کاربست نظریه‌های جرم‌شناختی در تحلیل و مقابله با جرایم سایبری

نویسندگان	وابستگی سازمانی
محدثه قوامی پور سرشکه	گروه حقوق، واحد لاهیجان، دانشگاه آزاد اسلامی، لاهیجان، ایران
امیر رضا محمودی *	گروه حقوق، واحد لاهیجان، دانشگاه آزاد اسلامی، لاهیجان، ایران
بهار فرهادی	گروه حقوق، واحد رشت، دانشگاه آزاد اسلامی، رشت، ایران

اطلاعات مقاله	
نوع مقاله	پژوهشی
صفحه	۱ - ۱۰
دوره ۱، شماره ۲	

اطلاعات نویسنده مسئول	
نویسنده مسئول	امیر رضا محمودی
کد ارکید	۰۰۰۰-۰۰۰۰-۰۰۰۰-۰۰۰۰
تلفن	۰۹۱۴۳۳۳۷۳۴۵
ایمیل	amirreza.mahmodi@gmail.com

سابقه مقاله	
تاریخ دریافت	۱۴۰۳/۰۹/۲۰
تاریخ ویرایش	۱۴۰۳/۱۰/۰۴
تاریخ پذیرش	۱۴۰۳/۱۰/۰۶
تاریخ انتشار	۱۴۰۳/۱۰/۱۲
روش پژوهش	توصیفی تحلیلی

چکیده

پیشرفت فناوری های نوین شکل بزهکاری ها را دگرگون کرده است. علوم جزایی نیز به دنبال این پیشرفت ها درصدد یافتن راه هایی در پیشگیری از جرایم ارتکابی می باشد. بنابریان نظریه‌های جرم‌شناختی می‌توانند نقش مهمی در پیشگیری از جرایم سایبری ایفا کنند. با استفاده از این نظریه‌ها، می‌توان عوامل مؤثر در وقوع این جرایم را شناسایی و راهکارهایی برای مقابله با آنها ارائه داد. افزایش احتمال شناسایی و دستگیری مجرمان سایبری، وضع قوانین سختگیرانه‌تر و افزایش مجازات‌ها می‌تواند از جمله راهکارهای مؤثر در این زمینه باشد. با افزایش آگاهی کاربران از خطرات فضای مجازی و روش‌های کلاهبرداری، می‌توان از قربانی شدن آنها جلوگیری کرد و در نتیجه منافع مجرمان را کاهش داد. با کاربست نظریه های جرم شناختی می توان از ترویج خشونت و جرم در فضای مجازی جلوگیری کرد و الگوهای مثبت را به کاربران معرفی کرد. با آموزش کاربران در مورد خطرات فضای مجازی و روش‌های پیشگیری از جرایم سایبری، می‌توان از آنها در برابر این جرایم محافظت کرد و افرادی که با فشارهای مختلفی مانند مشکلات مالی، اجتماعی یا روانی روبرو هستند، کمک کرد تا با فشارهای خود مقابله کنند و راه‌های قانونی برای حل مشکلاتشان پیدا کنند. با کاربست نظریه کنترل اجتماعی می توان روابط اجتماعی افراد را تقویت کرد و آنها را به مشارکت در فعالیت‌های مثبت جامعه تشویق کرد. همچنین با ایجاد احساس مسئولیت در افراد در قبال رفتارهای خود در فضای مجازی، می‌توان از وقوع جرایم سایبری جلوگیری کرد. علاوه بر این راهکارها، عوامل دیگری مانند ضعف قوانین و مقررات، عدم آگاهی کاربران از خطرات فضای مجازی و کمبود همکاری بین‌المللی نیز می‌توانند در وقوع جرایم سایبری مؤثر باشند. برای پیشگیری از این جرایم، باید به این عوامل نیز توجه کرد و راهکارهای مناسبی برای آنها ارائه داد.

واژگان کلیدی: *جرم، نظریه های جرمشناختی، جرایم سایبری، پیشگیری از جرایم سایبری*

توضیحات

نحوه استناد دهی: قوامی پور سرشکه، محدثه؛ محمودی، امیر رضا؛ فرهادی، بهار (۱۴۰۳)، کاربست نظریه‌های جرم‌شناختی در تحلیل و مقابله با جرایم سایبری، فصلنامه علمی مطالعات میان رشته ای حقوق و تربیت اسلامی، دوره ۱، شماره ۲، صفحات ۱ - ۱۰

Criminal Victimization & Its Manifestations in The Criminal Law of Iran & The United Arab Emirates	
Authors	**Organizational Affiliation**
Mohadeseh Ghavami Pour Sereshkeh	Department of Law, Lahijan Branch, Islamic Azad University, Lahijan, Iran
Amir Reza Mahmoodi *	Department of Law, Lahijan Branch, Islamic Azad University, Lahijan, Iran
Bahar Farhadi	Department of Law, Rasht Branch, Islamic Azad University, Rasht, Iran

Article Information		**Abstract**
Article Type	Research	The advancement of new technologies has transformed the form of crime. Following these advances, criminal science is also seeking ways to prevent crimes from being committed. Therefore, criminological theories can play an important role in preventing cybercrimes. Using these theories, it is possible to identify the factors that contribute to the occurrence of these crimes and provide solutions to combat them. Increasing the likelihood of identifying and arresting cybercriminals, enacting stricter laws, and increasing penalties can be effective solutions in this regard. By increasing users' awareness of the dangers of cyberspace and fraud methods, they can be prevented from becoming victims, and as a result, the interests of criminals can be reduced. By applying criminological theories, it is possible to prevent the promotion of violence and crime in cyberspace and introduce positive models to users. By educating users about the dangers of cyberspace and methods for preventing cybercrime, they can be protected from these crimes and people who are facing various pressures such as financial, social, or psychological problems can be helped to cope with their pressures and find legal ways to solve their problems. By applying the theory of social control, social relationships can be strengthened and they can be encouraged to participate in positive activities in society. Also, by creating a sense of responsibility in people for their behavior in cyberspace, the occurrence of cybercrime can be prevented. In addition to these solutions, other factors such as weak laws and regulations, users' lack of awareness of the dangers of cyberspace, and lack of international cooperation can also be effective in the occurrence of cybercrime. In order to prevent these crimes, these factors must also be considered and appropriate solutions must be provided for them.
Pages	1 - 10	
Volume 1, Issue 2		
Corresponding Author's Info		
Corresponding Author's	Amir Reza Mahmoodi	
ORCID	0000 – 0000 – 0000 - 0000	
Tell	09143337345	
Email	amirreza.mahmodi@gmail.com	
Article History		
Received	2024/12/10	
Revised	2024/12/24	
Accepted	2024/12/26	
Published Online	2025/01/01	
Research Method	Descriptive Analytical	
Keywords		*Crime, criminological theories, cybercrime, cybercrime prevention*

How to Cite This Article: Ghavami Pour Sereshkeh, Mohadeseh; Mahmoodi, Amir Reza; Farhadi, Bahar (2025), The Application of Criminological Theories in the Analysis and Confrontation of Cybercrime, Quarterly Journal of Interdisciplinary Studies in Islamic Law and Education , Volume 1, Issue 2, Pages 1 - 10

۱–مقدمه

جرایم سایبری نوعی جرم نوین هستند که با استفاده از کامپیوترها انجام می‌شوند و به دلیل وقوع در فضای الکترونیکی، شناسایی و ردیابی مجرمان را دشوار می‌کنند. از جمله انواع رایج این جرایم می‌توان به کلاهبرداری اینترنتی، انتشار اطلاعات نادرست، هک، آزار و اذیت آنلاین و سرقت هویت اشاره کرد اینترنت یکی از تأثیرگذارترین اختراعات امروزی است که زندگی روزانه افراد را به شدت تغییر داده و میلیون‌ها نفر را به فضای سایبری متصل کرده است. این فناوری نه تنها شیوه تعامل و یادگیری را دگرگون کرده، بلکه به طور کلی شیوه زندگی را نیز تغییر داده است. با پیشرفت اینترنت و فناوری‌های کامپیوتری، مجرمان نیز به دنبال استفاده از این فناوری‌ها برای انجام عمل‌های مخرب هستند. (شعاعی، خوانین زاده، ۱۴۰۱: ۱۸۸) جرم به طور کلی به معنای رفتاری است که از هنجارها و قواعد پذیرفته شده در جامعه تخطی می‌کند. در این شرایط، جرم به عنوان یک رفتار انحرافی شناخته می‌شود و دارای ویژگی‌های مشخصی است که در قوانین تعریف شده و مستلزم مجازات‌های مادی است. با گذشت زمان، برداشت ما از مفهوم جرم دچار تغییراتی شده است. در گذشته، مجازات‌ها برای مجرمان سخت‌تر بود، اما به تدریج راهکارهایی برای این افراد به جامعه ارائه شده است. بر اساس تعریف کنگره جرم‌شناسی بین‌المللی در توکیو، جرم به عنوان «هر نوع رفتار کلامی یا عملی با نیت آسیب رساندن به دیگران و عبور از مرزهای تعیین شده برای اطاعت» تعریف می‌شود. با پیشرفت مطالعات در زمینه جرایم سایبری، پژوهشگران به دنبال بهترین تعریف برای این اصطلاح بوده‌اند. تا کنون، تعریف جامع و کاملی از جرایم سایبری ارائه نشده است و این جرایم گاهی با عناوینی مانند جرم رایانه‌ای، جرم مبتنی بر فناوری یا جرم فضای سایبری شناخته می‌شوند. (امیریان و همکاران، ۱۳۹۹: ۱۹۴) در حوزه جرمشناسی، نظریه‌های مختلفی برای توضیح رفتارهای مجرمانه وجود دارد که می‌توانند به جرایم سایبری نیز تعمیم یابند. این نظریه‌ها شامل نظریه یادگیری اجتماعی، نظریه فشار عمومی و نظریه کنترل هستند. مطالعه حاضر به تحلیل این نظریه‌ها می‌پردازد تا مشخص کند کدام یک بهتر می‌تواند علت جرایم سایبری را توضیح دهد. مجرمان سایبری به دلایل خاصی به ارتکاب جرایم سایبری گرایش پیدا می‌کنند و برای جلوگیری از این جرایم، مأموران قانون باید به درک عمیق‌تری از ماهیت و علل آن‌ها دست یابند. (شعاعی و خوانین زاده، ۱۴۰۱: ۱۸۹) محققان جرایم سایبری، از جمله راجرز، اسموک و جیا، مجرمان سایبری را به نه گروه مختلف تقسیم کرده‌اند: مبتدیان، معتادان سایبری، فعالان سیاسی، سارقان، نویسندگان ویروس، افراد داخلی، هکرهای محافظ، مجرمان حرفه‌ای و تروریست‌های سایبری. این دسته‌بندی به درک بهتر انگیزه‌ها و ویژگی‌های مجرمان کمک می‌کند. (صبح خیز و همکاران، ۱۴۰۰: ۱۴۹) راجرز این گروه‌ها را بر اساس سطح مهارت و انگیزه در یک مدل دایره‌ای قرار داده و انگیزه‌های اصلی شامل انتقام، منافع مالی، کسب شهرت و کنجکاوی است. به عنوان مثال، فعالان سیاسی و مجرمان حرفه‌ای از بالاترین سطح مهارت برخوردارند، اما انگیزه‌های متفاوتی دارند. این تقسیم‌بندی می‌تواند در طراحی راهبردهای مقابله با جرایم سایبری مفید باشد. (کردعلیوند و میرزایی، ۱۳۹۷: ۲۰۶) محققان مختلفی به طبقه‌بندی جرایم سایبری پرداخته‌اند. گوردون و فورد جرایم سایبری را به دو دسته نوع یک (تکنیکی‌تر مانند هک) و نوع دو (تعامل انسانی مانند قمار آنلاین) تقسیم کرده‌اند. (دشتی و افشاری، ۱۳۹۸: ۸۸) با پیشرفت هوش مصنوعی و رباتیک، احتمال ظهور نوع سوم جرایم سایبری که توسط ابزارهای خودآموز انجام می‌شود، مطرح شده است. مک‌گوایر و دولینگ نیز جرایم سایبری را به «مؤثر» (جرایم سنتی تسهیل‌شده با کامپیوتر) و «وابسته» (طراحی‌شده برای فضای آنلاین) تقسیم کرده‌اند. (انصاری و همکاران،۱۳۹۸: ۱۳۲) محققان به این نتیجه رسیده‌اند که مجرمان سایبری به دلایل متنوعی اقدام به ارتکاب جرم می‌کنند. یکی از این دلایل انتقام‌جویی است؛ برخی افراد به دلیل نارضایتی یا اخراج از شغل خود، به اعمال خرابکارانه و سرقت روی می‌آورند. همچنین، برخی افراد برای احساس قدرت و اهمیت شخصی، به جرایم سایبری دست می‌زنند. مشکلات مالی نیز می‌تواند عاملی برای ارتکاب جرایم مالی سایبری، مانند سرقت اطلاعات بانکی یا داده‌های محرمانه باشد. احساس توانایی در کار با کامپیوتر نیز می‌تواند موجب شود که برخی افراد به این نوع جرایم روی آورند. علاوه بر این، انگیزه‌های

اقتصادی، حس رقابت و تمایل به آسیب رساندن به شرکت‌ها نیز از دیگر دلایل ارتکاب جرایم سایبری به شمار می‌روند. (امیریان و همکاران، ۱۳۹۹: ۲۲۳) برخی محققان عوامل انگیزشی مجرمان سایبری را در پنج دسته تقسیم‌بندی کرده‌اند. یکی از این دسته‌ها شامل اقدام به جرم به قصد بازی و سرگرمی است؛ به‌ویژه برخی جوانان کنجکاو و هکرها اینترنت را به عنوان محیطی برای تفریح در نظر می‌گیرند و صرفاً برای سرگرمی به دانلود موسیقی و فیلم، نفوذ غیرمجاز به شبکه‌های دیگران، کپی‌برداری از وب‌سایت‌ها و ارسال ویروس‌ها می‌پردازند. (کوره پز و همکاران، ۱۳۹۳: ۷۷) انگیزه‌های سیاسی برای جرایم سایبری در دو سطح قابل مشاهده است: سطح بازیگران غیردولتی و سطح بازیگران دولتی. در سطح بازیگران غیردولتی، انگیزه‌های سیاسی با احساسات نزدیک ارتباط دارند، زیرا افراد می‌توانند نسبت به مسائل سیاسی بسیار هیجانی باشند. این انگیزه‌های سیاسی در سطح غیردولتی معمولاً با گرایش های راست‌گرا مرتبط است. در سطح بازیگران دولتی، سیاست و سیاست خارجی کشورها را به سمت استفاده از تخریب و جاسوسی سایبری برای حفظ مزایای سیاسی و نظامی سوق داده است. این دسته از انگیزه‌ها را می‌توان با بررسی دو زیردسته سیاسی «مقاومت» و «جنگ سایبری / جاسوسی سایبری» بهتر درک کرد. هدف این مطالعه، ارائه دیدگاه جرمشناختی به جرایم سایبری و پر کردن بخشی از خلأ موجود در مبارزه با این نوع جرایم است.

۲– تاریخ تحول جرایم سایبری

تحول تاریخی جرایم سایبری به همان اندازه که با پیشرفت فناوری‌های اطلاعاتی، به ویژه اینترنت، همگام بوده است. با جایگزینی عصر اطلاعات به جای عصر صنعتی، تغییرات ریشه‌ای در جامعه و تعاملات اقتصادی ایجاد شده است. توسعه سریع فناوری‌های اطلاعاتی، کوچک‌تر شدن ابعاد و دسترس‌پذیری ارزان‌تر آنها، باعث افزایش تعداد کاربران شده است. از اوایل دهه ۱۹۹۰، با به هم پیوستن تعداد زیادی رایانه، افراد مستعد ارتکاب جرم در این حوزه گرد هم آمده‌اند و انواع جدیدی از جرایم ظهور کرده‌اند. اهمیت حیاتی شبکه‌های مجازی برای نهادهای رسمی، خطر حملات مداوم به این سیستم‌ها را افزایش داده است. در سال‌های اخیر، حملات به سازمان‌هایی مانند ناسا و ناتو و سایر شرکت‌های بزرگ باعث ایجاد خسارت‌های عظیم در سیستم‌های آنها شده است. قبل از حملات تروریستی ۱۱ سپتامبر، برخی از رویدادها ضعف فناوری اطلاعات در ارتش آمریکا و صنعت انرژی را آشکار کرده بود. این وضعیت موجب بی اعتمادی به سیستم های نظامی شد، در حالی که پس از ۱۱ سپتامبر، هشدارهای جدی از محافل سیاسی و نظامی به همراه گفتمان های مداوم تروریسم و امنیت، خطرات آشکار تروریسم سایبری را برجسته کرد. (دشتی و افشاری، ۱۳۹۸: ۱۰۱) تروریسم سایبری شامل تهدیدها و حملات غیرقانونی به رایانه ها، شبکه ها، اطلاعات و پایگاه های داده سازمان های رسمی به منظور ایجاد ترس و اجبار بر مراجع سیاسی و اجتماعی و افراد است. فراتر از این، برای تعریف یک حمله به عنوان تروریسم سایبری، بایستی آن شامل خشونت علیه افراد یا اموال باشد. حداقل باید به «خسارت کافی برای ایجاد ترس» منجر شود. نمونه هایی از تروریسم سایبری می توانند حملات مرگبار یا منجر به خسارت فیزیکی، یا حملات منجر به زیان اقتصادی شدید باشند. حملات جدی به مراکز زیرساخت های حیاتی، بر اساس تأثیر ایجاد شده، می توانند به عنوان تروریسم سایبری تعریف شوند. بسیاری از جرایم واقعی دنیای فیزیکی برای مدت طولانی در فضای سایبری تکرار می شوند. تروریسم و افراط گرایی تفاوتی ندارند. گروه های تروریستی امروزی از مزایای اینترنت استفاده می کنند. همانطور که همه چیز دیگر، جرم، تروریسم، خشونت و حتی جنگ به فضای سایبری تبدیل شده است: افراطی گری آنلاین به اندازه افراطی گری چهره به چهره مهم می شود، گروه های خشن آنلاین ظاهر می شوند و دولت ها از گروه های هکری برای حمله به دشمنان خود استفاده می کنند. در چنین زمینه ای، تروریسم سایبری به یک مسئله امنیت ملی تبدیل شده است. (حسین خانی، ۱۴۰۰، ۶۰) با افزایش کنترل مرزها و در دنیای نیروهای نظامی و انتظامی، احتمال دارد که تروریست ها راه نفوذ به مرزهای فیزیکی را گم کرده و به مرزهای سایبری روی آورند. افراط گرایان خشونت طلب همچنان با تلاش های مداوم مبارزه با تروریسم

بین المللی روبرو هستند و میدان در دنیای فیزیکی از دست می دهند. حملات سایبری برای گروه های تروریستی جذاب هستند زیرا می توانند از هر نقطه ای در جهان و با منابع نسبتاً کمتری انجام شوند. (نظری و همکاران، ۱۴۰۰: ۱۶۲) محیط تهدید سایبری فعلی نشان داده است که گروه های هکری تحت حمایت دولت ها، تهدیدی نزدیک تر از گروه های تروریستی هستند. احتمال دارد گروه های هکری تحت حمایت دولت ها به منابع و توانایی های لازم برای نفوذ به سیستم های رایانه ای محافظت شده و ایجاد خسارت های جدی دسترسی داشته باشند. با این حال، باید توجه داشت که توسعه توانایی های حمله سایبری و آغاز حملات ویرانگر زمان بر است. کشف وبگاه های امنیتی و دستیابی به دسترسی غیرمجاز نیاز به زمان و منابع زیادی دارد. گروه های تروریستی هم اکنون در مرحله آماده سازی هستند و در حال یادگیری نحوه سازگاری و پیشرفت در این محیط در حال تغییر هستند. اگر فعالیت آنها مختل نشود، در نهایت به این قابلیت دست خواهند یافت. در دفاع ملی، یک جابجایی پارادایم ادامه دارد که فراتر از حوزه های سنتی جنگ زمینی، دریایی و هوایی، به سمت عرصه دیگری به نام فضای سایبری سوق یافته است. دولت ها پشت پرده ناشناسی فضای سایبری پنهان شده و از گروه های هکری به عنوان ارتش نیابتی برای مقابله با رقبای خود استفاده می کنند. موفقیت نسبی گروه های مرتبط با جرائم سایبری و گروه های هکری وابسته به دولت ها، گروه های تروریستی را به سرمایه گذاری بیشتر در فضای سایبری تشویق کرده است.

۳– رویکردهای جرم شناختی تبیین کننده جرائم سایبری

مطالعات جرم شناسی از اوایل قرن بیستم به طور گسترده بحث کرده اند که رفتار مجرمانه آنقدر پیچیده است که نمی توان آن را به صرف اراده فرد تقلیل داد و باید برخی عوامل فرا فردی نیز در نظر گرفته شوند. مطالعات جرم شناسی جدید و در حال ظهور، به بررسی توضیحات مختلف جرم از رویکردهای بیولوژیکی تا رویکردهای فمینیستی می پردازند. به نظر می رسد تئوری های اخیر نیز به سمت یکپارچه سازی نظریات مستقل متمایل هستند. نظریات کلاسیک توضیح دهنده جرم بر این پایه بودند که افراد موجوداتی عقلانی هستند و در نتیجه آزادی ارتکاب جرم را نیز دارند. چشم اندازهای نظری که جرم شناسی در طول زمان برای توضیح جرم توسعه داده است، مبانی مهمی را برای توضیح جرائم سایبری نیز فراهم می کند. نظریه فشار بر این باور است که عدم دسترسی قانونی افراد به چیزهایی که تلاش می کنند به آن دست یابند، فشار و تنش ایجاد می کند و این فرایند افراد را به سوی ارتکاب جرم سوق می دهد. نظریه یادگیری نیز استدلال می کند که افراد جرم را بعدا از طریق مشاهده افراد اطراف خود و رسانه ها می آموزند. وجه مشترک این دو نظریه، بررسی دلایل ارتکاب جرم توسط افراد است. در مقابل، نظریه های کنترل اجتماعی استدلال می کنند که همه افراد مرتکب جرم نمی شوند و فاعلان جرم نسبت به افرادی که مرتکب جرم نمی شوند کمتر هستند، بنابراین در مبارزه با جرم، منطقی است که افراد قانونی را بررسی کرده و عوامل جلوگیری از ارتکاب جرم توسط آنها را شناسایی کرد. (وطنی و همکاران، ۱۳۹۵: ۵)

۳–۱– نظریه کنترل اجتماعی

نظریه کنترل اجتماعی به پیوستگی افراد به ارزش ها، هنجارها و نهادهای جامعه و پدیده کنترل اجتماعی ناشی از چنین پیوستگی توجه دارند. این نظریه پدیده انحراف را در چارچوب متغیرهای اجتماعی مؤثر بر رفتار افراد مانند ساختار خانواده، عوامل محیطی و باورها ارزیابی می کند. این نظریه اصلی ترین علت انحراف را فقدان کنترل اجتماعی می داند. فرض اصلی آن این است که انسان ها به سوی انحراف گرایش دارند و اگر کنترل نشوند، انحراف خواهند داشت. این رفتارها محصول کمبود پیوند اجتماعی هستند. در این زمینه، نظریه قابل توجه نظریه هیرشی است. او معتقد است که عامل جلوگیری از فعالیت های مجرمانه نوجوانان و جوانان پیوندهای اجتماعی است. (شفازاده، ۱۳۹۸: ۱۳۱)

این نظریه در اصل توسط جرم شناسان مایکل گاتفردسون و تراویس هیرشی توسعه داده شده است. آنها مدعی بودند که نظریه کنترل خود به تنهایی می تواند همه انواع جرم را توضیح دهد. افراد با کنترل خود پایین، با ریسک پذیری و ترجیح دادن امور ساده و راحت مشخص می شوند. این ویژگی ها توانایی فرد برای محاسبه صحیح پیامدهای انحراف را مختل می کند. بر اساس این نظریه، جرم به عنوان راهی برای به دست آوردن لذت فوری در نظر گرفته می شود و توانایی به تأخیر انداختن چنین تمایلات کوتاه مدت با کنترل خود مرتبط است. فرض می شود که افراد مستعد ارتکاب جرم از کنترل خود کافی برخوردار نیستند. علاوه بر این، افراد با کنترل خود پایین بدون فکر زیاد و صرفاً بر اساس آنچه در آن لحظه احساس می کنند، رفتار تکانشی دارند. این امر آنها را افرادی ریسک پذیر می کند زیرا به عواقب اقداماتشان فکر نمی کنند. در نهایت، افراد با کنترل خود پایین خودمحور هستند و از همدلی با دیگران بی بهره هستند. به گفته گاتفردسون و هیرشی، کنترل خود پایین از اجتماعی شدن اولیه ناکارآمد والدین ناشی می شود. بنابراین، والدین سهل انگار و بی توجه ممکن است نتوانند فرزندان خود را اجتماعی کنند. والدگری موثر که شامل محبت به فرزند، نظارت، تشخیص رفتار نامناسب و مجازات رفتار نامناسب است، برای تزریق (بالا) کنترل خود به کودکان کافی است. با این حال، آنچه مهمتر است، دوره حساس برای توسعه کنترل خود، ۸-۱۰ سال اول زندگی است. به گفته گاتفردسون و هیرشی، پس از کودکی، سطوح کنترل خود بین فردی ثابت می شود و کسانی که نمی توانند کنترل خود را توسعه دهند «به زندگی شرافتمندانه محکوم می شوند». در نتیجه، کودکان با سطوح پایین کنترل خود به طور بالقوه به جنایت گرایش بیشتری دارند و این تمایل به جنایت در ادامه زندگی آنها ادامه می یابد. ویژگی های کنترل خود پایین می تواند به برخی از اشکال ساده جرم سایبری از جمله هک نرم افزار اعمال شود. بروس و همکاران در مطالعه خود اشاره کردند که سطوح پایین کنترل خود مستقیماً با عمل هک نرم افزار مرتبط است. (ردایی، ۱۳۹۸: ۱۱۴۴) به عنوان مثال، احتمال دارد فردی به دلیل رفتار تکانشی و عدم توانایی در انتظار برای خرید نسخه برنامه، به هک نرم افزار بپردازد. این افراد احتمالاً از هرگونه درک نسبت به صاحبان حق تکثیر و نادیده گرفتن هرگونه مسئولیت بی بهره هستند. همچنین، احتمال دارد که این افراد تحت تأثیر هیجان و سهولت مشارکت در هک نرم افزار قرار گیرند. مطالعه همچنین نشان داد که کنترل خود پایین اثری بر هک نرم افزار دارد و عناصر نظریه یادگیری اجتماعی (یعنی ارتباط با همکاران منحرف و نگرش های مثبت نسبت به هک نرم افزار) این اثر را تعدیل می کند. بنابراین، از ویژگی های کنترل خود پایین، افرادی که سطوح پایین کنترل خود دارند به دلیل تمایل به ارضای فوری، محتمل است که درگیر رفتارهای انحرافی آنلاین و آفلاین شوند. نظریه کنترل اجتماعی توضیحی درباره اینکه چرا و چگونه مردم از قوانین و هنجارها پیروی می کنند ارائه می دهد. رفتار در انطباق با انتظارات جامعه است. بر اساس نظریه کنترل اجتماعی، محدودیت های درونی در دوران کودکی توسعه می یابند و جرم به واسطه محدودیت های ناکافی ایجاد می شود. به عبارت دیگر، اراده آزاد به مجرمان انتخاب رفتارهای انحرافی و در نتیجه مسئولیت داده است. نظریه کنترل اجتماعی ادعای حمایت کننده گستره آزادی که ناشی از گمنامی آنلاین است را تأیید می کند. به این ترتیب، نظریه کنترل اجتماعی افراد را به اجتناب از جرم و رفتارهای انحرافی مجبور نمی کند.

۳-۲- نظریه فشار

نظریه فشار که در مطالعات جرم شناسی توسعه یافته است، جرم را بازتابی از آنومی (استرس) یا فشار موجود در جامعه و محیط نزدیک فرد می داند. در این زمینه، اولاً دلایلی که فرد را به فشار و در نتیجه به سوی جرم سوق می دهند، نرسیدن به اهداف مورد ارزش اجتماعی مانند درآمد خوب، شغل موفق، والدین موفق و داشتن پیشرفت شغلی است. ثانیاً، درنتیجه استرس ناشی از از دست دادن اعضای خانواده که محرک های مثبت زندگی فرد هستند، فرد می تواند به سمت الکل، مواد مخدر و خشونت کشیده شود. نظریه فشار توسط مرتن توسعه یافته است. طبق نظریه کلاسیک فشار مرتن، آنومی به عنوان شکاف بین آنچه ساختار موجود از افراد انتظار دارد و آنچه افراد در قبال ساختار موجود می

خواهند تعریف شده است. به نظر مرتن، ظهور آنومی باعث می شود افراد راه های دیگری برای برآورده کردن نیازهای جامعه پیدا کنند، اما این امر با افزایش انحراف همراه است. مرتن می گوید که در جوامع آمریکایی و دیگر جوامع سرمایه داری، اهداف کسب ثروت و دارایی بیش از حد تأکید شده است، اما تدابیر اخلاقی و قانونی برای رسیدن افراد به این اهداف کمتر مورد تأکید قرار گرفته است. با گذشت زمان، این تفکر که هر کاری برای کسب ثروت مجاز است ظهور می کند و انحراف از هنجارهای اجتماعی را ایجاد می کند. به همین دلیل به نظر مرتن، جرم پدیده ای نیست که به تغییرات اجتماعی ناگهانی مربوط باشد، بلکه بیشتر پدیده ای ساختاری اجتماعی است. در این چارچوب، مرتن ریشه جرم را در ساختارهای اجتماعی جستجو کرده است. (سهلائی، ۱۳۹۷: ۶۴) کوهن که زیرفرهنگ فشار را بررسی کرده، آنها را بی فایده و منفی توصیف کرده است. کوهن به عنوان مثال، کسب اعتبار در چارچوب باندها از طریق دزدی، لذت بردن از ناراحتی دیگران و مخالفت با ارزش های طبقه متوسط را ذکر کرده است. نظریه های زیرفرهنگ فشار استدلال می کنند که برخی گروه ها یا زیرفرهنگ ها به جرم مشروعیت می بخشند. نظریه عمومی فشار آگنیو بیان می کند که فشار به ایجاد احساسات منفی منجر می شود و این می تواند به طیفی از پیامدها از جمله جرم منتهی شود. موارد خاص فشار مورد بحث در این نظریه عبارتند از: عدم دستیابی به اهداف با ارزش مثبت (مانند پول)، حذف محرک های با ارزش مثبت (مانند از دست دادن یک دارایی با ارزش) و معرفی محرک های با ارزش منفی. اولین فشار به شکاف بین انتظارات فرد و آنچه واقعاً به دست می آورد نگاه می کند که باعث سرخوردگی و احساس خیانت می شود. دومین نوع فشار زمانی ایجاد می شود که یک محرک با ارزش مثبت حذف شود و نتیجه آن جرم است. این رفتار مجرمانه ممکن است به عنوان تلاشی برای تخفیف یا تغییر محرک ظاهر شود. آخرین نوع فشار زمانی ایجاد می شود که با محرک های منفی مواجه شویم. این می تواند به جرم به عنوان ابزاری برای اجتناب یا پایان دادن به محرک های منفی منجر شود. آگنیو معتقد است که فشار مستقیماً به جرم منجر نمی شود، بلکه احساسات منفی مانند خشم و ناامیدی را تشویق می کند. این مستقیماً مرتبط با فرضیه ناامیدی تهاجم روانشناسان دانشگاه ییل است که معتقدند خشم قبل از سرخوردگی آمده و ناامیدی می تواند هم در رفتار تهاجمی و هم در رفتار غیرتهاجمی ظاهر شود. در مقابل، این احساسات منفی نیاز به واکنش های مقابله ای برای تسکین فشار درونی دارند. (سهلائی، ۱۳۹۷: ۸۱) رفتار غیرقانونی و خشونت به عنوان راه مقابله ممکن است به خصوص برای نوجوانان مناسب باشد، زیرا آنها نمی توانند از محیط های پر استرس و منابع محدود فرار کنند. در تحقیق خود، آنها استدلال می کنند که قربانیان سایبر زورگویی که به طور عمد از طریق الکترونیکی به طور مستقیم یا غیرمستقیم اذیت یا ارعاب می کنند، با یک مشکل جدی و رو به رشد روبرو هستند. در محیط دیجیتال، برخی عناصر منحصر به فرد مانند ناشناس بودن، اتصال پیوسته و ماندگاری وجود دارد. این فناوری جدید به قربانیان اجازه می دهد که در هر زمان مورد حمله قرار گیرند و ناشناس بودن سایبر زورگویان را شناسایی آنها را مشکل می کند. آگنیو استدلال می کند که فشار باعث می شود افراد خشمگین، ناامید و افسرده شوند و در نهایت فشار به قربانی برای اقدام اصلاحی وارد می کند. به عنوان پاسخی به این فشار، قربانیان ممکن است بخواهند با انجام یک اقدام اصلاحی به عنوان ابزاری برای تسکین احساسات بد واکنش نشان دهند. در نتیجه، برای برخی قربانیان، سایبر زورگویی ممکن است یکی از اقدامات اصلاحی باشد که نوجوانان می توانند برای کاهش احساسات بد خود انجام دهند و در مجموع، نظریه فشار عمومی و فرضیه ناامیدی-تهاجم درک روشنی از اینکه افراد، به ویژه نوجوانان، آیا دست به زورگویی علیه دیگران بزنند یا به رفتارهای انحرافی برای تسکین فشار منفی واکنش نشان دهند، ارائه می دهد. (ابتکاری و احمدی، ۱۳۹۸: ۱۱)

۳–۳– نظریه یادگیری اجتماعی

نظریه یادگیری اجتماعی جرم را در ارتباط با یادگیری هنجارها، ارزش ها و رفتارهای موجود در جامعه همراه با رویدادهای جرم شناختی توضیح می دهد. این نظریه، هم عقلانی سازی ارزش جرم در رفتارهای غیرقانونی و هم یادگیری تکنیک های جرم را در بر می گیرد. نظریه یادگیری اجتماعی همچنین شامل نظریه هایی مانند «مؤلفه های متمایز، تقویت متفاوت و خنثی سازی» است. (صابری، ۱۴۰۱: ۲۴) سادرلند جرم را با مفهوم تعامل اجتماعی توصیف می کند. به نظر سادرلند، تجمع مجرمان به تنهایی دلیل کافی برای ظهور رفتار مجرمانه نیست. زیرا فراوانی، مدت، اولویت و شدت ارتباط با گروه های مجرمانه مهم ترین دلایل شکل گیری رفتار مجرمانه هستند. طبق این نظریه، جرم ناشی از نقص های ذاتی مانند عقب ماندگی هوشی، اختلالات شخصیتی یا مشکلات اقتصادی مانند فقر نیست. جرم به عنوان فعالیت یادگیری در چارچوب تعامل اجتماعی ظهور می کند. این رویکرد استدلال می کند که رفتار مجرمانه آموخته می شود. افرادی که در جامعه، به ویژه در محیط فرهنگی خود تعامل دارند، رفتار مجرمانه را سریع تر می آموزند. نظریه یادگیری اجتماعی اکرز یک نظریه جرم شناختی کلی است که برای تبیین انواع مختلف رفتارهای مجرمانه استفاده شده است. این مطالعه چهار پیشنهاد اصلی را در خود جای داده است که شامل اشتراک ارتباطات، تعاریف متفاوت، تقویت متفاوت و تقلید است. نظریه یادگیری اجتماعی بر این ایده استوار است که افراد با برقراری ارتباط یا در معرض قرار گرفتن با افراد درگیر در جرم (یعنی ارتباط با همکاران منحرف) انگیزه و مهارت های لازم برای ارتکاب جرم را توسعه می دهند. اکرز استدلال کرد که در معرض قرار گرفتن رفتار انحرافی، تعاریفی را برای افراد فراهم می کند که رفتار را تأیید یا بی اثر می کند. (حسین خانی، ۱۴۰۰: ۷۰) این رفتار مجرمانه ابتدا از طریق فرآیند تقلید آموخته می شود، جایی که افراد رفتارها و اقدامات را از طریق مشاهده و یادگیری دیگران یاد می گیرند. بنابراین، هنگامی که فردی مرتکب جرم می شود، او اعمالی را تقلید می کند که دیگران انجام داده اند. در مورد جرائم سایبری، تحقیقات نشان داده است که نظریه یادگیری اجتماعی می تواند توسعه و استمرار هک نرم افزار را توضیح دهد. بروس و همکارن در مطالعه خود در مورد هک نرم افزار، دریافتند که افرادی که با همکاران منحرف ارتباط برقرار می کنند، رفتارهای انحرافی را یاد گرفته و سپس آنها را می پذیرند. هک نرم افزار نیاز به مهارت و دانش خاصی برای دسترسی دارد و این مهارت ها اصلاً باید از همتایان منحرف یاد گرفته شوند. همچنین، افراد منحرف رفتارهای مجرمانه خود را موجه می کنند و به توسعه شبکه ای کمک می کنند که این موجه سازی ها و رفتارها را به دیگران منتقل می کند. مطالعه همچنین پیشنهاد کرد که زمانی که افراد پاداش مثبتی را برای مشارکت دیگران مشاهده می کنند، احتمال بیشتری دارد که در هک نرم افزار شرکت کنند. هک نرم افزار نه تنها توسط نظریه کنترل اجتماعی توضیح داده می شود، بلکه عناصر این نظریه به سایر جرائم سایبری نیز قابل اسناد است. به عنوان مثال، در هر جرمی، مهارت ها باید آموخته شوند و رفتار باید از طریق ارتباطات و مشاهده دیگران تقویت شود. بنابراین، ایده اصلی پشت نظریه یادگیری اجتماعی این است که ما کسانی هستیم که توسط محیط مان تعیین می شویم و این توضیح می تواند برای تبیین جرائم سایبری استفاده شود. افراد منحرف رفتارهای مجرمانه خود را موجه می کنند و به توسعه شبکه ای کمک می کنند که این موجه سازی ها و رفتارها را به دیگران منتقل می کند.

۴– نتیجه گیری

کاربست نظریه کنترل اجتماعی، نظریه فشار و نظریه یادگیری اجتماعی در جلوگیری از جرایم سایبری می‌تواند نتایج مثبت و مؤثری در پی داشته باشد. نظریه کنترل اجتماعی بر اهمیت پیوندهای اجتماعی قوی در جلوگیری از جرم تأکید دارد. در فضای مجازی نیز تقویت پیوندها با خانواده، دوستان و گروه‌های مثبت می‌تواند از وقوع جرایم سایبری پیشگیری کند. برای مثال، افزایش نظارت والدین بر فعالیت‌های آنلاین فرزندان و مشارکت آن‌ها در گروه‌های اجتماعی سالم می‌تواند مؤثر باشد. ترویج ارزش‌های اخلاقی و قانونی در فضای مجازی و ایجاد باورهای

مثبت در مورد پیامدهای منفی جرایم سایبری می‌تواند به کاهش وقوع این جرایم کمک کند. نظریه فشار بیان می‌کند که فشار اجتماعی برای رسیدن به اهداف (مانند ثروت یا موفقیت) می‌تواند افراد را به سمت جرم سوق دهد. در فضای مجازی نیز تبلیغات فریبنده و انتظارات غیرواقعی می‌تواند این فشار را افزایش دهد. برای جلوگیری از این امر، باید آگاهی عمومی را در مورد این فشارها افزایش داد و راه‌های جایگزین و سالم برای رسیدن به اهداف را ترویج کرد. ارائه حمایت‌های اجتماعی به افرادی که در معرض فشار قرار دارند، می‌تواند از وقوع جرایم سایبری جلوگیری کند. این حمایت‌ها می‌تواند شامل مشاوره‌های روانشناسی، کمک‌های مالی و فرصت‌های آموزشی باشد. نظریه یادگیری اجتماعی بیان می‌کند که افراد از طریق مشاهده و تقلید، رفتارها را یاد می‌گیرند. در فضای مجازی نیز افراد ممکن است رفتارهای مجرمانه را از دیگران بیاموزند. برای مقابله با این امر، باید مهارت‌های مقابله با جرایم سایبری را به افراد آموزش داد و الگوهای مثبت را در فضای مجازی ترویج کرد. افزایش آگاهی عمومی در مورد جرایم سایبری و پیامدهای آن می‌تواند از وقوع این جرایم پیشگیری کند. این آگاهی‌بخشی می‌تواند از طریق رسانه‌ها، آموزش‌های رسمی و غیررسمی و کمپین‌های تبلیغاتی انجام شود. در کل، کاربست این سه نظریه به صورت ترکیبی می‌تواند نتایج مؤثری در جلوگیری از جرایم سایبری داشته باشد. با تقویت پیوندهای اجتماعی، کاهش فشار، آموزش مهارت‌های مقابله و افزایش آگاهی عمومی می‌توان به طور مؤثری از وقوع این جرایم پیشگیری کرد و فضای مجازی امن‌تری برای همه ایجاد کرد.

منابع

۱. ابتکاری، محمدحسین؛ احمدی، سیروس (۱۳۹۸)، ***«تحلیل جامعه شناختی پتانسیل رفتارهای نابهنجار با تأکید بر نظریه فشار عمومی اگنیو»***، انتظام اجتماعی، دوره ۱۱، شماره ۲

۲. امیریان، امین؛ عبدالصمدی، راضیه؛ حیدری فارسانی، فاطمه (۱۳۹۹)، ***«علت شناسی ارتکاب جرایم سایبری و سازوکارهای پیشگیری از آن»***، نشریه علوم خبری، دوره ۹، شماره ۳۵

۳. انصاری، جلال؛ عطازاده، سعید؛ قیوم زاده، محمود (۱۳۹۸)، ***«سیاست جنایی ایران و آمریکا در قبال جرائم کلاهبرداری و سرقت سایبری (مقاله مروری)»***، پژوهش های اطلاعاتی و جنایی، دوره ۱۴، شماره ۳

۴. حسین خانی، الهام (۱۴۰۰)، ***«جرم شناسی فضای مجازی با تاکید بر نظریه های جرم شناسانه بزهکار محور»***، فصلنامه تحقیقات کاربردی فقه و حقوق، دوره ۱، شماره ۲

۵. دشتی، بیتا؛ افشاری، مریم (۱۳۹۸)، ***«مطالعه تطبیقی جرایم سایبری در ایران و حقوق بین الملل»***، پژوهشنامه حقوق تطبیقی، دوره ۳، شماره ۱

۶. ردایی، مصطفی (۱۳۹۸)، ***«بررسی نظریه های جرم شناختی در تکوین جرم فضای سایبر»***، ماهنامه جامعه شناسی سیاسی ایران، دوره ۲، شماره ۴

۷. سهلانی، حسین (۱۳۹۷)، ***«آشنایی با تهدیدات فضای سایبر»***، تهران: نشر علوم انتظامی امین

۸. شعاعی، مرتضی؛ خوانین زاده، حسین (۱۴۰۱)، ***«تحلیل روند راهبردهای پیشگیرانه از جرایم سایبری»***، پژوهش های جرم شناختی پلیس، دوره ۳، شماره ۶

۹. شفازاده، احمد (۱۳۹۸)، ***«بررسی نظریه هیرشی در کنترل اجتماعی از دیدگاه قرآن»***، راهبرد اجتماعی فرهنگی، دوره ۸، شماره ۳۳

۱۰. صابری، راضیه (۱۴۰۱)، ***«علت یابی افزایش برخی از جرایم و پیشگیری از آن ها در پرتو نظریه یادگیری اجتماعی»***، فصلنامه قانون یار، دوره ۶، شماره ۲۳

۱۱. صبح خیز، رضا؛ پورقهرمانی، بابک؛ صفاری، علی (۱۴۰۰)، ***«الگوی مفهومی سیاست جنایی جرایم سایبری در ایران»***، مطالعات راهبردی ناجا، دوره ۶، شماره ۲۰

۱۲. کرد علیوند، روح‌الدین؛ میرزایی، محمد (۱۳۹۷)، ***«گونه‌شناسی جرایم سایبری با نگاهی به قانون جرایم رایانه‌ای و آمار پلیس فتا»***، مجله حقوقی دادگستری، دوره ۸۲، شماره ۱۰۲

۱۳. کوره پز، حسین محمد؛ میرخلیلی، سید محمود؛ توجهی، عبدالعلی؛ بهره مند، حمید (۱۳۹۳)، ***«نیمرخ جرم‌شناختی بزه‌کاران سایبری»***، فصلنامه پژوهش حقوق کیفری، دوره ۳، شماره ۹

۱۴. نظری، سید غنی؛ جعفر زاده، سیامک؛ نیک خواه سرنقی، رضا (۱۴۰۰)، ***«نقش سیاست جنایی مشارکتی در پیشگیری از جرایم سایبری در ایران»***، پژوهش های سیاسی جهان اسلام، دوره ۱۱، شماره ۴

۱۵. وطنی، امیر؛ اسدی، حمید (۱۳۹۵)، ***«سیاست جنایی جمهوری اسلامی ایران در جرایم سایبری با تاکید بر ویژگی های خاص این جرم»***، پژوهش نامه حقوق اسلام، دوره ۱۷، شماره ۱