت: «قاچاق انسان عبارت است از جابه‌جایی انسان از طریق اغفال، اجبار، تهدید یا مانند آن برای بهره‌کشی فرد به‌ویژه بهره‌کشی جنسی.»

۲.۲.۱.۳. قاچاق زنان

قاچاق زنان به دلیل اهمیت خاص آن در اسناد بین‌المللی آمده به‌گونه‌ای که در خصوص آن این‌گونه تعریف شده است. اولین تعریف از سوی مجمع‌عمومی ملل متحد در سال ۱۹۹۶ ارائه شده و در مورد قاچاق زنان این‌گونه می‌گوید: حرکت‌دادن غیرقانونی و مخفیانه اشخاص در عرض مرزهای ملی، عمدتاً از کشورهای درحال‌توسعه و کشورهای دارای اقتصاد در حال گذار باهدف نهایی واداشت زنان و دختران به وضعیت‌های بهره‌کشانه و ستمگرانه از لحاظ جنسی و اقتصادی به‌منظور سود به‌کارگیرندگان، قاچاقچیان و سندیکاهای جنایت‌کار و نیز دیگر فعالیت‌های مرتبط با قاچاق همچون کارخانگی اجباری، ازدواج دروغین، استخدام مخفیانه و فرزندخواندگی دروغین. در پروتکل پیشگیری، سرکوب و مجازات قاچاق انسان، به‌ویژه زنان و کودکان، مصوب سال ۲۰۰۰، در ماده‌ی سوم، قاچاق زنان بدین ترتیب تعریف شده است: «استخدام، انتقال، حمل‌ونقل، پناه‌دادن با دریافت اشخاص به‌وسیله تهدید با به‌کارگیری زور، یا دیگر اشکال تحمیل، آدم‌ربایی، تقلب، فریب، سوءاستفاده از قدرت با موقعیت آسیب‌پذیری با دادن با دریافت پرداخت‌ها با منافع جهت کسب رضایت فردی که بر شخص دیگری کنترل دارد، به‌منظور بهره‌کشی.»[۱] بهره‌کشی باید حداقل بهره‌کشی از روسپی‌گری دیگران یا دیگر اشکال بهره‌کشی جنسی، کار یا خدمات اجباری بردگی یا رویه‌های مشابه بردگی، بیگاری یا برداشتن اندام‌های بدن را در بر بگیرد. به دلیل زمینه‌سازی سایر جرایم مانند فحشا، برده‌داری و غیره با قاچاق زنان این پدیده از گذشته موردتوجه قرار گرفته و واکنش‌های مختلفی به طور خاص در این زمینه در نظر گرفته شده است.[۲]

با گسترش اینترنت و تبلیغ مواردی مانند کسب درآمد در کشورهای دیگر یا اخذ اقامت تحصیلی و غیره در کشورهای دیگر زمینه برای فریب زنان و دختران توسط باندهای قاچاق انسان فراهم شده است. قاچاق جنسی از جمله جرایم سازمان‌یافته بین‌المللی است، دلیل سازمان‌یافتگی آن می‌تواند منافع مادی سرشار و اقتصادی این جرم باشد. ناشناس بودن و نداشتن امنیت در فضای مجازی موجب تسهیل در کار افراد این سازمان‌ها شده است. فضاهای ارتباطی در اینترنت نظیر اتاق‌های گفت‌وگو،[۳] وب‌سایت‌ها،[۴] سایت‌های اجتماعی نظیر فیس‌بوک،[۵] تلگرام[۶] و اینستاگرام[۷] و... با افراد آشنا شده و پس از جلب‌اعتماد آنان، به طور مستقیم برای مثال تحت عنوان مهاجرت سریع یا غیرمستقیم با وعده‌های توخالی و دروغین جذب کرده و سبب قاچاق و انتقال آنان می‌شوند.[۸]

---

[۱] سیدزاده ثانی، م. (۱۳۹۲). کتاب راهنمای قانون مجازات اسلامی، انتشارات خرسندی. چاپ دوم. ص۱۹

[۲] ده آبادی، ا. سلیمی، ا (۱۳۹۳). اصول جرم‌انگاری در فضای سایبر (با رویکردی انتقادی به قانون جرایم رایانه‌ای). فصلنامه مجلس و راهبرد. سال بیست و یکم. شماره ۱۸۰

[۳] rooms

[4] Web sites
[5] Face book
[6] Telegram
[7] Instagram

[۸] شیرزاد، ک. (۱۳۹۷). جرایم رایانه‌ای از دیدگاه حقوق جزای ایران و حقوق بین‌الملل، انتشارات بهینه فراگیر. چاپ اول. ص ۶۷

زنان مانند کودکان نسبت به مردان در مقابل قاچاق انسان خصوصاً به‌منظور استفاده ابزاری جنسی آسیب‌پذیرند. بانوانی که با به واسطه فضای سایبر بزه‌دیده جرم قاچاق قرار می‌گردند از چند بعد بزه‌دیده می‌شوند؛ از نظر جسمانی و با اعمال خشونت‌هایی که علیه زن انجام می‌شود؛ مانند بیگاری، ضرب‌وجرح و تجاوز و... همچنین از بعد روانی و احساس مورد سوءاستفاده واقع‌شدن و حس انتقام‌جویی در زن بزه‌دیده و مشکلات روانی پس از سانحه. این اعمال ممکن است مشکلاتی را در جامعه مانند ترد شدن توسط خانواده و... را در پی داشته باشد.

۳.۱.۳. آزار و اذیت زنان به‌واسطه‌ی اینترنت

در خصوص پدیده آزار و زنان که در فضای مجازی انجام می‌گیرد؛ تعریف دقیقی ارائه نشده است، اما این واژه، برای اشاره به استفاده از اینترنت، پست الکترونیک و یا سایر ابزارهای ارتباطی الکترونیک برای ایجاد مزاحمت برای افراد دیگر به کار می‌رود. مزاحمت عموماً شامل آزار و همراه با رفتار تهدیدآمیزی است که فردی به طور مکرر در مورد فرد دیگری بکار می‌برد. اگرچه آزار و تهدید کامپیوتری می‌تواند اشکال متعددی داشته باشد، مزاحمت اینترنتی وجود تشابهی با مزاحمت در جهان واقعی دارد بسیاری از مزاحمان اینترنتی با در جهان واقعی به انگیزه کنترل قربانی‌هایشان دست به عمل می‌زنند و برای رسیدن به این هدف رفتار مشابهی دارند.

در این راستا می‌توان اذعان نمود که مزاحمت در دنیای مجازی که بر خلاف مزاحمت در فضای واقعی نیازمند ارتباط فیزیکی با بزه‌دیده نیست، باز هم سبب ایجاد ترس و نگرانی در قربانی که عموماً زن هم هست می‌گردد. تشابه ایذا در فضای مجازی و جهان واقعی به‌گونه‌ای است که این دو جرم را مشابه هم قرار می‌دهد[1] و ازاین‌رو می‌توان استدلال نمود که یافته‌های مرتبط با ایذا ارتکابی در جهان واقعی دررابطه‌با محیط‌های مجازی نیز قابلیت انطباق داشته باشد. فراگیری اینترنت و فراوانی استفاده روزمره آن در امور معمول موجب می‌شود تا مزاحمان بتوانند از سهولت ارتباطات به‌اندازه سهولت دستیابی به اطلاعات شخصی افراد سوءاستفاده نمایند. به‌علاوه، سهولت استفاده یک‌طرفه، غیرشخصی و گاه طبیعت ناشناس ماندن ارتباطات اینترنتی، ممکن است موانع مزاحمت اینترنتی را مرتفع کند. به‌عبارت‌دیگر، درحالی‌که یک مزاحم بالقوه ممکن است نسبت به‌مواجهه با قربانی به‌صورت شخصی یا با تلفن بی‌علاقه و یا ناتوان باشد، در ارسال پیام‌های آزاردهنده و یا تهدیدآمیز به قربانی تردید نمی‌کند. سرانجام، آزار و تهدید کامپیوتری، مثل مزاحمت جسمی می‌تواند مقدمه رفتار جدی‌تر باشد که شامل خشونت فیزیکی هم می‌شود.[2]

در خصوص چگونگی انجام‌گرفتن این مزاحمت‌ها می‌توان که فعل مزاحمت می‌تواند از روش‌های مختلفی و با انگیزه‌های گوناگون این آزار و اذیت‌ها علیه زنان اعمال گردد. در مواقعی بزهکاران با دست‌کاری وسیله متصل به اینترنت، بزه‌دیده را ناچار به تماشای تصاویر پورنوگرافی می‌کنند و یا با پخش موضوعات با محتوای پورنوگرافی جنسی آنان را آزار می‌دهند. همچنین مزاحم می‌تواند با آشکارکردن هویت قربانی و ارسال پیغام‌های تحریک‌کننده به اتاق‌های گپ‌زنی، باعث شود بینندگان آن، پیغام‌های آزاردهنده را به بزه‌دیده ارسال کنند. مزاحمان پیچیده‌تر، از برنامه‌هایی استفاده می‌کنند که با آن در دفعات منظم یا نامنظم پیام‌هایی را برای قربانی ارسال می‌کنند، بدون این که خود مزاحم ناچار باشد هر دفعه پای کامپیوتر بنشیند و برنامه را اجرا کند. مزاحمان باتجربه‌تر می‌توانند پیغام‌هایی بفرستند که کشف فرستنده آن غیرممکن باشد. این

[1] بهره‌مند، ح. کوره‌پز، ح. سلیمی، ا. (۱۳۹۹). راهبردهای وضعی پیشگیری از جرایم سایبری. آموزه‌های حقوق کیفری. شماره ۷. ص ۳۳

[2] صلاحی، ج. (۱۳۹۳) کلیات جرم‌شناسی و تئوری‌های جدید. چاپ اول. انتشارات مجد. ص ۵۵

مزاحمت‌ها به‌صورت افترا به فرد هم صورت می‌پذیرد. افترا فارغ از فرم و شکل کلاسیک آن یعنی اسناد جرم به نحو ارتجالی به‌غیراز طریق نطقی در مجامع و... در این حالت یعنی حالت سایبری می‌تواند به شکل بولتن الکترونیکی و محتوای افتراآمیز، از طریق پست الکترونیک و... ارتکاب یابد.[1] یعنی از پست الکترونیک برای ارسال یا در دسترس قراردادن مطالب افتراآمیز خواه در اصل فایل یا به‌صورت فایل همراه استفاده می‌شود. گاه از پست الکترونیک برای مطالب حاوی فحاشی و توهین استفاده می‌شود، مطلبی که می‌تواند تعدادی را ناراحت کند یا حتی فردی را برنجاند و به شکل پست الکترونیک ارسال می‌شود. حتی ارسال پیام‌ها با محتوای ناخواسته[2] در این گروه قرار می‌گیرد. لزومی ندارد محتوای پست الکترونیکی منفی و مضر باشد؛ بلکه عدم وجود رضایت دریافت‌کننده برای تحقق مزاحمت کفایت می‌کند.

مزاحمت‌های اینترنتی را می‌توان به انواع زیر تقسیم نمود:

۱. مزاحمتی که در فضای مجازی (سایبر) صورت می‌گیرد و در همان جا ادامه می‌یابد.
۲. مزاحمتی که در فضای مجازی (سایر) آغاز می‌شود و به فضای زندگی واقعی گسترش می‌یابد. این زمانی است که یک مزاحم ممکن است تلاش کند شماره‌تلفن با آدرس منزل قربانی را به دست آورد.

انواع مزاحم‌های اینترنتی شامل موارد زیر می‌شوند:

۱. مزاحم معمولی مجنون: این مزاحم فردی است که باور نمی‌کند رابطه‌اش با قربانی به طور کامل قطع شده است. وی را با یک عاشق بی‌خطر نباید اشتباه گرفت.
۲. مزاحم اینترنتی روان‌پریش: باور غلطی دارد که باعث وابستگی‌اش به قربانی می‌شود. او خیال می‌کند که قربانی وی را دوست دارد، حتی اگر هرگز وی را ندیده باشد. چنین مزاحمی اغلب فردی منزوی است و اغلب قربانیان خود را از میان زنان متأهل و فعال اجتماعی، مثل دکترها و معلمان انتخاب می‌کند. خلاص‌شدن از شر این مزاحم مشکل است.
۳. مزاحم انتقام‌جو: این فرد، به دلایل کوچکی که یا واقعی و یا حتی خیالی است، از قربانی خود عصبانی است. برای مثال، برخی از کارکنان اخراج شده بر این باور هستند که خودشان قربانی شده‌اند و باید از صاحب‌کار خود انتقام بگیرند. در مورد زنان، همسران قبلی آنان می‌توانند تبدیل به این نوع مزاحم شوند. مزاحمان اینترنتی با انگیزه‌های مختلفی دست به این آزار و اذیت می‌زنند[3].

۲.۳. راهکارهای پیشگیرانه از بزه‌دیدگی جنسی زنان در فضای مجازی

آنچه که مهم‌تر از حمایت‌های پس از بزه‌دیدگی است پیشگیری از بزه‌دیدگی است؛ چراکه هیچ روشی نمی‌تواند خسارات روانی ناشی از بزه را به طور کامل جبران نماید؛ لذا بهتر است که پیشگیری از بزه‌دیدگی محور تصمیمات کلان جنایی قرار گیرد، دراین‌خصوص می‌توان از چند جهت پیشگیری نمود.

۱.۲.۳.جرم‌انگاری تعرض به حریم خصوصی در فضای سایبر

[1] زندی، م. (۱۳۹۹)، تحقیقات مقدماتی در جرایم سایبری. انتشارات جنگل چاپ اول. ص ۱۹۸

[2] Spam

[3] عالی‌پور، ح (۱۳۹۶). مجموعه مقاله‌های همایش بررسی جنبه‌های حقوقی فناوری اطلاعات معاونت حقوقی و توسعه قضایی قوه قضائیه. مرکز مطالعات توسعه قضایی، انتشارات سلسبیل. چاپ اول. ص ۸۵

فضای سایبر بر خلاف اصول گذشته زمینه‌های تهدید و تعرض به اصل حفظ حریم خصوصی را بیشتر کرده است. از آن جا که این اصل به حریم و خلوت افراد مربوط می‌شود، نسبت به دیگر اصول بیشتر موردتوجه قرار گرفته و در این زمینه قوانین و مقررات سخت و لازم‌الاجرایی به تصویب رسیده است. به زبان ساده می‌توان گفت حریم خصوصی از آن دست مفاهیمی است که همه آن را می‌فهمند و درک می‌کنند اما نمی‌توانند تعریفی جامع و کامل از آن ارائه نمایند و بدین خاطر در اغلب موارد ما شاهد نوعی تعارض و یا حتی چالش در زمینه‌ی مسائل مربوط به حریم خصوصی هستیم.[1]

برخی از تدابیر پیشگیرانه در فضای سایبر حریم خصوصی الکترونیکی افراد را می‌تواند مورد تهدید یا تعرض قرار دهد. به طور مثال ابزارهای نظارتی که تردیدی در تعرض‌آمیز بودن آن‌ها نیست، در عین حالی که بازدارنده نیز هستند، تأثیرات سوء مستقیم و غیرمستقیم بسیاری بر فعالیت‌های شبکه‌ای می‌گذارند. چنانچه در محیطی این حس در مردم بیدار شود که به دلیل بی‌اعتمادی به آن‌ها همواره تحت نظارت قرار دارند این امر به‌شدت در نحوه‌ی فعالیت آن‌ها تأثیر خواهد گذاشت، اکنون فعالیت‌های مختلف اقتصادی، اجتماعی، فرهنگی و... بسیار متنوعی در فضای سایبر جریان دارد که تمامی آن به‌خاطر آزاد و عاری بودن این فضا از هر گونه محدودیت است. اما چنان چه کاربران شبکه‌ای احساس کنند فعالیت‌های آن‌ها تحت نظارت مستمر زنده یا غیرزنده قرار دارد، بی‌تردید در نحوه‌ی فعالیت خود تجدیدنظر خواهند کرد که این خود به معنای ناکام ماندن اهدافی است که از ظهور این فضا دنبال می‌شد.[2]

یکی دیگر از تدابیر پیشگیرانه که به‌صورت غیرمستقیم می‌تواند حریم افراد را در فضای سایبر تهدید کند، سیستم‌های تأیید هویت است. در فضای مجازی برای این که به اشخاص اجازه‌ی ورود به محیط‌های خاصی داده شود، برخی اطلاعات شامل اطلاعات شخصی یا حتی اطلاعات شخصی حساس می‌شود، از آن‌ها اخذ می‌گردد. نگرانی‌ای که در این جا وجود دارد راجع به امکان سوءاستفاده‌ی متصدیان این سایت‌ها از این اطلاعات و امکان افشای آن‌ها به دلایل مختلف نظیر فقدان یک سیستم امنیتی کارآمد جهت حمایت از آن‌ها است. البته باید اذعان نمود که بزه‌دیدگان سایبری نیز نقش بسیار مهمی در بروز بسیاری از جرایم ناقص حریم خصوصی ایفا می‌کنند و درعین‌حال می‌توانند در اقدامات پیشگیرانه علیه جرایم سایبری نقش‌آفرین باشند. بسیاری از بزه‌دیدگان و کسانی که حریم خصوصی آن‌ها در فضای مجازی نقض می‌گردد، استعداد قابل‌توجهی برای قربانی شدن از خود بروز می‌دهند و به‌راحتی طعمه‌ی بزهکاران سایبری می‌شوند. وجود ضعف شخصیتی، فقدان اطلاعات کافی دررابطه‌با محیط مجازی و عدم دقت در محافظت از داده‌ها و... مواردی است که قربانی بزه سایبری را در قربانی شدنش مساعدت می‌کند. این اشخاص باید نسبت به صیانت از حریم خصوصی خویش در فضای سایبر همت گمارند. البته نقش دولت و جامعه‌ی مدنی دراین‌خصوص بسیار مهم و تأثیرگذار است. دولت می‌تواند با آموزش و آگاهی‌بخشی به آحاد جامعه و اطلاع‌رسانی دقیق از احتمال ارتکاب برخی جرایم در این

[1] جلالی فراهانی، امیرحسین (۱۳۸۴) پیشگیری وضعی از جرایم سایبر در پرتو موازین حقوق بشر، مجله فقه و حقوق، ۱۳۸۴، ص ۱۸.

[2] نیازپور، ا.ح. (۱۳۹۷)، بزهکاری به عادت از علت تا پیشگیری، انتشارات فکرسازان، چاپ اول. ص ۱۱۲

زمینه و حفاظت و صیانت از حریم خصوصی افراد در فضای مجازی از تعرض به حریم خصوصی آن‌ها جلوگیری نماید.[1]

در قانون جرایم رایانه‌ای به موضوع حریم خصوصی توجه خاصی شده است که به طور خلاصه به برخی از مصادیق نقض حریم خصوصی در فضای سایبر که در قانون جرایم رایانه‌ای جرم‌انگاری شده است، اشاره می‌نماییم.

۱. دسترسی غیرمجاز به داده‌های رایانه‌ای یا مخابراتی نظیر هک، ایمیل یا اکانت اشخاص
۲. شنود غیرمجاز محتوای در حال انتقال در سیستم‌های رایانه‌ای یا مخابراتی نظیر استفاده از نرم‌افزارهای شنود چت‌های اینترنتی
۳. دسترسی غیرمجاز به داده‌های سری در حال انتقال در سیستم‌های رایانه‌ای یا مخابراتی یا حاصل داده یا تحصیل شنود آن
٤. در دسترس قراردادن داده‌های سری در حال انتقال در سیستم‌های رایانه‌ای یا مخابراتی یا حامل‌های داده برای اشخاص فاقد صلاحیت
٥. ممانعت از دسترسی اشخاص مجاز به داده‌ها با سیستم‌های رایانه‌ای یا مخابراتی به طور غیرمجاز
٦. هتک حیثیت از طریق انتشاریافتن صوت و فیلم تحریف شده دیگری به وسیله‌ی سیستم‌های رایانه‌ای مخابراتی
۷. نشر اکاذیب از طریق سیستم‌های رایانه‌ای یا مخابراتی به‌قصد اضرار به غیر یا تشویش اذهان عمومی[2]

۲.۲.۳.مکانیزم‌های قانونی برای کاهش صدمات و برگرداندن بزه‌دیدگان به وضعیت پیش از جنایت

جرم‌شناسان اتفاق‌نظر دارند که پیشگیری از وقوع حادثه و جرم از طریق اتخاذ تدابیری به‌مراتب بر واکنش و اعمال مجازات تقدم دارد، تقلیل آثار زیان‌بخش جرائم و حمایت از بزه‌دیدگان نوع پیشگیری وضعی است که در کنترل جرائم ازدیاد ضرر و خسارت نقش مؤثری را ایفا می‌نماید. مهم‌ترین تدابیر قانون‌گذار در این عرصه عبارت است از: «الزام مجرم به برگرداندن اوضاع به‌پیش از ارتکاب جرم و اجباری ساختن مساعدت با بزه‌دیدگان.»

۱.۲.۲.۳. الزام مجرم به برگرداندن اوضاع به‌پیش از ارتکاب جرم

قانون‌گذار در مواردی از قانون جزا به‌منظور تقلیل زیان‌های وارد بر بزه‌دیدگی زنان در فضای مجازی و در نهایت حمایت قانونی از او، بزهکار را به برگرداندن اوضاع به زمان پیش از وقوع جرم الزام نموده است. به‌عنوان نمونه شخصی که مطابق این قانون مجازات می‌شود اگر از طریق جرم مالی را به دست آورده باشد، به رد عین آن و اگر مال موجود نباشد به رد مثل یا قیمت آن به مالکش محکوم می‌شود. همچنین اجبار مجرم به برگرداندن فرد ربوده شده و اموال وی برگرداندن طفل را بعد از اتمام حضانت، استماع شکایت بزه‌دیدگی زنان در فضای مجازی در جرائم مادی و معنوی مانند قذف، دشنام، تهدید و افشایی آن با موافقت قربانی جرم از جمله مواردی است که هدف قانون‌گذار از تقنین آنها حمایت از بزه‌دیدگان و تسکین آلام و ناملایمات آنها بوده است.[3]

۲.۲.۲.۳. جبران خسارت بزه‌دیدگی زنان در فضای مجازی

[1] زندی، م. (۱۳۹۹)، تحقیقات مقدماتی در جرایم سایبری. انتشارات جنگل چاپ اول. ص ۲۰۰

[2] زکوی، م. (۱۳۹۰). بزه‌دیدگان خاص در پرتو بزه‌دیده‌شناسی حمایتی، انتشارات مجد. ص ۹۲

[3] سیدزاده ثانی، م. (۱۳۹۲). کتاب راهنمای قانون مجازات اسلامی، انتشارات خرسندی. چاپ دوم. ص۵۱

جبران خسارت یکی از اهداف عدالت کیفری است. جبران آثار بزه‌دیدگی شامل جبران خسارت پرداخت غرامت، اعاده وضع به سابق، اعاده‌حیثیت یا توان‌بخشی و تاوان است. سازوکار جبران به دو گونه رسمی و غیررسمی محقق می‌شود. باتوجه‌به اینکه بزه‌دیدگی انواع گوناگونی دارد، ازاین‌رو متناسب با ماهیت و ویژگی‌های بزه، می‌توان جبران خسارت را نیز طبقه‌بندی کرد.

در باب جبران، نظریات و رویکردهای متفاوتی وجود دارد.[1] توجه به بزه‌دیدگی زنان در فضای مجازی و ضرورت جبران خسارت وارده به وی در فرایند عدالت کیفری یکی از محورهای اصلی سیاست کیفری است، این مهم را قانون‌گذار در فرازهای مختلفی از قانون جزا اشاره نموده و بر لزوم خسارت بزه‌دیدگی زنان در فضای مجازی (اعم از مادی و معنوی) تأکید ورزیده است لازم به ذکر است که مواد فوق اگر چه در جهت حمایت از کلیه آسیب‌دیدگان تدوین گردیده و به بزه‌دیدگان اختصاص ندارد، لکن به جهت عمومیتی که دارد، یقیناً شامل بزه‌دیدگان نیز می‌شود، بلکه باتوجه‌به موقعیت بزه‌دیدگان و لزوم ترمیم ضرر و زیان آنان که ریشه در مبانی عقیدتی و ارزشی دارد، می‌توان بزه‌دیدگان را از مهم‌ترین مصادیق آن دانست.

۳.۲.۳. پیشگیری از بزه‌دیدگی زنان در فضای سایبری

بر مبنای نظریه‌ی سبک فعالیت‌های روزمره بنا بر آنچه در بالا ذکر گردید بزه‌دیدگی سایبری امری ملموس و البته قابل‌پیشگیری است و ازاین‌حیث می‌توان بر مبنای نظریه سبک فعالیت‌های روزمره، روش‌هایی را برای پیشگیری از این نوع بزه‌دیدگی پیشنهاد نمود که البته خود مستلزم شناسایی زمینه‌های بروز بزه‌دیدگی سایبری بر مبنای نظریه سبک زندگی روزمره است. در نتیجه ابتدا به عوامل مؤثر بر بزه‌دیدگی سایبری و تحقق آن می‌پردازیم و در ادامه بر مبنای همین عوامل به ترسیم بهترین روش‌های پیشگیری از بزه‌دیدگی سایبری بر مبنای نظریه سبک زندگی روزمره اشاره می‌شود. بر مبنای نظریه‌ی «سبک فعالیت‌های روزمره» بهترین روش بازدارندگی از بزه‌دیدگی سایبری زنان در فضای مجازی دشوار نمودن دسترسی به هدف یا همان بزه‌دیده است؛ زیرا امکان آموزش بزه‌دیده در راستای مقابله با بزهکاران سایبری به‌صورت حرفه‌ای بسیار دشوار است و تنها می‌توان به آموزش‌های ابتدایی بسنده نمود؛ حال‌آنکه در صورت جمع‌کردن حالت‌های مختلف اعم از آموزش افراد، اعمال تدابیر پیشگیرانه، نظارت بر کار فعالان حوزه‌ی سایبر و... می‌توان دسترسی به هدف یا همان بزه‌دیده را دشوار نمود و به این شکل از بزه‌دیدگی سایبری پیشگیری نمود.[2]

۱.۳.۲.۳. سیستم‌های امنیتی مناسب و به‌روز

با به‌کارگیری سیستم‌های امنیتی مناسب و به‌روز ارتکاب جرم در فضای سایبر بسیار مشکل می‌شود و از این طریق بزه‌دیدگی سایبری نیز به طور چشمگیری کاهش می‌یابد؛ البته به علت محدودیت عملکرد نیروهای کنترل اجتماعی رسمی در فضای سایبر تکیه بر روش‌های تدافعی فردی از اهمیت بیشتری برخوردار است که همان به‌کارگیری تجهیزات کافی جهت افزایش امنیت سیستم‌های رایانه‌ای است.

۲.۳.۲.۳. پرهیز از رفتارهای پرخطر

تفاوت افراد در رفتارهای روزمره سبب تفاوت سطح خطرپذیری بزه‌دیدگی آنان می‌شود؛ بدین معنا که میزان و نوع عملکرد کاربران در امکان بزه‌دیدگی آنان کاملاً مؤثر است. در این فرض کاربران

[1] ابراهیمی، ش. (۱۳۹۱). جرم‌شناسی پیشگیری. تهران. نشر میزان. چاپ اول. ص ۳۴

[2] شیرزاد، ک. (۱۳۹۷). جرایم رایانه‌ای از دیدگاه حقوق جزای ایران و حقوق بین‌الملل، انتشارات بهینه فراگیر. چاپ اول. ص ۱۲۲

آنلاین و خصوصاً کسانی که علاقه‌مند به مشاهده سایت‌های ناشناس، دانلود آهنگ‌ها، فیلم‌ها و یا برنامه‌های نرم‌افزاری رایگان هستند و یا بر روی آیکن‌ها و تبلیغات اینترنتی بدون اندیشه و احتیاط کلیک می‌کنند و به‌احتمال زیاد قربانی مجرمان سایبری می‌شوند.[1] به‌عبارت‌دیگر میزان فعالیت‌های شغلی و تفریحی آنلاین سبب افزایش یا کاهش فرصت‌های بزه‌دیدگی سایبری می‌شوند و البته یافته‌های علمی بسیاری مؤید این می‌طلبند که عوامل موجود در سبک زندگی نقش مهمی در بزه‌دیدگی افراد در جهان واقعی بازی می‌کنند. ازاین‌رو بنا بر نظریه سبک‌های زندگی روزمره نوع فعالیت‌های روزمره تأثیری مستقیمی بر فرایند بزه‌دیدگی در فضای سایبر دارند، ازاین‌رو است که «هیندلانگ» بیان می‌دارد: «فعالیت‌های شغلی و تفریحی اجزاء بسیار تعیین‌کننده‌ای در سبک زندگی هستند و تأثیر مستقیمی بر سطح بزه‌دیدگی دارند.»[2]

۳.۳.۲.۳. پرهیز از گرایش به رفتارهای مجرمانه

در تبیین این دیدگاه استدلال شده است که کسانی که درگیر سبک‌های زندگی مجرمانه شده‌اند، اغلب به هدفی مناسب برای بزهکاران بدل می‌شوند، چرا که ایشان تمایلی در به حرکت درآوردن نظام حقوقی از خود نشان نمی‌دهند؛ زیرا در اندیشه‌های مجرمانه خویش غرق شده و گمان می‌کنند که خود بر فعالیت‌های مجرمانه مسلط هستند و هیچگاه دچار بزه‌دیدگی نمی‌شوند. در واقع این اندیشه را می‌توان با دیدگاه‌های مطروحه در خصوص تفکر فرضیه‌ساز که در نوجوانان وجود دارد مقایسه نمود؛ در این تفکر فرد نوجوان خود را از آسیب‌هایی که ممکن است از اعمال و رفتارهایش به وی وارد شوند مصون می‌بیند و از همین رو اقدام به انجام برخی فعالیت‌های پرخطر می‌کند. در فرض ما نیز فردی که درگیر فعالیت‌های مجرمانه سایبری شده است تقریباً چنین وضعی دارد و خود را از هر نوع گزندی مصون می‌داند.[3] البته لازم به ذکر است که این دسته از افراد جزو مجرمین حرفه‌ای سایبری نیستند و غالباً کسانی هستند که از روش‌های ازرده‌خارج بزهکاری سایبری استفاده می‌کنند و یا از راه‌های ارائه شده توسط مجرمین سایبری به‌منظور گریز از برخی محدودیت‌های موجود در فضای سایبر بهره می‌گیرند؛ به‌عنوان‌مثال کسانی که از نرم‌افزارهای هک که به‌صورت عمده در بازار فروخته می‌شوند استفاده می‌کنند و یا از سایت‌های ناشناس این نرم‌افزارها را دانلود می‌کنند، در زمره همین افرادند و در غالب موارد از سوی طراحان اصلی نرم‌افزار مورد سوءاستفاده قرار می‌گیرند و یا اطلاعاتشان توسط آنها به سرقت می‌رود؛ عده دیگر شامل کسانی است که به‌عنوان‌مثال از نرم‌افزارها و یا سایت‌های فیلترشکن برای گریز از سد فیلترینگ اعمال شده از سوی دولت استفاده می‌کنند؛ ایشان نیز گاهی ناخواسته در دام مجرمین سایبری می‌افتند، چراکه در برخی موارد سیستم‌های گریز از فیلتر خود حاوی فایل‌های مضری است که اطلاعات شخصی کاربران را برای سازندگانشان ارسال می‌کنند. در این موارد استفاده‌کننده خود را فردی هوشمند می‌داند که از روش‌های نوین برای اعمال غیرقانونی بهره می‌گیرد، درحالی‌که خود به عروسک خیمه‌شب‌بازی در دست دیگری بدل گشته، و به تعبیری بزه‌دیده‌ی جرم سایبری‌ای که خود زمینه‌ساز آن شده، گردیده است.[4]

---

[1] جوان جعفری، ع. (۱۳۹۹) جرایم سایبر و رویکرد افتراقی با نگاهی به قانون مجازات اسلامی بخش جرایم رایانه‌ای. مجله دانش و توسعه علمی - پژوهشی. سال هفدهم. شماره ۳۴

[2] بهره‌مند، ح. کوره‌پز، ح. سلیمی، ا. (۱۳۹۹). راهبردهای وضعی پیشگیری از جرایم سایبری. آموزه‌های حقوق کیفری. شماره ۷. ص ۳۴۰

[3] میتنیک، ک. سیمون، و. (۱۳۹۰). آموزش مقابله با مهندسی اجتماعی در هک. انتشارات طاهریان چاپ اول. ص ۱۱۱

[4] ده آبادی، ا. سلیمی، ا (۱۳۹۳). اصول جرم‌انگاری در فضای سایبر (با رویکردی انتقادی به قانون جرایم رایانه‌ای). فصلنامه مجلس و راهبرد. سال بیست و یکم. شماره ۱۸۰ .

۴.۳.۲.۳. حضور نیروهای حفاظتی

حضور فعال و پر رنگ نیروهای حفاظتی که با استفاده از آخرین روش‌ها به رصد و پیگیری فعالیت‌های اشخاص در فضای سایبر می‌پردازند، عامل مؤثر دیگری است که می‌توان از آن به‌عنوان یکی از تأثیرگذارترین روش‌های پیشگیری از بزه‌دیدگی سایبری یاد نمود. در این روش متصدیان امر یا به تعبیری پلیس سایبری، به برخورد و مقابله با جرائم می‌پردازند و با پیگیری، تحت‌نظر قراردادن اشخاصی که فعالیت‌های پنهانی و مرموز دارند و نیز کنترل شناسه اینترنتی آنان در فضای سایبر به رهگیری اقداماتشان می‌پردازند، تا از اعمال مجرمانه ایشان علیه دیگران جلوگیری نمایند. طراحی چترهای حفاظتی و همچنین ارائه اخطارهای آموزشی به اشخاص و فعالان حوزه‌ی سایبر از مهم‌ترین اقدامات این گروه‌هاست.[۱]

۴.۲.۳. راهکارهای پیشگیرانه از بزه‌دیدگی زنان در فضای مجازی با تأکید بر نظریه‌ی شیوه زندگی

۱.۴.۲.۳. تدابیر غیرحقوقی

۱) کنترل دولتی: در این روش، سیاست کلی حاکم بر کشور اجازه‌ی دسترسی به پایگاه‌های مخرب و ضداخلاقی را نمی‌دهد و دولت شبکه‌های جهانی را از دروازه‌ی اتصال و ورود به کشور با فیلترهای مخصوص کنترل می‌کند.[۲]

۲) کنترل سازمانی: روش دیگر، کنترل سازمانی است که معمولاً سازمان، اداره یا تشکیلاتی که مسئولیت سرویس‌دهی و اتصال شهروندان را به اینترنت به عهده می‌گیرند، خود موظف به کنترل شبکه و نظارت بر استفاده‌ی صحیح از آن می‌شود تا با الزامات قانونی و اخلاقی توأمان انجام این وظیفه را تضمین کند.

۳) کنترل فردی: کنترل فردی روش دیگری است که قابل‌انجام است. در این نوع کنترل تمام تضمین‌های اجرایی، درون‌فردی است و شخص با بهره‌گیری از وجدان فردی، مبانی اخلاقی و تعهد دینی، مراقبت‌های لازم را در ارتباط با شبکه‌های جهانی به عمل آورد. این اعتقاد و فرهنگ در محدوده‌ی خانواده نیز اعمال می‌شود. البته شیوه‌ی اخیر در صورتی ممکن خواهد بود که واگذاری خط اشتراک *IP* پس از شناسایی کامل افراد و با ملاحظه‌ی خصوصیات اخلاقی آنان انجام پذیرد. در غیر این صورت تصور اعمال چنین کنترلی از سوی تک‌تک افراد جامعه صرفاً در حد آرزو باقی خواهد ماند.[۳]

۲.۴.۲.۳. تدابیر کیفری

۱) وجود یک نظام قانونمند اینترنتی: مورد دیگر که کارشناسان از آن به‌عنوان پادزهر آسیب‌های اینترنتی از قبیل اطلاعات نادرست و یا پیامدهای ضداخلاقی نام می‌برند، وجود یک نظام قانونمند اینترنتی در جامعه است که اداره‌ی آن از سوی یک متولی قدرتمند و کاردان می‌تواند اینترنت سرکش و افسارگسیخته را مهار کند و از آن به نحو شایسته بهره‌برداری نماید. این نظام اگر با یک نظام حقوقی و دادرسی جامع و عمیق توأم باشد، موارد تخلف و سوءاستفاده از این ابزار به‌راحتی قابل‌تشخیص و پیگیری قضایی خواهد بود. در این صورت امکان سوءاستفاده و تأثیرپذیری از فرهنگ‌های بیگانه که عموماً مغایر با اصول اخلاقی ماست، به طرز چشمگیری کاهش می‌یابد.

---

[۱] زندی، م. (۱۳۹۹)، تحقیقات مقدماتی در جرایم سایبری. انتشارات جنگل چاپ اول. ص ۲۱۰

[۲] نجفی ابرندآبادی، علی حسین، ۱۳۸۳، پیشگیری عادلانه از جرم، علوم جنایی، مجموعه‌مقالات در تحلیل از استاد آشوری، انتشارات سمت. ص:۵۲

[۳] نیازپور، ا.ح. (۱۳۹۷)، بزهکاری به عادت از علت تا پیشگیری، انتشارات فکرسازان، چاپ اول. ص ۱۵۵

۲) پیشگیری مشارکتی از بزه‌دیدگی زنان در فضای مجازی:
از زمان ظهور تفکر علمی در مورد جرم و پیشگیری، همواره توجه جرم‌شناسان معطوف به یک عنصر تحت عنوان شخص مجرم و شیوه‌های مهار بزهکاری و یا اصلاح و درمان او بوده است؛ بنابراین در عرصه‌ی سیاست جنایی، مرتکب جرم نقش اصلی را ایفا می‌نمود تا اینکه از سال ۱۹۴۰ میلادی عده‌ای از جرم‌شناسان به دنبال حل معمای بزهکاری و علت‌شناسی جرم، پژوهش‌های خود را بر روی کنشگر دیگر بزهکاری، یعنی «بزه‌دیده» که خود بازیگر نیمی از صحنه جرم است متمرکز نمودند. به‌این‌ترتیب برای وقوع یک جرم تقارن سه عنصر را ضروری می‌دانند. این سه عنصر عبارت‌اند از: وجود یک مرتکب باانگیزه، مهارت و ابزار لازم برای ارتکاب جرم و وجود یک آماج محافظت نشده[۱] باتوجه‌به عدم امکان شناسایی مجرمان بالقوه و آگاهی به انگیزه آنان در زمینه‌ی ارتکاب جرم می‌توان گفت در عمل مبارزه با این دو عنصر عملاً غیرممکن است. به‌این‌ترتیب تنها راه مبارزه، تقلیل موقعیت‌های ارتکاب جرم برای مجرمین است که از طریق تأثیرگذاری بر محیط فردی و اجتماعی اشخاص امکان‌پذیر است. برای نیل به این هدف کلیه تدابیر پیشگیرانه، باتوجه‌به وسعت و تنوع آن می‌بایست به‌عنوان سیاست جنایی یک دولت مطرح شود و برای رسیدن به این هدف نیز، دولت می‌تواند از همیاری و مشارکت گسترده مردمی و نهادهای غیردولتی بهره‌مند گردد. به‌عبارت‌دیگر، تغییر افق دید جرم‌شناسان از روش‌های پیشگیری کیفری به‌سوی پیشگیری غیرکیفری از چند دهه قبل سیاست جنایی را در این بعد تحت‌تأثیر قرار داده است. امروزه ارزیابی مدارک و تجربیات نیز، بیانگر آن است که استفاده از تدابیر غیرکیفری در شمار کاهش یا حذف جرائم خاص تأثیر بسزایی داشته است. در حال حاضر تصور یک نظام سیاست جنایی بدون مشارکت جامعه ممکن به نظر نمی‌رسد. سیاست جنایی گستره وسیعی از تدابیر را در بر می‌گیرد که چیدمان منطقی این تدابیر، ما را به اهداف آن رهنمون می‌سازد در این میان تدابیر پیشگیرانه مشارکتی به‌مثابه یکی از ابزار عمده تحقق سیاست جنایی مشارکتی مطرح است.[۲]

سیاست جنایی مشارکتی در برگیرنده تدابیر و اقدام‌هایی است که مردم مستقلاً و یا با مشارکت دولت و به‌صورت سازمان‌یافته و به‌منظور پیشگیری از جرم و مقابله با آن اتخاذ می‌نمایند. میزان مشارکت مردم در سیاست جنایی باتوجه‌به نظام سیاسی حاکم بر جوامع تغییر می‌یابد. در بسیاری از موارد، اجتماعی بودن پدیده جرم ایجاب می‌کند تا حتی‌المقدور برای پیشگیری و سرکوب جرائم از تمامی ظرفیت‌های اجتماعی استفاده شود. مشارکت سازمان‌های غیردولتی در فرایند کیفری یکی از این ظرفیت‌هاست؛ بنابراین می‌توان گفت، باتوجه‌به موضوع بحث، مشارکت مردم به‌عنوان سازمان‌های مردم‌نهاد مستقل از دولت در کنار سازمان‌های دولتی در حمایت از حقوق زنان و مبارزه با خشونت و آزار علیه آنان تأثیر بسزایی دارد.[۳]

۵.۲.۳. پیشگیری وضعی از بزه‌دیدگی زنان در فضای مجازی

یکی از راهکارهای مهم برای پیشگیری از بزه‌دیدگی زنان در فضای مجازی، پیشگیری وضعی[۴] است. کلارک پیشگیری وضعی از جرم را به‌عنوان اقدامات قابل‌سنجش و ارزیابی مقابله با جرم می‌داند. این اقدامات معطوف به اشکال خاصی از جرم بوده و از طریق اعمال مدیریت، یا مداخله در محیط بلاواسطه به شیوه‌های پایدار و سیستماتیک منجر به کاهش فرصت‌های جرم و افزایش خطرات

[۱] . جمشیدی، علیرضا، (۱۳۸۸)، گفتمان پیشگیری از سیاست جنایی مشارکتی در لوایح قضایی، مجله تحقیقات حقوقی، ویژه نامه بهار و تابستان

[۲] رایجیان اصلی، مهرداد، (۱۳۸۳)، رهیافتی نو به بنیان‌های نظری پیشگیری از جرم، مجله حقوقی دادگستری، شماره ۴۸

[۳] نجفی ابرندآبادی، علی حسین، (۱۳۸۸)، پیشگیری عادلانه از جرم، مجموعه مقالات علوم جنایی در تجلیل از دکتر آشوری، انتشارات سمت. ص۱۶۷

[۴] Situational Prevention

جرم که همواره مدنظر تعداد زیادی از مجرمین بوده است، می‌گردد. این پیشگیری به‌وسیله دست‌کاری و تغییر موقعیت و محیط در فرایند وقوع جرم به کاهش فرصت‌های ارتکاب جرم کمک می‌کند. از میان روش‌های مختلف پیشگیری از جرم، پیشگیری وضعی بهترین راهکارها را برای کاهش فرصت‌های ارتکاب جرم در جرائم سایبر و به‌تبع آن بزه‌دیدگی سایبر پیشنهاد می‌کند؛ بنابراین به‌منظور کاهش فرصت‌های جرم، می‌توان از تقسیم‌بندی بیست و پنج‌گانه کلارک استفاده نمود. [1]

در این راستا راهکارهای پیشنهاد شده، در پنج گروه عمده جای می‌گیرند و به برخی از آنها که درباره موضوع موردبحث در ارتباط هستند می‌پردازیم:

۱.۵.۲.۳. افزایش زحمات ارتکاب جرم

هرچه زحمات ارتکاب بزه کمتر باشد، بزهکاران آسان‌تر به ارتکاب جرم روی می‌آورند و برعکس. این رویکرد از پیشگیری وضعی سعی دارد با مشکل و سخت جلوه‌دادن آماج‌های جرم، بزهکاران بالقوه را از ارتکاب انواع بزه‌های مرتبط با بزه‌دیدگی زنان در فضای مجازی منصرف نماید و با قراردادن موانعی در سر راه بزهکاران بالقوه، به‌خصوص در محاسبه عقلانی، مزایای قابل‌پیش‌بینی از ارتکاب جرم را کمتر نشان داده و با استفاده از تکنیک‌های افزایش زحمات ارتکاب جرم باز دارد.

۲.۵.۲.۳. تکنیک‌های کنترل‌کننده یا محدودکننده ی دسترسی

مهم‌ترین دستاوردهای پیشگیری وضعی برای مقابله با بزه‌دیدگی زنان در فضای مجازی، تدابیر محدودکننده دسترسی است. بزه‌دیدگی زنان در فضای مجازی از طریق نفوذ در سیستم‌های اطلاعاتی با فناوری‌های دیجیتالی اعمال می‌گردد. افراد و گروه‌ها با سازمان‌دهی انواع حملات غیرقانونی به رایانه‌ها و اطلاعات ذخیره شده به‌منظور دسترسی به اهداف خود گام برمی‌دارند. در این تکنیک‌ها سعی می‌شود از دسترسی نفوذگرها به منابع شبکه، تأسیسات مختلف مبتنی بر فناوری‌های اطلاعاتی جلوگیری نمود. [2]

از جمله راهکارهای عملی عبارت‌اند از: جلوگیری از ورود یا ارسال برخی داده‌های غیرمجاز یا غیرقانونی از طریق نصب سیستم‌ها و برنامه‌های خاص بر روی گره‌های دسترسی به شبکه که شامل رایانه‌های شخصی، مسیریاب‌ها،[3] سیستم‌های ارائه‌دهنده‌ی خدمات شبکه‌ای و ایجادکنندگان نقطه تماس بین‌المللی با استفاده از سخت‌افزارها و نرم‌افزارهایی مانند: دیوار آتشین، سیستم‌های پالایش به‌منظور محدود نمودن دسترسی به شبکه و تارنماهای آلوده، سیستم‌های تشخیص نفوذ و پیشگیری از نفوذ، تعبیه فناوری‌های نوین تصدیق هویت و رمزنگاری، به‌کارگیری پالایش به‌منظور جلوگیری از دسترسی کاربران خانگی یا کارمندان مراکز دولتی به تارنماها و منابع آلوده به بد افزارهای رایانه‌ای، بالابردن و افزایش تعرفه‌های استفاده از اینترنت پر سرعت و همچنین محدودیت در ارائه فضای دریافت فایل به کاربران، به‌منظور کاهش دسترسی و مدت‌زمان استفاده از اینترنت، زیرا بر اساس نظریه فعالیت‌های روزمره، گذراندن مدت‌زمان طولانی در فضای اینترنت عاملی برای ارتکاب بزه و بزه‌دیدگی است.

۳.۵.۲.۳. تکنیک‌های کنترل‌کننده ورودی‌ها و دسترسی به اهداف در اماکن

[1] زندی، م. (۱۳۹۹)، تحقیقات مقدماتی در جرایم سایبری. انتشارات جنگل چاپ اول. ص ۲۱۸

[2] ابراهیمی، ش. (۱۳۹۱). جرم‌شناسی پیشگیری. تهران. نشر میزان. چاپ اول. ص ۷۷

[3] Router

این راهکار از پیشگیری وضعی سعی دارد با مشکل کردن دسترسی افراد بالقوه که توانایی بزه‌دیده واقع‌شدن را دارد به اهدافی که در مکان‌های خاصی وجود دارند، اقدام نماید. کنترل ورودی و خروجی‌ها مهم‌ترین و کارآمدترین روش محافظتی در امنیت فیزیکی و ممانعت از دسترسی بزهکاران در فضای مجازی به سخت‌افزارها، نرم‌افزارها و دارایی‌های اطلاعاتی است. در بسیاری از موارد افراد و گروه‌های بزهکار با رخنه در افراد و کارکنان مراکز دولتی و مجاورت با سیستم‌های حساس صنعتی با نظامی سعی در انجام عملیات بزهکارانه دارند. امروزه عموم مردم با استفاده از حافظه‌های قابل‌حمل، توانایی انتقال داده‌ها را بدون برقراری ارتباطاتی نظیر اینترنت را دارا هستند.[1] همچنین استفاده از شناسه کاربری و کلمه عبور، در نواحی خیلی محرمانه از تأیید دسترسی به مکان مذکور به‌وسیله مقام مافوق سازمان انجام بگیرد، محافظت از ورودی‌ها با استفاده از نیروهای انسانی بامهارت بالا و حرفه‌ای، استفاده از کارت‌های الکترونیکی عکس‌دار، استفاده از دروازه‌های بازرسی به‌منظور جلوگیری از حمل اشیای غیرمجاز که موجب اختلال سیستم‌های الکترونیکی می‌شود و همچنین حافظه‌های قابل‌حمل که با اتصال آنها به سیستم‌ها امکان انتقال بد افزارها به آنها امکان‌پذیر می‌شود، استفاده از پوشش مخصوص در مکان‌های حساس به‌منظور تفکیک اشخاص غیرمجاز، استحکام مراکز داده با استفاده از مصالح بتنی و فولادی به‌منظور نفوذ افراد غیرمجاز و همچنین به‌کاربردن فناوری‌های ویژه به‌منظور جلوگیری از نفوذ امواج الکترومغناطیسی به دستگاه‌های حساس، به‌ویژه بمب‌های الکترونیکی که قادر است در فواصل صدمتری با انتشار امواج مغناطیسی دستگاه‌های رایانه‌ای را منفجر نمایند. [2]

دراین‌ارتباط، به‌کارگیری اصول معماری ساختمان در مراکز حساس، به‌خصوص در مکان‌هایی که سرورها در آن قرار دارند، استفاده از سیستم‌های تشخیص نفوذ فیزیکی در مکان‌های خلوت و همچنین اتاق‌های رایانه و تجهیزات مخابراتی، از جمله راهکارهای پیشگیری وضعی است.

۴.۵.۲.۳. کنترل و محدودکردن دسترسی به ابزارهای تسهیل‌کننده ی بزه علیه زنان در فضای مجازی

یکی دیگر از رویکردهای پیشگیری وضعی به‌منظور مقابله با بزه‌دیدگی زنان در فضای مجازی، ابزارها و تسهیل‌کننده‌هایی هستند که برای ارتکاب جرم لازم بوده یا باعث تحریک و تشویق بزهکار به ارتکاب بزه می‌شوند. کنترل و محدودکردن دسترسی شامل تدابیری می‌شود که طی آن چگونگی و نحوه برقراری ارتباط بین کاربران و سیستم‌های رایانه‌ای و مخابراتی کنترل می‌شود و هدف از این تدابیر، جلوگیری از دسترسی غیرمجاز افراد به منابع اطلاعاتی است. نمونه‌ای از اقدامات محدودکننده دسترسی عبارت‌اند از: اعطای حق دسترسی محدود به کاربران نسبت به برخی داده‌ها، امکانات یا دستگاه‌های خاص به افرادی که برای انجام کار خود به آن نیاز دارند و استفاده اشتراکی از آنها ممنوع گردد. در این راستا با تدوین سیاست‌هایی از جمله افزایش نرخ تعرفه‌های دولتی توسط سازمان تنظیم مقررات و ارتباطات رادیویی کشور، در خصوص ارائه خدمات اینترنتی پر سرعت به شرکت‌ها، اپراتورها و خدمات‌دهندگان به‌خصوص شرکت‌های خصوصی، به‌کارگیری پالایش توسط دولت یکی دیگر از اقدامات عملی در ایمن نگه‌داشتن فضای سایبر است. از عمده دلایل فیلترکردن اینترنت در کشورهای مختلف را می‌توان در چهار تقسیم‌بندی کلی گنجاند: مسائل

[1] بهره‌مند، ح. کوره‌پز، ح. سلیمی، ا. (۱۳۹۹). راهبردهای وضعی پیشگیری از جرایم سایبری. آموزه‌های حقوق کیفری. شماره ۷. ص ۳۴۶

[2] میتنیک، ک. سیمون، و. (۱۳۹۰). آموزش مقابله با مهندسی اجتماعی در هک. انتشارات طاهریان چاپ اول. ص۱۱۶

سیاسی، مسائل اجتماعی، مسائل امنیتی و مسائل اخلاقی که همان‌طور در این تقسیم‌بندی دیده می‌شود، موضوعات امنیتی یکی از دلایل توجیه‌کننده در استفاده از پالایش به‌منظور ممانعت از دسترسی کاربران به منابع آلوده در اینترنت است و از این طریق می‌توان تا حدودی از دسترسی افراد به ابزارهای تسهیل‌کننده جرم، جلوگیری و محدودیت ایجاد نمود. در حوزه‌ی ادارات دولتی و مراکز مهم و زیرساخت‌های حیاتی، تعیین و تخصیص شناسه کاربری برای هر کارمند در محیط‌های اداری و مکان‌های حساس می‌تواند از گشت‌زنی‌های بی‌مورد و خطرناک کارمندان در فضای اینترنت جلوگیری نمود، زیرا در بسیاری از موارد بزهکاران با استفاده از شبکه‌های اجتماعی نسبت به اغفال افرادی که در محیط‌های خاصی مشغول به فعالیت هستند، نسبت به سرقت اطلاعات یا کسب اطلاعات محرمانه در مورد فعالیت شرکت‌های خصوصی و دولتی اقدام می‌نمایند. [1]

علاوه بر موارد فوق، محدودیت‌هایی از قبیل: ایجاد محدودیت در دسترسی کارمندان ادارات و شرکت‌ها به دارایی‌های اطلاعاتی در ساعات کار رسمی، کنترل دسترسی به ابزار مدیریت و کنترل اطلاعات برای کاربران با استفاده از صلاحیت دومرحله‌ای یعنی؛ تأیید مدیر و مسئول هم طراز، اعمال محدودیت در استفاده از تجهیزات ذخیره‌ساز همراه با دیسک‌ها و دیسکت‌ها به‌منظور جلوگیری از دسترسی و ذخیره‌سازی اطلاعات توسط کارکنان و سوءاستفاده‌های مربوط، محدودیت در دسترسی به نرم‌افزارهای انتقال داده مانند ***(FTP)*** در مراکز حساس. محدودیت در دسترسی به دیوارهای آتش، سیستم‌های تشخیص نفوذ و پیشگیری از نفوذ در مراکز حساس و زیرساخت‌های مبتنی بر فناوری اطلاعات به‌وسیله تخصیص کلمه عبور و ایجاد حساب‌های محدود کاربری، محدود نمودن خریداری و فروش سیستم‌های رایانه‌ای با مشخصات بالا و حرفه‌ای به افراد، زیرا اشخاص نفوذگر برای انجام حملات خود نیاز به رایانه‌هایی دارند که سرعت و پردازش بالایی داشته باشند؛ بنابراین می‌توان با استفاده از راهکارهای قانونی و هماهنگی فروشگاه‌های عرضه محصولات رایانه‌ای و حتی نرم‌افزاری، با مراکز پلیسی و امنیتی از دسترسی افراد خرابکار به آنها جلوگیری نمود.[2]

۵.۵.۲.۳. منحرف نمودن جهت ارتکاب اعمال مجرمانه

یکی دیگر از راهکارهای پیشگیری وضعی برای مقابله با جرائم، منحرف نمودن بزهکاران سایبری و به‌خصوص بزهکاران سایبری از آماج جرم است، از طریق این روش می‌توان با ایجاد فاصله بین بزهکاران بالقوه و آماج‌هایی که جذابیت فراوانی برای این دسته از افراد دارند، به‌منظور پیشگیری از وقوع عملیات علیه زنان در فضای سایبر جلوگیری نمود.[3] در محیط اینترنت و تارنماهای گوناگون به‌خصوص شبکه‌های اجتماعی که از انواع قشرهای جامعه در آن حضور دارند، با استفاده از بنرهای تبلیغاتی می‌توان به موضوعاتی نظیر قبیح جلوه‌دادن اعمال افرادی که به سرقت اطلاعات و دسترسی به داده‌های شخصی و یا دولتی می‌نمایند اقدام نمود و با استفاده از این امکانات نسبت به گردآوری افرادی که دارای قابلیت‌های بالقوه در زمینه ارتکاب اعمال تروریستی سایبری هستند، جهت به‌کارگیری آنها در مراکز آموزشی دانش‌های مرتبط

[1] مینولی، د. (۱۳۹۵). مهندسی اینترنت و اینترانت. (ترجمه او مهابادی). انتشارات آذرخش، چاپ دوم. ص۱۰۱

[2] استفاده رایگان و همه‌گیر کاربران اینترنت در سراسر جهان از تارنماهایی چون: گوگل ارث، ویکی مدیا و دیگر امکاناتی که در محیط اینترنت بدون محدودیت در اختیار همگان قرار دارد، به افراد بزهکار این امکان را می‌دهد که با جمع‌آوری اطلاعاتی همچون مکان‌یابی تأسیسات، دسترسی به آمارهای موجود در زمینه نفوذپذیری و نقاط آسیب‌پذیر مراکز حیاتی و نسبت به ارتکاب بزه آسان‌تر اقدام نمایند.

[3] نیازپور، ا.ح. (۱۳۹۷)، بزهکاری به عادت از علت تا پیشگیری، انتشارات فکرسازان، چاپ اول. ص ۱۶۷

با رایانه به‌منظور منحرف نمودن این افراد نسبت به عملیات مخرب جلوگیری اقدام نمایند.

۶.۵.۲.۳. افزایش خطرات قابل‌پیش‌بینی ارتکاب جرم

یکی از آورده‌های پیشگیری وضعی تشدید و افزایش خطرات قابل‌پیش‌بینی برای ارتکاب جرم خاصی است با پیش‌بینی این تمهیدات، بزهکاران جسارت کمتری برای انجام عملیات مجرمانه خواهند داشت. در خصوص بزه‌دیدگی زنان در فضای مجازی و آماج بالقوه جرم، یعنی زیرساخت‌های اطلاعاتی کشور، به‌کارگیری روش‌هایی که بزهکاران را متقاعد سازد که در صورت اقدام به اعمال مجرمانه منفعتی برای آنها در برنخواهد داشت و احتمال دستگیری و ردیابی آنها وجود دارد.[۱]

برآمد

رشد فناوری و پیشرفت جوامع پدیده‌ای فراگیر فضای مجازی را به وجود آورده که علی‌رغم استفاده مفید در زمینه‌های گوناگون در برخی مواقع مضراتی را به همراه دارد که یکی از این مضرات زمینه‌سازی برای به‌وجودآمدن جرایم سنتی در این بستر که صورتی نو به خود گرفته‌اند و یا حتی ظهور جرایم مختص فضای مجازی است به این جهت رویکرد بزه‌دیده شناختی در مواردی که بزه‌دیده در آن جرم بیشتر محور جرم قرار می‌گیرد می‌تواند بستری مناسب برای مطالعه باشد.

ویژگی‌های خاص فضای مجازی مثل ناشناس بودن در بستر ارتباطات اینترنتی، گستردگی، فراملی بودن، سرعت بسیار بالا در ارتکاب جرایم موجب دشوارشدن مطالعه دراین‌خصوص شده است.

در مقاله‌ی حاضر، با بررسی خصوصیات جرایم ارتکابی به‌خصوص جرایمی که بزه‌دیده آن زنان است و علل ارتکاب این جرایم یا فضاسازی که موجب تسهیل در ارتکاب جرایم می‌شود منتج گردید که بزه‌دیده با عدم توجه به مقررات استفاده از اینترنت یا هشدارهای پلیس در خصوص ارتباطات اینترنتی در به‌وقوع‌پیوستن جرم نقش فعالی دارد، البته خصوصیات ذاتی زنان نیز در موارد بزه‌دیدگی جنسی نقش دارد که نمی‌توان این نقش‌آفرینی را مستند به رفتار بزه‌دیده دانست و بخشی از تقصیر را بر عهده او گذاشت. این ویژگی ذاتی است که باعث شده اکثر جرایم جنسی چه به‌صورت کلاسیک و چه به‌صورت اینترنتی علیه بانوان بیشتر اتفاق بیفتد. در عرصه‌ی فضای مجازی می‌توان با چند روش گوناگون اقدام به پیشگیری نمود این پیشگیری را می‌توان به چند دسته تقسیم نمود که در فصل سوم تقسیماتی ارائه گردید، به نظر می‌رسد باتوجه‌به مطالعات انجام شده دولت به معنای اعم آن نتوانسته است به‌صورت تخصصی در خصوص جرایم رایانه‌ای با محوریت بزه‌دیدگی زنان جرم‌انگاری‌هایی انجام دهد اگرچه در سال‌های اخیر با جرم‌انگاری‌های کلی در این زمینه ورود کرده است؛ اما محوریت بیشتر اقدامات دولتی جرایم مالی بوده است.

آنچه که در حوزه‌ی پیشگیری بزه‌دیدگی زنان بیشتر اهمیت دارد اقدام به پیشگیری وضعی در این زمینه است چرا که در این نوع پیشگیری می‌توان اقدامات پیشگیرانه را بر اساس ویژگی‌های فضای مجازی اعمال نمود، همچنین به دلیل وضعیت خاص زنان به‌خصوص در سنین پایین اقدامات پیشگیرانه رشد مدار ضرورت دارد به‌طورکلی می‌توان به‌عنوان یک جمع‌بندی پیشنهادهای زیر را در خصوص پیشگیری از بزه‌دیدگی زنان در فضای مجازی ارائه نمود:

[۱] عالی‌پور، ح (۱۳۹۶). مجموعه مقاله‌های همایش بررسی جنبه‌های حقوقی فناوری اطلاعات معاونت حقوقی و توسعه قضایی قوه قضائیه. مرکز مطالعات توسعه قضایی، انتشارات سلسبیل. چاپ اول. ص ۹۸

۱. اقدام به قانون‌گذاری در خصوص جرم‌انگاری رفتارهای خطرناک علیه زنان به طور خاص با استفاده از اسناد بین‌المللی و بالابردن هزینه بزهکاری در این حوزه
۲. اقدام به تبلیغ استفاده صحیح از فضای مجازی و ارتباط با افراد در فضاهای ارتباطی مجازی
۳. تسهیل و شفاف‌سازی در خصوص اقداماتی که سوداگران در فضای مجازی با تبلیغ آن اقدام به فریب قربانی می‌کنند.
٤. پیش‌بینی اقدامات حمایتی در خصوص بزه‌دیدگان زن به‌خصوص در بزه‌های جنسی
٥. شفافیت در آمار بزه‌های مبتنی بر فضای مجازی برای تسهیل سیاست‌گذاری‌ها در مورد فضای مجازی
٦. ارائه سیستم‌های محافظتی و به‌روز برای مخاطبان فضای مجازی

سپاسگزاری

از معاونت محترم پژوهشی به خاطر حمایت حمایت معنوی در اجرای پژوهش حاضر سپاسگزاری می‌شود.
از آقای دکتر عبدالله علیزاده به خاطر بازبینی متن مقاله و ارائه نظرهای ساختاری تشکر و قدردانی می‌شود.
از داوران محترم به خاطر ارائه نظرهای ساختاری و علمی سپاسگزاری می‌شود.
نگارندگان بر خود لازم می‌دانند از آقای دکتر محمد رسول آهنگران به خاطر مطالعه متن مقاله حاضر و ارائه نظرهای ارزشمند سپاسگزاری نمایند.

منابع

ابراهیمی، ش. (۱۳۹۱). جرم‌شناسی پیشگیری. تهران. نشر میزان. چاپ اول

امینی، م (۱۳۹۴) طبقه‌بندی و آسیب‌شناسی جرائم رایانه‌ای، نشریه علوم انتظامی، شماره ۶

باستانی، بهزاد. (۱۳۸۹). جرایم کامپیوتری و اینترنتی، جلوهای نوین از بزهکاری، انتشارات بهنامی. چاپ دوم.

برنارد، ت (۱۳۸۰)، جرم‌شناسی نظری (گذری بر نظریه‌های جرم‌شناسی)، مترجم علی شجاعی، سمت، تهران.

برومند باستانی. م. (۱۳۹۳) جرائم رایانه‌ای و اینترنتی، تهران، انتشارات بهنامی،

بهره‌مند، ح. کوره‌پز، ح. سلیمی، ا. (۱۳۹۹). راهبردهای وضعی پیشگیری از جرایم سایبری. آموزه‌های حقوق کیفری. شماره ۷.

پاک‌نهاد، ا سدره نشین، ا. (۱۳۹۰). بررسی قانون جرایم رایانه‌ای از دیدگاه موازین حقوق کیفری فناوری اطلاعات، فصلنامه علمی‌ترویجی کارآگاه. دفتر تحقیقات کاربردی پلیس آگاهی ناجا. شماره ۱۷.

جلالی فراهانی، ا.ح (۱۳۸۴) پیشگیری وضعی از جرایم سایبر در پرتو موازین حقوق بشر، مجله فقه و حقوق.

جلالی فراهانی، ا.ح؛ باقری اصل، ر (۱۳۸۶). پیشگیری اجتماعی از جرائم و انحرافات سایبری مجله مجلس و پژوهش. شماره ۱۲۴

جمشیدی، ع، (۱۳۸۸)، گفتمان پیشگیری از سیاست جنایی مشارکتی در لوایح قضایی، مجله تحقیقات حقوقی، ویژه نامه بهار و تابستان

جوان جعفری، ع. (۱۳۹۹) جرایم سایبر و رویکرد افتراقی با نگاهی به قانون مجازات اسلامی بخش جرایم رایانه‌ای. مجله دانش و توسعه علمی – پژوهشی. سال هفدهم. شماره ۳۴

جوان جعفری، ع. شاهیده، ف. (۱۳۹۲). رفتار و گفتار تحریک‌آمیز بزه‌دیده در قوانین و مقررات کیفری و رویه قضایی ایران – مجله آموزه‌های حقوق کیفری. دانشگاه علوم اسلامی رضوی

حسن‌بیگی، ا. (۱۳۹۳) آسیب‌شناسی شبکه جهانی اطلاع‌رسانی اینترنت و ارائه راهبردهای مناسب جهت مقابله با تهدیدها از دیدگاه امنیت ملی با تأکید بر جنبه‌های حقوقی و فنی، پایان‌نامه دکتری، دانشگاه عالی دفاع ملی

دزبانی، م.ح. (۱۳۹۳) مقدمه‌ای بر ماهیت و تقسیم‌بندی تئوریک جرائم کامپیوتری (سایبری)، خبرنامه انفورماتیک، شماره ۱۸۷

ده آبادی، ا. سلیمی، ا (۱۳۹۳). اصول جرم‌انگاری در فضای سایبر (با رویکردی انتقادی به قانون جرایم رایانه‌ای). فصلنامه مجلس و راهبرد. سال بیست و یکم. شماره ۱۸۰

دهخدا، ع.ا. (۱۳۸۸) لغت‌نامه، دانشگاه تهران، انتشارات دانشکده ادبیات

رایجیان اصلی، م. (۱۳۸۴) بزه‌دیده‌شناسی حمایتی، چاپ اول، نشر دادگستر

رایجیان اصلی، م. (۱۳۹۰)، بزه‌دیده‌شناسی حمایتی، چاپ دوم، تهران: انتشارات دادگستر.

رایجیان اصلی، م. (۱۳۸۳)، رهیافتی نو به بنیان‌های نظری پیشگیری از جرم، مجله حقوقی دادگستری، شماره ۴۸

رضوی، م. صادقی، ر. (۱۳۹۹). اینترنت. انتشارات ستایش. چاپ اول.

رمضان نرگسی، ر. (۱۳۸۴) تجاوز و بزه‌دیدگی زنان، فصلنامه کتاب زنان، شماره ۲۰

زررخ، مالمیر (۱۳۸۹)، پیشگیری از بزه‌دیدگی سایبری، فصلنامه علمی – ترویجی مطالعات پیشگیری از جرم

زکوی، م. (۱۳۹۰). بزه‌دیدگان خاص در پرتو بزه‌دیده‌شناسی حمایتی، انتشارات مجد.

زندی، م. (۱۳۹۹)، تحقیقات مقدماتی در جرایم سایبری. انتشارات جنگل چاپ اول.

سیدزاده ثانی، م. (۱۳۹۲). کتاب راهنمای قانون مجازات اسلامی، انتشارات خرسندی. چاپ دوم.

شیرزاد، ک. (۱۳۹۷). جرایم رایانه‌ای از دیدگاه حقوق جزای ایران و حقوق بین‌الملل، انتشارات بهینه فراگیر. چاپ اول.

صادقیان، د. (۱۳۹۱) کالبدشناسی جرائم سایبری در ایران، روزنامه اطلاعات.

صلاحی، ج. (۱۳۹۳) کلیات جرم‌شناسی و تئوری‌های جدید. چاپ اول. انتشارات مجد.

عالی‌پور، ح (۱۳۹۶). مجموعه مقاله‌های همایش بررسی جنبه‌های حقوقی فناوری اطلاعات معاونت حقوقی و توسعه قضایی قوه قضائیه. مرکز مطالعات توسعه قضایی، انتشارات سلسبیل. چاپ اول.

فضلی، م (۱۳۸۹)، مسئولیت کیفری در فضای سایبر. چاپ نخست. تهران: انتشارات خرسندی

معاونت آموزش و تحقیقات قوه قضائیه (۱۳۹۲) مسائل قضایی هرزه‌نگاری در محیط سایبر، تهران، انتشارات راه نوین

میتنیک، ک. سیمون، و. (۱۳۹۰). آموزش مقابله با مهندسی اجتماعی در هک. انتشارات طاهریان چاپ اول

مینولی، د. (۱۳۹۵). مهندسی اینترنت و اینترانت. (ترجمه او مهابادی). انتشارات آذرخش، چاپ دوم.

نجفی ابرندآبادی، ع.ح. (۱۳۸۳) پیشگیری عادانه از جرم، علوم جنایی، مجموعه مقالات در تحلیل از استاد آشوری، انتشارات سمت.

نجفی ابرندآبادی، ع.ح. (۱۳۸۸)، پیشگیری عادلانه از جرم، مجموعه مقالات علوم جنایی در تجلیل از دکتر آشوری، انتشارات سمت.

نجفی ابرندآبادی، ع.ح؛ هاشم بیگی، ح (۱۳۸۷)، دانشنامه جرم‌شناسی، انتشارات دانشگاه شهید بهشتی، تهران

نیا فیلی، ز. (۱۳۷۹) بزه‌دیده و بزه‌دیده‌شناسی. ترجمه روحالدین کردعلیوند و احمد محمدی. تهران: مجمع علمی و فرهنگی مجد.

نیازپور، ا.ح. (۱۳۹۷)، بزهکاری به عادت از علت تا پیشگیری، انتشارات فکرسازان، چاپ اول.

وراویی، ا؛ مؤمنی پور، ح. (۱۳۹۰) جرایم سایبری: از علت‌شناسی تا پیشگیری، چاپ اول. انتشارات سمت