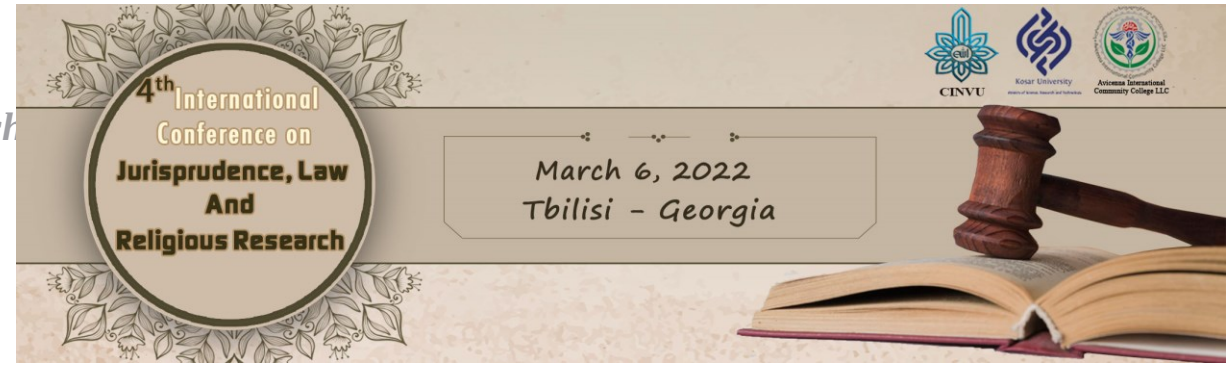

نوآوری‌های حقوق جزا در حوزه جرایم سایبری با تاکید بر بزه‌دیدگان آسیب‌پذیر

سوگند کاری[1]

۱-گروه حقوق، دانشکده حقوق و علوم سیاسی، واحد چالوس، دانشگاه ازاد اسلامی، چالوس، ایران

چکیده

با پیشرفت فناوری اطلاعات و ارتباطات، تحولاتی اساسی در زیست انسانی صورت گرفته است. آن دسته از رفتارهای انسانی که به شکل سنتی جرم تلقی می‌شد؛ امروز به شکل ترجمه ایده‌های مجرمانه به زبان خاص رایانه و یا از طریق فضای سایبری تحقق می‌یابد. به این ترتیب، فضای جدیدی به نام فضای سایبر ایجاد شده است که در آن مرز و محدوده به شکل سنتی معنی ندارد. با این همه می‌توان ادعا کرد که جدیدترین و بزرگ‌ترین چالش حقوق کیفری نیز، مقابله با جرایم سایبری است. لأ قوانین کیفری و مطالعات جرم‌شناسی موجود در زمینه جرایم سایبری، امکان ارتکاب جرم را نه فقط برای مجرمان بلکه حتی برای شهروندان متعارف اینترنت نیز بسیار بیشتر از شهروندان دنیای واقعی کرده است؛ به همین جهت آمار بزه دیدگی سایبری هم شدیداً رشد داشته است. در این پژوهش، نوآوری‌های حقوق جزا در حوزه جرایم سایبری با تاکید بر بزه‌دیدگان آسیب‌پذیر، مورد بررسی قرار گرفت. گونه‌های حمایت از بزه‌دیدگان جرایم سایبری در این پژوهش معرفی شدند. که عبارتند از حمایت ماهوی (شامل حمایت کیفری ساده و حمایت کیفری خاص یا ویژه)، حمایت شکلی و حمایت‌های مادی و معنوی.

واژگان کلیدی: حقوق جزا، جرایم سایبری، حمایت از بزه‌دیدگان

مقدمه

پیدایش و رشد بی‌سابقه فناوری‌های رایانه‌ای شبکه‌محور، تحولات شگرف و دستاوردهای سترگی را در جهت جامعه انسانی به سوی قله‌های پیشرفت اجتماعی همراه داشته است. اما ظهور فضای جدید نیز خالی از هرگونه ایراد و اشکال نبوده و موجب شده تا فضای مجازی که حاصل پیشرفت فناوری رایانه‌ای می‌باشد همچون رهآوردهای دیگر حقوقی مقررات و رژیم حقوقی خاصی را پدید آورد و کنشگران موجود در این فضا را مورد حمایت قرار دهد (اسلامی، ۱۳۹۵). یکی از جنبه‌های سیاست جنایی[1] که مظلوم واقع شده است و جزو گروه فراموش‌شده‌ها است؛ بحث بزه‌دیده[2] است. شناخت بزه‌دیده یا همان قربانیِ جرم، چند دهه است که در میان جرم‌شناسان مطرح شده است. و در تمامی جرایم از جمله جرایم رایانه‌ای بحث بزه‌دیده قابل طرح است. به ویژه آنکه توسعه رو به رشد فضای سایبر، مورد تهاجم بیشتر مجرمان رایانه‌ای و به تبع آن بزه‌دیدگان رایانه‌ای[3] بیشتر واقع شده است. به نحوی که بر اساس آمارها، ۶۵٪ از استفاده کنندگان شبکه جهانی، قربانی جرم سایبری می‌شوند (پورقهرمانی، ۱۳۹۶). عوامل مؤثر بر بزه‌دیدگی رایانه‌ای می‌تواند مختلف باشد؛ ولی بر اساس بررسی‌های انجام شده عوامل مؤثر بر بزه‌دیدگی رایانه‌ای به سطح دانش رایانه‌ای، مدت و نوع استفاده از رایانه، نوع و کیفیت ابزارهای مورد استفاده، جنسیت، سن و اشتغال برمی‌گردد (مالمیر و زررخ، ۱۳۸۹) و شناخت این عوامل می‌تواند به پیش‌گیری از بزه‌دیدگی رایانه‌ای و حمایت از بزه‌دیدگان ناهنجاری‌های فوق کمک مؤثری داشته باشد. بر پایه این یافته‌های جرم‌شناسی زنان نه تنها کمتر از مردان جرم مرتکب می‌شوند بلکه میزان بزه‌دیدگی‌شان نیز به طور کلی کمتر است. مطالعات پدیدارشناسی بزه‌دیدگی در بستر سایبر، نشان می‌دهد که زنان، از جمله «آسیب‌پذیرترین اقشار» در فضای سایبری هستند. در این پژوهش به بررسی تحولات حقوق جزا در حوزه جرایم سایبری در زمینه‌ی بزه‌دیدگان آسیب‌پذیر پرداخته شده است.

یافته‌ها

در ابتدا به منظور تبیین مبانی نظری پژوهش، تعاریف و مفاهیم برخی از اصطلاحات و متغیرهای پژوهش ارائه می‌گردد.

فضای سایبری

فضای سایبر در معنای عام آن به عنوان مجموعه تعامل‌های انسان‌ها از طریق رایانه و فنآوری‌های نوین ارتباطات، بدون در نظر گرفتن «زمان» و «مکان»، توسط ویلیام گیبسون[4] نویسنده‌ی کتاب نورومونسر[5] در سال ۱۹۸۴ به کار برده شد. وی فضای سایبر را بازنمایی گرافیکی از داده‌ها از نظام‌های رایانه‌ای می‌داند. مفهومی که مورد نظر گیبسون بود؛ شاید به نوعی به

[1] Criminal Policy
[2] Victim
[3] Cyber Victims
[4] William Gibson
[5] Neuromonce

هوش مصنوعی و روبوتیک نزدیک‌تر است تا آنچه اکنون به نام «فضای سایبر» شناخته می‌شود (Brier, 2010). این مفهوم نه چندان روشن اولیه، به تدریج دستمایه گفتمانی فلسفی در حوزه سایبر شد و چندی نپایید که حوزه سایبر نه به عنوان محدودهای آزمایشگاهی یا علمی، که خود به مثابه جهانی مستقل، مورد بررسی قرار گرفت (بل، ۱۳۸۹). این سخن درستی است که با گسترش استفاده از مفهوم نوین «سایبر»، هر آنچه پس یا پیش از واژه «سایبر» قرار گیرد، به نوعی به بیان رابطه انسان و رایانه می‌پردازد. در عین حال، رویکردهای گوناگون به فضای سایبر قابل انکار نیست. مفهوم فضای سایبری معطوف به فضای ساختگی و خیالی واقعیت مجازی و اینترنت است که انسان از طریق آن به فضای واقعیت مجازی وارد می‌شود. بدون فنآوری، فضای سایبر بی‌معنا خواهد بود. اکنون، فضای سایبر را با موضوعات علمی - تخیلی مقایسه می‌کنند. این نوعی ناکجاآباد است که در آن می‌توان هویت‌های چندگانه داشت (Haney, 2006). در واقع، اینترنت دروازه فضای سایبر است؛ اما فضای سایبر، با ویژگی‌هایی چون میزان و چگونگی دسترسی، راهبری، فعالیت اطلاع‌یابی، بالندگی و اعتماد شناخته می‌شود(Folsom, 2007). نگرش فناورانه به فضای سایبر به مؤلفه‌هایی چون سخت‌افزار، نرم‌افزار، کیفیت و کمیت انتقال داده‌ها و تعامل در شبکه می‌پردازد. در حالی که رویکرد روان‌شناسانه، اجتماعی و حقوقی در قالب مقوله‌هایی چون فضای ذهنی، الگوی رفتاری انسان و رایانه، تخیل، هویت و شخصیت، به مرز بین واقعیت و خیال و مانند آن توجه می‌کند (Suler, 2004). دیدگاه جامعه‌شناسانه درباره فضای سایبر نیز به دلیل پرداختن به جماعت‌های برخط، شبکه‌های اجتماعی سایبر، و آثار اجتماعی تعامل انسان و رایانه حائز اهمیت است. اما، این در برگیرنده تمامی رویکردهای موجود نیست. با توجه به تفاوت رویکردهای موجود درباره فضای سایبر، دیوید بل تعریف این مقوله پیچیده را می‌داند. وی ضمن اشاره به گونه‌های مختلف تفسیری فضای سایبری به توصیف مایکل بندیکت از فضای سایبر اشاره می‌کند که حائز اهمیت است: «یک دنیای جدید، یک دنیای موازی است که با خطوط ارتباطی و کامپیوترهای جهان خلق و نگهداری می‌شود. دنیایی که در آن تردد جهانی دانش، رموز سنجش‌ها، شاخص‌ها، سرگرمی‌ها و عاملیت دیگری انسانی شکل می‌گیرد. تاکنون، هرگز بر روی زمین دیده نشده است که امور دیدنی، صداها و حضورها در یک روشنایی عظیم الکترونیکی شکوفا شوند (بل، ۱۳۸۹). در زبان فارسی مفهوم دقیق و کاملاً پذیرفته‌شده‌ای از اصطلاح «سایبر» وجود ندارد. برخی از 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. با این وجود در زبان فارسی لغت «سایبر» را معادل واژه «مجاز» و لغت «اسپیس» را معادل واژه «فضا» ترجمه کرده‌اند و ترکیب «سایبر اسپیس» را معادل «فضای مجازی» دانسته‌اند. در همین معنا ترکیبات دیگری نظیر «جامعه مجازی» یا «شهروند مجازی» و «فروشگاه‌های مجازی» و امثال آن مطرح می‌شود. همه این ترکیبات در فضای مجازی مطرح می‌شوند (باستانی، ۱۳۸۳). از لحاظ لغوی سایبر به معنی مجازی و غیر ملموس می‌باشد؛ نخستین بار این اصطلاح «سایبرنتیک» توسط ریاضی‌دانی به نام نوربرت وینر در کتابی با عنوان «سایبرنتیک و کنترل در ارتباط بین حیوان و ماشین» در سال ۱۹۴۸ به کار برده شده است. سایبرنتیک علم مطالعه و کنترل مکانیزم‌ها در سیستم‌های انسانی،

ماشینی (و کامپیوترها) است. فضای سایبر در معنا به مجموعه‌هایی از ارتباطات درونی انسان‌ها از طریق کامپیوتر و مسائل مخابراتی بدون در نظر گرفتن جغرافیای فیزیکی گفته می‌شود. یک سیستم برخط نمونه‌ای از فضای سایبر است که کاربران آن می‌توانند از طریق ایمیل با یکدیگر ارتباط برقرار کنند. برخلاف فضای واقعی، در فضای سایبر نیاز به جابجایی‌های فیزیکی نیست و کلیه اعمال فقط از طریق فشردن کلیدها یا حرکات ماوس صورت می‌گیرد (عاملی، ۱۳۹۰). با توجه به بررسی سنجه‌های گوناگون از تعریف فضای سایبر می‌توان گفت که فضای سایبر، «محیطی تشکیل‌یافته از سامانه‌ها و شبکه‌های ارتباطی متصل به هم است که قابلیت هر نوع رفتار متناسب با محیط مبادله داده، ذخیره و انتشار اطلاعات را دارد.» در معنای خاص و تعریف جزئی از فضای سایبری و در نتیجه‌گیری از تعاریف بالا، می‌توان بیان داشت که منظور از فضای سایبری – به ویژه در پژوهش حاضر- فضا و بستری است که در اینترنت و شبکه‌های اجتماعی بر پایه‌ی اینترنت وجود دارد.

جرایم سایبری

جرم سایبری در اصطلاح به جرمی گفته می‌شود که در محیطی غیر فیزیکی علیه فناوری اطلاعات با حالات شبیه‌سازی و مجازی‌سازی ارتکاب می‌یابد (جاویدنیا، ۱۳۸۸). امروزه بسیاری از جرائم سنتی، همزمان با پیشرفت فناوری اطلاعات و ارتباطات به شدت متحول شده و به جرائم سایبری تبدیل شده‌اند (پرویزی، ۱۳۸۴). جرائم سایبری نیز به جهت گسترش خود، رفته رفته جانشین عباراتی چون جرم‌های رایانه‌ای و جرم‌های اینترنتی می‌شوند. به جرائم سایبر، جرائم علیه فناوری اطلاعات نیز گفته می‌شود. سیر تعریف جرم رایانه‌ای در سده جدید دچار یک دگردیسی شد. قبل از سال ۲۰۰۱ اکثر تعریف‌ها، جرم رایانه‌ای را به عنوان یک واسطه برای حمله به فعالیت‌های اقتصادی و تکنیک‌های نفوذ در امنیت نظیر نفوذگری و رخنه‌گری[6] تبیین می‌کردند. کنوانسیون جرایم رایانه‌ای (۲۰۰۱)، این اصطلاح را با گنجاندن جرائم علیه کودکان که به وسیله اینترنت صورت گرفته و نیز حملات به عواطف انسانی وسیع‌تر کرد تا به کارگیری «واژگان نامناسب[7]» در فضای سایبر را ممنوع کند. این عمل در حقیقت برای پیش‌گیری از کاربرد لفظ‌های موهن که ممکن است تروریسم، ایجاد خطر برای امنیت ملی و یا تنفر و تبعیض نژادی را در پی داشته باشد؛ صورت گرفت. با وجود این، رویکرد خاص کنوانسیون جرایم رایانه‌ای (۲۰۰۱) به بخشی از دانشگاهیان و پژوهش‌گران کمک کرد تا از تصور رایج در مورد جرایم رایانه‌ای در گذشته یعنی همه چیز یا مربوط به نفوذگری یا حمله به تراکنش‌های تجارت الکترونیک[8] است؛ فاصله بگیرند. این عقب‌نشینی باعث شد تا حملات عاطفی به کاربران اینترنت به عنوان یک جرم در نظر گرفته شود. به بیان دیگر، اولویت درک جرم رایانه‌ای به مثابه حمله به یک وسیله یا سازمان، به یک رویکرد پیشرفته‌تر برای نگریستن به آن از منظر شخص

[6] Cracking
[7] Improper words
[8] E-commercial transactions

بزه‌دیده تبدیل شد. وال[9] جرایم رایانه‌ای را به عنوان «جرائمی که در فضای سایبر رخ می‌دهند» تعریف می‌کند. او همچنین عنوان می‌کند که در این دوران اینترنت، اصطلاح جرم رایانه‌ای، نماد عدم امنیت و خطر بر خط است (Wall, 2007). تعریف ارائه شده توسط Answers.com شاید فشرده و موجزترین پاسخ به چیستی جرم رایانه‌ایست باشد. جرم رایانه‌ای هر نوع به کارگیری رایانه به عنوان یک ابزار برای پی هدف‌های غیر قانونی، نظیر ارتکاب کلاهبرداری، قاچاق در هرزه‌نگاری به چیستی جرم رایانه‌ای در هرزه‌نگاری کودکان و مالکیت معنوی[10]، سرقت هویت[11]، یا نقض حریم خصوصی[12] است. به عقیده میسون، «تفکر در مورد جرم رایانه‌ای به عنوان هر جرمی که در آن یک رایانه یا سایر تجهیزات دیجیتال ایفاء نقش می‌کنند که می‌توان گفت شواهد دیجیتال موجود است. صرف نظر از این که آیا جرم با قالب تعریف قانونی از جرم رایانه‌ای مطابقت دارد یا نه مفید است». او همچنین تعریفی کارکردی از جرم رایانه‌ای ارائه می‌دهد که خود رایانه را به عنوان یک هدف، یک ابزار و حتی حاوی شواهد نشان می‌دهد (Misson, 2008). این تعریف مجدداً تعریفی گسترده‌تر از جرم رایانه‌ای ست که شامل حملات به کمک رایانه و فناوری اطلاعات از هر منظر است. وال (۲۰۰۸) نیز جرائم رایانه‌ای را این گونه تعریف می‌کند: «خطر و نا امنی بر خط که امروزه به طور گسترده برای تعریف جرائم و آسیب‌هایی که با استفاده از فناوری‌های شبکه‌ای ارتکاب می‌یابند؛ استفاده می‌شود». خاطر نشان می‌کنیم که وال (۲۰۰۸) از واژه «آسیب[13]» برای تعریف جرم رایانه‌ای استفاده کرده است. این واژه خاص چنین تعریفی را مایل به جرائم علیه عواطف انسانی نظیر تعقیب ایذائی[14]، آزار و اذیت[15]، مزاحمت[16] و غیره می‌کند. با وجود این، گرایش‌های نوین در تعریف جرم رایانه‌ای معنای این اصطلاح را به نحوی گسترش داده که جرائم رایانه‌ای مختلف نظیر سرقت هویت[17]، قماربازی غیرقانونی[18]، پول‌شویی سایبری[19]، فیشینگ[20]، تروریسم رایانه‌ای[21]، تله رایانه‌ای[22] که کودکان را آماج قرار می‌دهند، نظیر ایجاد و توزیع هرزه‌نگاری کودکان، مزاحمت رایانه‌ای، معاونت در جرائم متعددی – که در آنها اینترنت به عنوان یک

---

[9] Wall
[10] Intellectual property
[11] Stealing identities
[12] Violating privacy
[13] Harm
[14] معادل انگلیسی آن Stalking است و منظور نظارت ناخواسته و یا مکرری است که توسط یک فرد یا گروه نسبت به فرد دیگری است.
[15] Harassing
[16] Bullying
[17] Identity theft
[18] Illegal gambling
[19] Cyber money laundering
[20] فیشینگ (به انگلیسی: Phishing) به تلاش برای بدست آوردن اطلاعاتی مانند نام کاربری، گذرواژه، اطلاعات حساب بانکی و... از طریق جعل یک وب‌سایت، آدرس ایمیل و... گفته می‌شود و یا به عبارت ساده‌تر وقتی شخصی سعی می‌کند شما را فریب دهد تا اطلاعات شخصی‌تان را در اختیارش بگذارید، یک حمله فیشینگ اتفاق می‌افتد.
[21] Cyber terrorism.
[22] Cyber squatting.

ابزار به کار می‌رود- و غیره را نیز در بر می گیرد (هالدر و جیشانکار، ۱۳۹۳). در همه این موردها، سامانه رایانه‌ای و اینترنت تنها ابزار و انگیزه اساسی برای آسیب عامدانه به حیثیت بزه‌دیده است؛ صرف نظر از این که مرتکب بزه‌دیده را بشناسد یا خیر. قتل رایانه‌ای یکی از پدیده‌های وحشتناک عصر فناوری اطلاعات است که در آن یک قربانی یا گروهی از قربانیان مستقیما آماج قرار گرفته، با یک طعمه به خارج از فضای سایبر آمده و سپس در فضای مادی به طور فیزیکی مورد حمله قرار گرفته و یا حتی به قتل می‌رسند. انگیزه چنین اعمالی ممکن است از تنفر شخصی، خشم، ناامیدی گرفته تا اعمال تسویه حساب غیر صلح آمیز متغیر باشد.

بزه‌دیده و بزه‌دیدگی

واژه «بزه‌دیده[۲۳]» در نوشتگان مختلف فارسی و انگلیسی در معانی گوناگون به کار رفته است. در متون فارسی این واژه در معنی عام‌اش، معادل واژه «قربانی» به کار رفته است. قربانی یعنی: «۱ - ویژگی آنچه، یا آنکه به نیت به دست آوردن رضای خداوند ذبح می‌شود. ۲- ویژگی آنکه در راه هدفی جان خود را برای دیگران به خطر بیندازد و فدا کند. ۳- آنکه در اثر حادثه‌ای ناخواسته، جان خود را از دست بدهد: قربانی تصادف، زلزله، .... ۴- آنکه به خاطر وضع دشوار و محیط نامناسب، دچار مشکل و مصیبت شده است: آدم معتاد قربانی جامعه نابسامان است. ۵- عمل قربانی کردن گوسفند، شتر و مانند اینها در روز عید قربان» (انوری، ۱۳۸۶). واژه «بزه‌دیده» در فرهنگ لغات انگلیسی آکسفورد، در معانی ذیل به کار رفته است: «الف- شخصی که در پی یک رویداد یا حادثه، آسیب دیده یا کشته شود. ب- شخصی یا چیزی که به دنبال یک اعتراض یا در جهت ارضای خشم و غضب و غیره آسیب دیده یا نابود شود. ج - شکار یا طعمه: برای مثال، به دام افتادن قربانی در یک حقه بازی یا نیرنگ. د- موجود زنده‌ای که برای خدا یا در یک آیین مذهبی ذبح می‌شود[۲۴]. مفهوم بزه‌دیده در زبان فارسی معادل واژه‌های عربی قربانی، مجنی‌علیه و زیان‌دیده است. این واژه در انگلیسی به معنای Victim (قربانی) به کار رفته است و در ادبیات بحث جرم‌شناسی و کتاب‌های حقوقی، تعریف‌های متفاوتی دارد. در مجموع می‌توان آنها را به تعریف موسع و مضیق دسته‌بندی کرد. 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 (ژنیافیلی، ۱۳۷۹). اما واژه بزه‌دیده در معنی خاص‌اش، فی‌الواقع مفهومی مضیق و همسنگ با واژه معروف حقوق جزا یعنی «مجنی‌علیه» است و «مجنی‌علیه» در واژه‌شناسی یعنی «آنکه جرمی به ضرر او واقع شده است» (انوری، ۱۳۸۶). یا «شخصی که در اثر جرم، شبه‌جرم یا خطای دیگر زیان‌دیده است» ((Garner, 2004). در تعریفی دیگر بزه‌دیده کسی است که یک خسارت قطعی آسیبی به تمامیت جسمی او وارد کرده است و اکثر افراد جامعه هم به این مسأله اذعان دارند.

[23] Victim.
[24] Oxford English Dictionary, 2000, p 1228.

هانس فون هنتینگ پدر علم بزه دیده‌شناسی، بزه‌دیده را چنین تعریف نموده: که بزه‌دیده جرم مانند کسی است که کالبد عمل مجرمانه را تشکیل داده است. هنتینگ بزه‌دیده را در مفهوم مضیق خود مطرح ساخت که ناظر بر مجنی‌علیه است.

بزه‌دیده آسیب‌پذیر

از یک منظر، بزه‌دیدگان رفتارهای مجرمانه را می‌توان به دو دسته ذیل تقسیم‌بندی نمود: ۱- بزه دیده عادی؛ همان‌طور که پیش‌تر نیز بیان شد؛ شامل کلیه اشخاصی می‌شود که در پی فعل یا ترک فعل‌های ناقض قوانین کیفری دچار آسیب اعم از جسمی، روانی، درد و رنج عاطفی، اقتصادی و غیره شده‌اند. این مفهوم از بزه‌دیده، دربرگیرنده بزه‌دیده خاص نیز هست. ۲- بزه‌دیده آسیب‌پذیر[۲۵] یا خاص؛ این اصطلاح یادآور عنوانی مشابه «بزه‌دیده بی‌گناه» است. دانشمندان در نوشته‌هایشان به جای «بزه‌دیده بی‌گناه» از عناوین دیگری مانند «بزه‌دیده پنهان» یا «بزه‌دیده ایده‌آل» استفاده می‌کنند (حاجی‌تبار فیروزجائی، ۱۳۹۰). کلمه‌ی آسیب‌پذیر در واژه‌شناسی به معنی آنکه یا آنچه آمادگی آسیب دیدن را داشته باشد؛ ناتوان در برابر ناملایمات و صدمات و ضعیف به کار رفته است (انوری، ۱۳۸۶). در اکثر نوشته‌های انگلیسی واژه‌ی آسیب‌پذیر مترادف اصطلاح «Vulnerable Adult» نیز به کار رفته است. به عنوان مثال در فرهنگ لغت تخصصی حقوق این اصطلاح به معنی «یک فرد بالغی که از لحاظ فیزیکی یا روانی ناتوان است؛ شخص وابسته به سرویس‌های خدماتی» تعبیر شده است (Garner, 2004). آسیب‌پذیری در مفهوم وسیع پزشکی به «قابلیت و آمادگی شخص برای ضعف سلامتی» گفته می‌شود. منظور از «بزه‌دیدگان بی‌گناه یا بالقوه»، کسانی هستند که هیچ‌گونه نقشی حتی جزئی در وقوع رفتار مجرمانه و بزه‌دیدگی‌شان ندارند و بزه‌دیده واقع شدن آنان صرفاً نتیجه شرایط و اوضاع و احوال خاص خواهد بود. به عبارت دیگر، این دسته از بزه‌دیدگان به خاطر داشتن شرایط و ویژگی‌های خاص، آمادگی و استعداد خاص برای بزه‌دیده واقع شدن را دارند.

گونه‌های حمایت از بزه‌دیدگان سایبری

حمایت کیفری ساده

قانون‌گذار به دنبال جرم‌انگاری هر رفتار ممنوعه، ضمانت اجرای آن را نیز تعیین می‌کند این نوع جرم‌انگاری در کنار بازدارندگی از مرتکبان جرایم، تدبیری برای پیش‌گیری از بزه‌دیدگی از گذر حمایت کیفری به شمار می‌رود. مقنن ایران، در قوانین متعدد به جرم‌انگاری‌های اعمال و رفتارهای ممنوعه در محیط رایانه‌ای پرداخته است که در هر کدام از آنها سیاست کیفری خاصی دنبال شده است از جمله: قانون تجارت الکترونیکی مصوب ۱۳۸۲، قانون نحوه مجازات اشخاصی که در امور سمعی و بصری فعالیت‌های غیر مجاز می‌کنند مصوب[۲۶] ۱۳۸۶، قانون جرایم رایانه ای مصوب ۱۳۸۸

[25] Vulnerable victim.

[۲۶] ماده ۱۰: انتشار آثار مستهجن و مبتذل از طریق ارتباطات الکترونیکی و سایت‌های کامپیوتری با وسیله و تکنیک مشابه دیگر از مصادیق تکثیر و انتشار محسوب و مرتکب حسب مورد به مجازات مقرر در این قانون محکوم می‌شوند.

نکته قابل توجه از بررسی قوانین مذکور اینکه، قانون‌گذار در کنار جرم‌انگاری رفتارهای ضد اجتماعی باید ضمانت اجرای متناسبی را تعیین کند و اگر قانون‌گذار در تعیین ضمانت اجراها دچار لغزش شود نقش پیش‌گیرنده و حمایتی قانون عقیم می‌ماند. در حالی که به نظر می‌رسد این اصل (تناسب بزه و کیفر) در سیاست کیفری ایران در قبال جرایم رایانه‌ای رعایت نشده است. برای نمونه «کلاه‌برداری کامپیوتری» مندرج در ماده ۶۷ قانون تجارت الکترونیک با ضمانت اجرای «یک تا سه سال حبس و پرداخت جزای نقدی معادل مال مأخوذه» جرم‌انگاری شده است و کلاهبرداری رایانه‌ای مندرج در ماده ۱۳ قانون جرایم رایانه‌ای با کیفرگذاری «یک تا پنج سال حبس یا جزای نقدی از بیست تا یکصد میلیون ریال یا هر دو مجازات» جرم‌انگاری شده است و حال آنکه کلاهبرداری سنتی در ماده ۱ قانون تشدید مرتکبین ارتشاء اختلاس و کلاهبرداری با مجازات «یک تا هفت سال و پرداخت جزای نقدی معادل مال مأخوذه» جرم‌انگاری شده است (مالمیر، ۱۳۹۵). این در حالی است که از لحاظ ماهیت فرقی بین بزه‌دیده جرم واحد مندرج در قوانین متعدد وجود ندارد و حتی بزه‌دیدگی در محیط سایبری و رایانه‌ای بیشتر از محیط سنتی است و لذا حمایت کیفری مندرج در قانون جرایم رایانه‌ای به تنهایی برای پیش‌گیری از بزه‌دیدگی کافی نیست و در کنار آن باید ضمانت اجراهای اجتماعی متناسب و متنوع نیز در نظر گرفته شود. کنوانسیون جرایم سایبر نیز در راستای حمایت کیفری از بزه‌دیدگان جرایم رایانه‌ای با ارائه فهرست حداقل جرایم، راهبردهایی را برای کشورهای عضو ارائه می‌دهد تا کشورها موارد مندرج در کنوانسیون (مواد ۲ – ۱۳) را در قوانین خویش جرم‌انگاری کنند که البته این فهرست مانع از بسط محدوده فوق در حقوق داخلی نیست. جرم‌انگاری اعمال شروع به جرم، «مشارکت در جرم» و نیز به رسمیت شناختن مسئولیت کیفری برای اشخاص حقوقی در کنوانسیون جرایم سایبر تدابیر دیگری برای حمایت از بزه‌دیدگان جرایم رایانه‌ای است. همچنین در راستای حمایت از بزه‌دیدگان، کشورهای عضو ملزم شده‌اند؛ به گونه‌ای اقدام به وضع قوانین و سایر تدابیر کنند که در صورت لزوم اطمینان دهند. جرایم مندرج در کنوانسیون از مجازات‌هایی مؤثر، بازدارنده و مناسب[۲۷] که شامل مجازات سالب آزادی[۲۸] می‌شود برخوردارند (ماده ۱۳).

حمایت کیفری خاص یا ویژه[۲۹]

اگر جرم‌انگاری همراه با پیش‌بینی یک ضمانت اجرای کیفری مناسب، ساده‌ترین گونه حمایت کیفری است گاهی مصالح سیاست جنایی اقتضاء می‌کند که با تشدید ضمانت اجراها به این حمایت کیفری جامه عمل پوشانده شود و به عبارتی به یک حمایت کیفری افتراقی می‌انجامد. این تدبیر، گونه ویژه‌ای از تشدید شخصی است که با تأکید بر شخص بزه‌دیده،

[27] Effective proportionate and dissuasive sanctions
[28] Deprivation of liberty
[۲۹] برخی از متخصصان امر، حمایت کیفری را چهار گونه دانسته‌اند: ۱.حمایت کیفری ساده؛ ۲.حمایت کیفری تشدیدی ۳.حمایت کیفری ویژه و حمایت کیفری دنباله‌دار (رایجیان اصلی، ۱۳۹۰، ۱۰۸) ولی به نظر می‌رسد که حمایت کیفری تشدیدی و دنباله‌دار در راستای حمایت کیفری ویژه است و با کمی تسامح با هم منطبق هستند و نمی‌توان برای آنها عنوان‌های مستقلی قائل شد.

حمایت کیفری از او را دنبال می‌کند. بر پایه این یافته‌ها، آسیب‌پذیری برخی از اشخاص مانند زنان و کودکان به دلایلی همچون جنس و سن، آنان را بیش از دیگران شایسته توجه و حمایت ویژه می‌سازد (رایجیان اصلی، ۱۳۹۰). که به این نوع حمایت از بزه‌دیدگان، اصطلاحاً حمایت از «بزه‌دیدگان خاص» می‌گویند. یکی از بزه‌دیدگان خاص که در محیط رایانه‌ای بیشتر در معرض بزه‌دیدگی خاصی هستند کودکان و بهره‌برداری از آنها در هرزه نگاری است. به عنوان نمونه در این راستا مقتن ایرانی در قانون نحوه مجازات اشخاصی که در امور سمعی و بصری فعالیت های غیرمجاز می نمایند. (مصوب ۱۳۸۶) در تبصره ۳ ماده ۳ مقرر نموده است: «استفاده از صغار برای نگهداری، نمایش، عرضه، فروش و تکثیر نوارها و لوح های فشرده غیر مجاز موضوع این قانون موجب اعمال حداکثر مجازاتهای مقرر برای عامل خواهد بود» در نگاه اول، به نظر می‌رسد قانون گذار درصدد حمایت کیفری ویژه از کودکان در قبال هرزه‌نگاری بوده است. در صورتی که چنین نیست زیرا قانون‌گذار به آثار غیرمجاز اشاره کرده است نه آثار سمعی و بصری مستهجن و مبتذل. و بنابراین قانون‌گذار جرایم مذکور در متن ، مواد ۱ و ۲ این قانون را مدنظر داشته که جرایم نسبتاً سبکی‌اند و غالباً به نقض حق نشر مربوط می‌شوند.

از سوی دیگر هرزه‌نگاری کودکان[۳۰] در لایحه پیشنهادی جرایم رایانه‌ای با تأسی از کنوانسیون جرایم سایبر مورد توجه قرار گرفته بود ولی در تصویب نهایی قانون‌گذار ایران برخلاف نظر تدوین‌کنندگان لایحه که همسو با معیارهای جهانی بود، با عدم پذیرش، به رویکرد مطلق هرزه‌نگاری رایانه‌ای مبادرت کرده‌اند. ماده ۱۴ قانون جرایم رایانه‌ای که در ذیل فصل «جرایم علیه اخلاق و عفت عمومی» آمده است؛ ضمن کاهش مجازات‌های مقرره، در قانون مجازات اشخاصی که در امور سمعی و بصری فعالیت‌های غیرمجاز می‌نمایند»؛ هیچگونه رویکرد افتراقی از رهگذر کیفرگذاری مشدد به دلیل کودکی بزه‌دیده اتخاذ نکرده است (بای و پورقهرمانی، ۱۳۸۸). در حالی که این رویکرد با اسناد خاص هرزه‌نگاری کودکان مغایرت دارد. که این اسناد خاص بیشتر مصوب سال ۱۹۹۹ می‌باشد که سال با اهمیتی در زمینه توجه جامعه جهانی به هرزه‌نگاری کودکان در فضای مجازی است. که از جمله آنها کنفرانس پکن (۱۹۹۹) در مورد «مبارزه با استفاده از اینترنت برای استثمار کودکان» می‌باشد (پورقهرمانی، ۱۳۹۶).

حمایت شکلی

حمایت شکلی (آیین دادرسی مدار) عبارتست از پیش‌بینی سازوکارهایی برای احقاق این حق‌ها و برآورده کردن نیازهای بزه‌دیدگان به ویژه «جبران خسارت[۳۱]» یا تسهیل آن در سراسر فرایند جنایی. از آنجا که این حق‌ها به طور معمول در قوانین آیین دادرسی جنایی به رسمیت شناخته می‌شود؛ از آن می‌توان به «سازو کارهای مبتنی بر آیین دادرسی[۳۲]» یا «آیین دادرسی‌مدار» نیز یاد کرد (رایجیان اصلی، ۱۳۸۴). علاوه بر سازکارهای کلی که در مورد حمایت شکلی از بزه‌دیدگان، وجود دارد از جمله حق داشتن وکیل در سراسر فرایند جنایی، حق طرح دعوای ضرر و زیان و پیش‌بینی شرایط آن، حق

[30] Child pornography
[31] Restitution
[32] Procedural mechanisms.

درخواست پژوهش از دعوی ضرر و زیان و .... (آشوری وخدادادی، ۱۳۹۰)، قانون‌گذار در قانون جرایم رایانه‌ای در بخش دوم مربوط به آیین دادرسی جرایم رایانه‌ای، حمایت‌های شکلی ویژه‌ای از بزه‌دیدگان جرایم رایانه‌ای کرده است. در باب صلاحیت، قانون‌گذار در برخی موارد با توجه به وضعیت بزه‌دیده مراجع قضایی ایران را صالح به رسیدگی دانسته است. بر اساس بند (ج) ماده ۲۸ قانون جرایم رایانه‌ای (بند (پ) ماده ۶۶۴ قانون آیین دادرسی کیفری ۱۳۹۲): «جرم توسط هر ایرانی یا غیرایرانی در خارج از ایران علیه سازمان‌های رایانه‌ای و مخابراتی و تارنماهای (وب‌سایت‌های) مورد استفاده یا تحت کنترل قوای سه گانه یا نهاد رهبری یا نمایندگی‌های رسمی دولت یا هر نهاد یا مؤسسه‌ای که خدمات عمومی ارائه می‌دهد یا علیه تارنماهای (وب‌سایت‌های) دارای دامنه مرتبه بالای کد کشوری ایران در سطح گسترده ارتکاب یافته باشد» که به نظر می‌رسد این بند از ماده که به تعبیر برخی صلاحیت حمایتی[۳۳] یا (واقعی) محسوب می‌شود، در راستای حمایت شکلی از بزه دیدگان جرایم رایانه‌ای می‌باشد و حتی دیوان عالی کشور در رای وحدت رویه‌ای (۷۲۹-۱۳۹۱/۱۲/۰۱) بر این مبنا نظر داده است: «نظر به این که در صلاحیت محلی، اصل صلاحیت دادگاه محل وقوع جرم است و این اصل نیز مستفاد از ماده ۲۹ قانون جرایم رایانه‌ای (مصوب ۱۳۸۸) مورد تائید قانون‌گذار قرار گرفته، بنابراین در جرم کلاهبرداری مرتبط با رایانه، هرگاه تمهید مقدمات و نتیجه حاصله از آن در حوزه‌های قضایی مختلف صورت گرفته باشد؛ دادگاهی که بانک افتتاح‌کننده حساب زیان‌دیده از بزه که پول به طور متقلبانه از آن برداشت شده در حوزه آن قرار دارد، صالح به رسیدگی است». مبنای این حق در مواد ۴ و ۵ کنوانسیون جرایم به نوعی مطرح شده است ولی بر خلاف صلاحیت‌های سرزمینی و تابعیتی، کنوانسیون جرایم سایبر هیچ اشاره‌ای به حق کشورها در اعمال این قسم از صلاحیت فراسرزمینی نکرده است که جای تامل دارد (همان، ۱۵۲). همچنین بر اساس بند (د) ماده ۲۸ (ماده ۶۶۴ ق.آ.د.ک ۹۲) یکی از مواردی که دادگاههای ایران صلاحیت دارند و در راستای بزه‌دیده محوری است اینکه: «جرایم رایانه‌ای متضمن سوء استفاده از اشخاص کمتر از ۱۸ سال اعم از آنکه مرتکب یا بزه‌دیده ایرانی یا غیر ایرانی باشد». حمایت شکلی دیگر از بزه‌دیدگان جرایم رایانه‌ای اختصاص دادن برخی از شعب دادسرا و دادگاه‌ها برای رسیدگی به جرایم رایانه‌ای است. بر اساس ماده ۳۰ قانون جرایم رایانه ای (ماده ۶۶۶ ق.آ.د.ک ۹۲): «قوه قضائیه موظف است به تناسب ضرورت شعبه یا شعبی از دادسرا، دادگاه‌های کیفری یک، کیفری دو، اطفال و نوجوانان، نظامی و تجدید نظر را برای رسیدگی به جرایم رایانه‌ای اختصاص دهد» و بر اساس تبصره ماده فوق «قضات دادسرا و دادگاههای مذکور از میان قضاتی که آشنایی لازم به امور رایانه دارند انتخاب خواهند شد[۳۴]». «اختصاصی کردن شعب دادسراها و دادگاه‌ها» و نیز «متخصص کردن قضات دادگاه‌ها» می‌تواند نقطه عطفی بر حمایت از بزه‌دیدگان جرایم رایانه‌ای در راستای مراجعه به دادگاه صالح

[33] Protective Principle

[۳۴] قوه قضاییه از سال ۱۳۸۲ با برگزاری کلاس‌های آموزش ضمن خدمت قضات دو عنوان درسی آموزشی در خلال برنامه‌های دوره گنجانده است که عبارتند از، «جرایم سایبر» برای قضات کیفری و «حقوق فناوری اطلاعات» برای قضات حقوقی.

باشد که البته در این راستا پلیس جرایم سایبری یا پلیس فتا (فضای تبادل اطلاعات) که به صورت تخصصی در این راستا فعالیت می‌کند؛ می‌تواند نقطه مثبتی در حمایت از بزه‌دیدگان تلقی شود (به نقل از پورقهرمانی، ۱۳۹۶).

بنابراین یکی از راهکارها و گونه‌های حمایت از بزه‌دیدگان جرایم سایبری، رویکردهای مربوط به شکل و ساختار دادرسی در این‌گونه جرایم است. این گونه از حمایت در اسناد بین‌المللی صرفاً به صورت پیش‌بینی مقررات کلی شکلی و در حقوق کیفری ایران در سه بعد پیش‌بینی صلاحیت حمایتی، اختصاصی کردن دادسراها و دادگاه‌ها و تشکیل پلیس فتا نمود پیدا کرده است.

حمایت‌های مادی و معنوی

پیش‌بینی ساز و کار جبران آثار ناشی از بزه‌دیدگی یکی از مهم‌ترین مؤلفه‌های حقوق کیفری در راستای حمایت از بزه‌دیدگان جرایم رایانه‌ای می‌باشد. برخلاف مؤلفه‌های حمایتی پیشین، آثار سازوکار جبران، به طور مستقیم بر بزه‌دیدگان جرایم فوق تبلور می‌یابد و هرچه گسترده باشد از گسترش آسیب وارده در اثر ارتکاب جرم علیه بزه‌دیدگان جلوگیری می‌کند. جبران آثار بزه‌دیدگی شامل جبران خسارت، پرداخت غرامت[۳۵]، اعاده وضع به حالت سابق، اعاده حیثیت یا توان بخشی و تاوان است. این ساز و کار به دو شکل رسمی[۳۶] (جبران خسارت مادی و معنوی و نیز پرداخت غرامت، دولتی، عمومی و فردی) و غیررسمی[۳۷] (مثل میانجیگری[۳۸]، سازش[۳۹]، داوری[۴۰]، صلح و آشتی[۴۱]) قابل اعمال است. در جمهوری اسلامی ایران جبران‌پذیری مالی خسارت‌های مادی به طور کلی پذیرفته شده است. (ماده ۲۱۴ ق.م.ا مصوب ۹۲ و ماده ۱۴ ق. آ. د. ک مصوب ۹۲) و از این جهت می‌توان گفت که نظام کیفری ایران هم‌سو با اصول و معیارهای پذیرفته شده در زمینه حمایت‌های مالی، جبران خسارت مادی[۴۲] را مبنای حمایت مالی از بزه دیدگان قرار داده است (رایجیان اصلی، ۱۳۹۰) که جلوه‌هایی از آن هم به نوعی در قوانین مرتبط با جرایم رایانه‌ای متبلور یافته است. از جمله در بحث کلاهبرداری مرتبط با رایانه (ماده ۳ قانون جرایم رایانه‌ای) و نیز کلاهبرداری کامپیوتری (مندرج در ماده ۶۷ قانون تجارت الکترونیک) علاوه بر مجازات‌های مندرج، شخص مرتکب باید به «رد مال» هم محکوم شود. و نیز در ماده ۷۸ قانون تجارت الکترونیک آمده است: «هرگاه در بستر مبادلات الکترونیکی در اثر نقض یا ضعف سیستم مؤسسات خصوصی و دولتی، به جز در نتیجه قطع فیزیکی ارتباط الکترونیکی، خسارتی به اشخاص وارد شود مؤسسات مزبور مسئول جبران خسارت وارده می‌باشند مگر اینکه خسارات وارده ناشی از فعل اشخاصی باشد که در این صورت جبران خسارات بر عهده این

[35] Compensation.
[36] Formal remedy.
[37] Informal remedy.
[38] Mediation.
[39] Conciliation.
[40] Arbitration.
[41] Peacemaking.
[42] Material restitution.

اشخاص خواهد بود». ماده مذکور نقطه عطف مثبتی در راستای حمایت از بزه‌دیدگان می‌تواند تلقی شود. هرچند در قانون جرایم رایانه‌ای، آن طور که شایسته و بایسته است به بحث حمایت‌های مالی پرداخته نشده است؛ ولی به نظر می‌رسد عدم ذکر به معنای عدم جبران نیست و از اصول و قواعد عمومی این امر قابل استنباط است. در کنار جبران خسارات مادی، حمایت های معنوی (عاطفی و حیثیتی) هم نسبت به بزه‌دیدگان جرایم رایانه‌ای باید مورد توجه قرار گیرد. روشن است که هر جرمی گذشته از خسارت‌های مادی، آزردگی خاطر بزه‌دیده را نیز به همراه دارد. (Currani, 2007). این آزردگی خاطر که از آسیب به عواطف و احساسات فرد یا حیثیت شخص برمی‌خیزد و در جرم‌های مختلف بازتاب‌های گوناگون دارد «درد و رنج عاطفی و حیثیتی[43]» نامیده می‌شود. (بهمن، ۱۳۹۷). جبران درد و رنج‌های عاطفی به دلیل برآوردناپذیری مالی از جبران خسارات مادی جداست. حمایت عاطفی کمک‌های روانشناسانه‌ای است که برای ترمیم درد و رنج‌های عاطفی بزه‌دیدگان انجام می‌شود و پیش از هر چیز نقش روانشناسان و روان‌کاوان در آن برجسته است. حمایت عاطفی از بزه‌دیدگان را می‌توان از گذر مراکز خصوصی روان‌درمانی بهره‌مند از روان‌شناسان متخصص تضمین کرد (فیلیزولا، ۱۳۷۹).

از نظر سیاست جنایی، مقنن قانون جرایم رایانه‌ای به جبران خسارت معنوی[44] توجه آن چنانی نداشته است، به نحوی که در برخی موارد به صرف جرم‌انگاری اعمالی که علیه حیثیت افراد است (با ضمانت اجراهای نسبتاً ضعیف حبس یا جزای نقدی) اکتفا شده است (مواد ۱۸-۱۶)و به جبران ضرر و زیان معنوی ناشی از بزه‌دیدگی جرایم مذکور توجه خاصی نشده است و صرفاً در ماده ۱۸، آن هم به صورت مردد بر جبران خسارات معنوی «... افزون بر اعاده حیثیت (در صورت امکان)....» نظر شده است. ولی با وجود مسائل فوق، به نظر می‌آید که بر اساس قانون مسئولیت مدنی (ماده ۱۰) و قانون آیین دادرسی کیفری ۱۳۹۲ (تبصره ۱ ماده ۱۴) جبران خسارات معنوی علاوه بر خسارات مادی پیش‌بینی شده است. هرچند در عمل با بی‌اقبالی مراجع قضایی مواجه شده است. نکته‌ای که در راستای سیاست جنایی ایران در قبال حمایت از بزه‌دیدگان به طور کلی (نه خاص جرایم رایانه‌ای) می‌توان اشاره کرد «دستور العمل و ضوابط اجرایی کمک و حمایت از بزه‌دیدگان» است که توسط وزارت دادگستری در مورخ ۱۳۸۸/۰۴/۳۱ به تصویب رسیده است که نقطه عطف مثبتی در راستای حمایت مادی و معنوی از تمام اقشار بزه‌دیده است. ولی نکته قابل تامل در این دستورالعمل، این است که اجرای آن به صورت آزمایشی تا پایان سال ۱۳۸۸ بوده و پس از پایان مدت اجرای آزمایشی و برای سال‌های بعد منوط به تأمین بودجه شده است که به نظر می‌رسد اصل وجود چنین مقرراتی ضروری بوده ولی نه به شکل فعلی که، قابل اجرا نباشد بلکه لوازم اجرای چنین مقرراتی فراهم شود که انتظار می‌رود در راستای اجرای بهتر، سطح قانونی آن از «دستورالعمل» به «قانون» ارتقاء یابد (پورقهرمانی، ۱۳۹۶). همچنین مصوبه‌ای تحت عنوان «بسته اجرایی وزارت دادگستری

[43] Emotional suffering
[44] Immaterial restitution

(۱۳۹۰-۱۳۹۴)» موضوع ماده ۲۱۷ قانون برنامه پنج ساله پنجم توسعه جمهوری اسلامی ایران» منتشر شد که بر اساس آن یکی از راهبردهای اساسی بسته فوق «اجرای تکالیف بیت‌المال در پرداخت دیه و سایر خسارات و حقوق آسیب‌دیدگان از جرائم» معرفی شده است و در راستای آن سیاست‌های اجرایی متناظر با راهبرد فوق «ایجاد سازکار لازم برای پرداخت دیه و اجرای آرای محاکم قضایی و ایجاد ساز و کار لازم برای حمایت از بزه‌دیدگان» شناخته شده است که وجود و اجرای چنین مقرراتی نقطه عطف مثبت در راستای حمایت مادی و معنوی از بزه‌دیدگان جرایم می‌تواند تلقی شود.

بحث و نتیجه‌گیری

با رشد وخامت بزه‌دیدگی مستقیمِ ابنای بشر در برابر تهدیدهای سایبری، تعریف جرم سایبری نیز دگرگون شد. به گونه‌ای که کنوانسیون جرایم سایبری در سال ۲۰۰۱، با لحاظ «جرایم مرتبط با محتوا» در کنار جرایم علیه محرمانگی، صحت و تمامیت و دسترس‌پذیری داده‌ها و سیستم‌های رایانه‌ای، «جرایم مرتبط با رایانه» و «جرایم مرتبط با نقض حق نشر» به نوعی جرم‌انگاری حمله به «حیثیت» و «کرامت» انسان‌ها را به دولت‌ها پیشنهاد داده است. از سوی دیگر یکی از جنبه‌های سیاست جنایی که مظلوم واقع شده است و جزو گروه فراموش‌شده‌ها است؛ بحث بزه‌دیده است. شناخت بزه‌دیده یا همان قربانیِ جرم، چند دهه است که در میان جرم‌شناسان مطرح شده است. و در تمامی جرایم از جمله جرایم رایانه‌ای بحث بزه‌دیده قابل طرح است. به ویژه آنکه توسعه رو به رشد فضای سایبر، مورد تهاجم بیشتر مجرمان رایانه‌ای و به تبع آن بزه‌دیدگان رایانه‌ای بیشتر واقع شده است. به نحوی که بر اساس آمارها، ۶۵٪ از استفاده‌کنندگان شبکه جهانی، قربانی جرم سایبری می‌شوند. در این پژوهش در ابتدا کوشیده شد تا به برخی از تعاریف مهم، اشاره شود. جرم سایبری در اصطلاح به جرمی گفته می‌شود که در محیطی غیر فیزیکی علیه فناوری اطلاعات با حالات شبیه‌سازی و مجازی‌سازی ارتکاب می‌یابد. امروزه بسیاری از جرائم سنتی، همزمان با پیشرفت فناوری اطلاعات و ارتباطات به شدت متحول شده و به جرائم سایبری تبدیل شده‌اند. جرائم سایبری نیز به جهت گسترش خود، رفته‌رفته جانشین عباراتی چون جرم‌های رایانه‌ای و جرم‌های اینترنتی می‌شوند. به جرائم سایبر، جرائم علیه فناوری اطلاعات نیز گفته می‌شود. گونه‌های حمایت از بزه‌دیدگان جرایم سایبری در این پژوهش معرفی شدند. که عبارتند از حمایت ماهوی (شامل حمایت کیفری ساده و حمایت کیفری خاص یا ویژه)، حمایت شکلی، حمایت‌های مادی و معنوی،حمایت اجتماعی و حمایت بین‌المللی.

منابع و مراجع

آشوری، محمد و خدادادی، ابوالقاسم، حقوق بنیادین بزه‌دیده در فرایند دادرسی کیفری، فصلنامه آموزه‌های حقوق کیفری، دانشگاه علوم اسلامی رضوی، شماره ۲، ۱۳۹۰، صفحات ۳ – ۳۶.

اسلامی، ابراهیم، جایگاه حمایت از بزه‌دیدگان جرایم سایبری درمقررات کیفری حقوق داخلی وحقوق بین‌الملل، پژوهشنامه حقوق اسلامی، سال هفدهم، شمارهٔ اول (پیاپی ۴۳)، ۱۳۹۵، صفحات ۱۵۷ تا ۱۸۲.

انوری، حسن، ۱۳۸۶، فرهنگ بزرگ سخن، چاپ چهارم، تهران: انتشارات سخن.

باستانی، برومند، ۱۳۸۳، جرائم رایانه‌ای و اینترنتی، تهران: انتشارات بهنامی.

بای، حسینعلی و پورقهرمانی، بابک، بررسی فقهی – حقوقی هرزه‌نگاری در فضای مجازی، فصلنامه‌ی حقوق اسلامی، سال ششم، شماره‌ی ۲۳، ۱۳۸۸، صفحات ۹۷ – ۱۲۵.

بل، دیوید ۱۳۸۹، درآمدی بر فرهنگ‌های سایبر، ترجمه مسعود کوثری و حسین حسنی، تهران: انتشارات جامعه‌شناسان.

پرویزی، رضا، ۱۳۸۴، پی‌جویی جرائم رایانه‌ای، چاپ اول، تهران: جهان جام جم.

پورقهرمانی، بابک، مطالعه‌ی تطبیقی سازکارهای حمایت از بزه‌دیدگان جرایم رایانه‌ای در حقوق کیفری ایران و اسناد بین‌المللی با تأکید بر کنوانسیون بوداپست، پژوهشنامه‌ی حقوق کیفری، سال هشتم، شماره اول، ۱۳۹۶، صفحات ۷ تا ۳۶.

جاویدنیا، جواد، ۱۳۸۸، جرائم تجارت الکترونیکی، چاپ دوم، تهران: انتشارات خرسندی.

رایجیان اصلی، مهرداد، ۱۳۸۴، بزه‌دیده‌شناسی حمایتی، چاپ اول، تهران: نشر دادگستر.

ژنیافیلی، زولا، ۱۳۷۹، بزه‌دیده و بزه‌دیده‌شناسی، ترجمه‌ی روح‌الدین کردعلیوند و احمد محمدی، تهران: مجتمع علمی و فرهنگی مجد.

عاملی، سعیدرضا، ۱۳۹۰، رویکرد قضایی به آسیب‌ها، جرائم و قوانین و سیاست‌های فضای مجازی، انتشارات امیرکبیر، چاپ اول.

مالمیر، محمود و زررخ، احسان، «پیشگیری از بزه‌دیدگی سایبری»، فصلنامه علمی-ترویجی مطالعات پیشگیری از جرم، سال پنجم، شماره ۱۷، ۱۳۸۹، صفحات ۵۹ تا ۸۶.

مالمیر، محمود، ۱۳۹۵، جرم‌شناسی جرایم سایبری از منظر پیشگیری، تهران: انتشارات مجد.

هالدر، دباراتی، جیشانکار، کی، ۱۳۹۳، جرم رایانه‌ای و بزه‌دیدگی زنان: قانون‌ها، حق‌ها و مقرره‌ها، ترجمه‌ی حسین‌محمد کوره‌پز، احسان سلیمی و مهرداد رایجیان‌اصلی، چاپ اول، تهران: انتشارات مجد.

Brier, Søren (2010) Cybersemiotics and the question of knowledge. In:Information and Computation. Gordana Dodig-Crnkovic & Mark Burgin(eds). World Scientific Publishing Co.

Folsom, Thomas C. (2007) Defining Cyberspace (Finding Real Virtue in the Place of Virtual Reality) (2006). Tulane Journal of Technology & Intellectual Property, Vol. 9.
Garner, Brayan A (2004), black, s Law Dictionary, Eight Edition, Thomson.
Haney, Michel (2006), An introduction to cyber peacekeeping, Computers in Human Behavior, Volume 61, October 2006, Pages 22-48.
Misson, A (2008) Cyerspace: The human dimension, Newyork, W.H. Freman and Compamy.
Suler, John (2004) The Psychology of Cyberspace. http://truecenterpoint.com/ce/ index.html.
Wall, D. S. (2007). Cybercrime: The transformation of crime in the information age. Cambridge, UK: Polity.