



ارزیابی اثرات تبلیغات و رفتارهای مجرمانه آنلاین بر امنیت داخلی: رویکرد کیفری و جرم‌شناسی

محمدزمان رضا زاده پاشا^۱، محدثه صادقیان لمراسکی^۲

چکیده

رشد فزاینده فناوری‌های ارتباطی و توسعه شبکه‌های اجتماعی، علاوه بر فرصت‌های اطلاع‌رسانی و تجاری، بستر جدیدی برای ارتکاب جرایم و تهدید علیه امنیت داخلی فراهم کرده است. مسئله اصلی پژوهش حاضر، ارزیابی اثرات تبلیغات انحرافی و رفتارهای مجرمانه آنلاین بر امنیت داخلی از منظر کیفری و جرم‌شناختی است. پرسش محوری این است که «تبلیغات سایبری و رفتارهای مجرمانه چه تأثیری بر امنیت داخلی دارند و سیاست کیفری تا چه اندازه می‌تواند در مهار این تهدیدات مؤثر واقع شود؟» فرضیه پژوهش بیان می‌دارد که تبلیغات تحریک‌آمیز و رفتارهای مجرمانه در فضای مجازی، به‌طور مستقیم با افزایش ناامنی، تهدید اعتماد عمومی و تضعیف انسجام اجتماعی ارتباط دارد و اتخاذ پاسخ‌های کیفری کارآمد و مبتنی بر یافته‌های جرم‌شناسی می‌تواند سطح تهدیدات را کاهش دهد. روش تحقیق به‌صورت توصیفی تحلیلی و با اتکا بر منابع کتابخانه‌ای، اسنادی و تحلیل محتوای متون تخصصی انجام شده است. یافته‌ها نشان می‌دهد که تبلیغات مخرب و بهره‌برداری ابزاری از فضای مجازی، زمینه ارتکاب جرایمی همچون کلاهبرداری رایانه‌ای، نفوذ غیرمجاز، فیشینگ و ترویج افراط‌گرایی را تقویت می‌کند. همچنین، خلأهای حقوقی و ضعف هماهنگی نهادی در نظام کیفری، موجب افزایش آسیب‌پذیری امنیت داخلی در برابر تهدیدات نوین می‌گردد. نتیجه‌گیری پژوهش حاکی از آن است که بهره‌گیری هم‌زمان از رهیافت‌های جرم‌شناختی (پیشگیری اجتماعی و وضعی) و اصلاح سیاست کیفری (با تمرکز بر پاسخ‌های بازدارنده و بازپرورانه)، می‌تواند نقش مؤثری در ارتقای تاب‌آوری امنیت داخلی در مواجهه با جرایم و تبلیغات سایبری ایفا کند.

واژگان کلیدی: تبلیغات سایبری، جرایم آنلاین، امنیت داخلی، سیاست کیفری، پیشگیری اجتماعی و وضعی، تاب‌آوری امنیتی.

۱. گروه حقوق، واحد گرگان، دانشگاه آزاد اسلامی، گرگان، ایران. M.rezazadepasha@iau.ir

۲. گروه حقوق، واحد گرگان، دانشگاه آزاد اسلامی، گرگان، ایران. (نویسنده مسئول)

E-mail: Mo.sadeghain1360@iau.ac.ir

Assessing the Effects of Online Advertising and Criminal Behavior on Internal Security: A Criminal and Criminological Approach

Mohammad Zaman Rezazade Pasha¹, Mohadeseh Sadeghian Lemr Eski²

Abstract

The exponential growth of communication technologies and social networks has, alongside opportunities for information dissemination and commerce, generated new grounds for criminal activities and threats against internal security. The central issue of this study is to assess the impact of deviant online advertising and cybercriminal behaviors on internal security through criminal law and criminological perspectives. The core research question asks: “How do cyber advertising and criminal behaviors affect internal security, and to what extent can criminal justice policies effectively mitigate these threats?” The hypothesis posits that provocative online advertising and cyber-offense are directly associated with increased insecurity, erosion of public trust, and weakening of social cohesion; while effective penal responses, informed by criminological findings, can substantially reduce such risks. Employing a descriptive-analytical methodology and relying on library sources, documentary evidence, and specialized content analysis, the findings demonstrate that manipulative advertising and instrumental exploitation of cyberspace facilitate crimes such as computer fraud, unauthorized access, phishing, and extremist propaganda. Moreover, legal loopholes and institutional incoherence within the criminal justice system amplify domestic vulnerability to emerging threats. The study concludes that an integrated approach—combining criminological strategies (social and situational prevention) with a reformed criminal policy emphasizing deterrent and rehabilitative responses—can significantly enhance domestic resilience against cybercrime and harmful online advertising.

Keywords: Cyber Advertising, Online Crimes, Internal Security, Criminal Policy, Social and Situational Prevention, Security Resilience..

1. Law Department, Gorgan Branch, Islamic Azad University, Gorgan, Iran
M.rezazadepasha@iau.ir

2. Law Department, Gorgan Branch, Islamic Azad University, Gorgan, Iran
(Writer-in-charge) Mo.sadeghain1360@iau.ac.ir



مقدمه

در دهه‌های اخیر، با گسترش فناوری اطلاعات و ارتباطات، فضای مجازی به بستری گسترده برای تعاملات اجتماعی، اقتصادی، سیاسی و فرهنگی بدل شده است. این فضا به‌طور همزمان فرصتی بی‌نظیر برای رشد و توسعه و تهدیدی جدی برای امنیت داخلی کشورها محسوب می‌شود (کاستلز، ۱۴۰۴: ۷). یکی از مهم‌ترین نمودهای این تهدید، ظهور و گسترش تبلیغات و رفتارهای مجرمانه آنلاین است که در قالب فعالیت‌هایی همچون تبلیغ مواد مخدر، تشویق به خشونت، کلاهبرداری اینترنتی، پول‌شویی، نشر اکاذیب و همچنین ترویج اندیشه‌های افراطی و تروریستی خود را نشان می‌دهد. برخلاف جرایم سنتی که محدود به مرزهای جغرافیایی بودند، جرایم آنلاین ماهیتی فراملی دارند و مرزهای فیزیکی را در می‌نوردند (کاپورو، ۱۴۰۰: ۲۶). این ویژگی، نه تنها تعقیب و مقابله کیفری را دشوار کرده بلکه بر امنیت داخلی کشورها نیز تأثیرات عمیق گذاشته است. تبلیغات سازمان‌یافته در فضای مجازی می‌تواند افکار عمومی را تحت تأثیر قرار داده، ناهنجاری‌های اجتماعی را گسترش دهد و بستر ارتکاب جرایم دیگر را فراهم آورد (سما ادماز و همکاران، ۲۰۲۴: ۲۴۹).

از طرفی، در عصر کنونی، توسعه چشمگیر ارتباطات بر اساس فناوری‌های نوین و ابرمدرن همچون هوش مصنوعی، دامنه تهدیدات امنیتی این موضوع بیش از پیش افزایش یافته است به نحوی که فعالان حوزه تبلیغات در فضای مجازی و مراجعه کنندگان این حوزه در گام نخست به موضوع امنیت و دامنه نفوذ اطلاعات توجه بسیار نشان می‌دهند، زیرا گذشته از موضوع افشای اطلاعات، سرقت داده‌ها و دارایی افراد و سازمان‌ها، امروزه دامنه تهدیدات به مراتب فراتر رفته و در موضوعاتی همچون سایبر تروریسم با هدف حذف و نابودی افراد توجّهات حقوقی، سیاسی و امنیتی زیادی را ایجاد نموده است (وی، ۲۰۲۴: ۳۱۷).

اهمیت پژوهش حاضر را می‌توان از چند منظر بررسی کرد. نخست از بعد امنیتی بایستی اذعان داشت که اساساً تبلیغات مجرمانه آنلاین، امنیت داخلی را به‌ویژه در حوزه‌های اقتصادی، فرهنگی و اجتماعی تهدید می‌کند. انتشار گسترده اطلاعات نادرست یا محتوای مجرمانه می‌تواند اعتماد عمومی را تضعیف کرده و انسجام اجتماعی را دچار اختلال کند. از طرفی، در بعد حقوقی نیز قوانین بسیاری از کشورها هنوز با تحولات سریع فضای مجازی همگام نشده‌اند. این عدم تناسب موجب

1. Sema Admass

2. Wei





خألهای حقوقی در تعقیب و مجازات مرتکبان می‌شود. از بعد جرم‌شناسی نیز بایستی خاطرنشان کرد که شناخت علل و انگیزه‌های روی‌آوری افراد و گروه‌ها به تبلیغات مجرمانه آنلاین، پیش‌نیاز تدوین سیاست‌های پیشگیرانه مؤثر است. نهایتاً آنکه در بعد سیاست‌گذاری ذکر این موضوع از اهمیت بالایی برخوردار است که برای کشورهایی مانند ایران که به دلیل موقعیت ژئوپلیتیک و اجتماعی حساسیت‌های امنیتی خاصی دارند، مطالعه تأثیرات این پدیده و یافتن راهکارهای مقابله با آن از اهمیتی دوچندان برخوردار است. از طرفی، چند عامل ضرورت پرداختن به این موضوع را توجیه می‌کند. نخست؛ رشد روزافزون جرایم سایبری. طبق آمارهای جهانی، نرخ ارتکاب جرایم در فضای مجازی هر سال افزایش می‌یابد و حوزه‌های جدیدی از بزهکاری ظهور پیدا می‌کند. همچنین از حیث نقش تبلیغات در گسترش جرایم نیز این نکته مهم است که تبلیغات آنلاین نه تنها به معرفی محصولات یا خدمات غیرقانونی می‌پردازد، بلکه بزهکاران را قادر می‌سازد شبکه‌های خود را گسترش دهند و مخاطبان بیشتری را جذب کنند. از حیث پیچیدگی‌های حقوقی و فنی باید اذعان داشت که فضای مجازی ماهیتی ناشناخته و متغیر دارد که نظام‌های کیفری سنتی برای مواجهه با آن کافی نیستند. نهایتاً آنکه از حیث تأثیر مستقیم بر امنیت داخلی نیز این موضوع ضرورت دارد که جرایم سازمان‌یافته آنلاین می‌توانند با ناامن‌سازی فضای عمومی، تضعیف اقتصاد ملی، کاهش اعتماد به نهادهای حکومتی و ایجاد آشوب‌های اجتماعی، تهدیدی بنیادین برای امنیت داخلی باشند.

با این مقدمات، هدف اصلی پژوهش حاضر، تحلیل اثرات تبلیغات و رفتارهای مجرمانه آنلاین بر امنیت داخلی و تبیین ابعاد مختلف تأثیر این جرایم بر ساختارهای سیاسی، اقتصادی و اجتماعی کشور است. بر اساس هدف اصلی پژوهش، پرسش اساسی نیز عبارت است از: «تبلیغات و رفتارهای مجرمانه آنلاین چه تأثیری بر امنیت داخلی کشورها دارند و نظام کیفری و جرم‌شناسی چه رویکردی می‌تواند برای پیشگیری و مقابله با آنها اتخاذ کند؟»

مبانی نظری و پیشینه‌شناسی تحقیق

پیشینه‌شناسی تحقیق

نویسندگان با جستجو در میان پایگاه‌های علمی مطرح داخلی همچون نورمگز، مگیران و ایرانداک با طیف گسترده‌ای از پژوهش‌های صورت گرفته با محوریت رفتارهای کاربران در فضای مجازی با رویکردهای اقتصادی - تجاری، امنیتی، فرهنگی و حتی آموزشی مواجه شدند اما نوآوری پژوهش



حاضر در دو موضوع اصلی است. نخست آنکه تا کنون پژوهش مستقلی با محوریت ارزیابی اثرات تبلیغات و رفتارهای مجرمانه آنلاین بر امنیت داخلی صورت نپذیرفته است. نکته مهمتر آنکه تا کنون پژوهشی به بحث و بررسی جامع این موضوع از منظر رویکرد کیفری و جرم‌شناسی نپراخته و نیز به ارزیابی رویکردهای کشورهای دیگر نیز اقدام نکرده است. با اینحال برخی از پژوهش‌های مرتبط و صورت پذیرفته با هدف و عنوان پژوهش حاضر به اجمال در ذیل بررسی خواهند شد.

- سپهری و همکاران (۱۴۰۳) در پژوهشی با هدف واکاوی سیاست کیفری مقابله با تروریسم محیط زیستی با تاکید بر تمهیدات بازدارنده با استفاده از روش توصیفی تحلیلی به این نتیجه دست یافتند که در یک سیاست کیفری کارآمد علاوه بر جرم‌انگاری تروریسم محیط زیستی همراه با مفهوم و عناصر اختصاصی مشخص، انتظار می‌رود که اقداماتی تخصصی در شناسایی و جرم‌انگاری رفتارهایی صورت پذیرد، که صرف نظر از سطح قباح اجتماعی و میزان خسارات ناشی آنها برای جامعه، نسبت به تروریسم محیط زیستی جنبه مقدماتی دارند و جرم‌انگاری اینگونه رفتارها، در قالب جرائم مانع در پیشگیری از این پدیده جنایی امری ضروری به نظر می‌رسد.

- زارعی و نیکخواه (۱۴۰۳) در پژوهشی با هدف بررسی و ارائه الگوی ضدبازاریابی جهت پیشگیری از رفتارهای مجرمانه در فضای کسب و کارهای آنلاین و دیجیتالی با استفاده از روش مطالعات کیفی، کاربردی و اکتشافی نشان دادند مدل ضدبازاریابی برای جلوگیری از رفتارهای مجرمانه در فضای کسب و کار آنلاین و دیجیتالی، پیامدهای مهم متفاوت و مثبتی ارائه کرد که با محتوای مصاحبه‌ها مشخص شدند. این پیامدها شامل منع رفتارهای مجرمانه، تقویت بازاریابی دیجیتال، ترویج آنلاین معنویت اخلاقی، تقویت قانون‌مداری کسب آنلاین، تقویت فرهنگ محیط آنلاین و تقویت جامعه دیجیتالی است.

- بختیاری و همکاران (۱۴۰۳) در پژوهشی با هدف بررسی طرح راهبردی بازنمایی پلیس از جرم در فضای مجازی با رویکرد پیشگیری اجتماعی با استفاده از روش توصیفی تحلیلی بر اهمیت مشارکت اجتماعی، آموزش‌های عمومی و استفاده از فناوری‌های نوین در جلوگیری از جرایم فضای مجازی تاکید نمودند. در نهایت، نویسندگان بر اهمیت ایجاد هم‌افزایی میان نهادهای دولتی، خصوصی و جامعه مدنی در جهت کاهش و پیشگیری از جرایم آنلاین تاکید کردند.

- مهرابی و میرمجیدی (۱۴۰۳) در پژوهشی با هدف پیش‌بینی پذیری بروز رفتارهای پرخطر



و مجرمانه بزه‌کاران کانون اصلاح و تربیت شهر تهران؛ با تأکید بر نقش رسانه‌های اجتماعی با استفاده از روش پیمایشی مقطعی به این نتیجه دست یافتند که رابطه مثبت بین «سهولت استفاده» از رسانه‌های اجتماعی و بروز رفتارهای پرخطر و مجرمانه نشان می‌دهد دسترسی ساده‌تر به رسانه‌های اجتماعی، امکان بروز این رفتارها در بین نوجوانان و جوانان را تقویت می‌کند. بین استفاده از رسانه‌های اجتماعی با هدف «ایجاد تعامل اجتماعی» و «سرگرمی» نیز با انجام رفتارهای پرخطر و مجرمانه ارتباط معنادار آماری مشاهده شد، اگرچه بین «میزان استفاده» از رسانه‌های اجتماعی با انجام رفتارهای پرخطر و مجرمانه رابطه معناداری مشاهده نشد. همچنین همبستگی مثبت متوسط اما معناداری بین انجام رفتارهای پرخطر و مجرمانه با «هنجارهای اجتماعی» مشاهده شد.

- پاسبان (۱۴۰۲) در پژوهشی با هدف بررسی حاکمیت حقوقی دولت‌ها بر فضای مجازی و تأثیر آن بر امنیت ملی با استفاده از روش توصیفی تحلیلی نشان داد که تأسیس ساختاری قدرتمند و فرا قوه‌ای مبتنی بر الزامات حقوقی برای سیاست‌گذاری، قانون‌گذاری، جرم‌انگاری و همچنین ساماندهی فضای مجازی در کشور و راه‌اندازی شبکه ملی اطلاعات می‌تواند در رفع بسیاری از مشکلات در این حوزه مؤثر باشد.

مبانی نظری

۱-۲- مفاهیم کلیدی

امنیت داخلی

امنیت داخلی به معنای حفاظت از نظم و ثبات سیاسی، اجتماعی و اقتصادی کشور در برابر تهدیدات داخلی و خارجی است. در دنیای امروز، امنیت داخلی صرفاً به معنای نبود جنگ یا شورش نیست، بلکه شامل احساس امنیت شهروندان در زندگی روزمره، اعتماد به نهادهای حکومتی و مصون بودن از تهدیدات سایبری، تبلیغاتی و روانی نیز می‌شود. ظهور فضای مجازی، مرزهای سنتی امنیت داخلی را گسترش داده و تهدیدات جدیدی را به وجود آورده است که بسیاری از آنها ماهیت دیجیتال دارند (وندنهارک، ۱۴۰۳: ۱۲).

تبلیغات مجرمانه آنلاین

تبلیغات مجرمانه به هرگونه اقدام سازمان‌یافته یا فردی در فضای مجازی اطلاق می‌شود که به



منظور ترویج و اشاعه رفتارهای غیرقانونی یا ناهنجار انجام می‌گیرد. این تبلیغات می‌تواند شامل معرفی کالاهای غیرمجاز (مانند مواد مخدر یا سلاح)، آموزش ارتکاب جرایم (هک، کلاهبرداری، فیشینگ)، یا حتی ترویج ایدئولوژی‌های افراطی باشد. ویژگی مهم تبلیغات آنلاین، دسترسی پذیری گسترده، ناشناس بودن مرتکبان و پایین بودن هزینه انتشار است (ویشواکارما^۱، ۲۰۲۴: ۲).

رفتارهای مجرمانه آنلاین

رفتارهای مجرمانه آنلاین مجموعه‌ای از اعمال هستند که با استفاده از بسترهای دیجیتال و شبکه‌های ارتباطی صورت می‌گیرند. این رفتارها ممکن است به صورت مستقیم (مانند سرقت داده‌های شخصی یا حملات باج‌افزاری) یا غیرمستقیم (مانند تشویق افراد به ارتکاب جرم یا انتشار اطلاعات گمراه‌کننده) انجام شوند. ویژگی مشترک آنها عبور از مرزهای جغرافیایی و دشواری شناسایی عاملان است (اونودیامو^۲، ۲۰۲۵: ۳۳).

۲-۲- نظریه‌های جرم‌شناسی مرتبط

برای درک بهتر چرایی و چگونگی گسترش تبلیغات و رفتارهای مجرمانه آنلاین، بهره‌گیری از نظریه‌های جرم‌شناسی ضروری است.

نظریه فشار^۳

این نظریه که نخستین بار توسط رابرت مرتن^۴ مطرح شد، بیان می‌کند افراد زمانی به سمت ارتکاب جرم می‌روند که بین اهداف فرهنگی جامعه (مانند موفقیت مالی یا اجتماعی) و ابزارهای مشروع برای دستیابی به آنها شکاف وجود داشته باشد. در فضای مجازی، بسیاری از افراد که امکان تحقق اهداف خود در دنیای واقعی را ندارند، به تبلیغات غیرقانونی یا فعالیت‌های مجرمانه روی می‌آورند. مثال بارز آن کلاهبرداران اینترنتی یا کسانی است که از طریق تبلیغ فروش داروهای غیرمجاز کسب درآمد می‌کنند (مرتن، ۲۰۲۲: ۵۷).

1. Vishwakarma
2. Onwuadimu
3. Strain Theory
4. Robert K. Merton



نظریه یادگیری اجتماعی^۱

آلبرت باندورا^۲ و سایر نظریه‌پردازان این حوزه بر نقش یادگیری از طریق مشاهده و تعامل با دیگران تأکید دارند. فضای مجازی بستری است که در آن افراد به راحتی الگوهای مجرمانه را مشاهده می‌کنند و با گروه‌های بزهکار ارتباط برقرار می‌نمایند. تبلیغات آنلاین در این نظریه نقش «عامل آموزش‌دهنده» دارد و بزهکاری را به نسل‌های جدید منتقل می‌کند (باندورا، ۲۰۲۲: ۱۷).

نظریه انتخاب عقلانی^۳

بر اساس این نظریه، افراد پیش از ارتکاب جرم هزینه‌ها و منافع احتمالی آن را می‌سنجند. فضای مجازی با ناشناس‌سازی هویت و دشواری تعقیب قانونی، هزینه ارتکاب جرم را پایین آورده و انگیزه‌ها را افزایش داده است. بنابراین، تبلیغات مجرمانه و رفتارهای بزهکارانه آنلاین با اتکا به این مزیت، گسترش می‌یابند (کالا^۴، ۲۰۲۴: ۳۰).

نظریه فعالیت‌های روزمره^۵

این نظریه سه عامل لازم برای وقوع جرم را معرفی می‌کند. وجود مجرم انگیزه‌دار، حضور قربانی مناسب، و فقدان نگاهبان مؤثر. در فضای آنلاین هر سه عامل به‌وفور وجود دارند. مجرمان انگیزه‌دار در هر نقطه دنیا حاضرند؛ قربانیان بالقوه شامل میلیون‌ها کاربر هستند؛ و فقدان نظارت یا کنترل مؤثر نیز شرایط را تسهیل می‌کند (استادنیکی^۶ و همکاران، ۲۰۲۴: ۶).

۲-۳- رویکردهای کیفری در مواجهه با جرایم آنلاین

جرم‌انگاری^۷

نخستین اقدام نظام‌های حقوقی برای مقابله با تبلیغات و جرایم آنلاین، جرم‌انگاری این رفتارهاست. بسیاری از کشورها قوانینی خاص برای جرایم سایبری وضع کرده‌اند. در ایران نیز

1. Social Learning Theory
2. Albert Bandura
3. Rational Choice Theory
4. Kala
5. Routine Activity Theory
6. Stadnicki
7. Criminalization



«قانون جرایم رایانه‌ای» مصوب ۱۳۸۸ نمونه‌ای از این تلاش است. با این حال، تحولات سریع فناوری سبب می‌شود قوانین به سرعت ناکارآمد شوند و نیاز به بازنگری مداوم داشته باشند (دی‌نیکولا^۱، ۲۰۲۲: ۶۹۲).

کیفرگذاری^۲

کیفرگذاری مناسب یکی از چالش‌های مهم است. در فضای آنلاین، گاهی مجازات‌های سنتی (حبس یا جزای نقدی) بازدارندگی کافی ندارند. برخی کشورها از تدابیری مانند محرومیت از دسترسی به اینترنت، ضبط ابزارهای الکترونیک یا مسدودسازی حساب‌های دیجیتال استفاده می‌کنند (وانگ و ژانگ^۳، ۲۰۲۳: ۱۴۶۲).

همکاری بین‌المللی

ماهیت فراملی جرایم آنلاین ایجاب می‌کند که کشورها همکاری‌های گسترده‌تری داشته باشند. کنوانسیون بوداپست (۲۰۰۱) نخستین سند بین‌المللی در این زمینه است که بر هماهنگی قوانین داخلی و تبادل اطلاعات تأکید دارد. برای کشورهایی مانند ایران، پیوستن به این سازوکارها می‌تواند فرصت‌ها و چالش‌های خاصی به همراه داشته باشد (لان^۴ و همکاران، ۲۰۲۴: ۵۵).

پیشگیری وضعی و اجتماعی

سیاست کیفری نباید صرفاً واکنشی باشد، بلکه باید پیشگیرانه نیز عمل کند. پیشگیری وضعی شامل تقویت زیرساخت‌های امنیت سایبری، استفاده از فناوری‌های شناسایی و رهگیری و محدودسازی دسترسی بزهکاران به ابزارهای تبلیغاتی است. پیشگیری اجتماعی نیز از طریق آموزش کاربران، ارتقای سواد رسانه‌ای و آگاهی‌بخشی عمومی دنبال می‌شود (آکینبواله^۵ و همکاران، ۲۰۲۴: ۱۱).

1. Di Nicola
2. Penalization
3. Wang and Zhang
4. Lan
5. Akinbowale

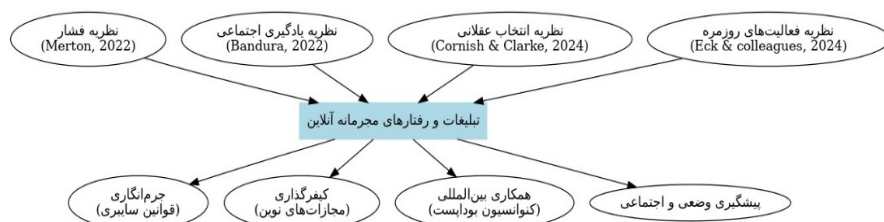


۲-۴- پیوند جرم‌شناسی و حقوق کیفری

چارچوب نظری این پژوهش بر پیوند میان دو حوزه استوار است: جرم‌شناسی (که به علل و عوامل بزهکاری می‌پردازد) و حقوق کیفری (که ابزارهای قانونی مقابله با آن را فراهم می‌آورد). تنها با ترکیب این دو حوزه می‌توان به درک جامعی از تبلیغات و رفتارهای مجرمانه آنلاین رسید. جرم‌شناسی کمک می‌کند بفهمیم چرا افراد به این مسیر کشیده می‌شوند و حقوق کیفری ابزارهایی برای کنترل و مهار آنها فراهم می‌آورد.

به طور کلی بایستی اذعان داشت فضای مجازی محیطی است که بزهکاری در آن نه تنها تسهیل می‌شود، بلکه از طریق تبلیغات و ارتباطات گسترده تشدید می‌گردد. نظریه‌های جرم‌شناسی به ما نشان می‌دهند که انگیزه‌های اقتصادی، اجتماعی و روانی در کنار فرصت‌های فناورانه، زمینه‌ساز گسترش این پدیده‌اند. از سوی دیگر، نظام کیفری باید با بهره‌گیری از ابزارهای نوین، رویکردی ترکیبی از جرم‌انگاری، کیفرگذاری، پیشگیری و همکاری بین‌المللی اتخاذ کند تا بتواند آثار منفی آن بر امنیت داخلی را کاهش دهد.

با بحث و بررسی ادبیات نظری مطرح شده در این پژوهش، نویسندگان در راستای تحقق هدف اصلی و ارائه پرسشی مستدل و متقن به سوال اصلی پرسش، مبادرت به ارائه چارچوب مفهومی برای پژوهش کنونی نموده‌اند. در این راستا، چارچوب مفهومی ارائه شده، رابطه علت‌مند میان نظریه‌های کلیدی جرم‌شناسی و پدیده «تبلیغات و رفتارهای مجرمانه آنلاین» را نشان می‌دهد: نظریه‌های فشار، یادگیری اجتماعی، انتخاب عقلانی و نظریه فعالیت‌های روزمره به عنوان عوامل تبیینی ورود و گسترش رفتارهای مجرمانه در محیط سایبری عمل می‌کنند. این پدیده سپس به عنوان ورودی به مجموعه‌ای از راهکارهای کیفری و سیاست‌گذاری (جرم‌انگاری، کیفرگذاری، همکاری بین‌المللی و پیشگیری وضعی/اجتماعی) منتهی می‌شود؛ به عبارت دیگر چارچوب، از تبیین علی تا پاسخ‌های سیاست‌محور را در یک مدل ساده و قابل فهم جمع می‌کند. ساختار نمودار به‌صورتی است که روشن می‌سازد هر نظریه چگونه به تفکیک سهم خود را در شکل‌گیری انگیزه‌ها، الگوها و شرایط مرتکبین دیجیتال ایفا می‌کند و در نهایت چه نوع واکنش کیفری و پیشگیرانه‌ای می‌تواند متناسب با آن باشد.



شکل ۱- چارچوب مفهومی پژوهش (طراحی: نویسندگان)

روش‌شناسی تحقیق

روش تحقیق در پژوهش حاضر بر رویکرد توصیفی تحلیلی استوار است؛ بدین معنا که ابتدا با گردآوری داده‌ها از طریق منابع کتابخانه‌ای، اسناد حقوقی، مقالات علمی و متون تخصصی، مبانی نظری و چارچوب مفهومی موضوع استخراج شده است. سپس این داده‌ها با بهره‌گیری از روش تحلیل محتوا و مقایسه تطبیقی، مورد بررسی قرار گرفته‌اند تا ابعاد کیفری و جرم‌شناختی تبلیغات مجرمانه آنلاین روشن شود. این شیوه به پژوهشگر امکان داده است تا با ترکیب داده‌های نظری و شواهد مستند، تصویری جامع از تهدیدات فضای مجازی و کارآمدی سیاست کیفری در مقابله با آن ارائه دهد.

یافته‌ها و تجزیه و تحلیل داده‌ها

۳-۱- مصادیق تبلیغات و رفتارهای مجرمانه آنلاین

۳-۱-۱- تبلیغات مرتبط با مواد مخدر و کالاهای غیرقانونی

در بسیاری از کشورها، گروه‌های تبهکار از شبکه‌های اجتماعی و حتی بازی‌های آنلاین برای تبلیغ مواد مخدر استفاده می‌کنند. برای نمونه، در گزارش سال ۲۰۲۲ دفتر مقابله با مواد مخدر و جرم سازمان ملل^۱، اشاره شده بود که کانال‌های تلگرام و صفحات اینستاگرام در منطقه خاورمیانه و آمریکای لاتین به‌طور گسترده برای عرضه مواد محرک مانند مت‌آمفتامین و کوکائین به کار می‌روند (کارپ^۲، ۲۰۲۴: ۱۰۲). در کشور ایران نیز بارها پلیس فتا اعلام کرده که کانال‌های تلگرامی

1. UNODC

2. Karp



و صفحات اینستاگرامی فروش داروهای قاچاق یا قرص‌های روان‌گردان شناسایی و مسدود شده‌اند. در واقع، ناشناس ماندن فروشندگان (به دلیل استفاده از VPN و حساب‌های جعلی) و ابزارهای پرداخت دیجیتال، شناسایی و پیگیری را دشوار می‌کند. این موضوع اقتدار دولت در کنترل بازارهای غیرقانونی را به چالش می‌کشد و امنیت بهداشتی و اجتماعی را تهدید می‌کند.

۲-۱-۳- تبلیغات تروریستی و افراط‌گرایانه

گروه‌های افراطی و تروریستی از فضای مجازی برای جذب نیرو، آموزش و تأمین مالی بهره می‌برند. آنها با استفاده از تبلیغات دیجیتال، پیام‌های ایدئولوژیک خود را در قالب محتوای ویدیویی، متنی یا تصویری منتشر می‌کنند و مخاطبان بالقوه را جذب می‌نمایند. تجربه داعش نشان داد که چگونه یک گروه می‌تواند با اتکا به تبلیغات آنلاین، هزاران نفر از نقاط مختلف جهان را جذب کرده و تهدیدی جهانی ایجاد کند. در واقع گروهک تروریستی - تکفیری داعش نشان داد که چگونه می‌توان با استفاده از ویدئوهای حرفه‌ای، پادکست‌ها و نشریات دیجیتال مثلاً مجله Dabiq هزاران نفر را از اروپا، آسیا و آفریقا جذب کرد. در این راستا، در سال‌های ۲۰۱۴ تا ۲۰۱۷، توییت‌ر و فیس‌بوک مجبور شدند میلیون‌ها حساب کاربری وابسته به داعش را مسدود کنند (برزگرزاده زرنندی و نورعلی^۱، ۲۰۲۵: ۵۸۶). بنابراین این نوع تبلیغات علاوه بر جذب نیرو، ابزار مهمی برای تأمین مالی (از طریق بیت‌کوین یا پلتفرم‌های خیریه جعلی) محسوب می‌شود. بنابراین، تبلیغات تروریستی در فضای مجازی نه تنها تهدید امنیت داخلی یک کشور، بلکه تهدیدی جهانی است.

۳-۱-۳- کلاهبرداری‌های اینترنتی و فیشینگ

کلاهبرداری آنلاین یکی از رایج‌ترین مصادیق جرایم سایبری است. تبلیغات جعلی در قالب فروشگاه‌های اینترنتی، پیام‌های بانکی یا پیشنهادات و سوسه‌انگیز، کاربران را فریب داده و منجر به سرقت داده‌های مالی یا هویتی آنها می‌شود. این گونه تبلیغات، اعتماد عمومی به نظام اقتصادی و بانکی را کاهش داده و خسارت‌های سنگینی به شهروندان و دولت وارد می‌کند (هاکمه^۲، ۲۰۲۴: ۱۲۷). کلاهبرداری آنلاین گستره وسیعی دارد؛ از پیامک‌های جعلی بانکی گرفته تا فروشگاه‌های

1. Barzegarzadeh Zarandi and Noorali

2. Hakmeh



اینترنتی ساختگی ار میتوان در این رابطه ذکر نمود. در سال ۲۰۲۱، پلیس اروپا^۱ اعلام کرد که میلیون‌ها یورو از طریق کمپین‌های فیشینگ با ظاهر بانک‌های معتبر از حساب مردم اروپا سرقت شده است (کلی^۲ و همکاران، ۲۰۲۳: ۸۶۶). در ایران نیز بارها اخطار داده شده که پیامک‌های جعلی با عنوان «یارانه»، «برنده شدن در قرعه کشی» یا «پرداخت قبض» باعث سرقت اطلاعات کارت بانکی شهروندان شده است. این نوع تبلیغات مجرمانه اعتماد عمومی به بانک‌ها، فروشگاه‌های آنلاین و حتی دولت را تضعیف می‌کند و آثار روانی و اقتصادی قابل توجهی به جا می‌گذارد.

۳-۱-۴- شایعه‌پراکنی و جنگ روانی

بخشی از تبلیغات مجرمانه آنلاین در قالب انتشار اخبار جعلی، شایعات و محتوای گمراه‌کننده صورت می‌گیرد. این اطلاعات نادرست می‌توانند در کوتاه‌ترین زمان، افکار عمومی را متشنج کرده، بحران‌های اجتماعی ایجاد کنند و اعتماد مردم به نهادهای رسمی را تضعیف نمایند. نمونه‌های متعدد در زمینه شایعات اقتصادی، اخبار جعلی درباره بیماری‌ها یا حوادث امنیتی، نشان می‌دهد که چنین تبلیغاتی مستقیماً بر امنیت داخلی اثرگذار است. بنابراین، پدیده «اخبار جعلی»^۳ به یکی از ابزارهای مؤثر در جنگ‌های اطلاعاتی تبدیل شده است. در همه‌گیری کرونا، اخبار جعلی درباره داروها و واکسن‌ها در فیسبوک و واتساپ باعث شد برخی مردم از واکسیناسیون اجتناب کنند (هیرونی^۴، ۲۰۲۴: ۴۳). در ایران نیز انتشار شایعات درباره قیمت ارز و سکه در شبکه‌های اجتماعی بارها منجر به التهاب در بازار شده است. بنابراین بایستی بر این نکته مهم اذعان داشت که تبلیغات مبتنی بر شایعه می‌تواند در کوتاه‌ترین زمان اعتماد عمومی به رسانه‌های رسمی را تضعیف کرده، بحران‌های اجتماعی و حتی امنیتی ایجاد کند. این امر نشان می‌دهد که فضای مجازی به عرصه‌ای برای جنگ نرم و روانی تبدیل شده است.

۳-۱-۵- جرایم سازمان‌یافته دیجیتال

بسیاری از تبلیغات و فعالیت‌های مجرمانه آنلاین توسط شبکه‌های سازمان‌یافته هدایت می‌شوند. این شبکه‌ها در حوزه‌هایی مانند قاچاق انسان، پول‌شویی، قمار آنلاین و سرقت داده‌های

1. Europol
2. Kelley
3. Fake News
4. Hiruni



حساس فعالیت دارند. تبلیغات آنها عمدتاً با هدف جذب مشتری یا همکار جدید صورت می‌گیرد و ماهیت فراملی آنها مقابله با آنها را دشوارتر می‌سازد. شبکه‌های سازمان‌یافته، از دارکوب^۱ به‌عنوان فضای اصلی تبلیغ و فروش کالاهای غیرقانونی استفاده می‌کنند. بازار «Silk Road» در دارکوب که در سال ۲۰۱۳ توسط FBI مسدود شد، نمونه‌ای معروف از یک بازار سیاه آنلاین بود که در آن مواد مخدر، اسلحه و حتی خدمات هکری معامله می‌شد (ولان^۲ و همکاران، ۲۰۲۳: ۳۲۲). در ایران، پلیس فتا بارها اعلام کرده که باندهای قاچاق انسان یا شرط‌بندی آنلاین با شبکه‌های پیچیده و بین‌المللی در ارتباط هستند. ماهیت فراملی این شبکه‌ها، تعقیب قضایی را دشوار می‌کند و نیازمند همکاری‌های بین‌المللی (مانند کنوانسیون بوداپست درباره جرایم سایبری) است. تبلیغات این شبکه‌ها با هدف جذب مشتری و همکار جدید، یکی از ابزارهای مهم بقای آن‌هاست.

۳-۲- تأثیر تبلیغات و رفتارهای مجرمانه آنلاین بر امنیت داخلی

۳-۲-۱- تأثیر بر امنیت سیاسی

تبلیغات مجرمانه می‌تواند مشروعیت نظام سیاسی را تضعیف کند. انتشار گسترده اخبار جعلی و تخریب‌کننده، بی‌اعتمادی عمومی نسبت به نهادهای دولتی و امنیتی را افزایش می‌دهد. همچنین، تبلیغات تروریستی یا افراط‌گرایانه می‌تواند زمینه‌ساز ناآرامی‌های سیاسی و اجتماعی شده و انسجام ملی را تهدید کند. به بیانی دیگر، تبلیغات مجرمانه، به‌ویژه در قالب اخبار جعلی، کمپین‌های تخریب شخصیت سیاسی یا محتوای تروریستی، می‌تواند پایه‌های اعتماد عمومی به حاکمیت را سست کند (تیچمن^۳، ۲۰۲۳: ۴۰۴). وقتی شهروندان در فضای مجازی با انبوهی از اخبار منفی و بدون منبع معتبر روبه‌رو می‌شوند، به تدریج مشروعیت و کارآمدی نهادهای سیاسی زیر سؤال می‌رود. نمونه بارز آن، مداخلات سایبری در انتخابات برخی کشورهاست؛ مثل پرونده دخالت روسیه در انتخابات ریاست جمهوری آمریکا در سال ۲۰۱۶ که نشان داد تبلیغات دیجیتال می‌تواند بر جهت‌گیری سیاسی یک ملت تأثیر بگذارد (زوکا و فیورینلی^۴، ۲۰۲۵: ۷۸). در ایران نیز انتشار شایعات گسترده درباره تصمیمات سیاسی یا امنیتی می‌تواند به بی‌ثباتی داخلی، کاهش

1. Dark Web
2. Whelan
3. Teichmann
4. Zucca and Fiorinelli



مشارکت سیاسی و حتی اعتراض‌های خیابانی دامن بزند. بنابراین، تبلیغات مجرمانه نه تنها یک جرم سایبری ساده، بلکه تهدیدی مستقیم علیه امنیت ملی و انسجام سیاسی است.

۳-۲-۲- تأثیر بر امنیت اقتصادی

کلاهبرداری‌های اینترنتی، حملات سایبری و تبلیغات مربوط به بازارهای غیرقانونی، امنیت اقتصادی کشور را تضعیف می‌کند. خروج ارز، کاهش اعتماد به نظام بانکی، گسترش اقتصاد زیرزمینی و کاهش سرمایه‌گذاری خارجی از جمله پیامدهای مستقیم این پدیده است. فعالیت‌های مجرمانه آنلاین مانند کلاهبرداری‌های مالی، فیشینگ، تبلیغات داروها و کالاهای قاچاق و نیز حملات سایبری به زیرساخت‌های مالی، تهدیدی جدی برای امنیت اقتصادی کشور محسوب می‌شوند (جانسون^۱، ۲۵: ۱۲۹). خروج ارز از طریق سایت‌های شرط‌بندی یا پول‌شویی دیجیتال، کاهش اعتماد عمومی به بانک‌ها و نهادهای مالی، و شکل‌گیری بازارهای زیرزمینی دیجیتال از پیامدهای مستقیم این تبلیغات هستند (ولان و همکاران، ۲۳: ۳۲۶). برای مثال، در برخی کشورها، تنها یک حمله سایبری موفق به سیستم‌های بانکی باعث سقوط ارزش پول ملی و فرار سرمایه‌گذاران خارجی شده است. همچنین تبلیغات جعلی فروشگاه‌های اینترنتی، موجب فریب هزاران کاربر و کاهش تمایل شهروندان به استفاده از خدمات تجارت الکترونیک می‌شود. این عوامل در مجموع می‌توانند نرخ بیکاری را افزایش داده، تولید داخلی را تضعیف کنند و کشور را در شرایط بحران اقتصادی قرار دهند.

۳-۲-۳- تأثیر بر امنیت اجتماعی و فرهنگی

انتشار گسترده تبلیغات مربوط به مواد مخدر، مشروبات الکلی یا رفتارهای انحرافی، موجب تضعیف ارزش‌های فرهنگی جامعه می‌شود. همچنین، تبلیغات مجرمانه در حوزه قمار یا خشونت، می‌تواند الگوهای ناهنجار را میان جوانان ترویج کرده و نظم اجتماعی را برهم زند. تبلیغات مجرمانه در حوزه‌هایی مانند مواد مخدر، مشروبات الکلی، قمار آنلاین یا خشونت‌های خیابانی، به‌طور مستقیم ارزش‌های فرهنگی و هنجارهای اجتماعی جامعه را تضعیف می‌کند. برای مثال، کانال‌ها و صفحات مجازی که مصرف مواد مخدر را عادی‌سازی می‌کنند، به‌ویژه در میان نوجوانان، موجب تغییر الگوهای رفتاری و تضعیف نظام خانواده می‌شوند (تیچمن، ۲۳: ۴۰۶). همچنین

1. Johnson



تبلیغ محتوای خشونت‌آمیز یا جنسی می‌تواند به تغییر ذائقه فرهنگی نسل جوان منجر شده و شکاف‌های فرهنگی را افزایش دهد. تجربه جوامعی که با موج تبلیغات قمار آنلاین یا محتوای افراط‌گرایانه روبه‌رو بوده‌اند نشان می‌دهد که این پدیده‌ها مستقیماً به افزایش جرم و کاهش انسجام اجتماعی منجر می‌شوند. از این رو، تبلیغات مجرمانه تنها یک مسئله سایبری نیست، بلکه تهدیدی برای فرهنگ بومی، سنت‌ها و سرمایه اجتماعی جامعه است.

۳-۲-۴- تأثیر بر امنیت روانی جامعه

فضای مجازی پر از تبلیغات جعلی و تهدیدآمیز، می‌تواند احساس ناامنی و بی‌اعتمادی را در جامعه گسترش دهد. این ناامنی روانی، خود به کاهش سرمایه اجتماعی و افزایش شکاف‌های اجتماعی منجر می‌شود. یکی از ابعاد کمتر دیده‌شده اما بسیار مهم تبلیغات مجرمانه، تأثیر آن بر امنیت روانی شهروندان است. هنگامی که کاربران به‌طور مداوم با تبلیغات تهدیدآمیز، اخبار جعلی یا محتوای اضطراب‌آور مواجه می‌شوند، احساس ناامنی و بی‌ثباتی در جامعه گسترش می‌یابد. این امر به‌ویژه در مواقع بحران (مانند شیوع بیماری‌های واگیردار یا ناآرامی‌های سیاسی) شدت می‌گیرد و می‌تواند موجب افزایش استرس جمعی، ناامیدی اجتماعی و گسترش بدبینی نسبت به آینده شود (بوچکوار^۱ و همکاران، ۲۰۲۵: ۵۰-۵۱). برای نمونه، در دوران کرونا، تبلیغات جعلی درباره کمبود دارو یا اثربخشی واکسن‌ها باعث شد بخش زیادی از مردم دچار اضطراب شدید شوند. در بلندمدت، چنین فضایی به کاهش اعتماد متقابل میان مردم و نهادهای رسمی، تضعیف سرمایه اجتماعی و افزایش شکاف‌های اجتماعی منجر می‌شود.

۳-۳- مطالعه تطبیقی قوانین و سیاست‌ها

۳-۳-۱- ایالات متحده آمریکا

ایالات متحده با تصویب قوانینی همچون قانون کلاهبرداری و سوءاستفاده رایانه‌ای^۲ و ایجاد نهادهایی مانند FBI Cyber Division، تلاش کرده است تا تبلیغات و جرایم آنلاین را کنترل کند. همچنین، شرکت‌های فناوری مانند فیسبوک و توییتر موظف به حذف محتوای تروریستی و تبلیغات مجرمانه شده‌اند. ایالات متحده بر خوردی ترکیبی از ابزارهای کیفری کلاسیک و

1. Botchkovar
2. CFAA



مکانیزم‌های فنی - سازمانی را در پیش گرفته است. قانون “Computer Fraud and Abuse Act” به عنوان یکی از پایه‌های تعقیب جرایم رایانه‌ای، امکان پیگرد هکرها و مجرمان سایبری را فراهم می‌آورد؛ با این حال کاربرد گسترده و فراگیر این قانون باعث بحث‌های حقوقی درباره دامنه شمول و نسبت آن با فعالیت‌های روزمره آنلاین شده است (باتن^۱، ۲۰۲۵: ۶۳). نهادهایی مانند FBI Cyber Division و آژانس‌های امنیت سایبری دولت فدرال از جمله CISA مسئولیت شناسایی، پیگرد و هماهنگی پاسخ به تهدیدات سایبری فراملی را دارند که شامل تبلیغات مجرمانه و محتوای تروریستی نیز می‌شود (لین^۲ و همکاران، ۲۰۲۴: ۳۷۱). در عمل، فشار قانونی و عمومی بر شرکت‌های فناوری برای حذف محتوای تروریستی و تبلیغات مجرمانه افزایش یافته؛ این شرکت‌ها از یک‌سوز مصونیت‌های حقوقی مانند Section 230 برخوردار بوده‌اند و از سوی دیگر با انتقادات و الزام‌های نظارتی روبه‌رو می‌گردند که در سال‌های اخیر شدت گرفته است. نمونه‌های عملی مانند پرونده‌هایی علیه بازارهای مخفی دارکوب یا عملیاتی بین‌المللی برای بستن شبکه‌های فروش غیرقانونی نشان می‌دهد که ترکیب ظرفیت‌های اطلاعاتی و همکاری بین‌المللی برای موفقیت در مقابله با تبلیغات مجرمانه ضروری است (منت^۳، ۲۰۲۵: ۴-۵). در مجموع، رویکرد ایالات متحده ترکیبی از مجازات کیفری، عملیات اطلاعاتی و فشار سیاسی - حقوقی بر پلتفرم‌هاست که با چالش‌های حقوقی و عملی در عصر رمزارزها و رمزنگاری مواجه است.

۳-۲- اتحادیه اروپا

اتحادیه اروپا با مقررات سخت‌گیرانه در حوزه حفاظت از داده‌ها^۴ و نیز تصویب دستور العمل‌هایی برای مقابله با محتوای تروریستی، تلاش کرده است از شهروندان در برابر تبلیغات مجرمانه محافظت کند. همکاری فراملی میان کشورهای عضو نیز از ویژگی‌های برجسته این نظام است (ولان و همکاران، ۲۰۲۳: ۳۲۷). اتحادیه اروپا در سال‌های اخیر به سمت وضع مقررات منسجم و جامع برای فضای دیجیتال حرکت کرده است؛ مهم‌ترین نمونه آن “Digital Services Act” است که چارچوبی برای مسئولیت‌پذیری پلتفرم‌ها، شفافیت الگوریتمی و حذف محتوای مضر

1. Button
2. Lin
3. Menet
4. GDPR
5. DSA



فراهم می‌آورد. علاوه بر DSA، سیاست‌گذاری اختصاصی برای مقابله با انتشار محتوای تروریستی و افراط‌گراییانه نیز دنبال شده و قوانین یا توصیه‌نامه‌هایی برای حذف سریع این گونه محتوا و همکاری میان تنظیم‌کنندگان ملی تدوین شده است؛ این اقدامات نشان‌دهنده گرایش اتحادیه به راه‌حل‌های حقوقی-نظارتی فراملی و تاکید بر مسوولیت پلتفرم‌هاست (فن برکل^۱ و همکاران، ۲۰۲۵: ۱۹۲-۱۹۳). از منظر عملی، سازوکارهای هم‌افزایی میان نهادهای نظارتی کشورهای عضو، تبادل اطلاعات سیگنالی‌نگ و امکان اعمال جریمه‌های اقتصادی سنگین (تا درصدی از درآمد جهانی پلتفرم‌ها) ابزارهای مؤثری برای فشار به شرکت‌ها به شمار می‌آیند. با این وجود، چالش‌های جدی نیز وجود دارد. تعریف دقیق «محتوای غیرقانونی»، تضمین تضاد حقوقی میان امنیت و آزادی بیان، و ظرفیت نظارتی در برابر بازیگران فراملی. تجربه اخیر نشان می‌دهد که اتحادیه اروپا در عمل دنبال ایجاد تعادل بین حفاظت شهروندان و حفظ حقوق اساسی بوده و در عین حال از طریق ابزارهای قانونی سعی در کاهش مخاطرات تبلیغات مجرمانه در فضای آنلاین دارد.

۳-۳-۳- کشورهای آسیایی

کشورهایی مانند چین با سیاست‌های سخت‌گیرانه فیلترینگ و کنترل شدید اینترنت، رویکردی امنیت‌محور در قبال تبلیغات مجرمانه اتخاذ کرده‌اند. در مقابل، کشورهایی مانند هند بیشتر بر آموزش و افزایش آگاهی عمومی تمرکز کرده‌اند. در آسیا رویکردها بسیار متنوع و اغلب تابعی از ساختارهای سیاسی و فرهنگی هر کشور است. برای نمونه، چین با استفاده از سازوکارهای گسترده فیلترینگ "Great Firewall" سیاست‌های ثبت‌نام با نام واقعی، کنترل شدید اپراتورها و اعمال مقررات سخت‌گیرانه نسبت به محتوای آنلاین، رویکردی امنیت‌محور و کنترلی اتخاذ کرده است؛ این سیاست‌ها با بهره‌گیری از فناوری‌های نوین نظارتی و حتی شناسه‌های دیجیتال ملی تقویت می‌شود (لو و ژائو^۲، ۲۰۲۵: ۷۶). در مقابل، کشورهایی مانند هند با وجود تشدید مقررات میانی‌گرو^۳ و الزام به پاسخ‌گویی پلتفرم‌ها، راهبردی ترکیبی را دنبال می‌کنند که علاوه بر مقررات، بر آموزش، آگاهی‌رسانی و تقویت ظرفیت‌های محلی برای شناسایی محتوای مضر تأکید دارد. البته در هر دو نمونه مسائل مهمی مانند سوءاستفاده از ابزار نظارتی برای سرکوب

1. Van Berkel
2. Luo and Zhao
3. IT Rules 2021



انتقادات مشروع، مشکلات حریم خصوصی، و موانع فنی اجرای مقررات، مطرح بوده و نیازمند شفاف‌سازی و تضمین حقوقی است. به‌علاوه، ظهور فن‌آوری‌هایی مانند رمزنگاری سرتاسری و رمزارزها، مبارزه با تبلیغات مجرمانه فراملی را پیچیده‌تر ساخته و کشورهای آسیایی را وادار به تقویت همکاری‌های منطقه‌ای و بین‌المللی کرده است (وی و پان^۱، ۲۰۲۴: ۵۵۸-۵۵۹). لذا در منطقه آسیا شاهد تنوعی از رویکردها هستیم که از کنترل مطلق تا تاکید بر آموزش و تکالیف پلتفرم‌ها را در بر می‌گیرد.

۳-۳-۴- جمهوری اسلامی ایران

در ایران، قانون جرایم رایانه‌ای (۱۳۸۸) مهم‌ترین ابزار قانونی برای مقابله با تبلیغات و جرایم آنلاین است. با این حال، به دلیل سرعت بالای تحولات فناوری و ظهور جرایم جدید، این قانون نیازمند بازنگری و به‌روزرسانی مستمر است. همچنین، ضعف همکاری‌های بین‌المللی و محدودیت‌های فنی از جمله چالش‌های جدی در مقابله با این پدیده به شمار می‌آیند. ساختار نهادی در ایران شامل سازمان‌های متعددی (پلیس فتا، مرکز ملی فضای مجازی و قوه قضاییه) است که هر یک نقش‌هایی در شناسایی، فیلترینگ، و پیگیری قضایی ایفا می‌کنند؛ ولی فقدان همکاری‌های بین‌المللی کامل و محدودیت‌های تکنولوژیک (مانند دسترسی دشوار به داده‌های میزبان خارجی یا محدودیت همکاری میان‌المللی به دلیل تحریم‌ها) کار را برای تعقیب بازیگران فراملی پیچیده می‌سازد (شعبانی، ۱۴۰۳: ۲۲). علاوه بر آن، مسائل مربوط به حقوق شهروندی، آزادی بیان و شفافیت در اجرای مقررات از جمله نگرانی‌هایی است که می‌تواند مشروعیت اقدامات کنترلی را زیر سؤال ببرد و در عمل کارآیی مقابله را کاهش دهد. بنابراین نیاز به بازنگری‌های هدفمند در قانون، تقویت ظرفیت فنی-تحقیقی، توسعه کانال‌های قانونی همکاری بین‌المللی و تعادل بخشی بین امنیت و حقوق شهروندی از اولویت‌های راهبردی است تا سیاست‌ها در برابر تبلیغات مجرمانه آنلاین موثر و مشروع باقی بمانند.

۳-۴- نقاط ضعف و چالش‌های سیاست کیفری ایران

خلاف‌های قانونی: بسیاری از جرایم نوظهور مانند تبلیغات مرتبط با ارزهای دیجیتال یا تبلیغات در پلتفرم‌های غیرمتمرکز هنوز در قوانین پیش‌بینی نشده‌اند؛



کمبود تخصص فنی؛ نیروهای انتظامی و قضایی نیازمند آموزش‌های تخصصی و تجهیزات به‌روز برای مقابله با جرایم سایبری هستند؛ ضعف در همکاری‌های بین‌المللی؛ به دلیل محدودیت‌های سیاسی و حقوقی، ایران دسترسی محدودی به نهادهای بین‌المللی مقابله با جرایم سایبری دارد؛ چالش‌های فرهنگی و اجتماعی؛ نبود آگاهی کافی در میان کاربران و فقدان سواد رسانه‌ای، زمینه سوءاستفاده بزهکاران را فراهم می‌کند؛ عدم تناسب مجازات‌ها؛ برخی از مجازات‌های پیش‌بینی‌شده در قانون، بازدارندگی لازم را ندارند و نیاز به اصلاح دارند.

نتیجه‌گیری و پیشنهاد

رشد بی‌سابقه فناوری‌های ارتباطی و گسترش شبکه‌های اجتماعی، علاوه بر فرصت‌های گسترده‌ای که در حوزه‌های اقتصادی، فرهنگی و سیاسی ایجاد کرده است، تهدیدهای تازه‌ای را نیز پیش روی نظام‌های امنیتی قرار داده است. یکی از ابعاد مهم این تهدیدها، شکل‌گیری تبلیغات انحرافی و رفتارهای مجرمانه آنلاین است که نه تنها بنیان‌های اعتماد اجتماعی را سست می‌کند بلکه انسجام ملی و امنیت داخلی را نیز هدف قرار می‌دهد. پژوهش حاضر با تکیه بر رویکرد کیفی و جرم‌شناختی نشان داد که سیاست‌گذاری امنیتی بدون در نظر گرفتن واقعیت‌های نوین فضای سایبری ناکافی خواهد بود. از این رو، نتیجه‌گیری نهایی به دنبال روشن ساختن ابعاد مختلف این پدیده و ارائه راهکارهای مؤثر برای مهار آن است.

بر این اساس، هدف نویسندگان در پژوهش حاضر بحث و ارزیابی اثرات تبلیغات و رفتارهای مجرمانه آنلاین بر امنیت داخلی؛ رویکرد کیفی و جرم‌شناسی بوده است. تحلیل داده‌ها و یافته‌های این پژوهش نشان می‌دادهد که تبلیغات انحرافی و رفتارهای مجرمانه در فضای مجازی ماهیتی پیچیده، پویا و چندبعدی دارند. فضای سایبری به دلیل ویژگی‌های منحصر به فرد خود مانند سرعت انتقال اطلاعات، گستردگی مخاطبان، ناشناس ماندن کاربران و دشواری نظارت بستر مناسبی برای ارتکاب جرایم و فعالیت‌های تبلیغاتی مخرب فراهم کرده است. این ویژگی‌ها موجب می‌شود تا جرم در محیط مجازی نه تنها به سرعت تکثیر گردد، بلکه به سادگی از مرزهای جغرافیایی عبور کند و امنیت داخلی کشورها را با تهدیدهای تازه مواجه سازد.

از منظر امنیت سیاسی، تبلیغات مخرب می‌تواند کارکرد حیاتی رسانه‌های اجتماعی در



شکل‌دهی افکار عمومی را به ابزاری برای بی‌ثبات‌سازی نظام‌های سیاسی تبدیل کند. انتشار سازمان‌یافته اخبار جعلی، کمپین‌های تخریب شخصیت‌ها، و تبلیغات افراط‌گرایانه می‌تواند اعتماد عمومی را نسبت به نهادهای رسمی کاهش داده و مشروعیت سیاسی را سست نماید. نمونه‌های جهانی از مداخلات انتخاباتی یا جذب نیرو توسط گروه‌های تروریستی به‌خوبی نشان می‌دهد که تهدیدهای سایبری چگونه می‌توانند نظم سیاسی کشورها را به چالش بکشند. بنابراین، سیاست کیفری باید هم در سطح ملی و هم در سطح بین‌المللی به دنبال ابزارهایی برای کنترل و مهار این دست از تبلیغات باشد. از نظر امنیت اقتصادی، نتایج نشان داد که تبلیغات مجرمانه در قالب فیشینگ، کلاهبرداری اینترنتی، شرط‌بندی آنلاین و فروش کالاهای غیرقانونی، تهدیدی جدی برای ثبات اقتصادی کشورها محسوب می‌شود. این پدیده‌ها موجب خروج غیرقانونی سرمایه، افزایش هزینه‌های امنیت سایبری، تضعیف اعتماد عمومی به نظام بانکی و در نهایت گسترش اقتصاد زیرزمینی می‌شوند. چنین وضعیتی نه تنها زیان‌های مالی قابل توجهی به شهروندان و دولت وارد می‌کند، بلکه در سطح کلان می‌تواند سرمایه‌گذاری خارجی را نیز کاهش دهد و امنیت اقتصادی را با بحران روبه‌رو کند. سیاست کیفری در این حوزه باید بر دو بعد متمرکز شود: نخست، پیشگیری از طریق ارتقای آگاهی عمومی و تقویت نظارت نهادی؛ دوم، واکنش کیفری مؤثر علیه شبکه‌های سازمان‌یافته و بین‌المللی که در این فضا فعالیت می‌کنند.

در بعد اجتماعی و فرهنگی، تبلیغات مجرمانه تهدیدی عمیق‌تر دارد. ترویج مصرف مواد مخدر، مشروبات الکلی، قمار و محتوای خشونت‌آمیز می‌تواند ارزش‌های فرهنگی جامعه را تضعیف کند و به تدریج هنجارهای ناسالم را به بخشی از فرهنگ عمومی تبدیل نماید. به‌ویژه برای جوانان، که بیشترین کاربران فضای مجازی هستند، مواجهه مداوم با چنین تبلیغاتی به تغییر سبک زندگی، سست‌شدن بنیان خانواده و بروز ناهنجاری‌های اجتماعی منجر می‌شود. در اینجا، جرم‌شناسی پیشگیرانه و سیاست‌های فرهنگی مکمل باید در کنار سیاست کیفری قرار گیرند تا بتوانند مانع از بروز و گسترش چنین آسیب‌هایی شوند. از جنبه امنیت روانی جامعه، تبلیغات سایبری با القای اخبار جعلی و تهدیدآمیز، احساس بی‌اعتمادی و ناامنی را در میان مردم افزایش می‌دهد. این موضوع به کاهش سرمایه اجتماعی، تشدید بدبینی عمومی و گسترش شکاف‌های اجتماعی منجر می‌شود. جامعه‌ای که در آن شهروندان دائماً احساس کنند در معرض تهدید هستند، به تدریج توان اعتماد به نهادهای رسمی و یکدیگر را از دست



می‌دهد. بنابراین، امنیت روانی به‌عنوان یکی از مؤلفه‌های کلیدی امنیت داخلی، نیازمند توجه ویژه سیاست‌گذاران است.

نتایج پژوهش همچنین نشان داد که خلأهای حقوقی و ضعف هماهنگی نهادی در مقابله با تبلیغات مجرمانه، آسیب‌پذیری کشورها را افزایش می‌دهد. قوانین سنتی و ثابت توانایی پاسخگویی به سرعت تحولات فناوری را ندارند و همین امر موجب می‌شود تا مجرمان از شکاف‌های قانونی سوءاستفاده کنند. علاوه بر این، ناهماهنگی میان نهادهای مختلف از پلیس و دستگاه قضایی گرفته تا وزارتخانه‌های مرتبط سبب ائتلاف منابع و کاهش کارآمدی پاسخ‌ها می‌شود. بنابراین، اصلاح ساختاری سیاست کیفری و بازنگری مستمر در قوانین و آیین‌نامه‌ها یک ضرورت اجتناب‌ناپذیر است. از منظر جرم‌شناسی، پژوهش تأکید دارد که صرفاً برخورد کیفری نمی‌تواند به تنهایی مانع بروز این پدیده‌ها شود. لازم است رهیافت‌های پیشگیرانه نیز به کار گرفته شوند. پیشگیری اجتماعی از طریق ارتقای سواد رسانه‌ای و آموزش کاربران، و پیشگیری وضعی با تقویت تدابیر فنی و مدیریتی، می‌تواند زمینه بروز جرم را محدود کند. به عبارت دیگر، سیاست کیفری باید هم‌زمان بر دو محور «بازدارندگی از طریق مجازات» و «بازپروری و اصلاح اجتماعی» متمرکز باشد تا به ارتقای تاب‌آوری امنیت داخلی منجر شود.

در یک جمع‌بندی کلی می‌توان گفت که تبلیغات انحرافی و رفتارهای مجرمانه آنلاین یکی از مهم‌ترین تهدیدهای امنیت داخلی در عصر دیجیتال است. مقابله با این تهدید نیازمند ترکیبی از ابزارهای حقوقی، نهادی، فنی و آموزشی است. سیاست کیفری در این مسیر نقش کلیدی دارد، اما تنها در صورتی موفق خواهد بود که با رویکرد جرم‌شناختی و همکاری بین‌المللی تکمیل شود.

ارائه پیشنهادها و راهکارها

۱. بازنگری و به‌روزرسانی مستمر قوانین: تدوین مقررات جامع و انعطاف‌پذیر که بتواند با سرعت تحولات فناوری و ظهور جرایم نوین همگام شود؛
۲. تقویت هماهنگی نهادی: ایجاد سازوکارهای مشترک میان دستگاه قضایی، پلیس سایبری، وزارتخانه‌های مرتبط و نهادهای امنیتی برای جلوگیری از موازی‌کاری؛
۳. گسترش همکاری‌های بین‌المللی: پیوستن به معاهدات بین‌المللی و استفاده از تجارب جهانی برای مقابله مؤثر با جرایم فراملی؛
۴. ارتقای سواد رسانه‌ای عمومی: آموزش شهروندان در زمینه شناسایی اخبار جعلی، تبلیغات



انحرافی و روش‌های کلاهبرداری آنلاین؛

۵. توسعه زیرساخت‌های فنی: سرمایه‌گذاری در ابزارهای هوش مصنوعی و سامانه‌های پایش هوشمند برای شناسایی و حذف سریع محتوای مجرمانه؛
۶. اتخاذ سیاست‌های بازپرورانه: به‌جای تمرکز صرف بر مجازات، طراحی برنامه‌های اصلاحی و بازپرورانه برای مجرمان سایبری جهت کاهش تکرار جرم؛
۷. ایجاد چارچوب‌های شفاف حقوق شهروندی: توجه هم‌زمان به امنیت و آزادی‌های مشروع کاربران برای افزایش اعتماد عمومی به سیاست‌های مقابله‌ای.



فهرست منابع

۱. بختیاری، تقی؛ درویشی، علی اکبر؛ عبدالرحمانی، رضا و عبادی نژاد، علی. (۱۴۰۳). «طرح راهبردی بازنمایی پلیس از جرم در فضای مجازی با رویکرد پیشگیری اجتماعی». *آموزش علوم دریایی*، ۱۱(۴)، ۲۲۰-۲۳۶.
۲. پاسبان، ابوالفضل. (۱۴۰۲). «حاکمیت حقوقی دولت‌ها بر فضای مجازی و تأثیر آن بر امنیت ملی». *سیاست دفاعی*، ۳۲(۱۲۵)، ۱۱-۴۸.
۳. زارعی، قاسم و نیکخواه، یونس. (۱۴۰۳). «ارائه الگوی ضدبازاریابی جهت پیشگیری از رفتارهای مجرمانه در فضای کسب و کارهای آنلاین و دیجیتالی». *مدیریت بازرگانی*، ۱۶(۶۰)، ۳۴۹-۳۸۷.
۴. سپهری، بهروز؛ کارگر، نوروز؛ آشوری، محمد و قاسمی، قاسم. (۱۴۰۳). «واکاوی سیاست کیفی مقابله با تروریسم محیط زیستی با تأکید بر تمهیدات بازدارنده». *محیط زیست و توسعه فرابخشی*، ۱۱۷-۹۹، (۸۵).
۵. شعبانی، میثم. (۱۴۰۳). *تحلیل چگونگی کیفرگذاری جرم‌های مشابه در قانون جرایم رایانه‌ای و قانون تعزیرات*. تهران: دادیار.
۶. کاپورو، رافائل. (۱۴۰۴). *اخلاق اطلاعات و فضای مجازی*. ترجمه محمد خندان، تهران: سوره مهر.
۷. کاستلز، مانوئل. (۱۴۰۴). *ارتباطات موبایلی و جامعه*. ترجمه سعیده فراهانی، تهران: خزه.
۸. مهربانی، داود و میرمجیدی، سپیده. (۱۴۰۳). «پیش‌بینی‌پذیری بروز رفتارهای پرخطر و مجرمانه بزهکاران کانون اصلاح و تربیت شهر تهران؛ با تأکید بر نقش رسانه‌های اجتماعی». *جامعه پژوهی فرهنگی*، ۱۱۵(۱)، ۲۴۹-۲۱۹.
۹. وندنهارک، ماری. (۱۴۰۳). *ارتباطات بحران در رسانه‌های اجتماعی*. ترجمه عباس رضایی، چاپ سوم، تهران: ثانیه.
10. Akinbowale, O., Zerihun, M., and Mashigo, P. (2024). Application of Situational Crime Prevention Framework for Cybercrime Mitigation. *International Journal of Cyber Behavior, Psychology and Learning*, 14(1), 1-23.
11. Bandura, A. (2022). *Social Learning Theory*. New York: Prentice-Hall.
12. Botchkovar, E., Cui, K., Antonaccio, O., Perkins, R., and Maimon, D. (2025). The organized activities of ransomware groups: A social network approach. *Journal of Technology in Society*, (82), 46-66.



13. Button, M. (2025). An Anatomy of 'Pig Butchering Scams': Chinese Victims' and Police Officers' Perspectives. *Journal of Deviant Behavior*, 36(1), 52-77.
14. Di Nicola, A. (2022). Towards digital organized crime and digital sociology of organized crime. *Journal of Trends in Organized Crime*, 44(2), 686-704.
15. Hakmeh, J. (2024). The UN convention on cybercrime: a milestone in cybercrime cooperation. *Journal of Cyber Policy*, 9(2), 125-130.
16. Hiruni, C. (2024). Psychological Warfare in the Digital Age: The Role of Cyber Operations in Modern PsyOps. *Journal of Law and Security Review*, 26(2), 34-52.
17. Johnson, B. (2025). Using global security assemblages to combat transnational organized crime. *Journal of Economic Criminology*, (7), 120-141.
18. Kala, E. (2024). Influence of Online Platforms on Criminal Behavior. *International Journal of Research Studies in Computer Science and Engineering*, 10(1), 25-37
19. Karp, R. (2024). *Ontological Security-Seeking: National Identities under Stress*. London: Routledge.
20. Kelley, N., Hurley-Wallace, A., Warner, K., and Hanoch, Y. (2023). Analytical reasoning reduces internet fraud susceptibility. *Journal of Computers in Human Behavior*, (142), 312-330.
21. Lan, Y., Qiyang, C., and Sixin, L. (2024). Study on International Cooperation to Address Cross-border Telecommunication Network Fraud Offence. *Journal of Politics and Law*, 17(2), 44-63.
22. Lin, X., Wu, W., Lan, H., and Ma, Y. (2024). The impact of anti-organized crime on business environment: Evidence from China's anti-Mafia campaign. *International Review of Economics & Finance*, (95), 363-385.
23. Luo, K., and Zhao, Y. (2025). Butcher or be butchered: understanding the

- unwitting recruitment by cybercrime groups in China. *Journal of Trends in Organized Crime*, 28(3), 65-89.
24. Menet, S. (2025). *Policing Beyond Borders: China's Law-Enforcement Expansion in the Mekong Region*. London: SAGE.
25. Merton, R. (2022). *Social Theory and Social Structure*. New York: Macmillan
26. Onwuadiamu, G. (2025). Cybercrime in criminology; A systematic review of criminological theories, methods, and concepts. *Journal of Journal of Economic Criminology*, (8), 28-47.
27. Sema Admass, W., Yayeh Munaye, Y., & Abeshu Diro, A. (2024). Cyber security: State of the art, challenges and future directions. *Journal of Cyber Security and Applications*, (2), 241-259.
28. Stadnicki, I., Corsini, M., and Szulkin, M. (2024). Application of criminology in urban ecology and evolution: Routine Activity Theory and field equipment disappearance dynamics. *Journal of Ecological Indicators*, (165), 1-23.
29. Teichmann F. (2023). Ransomware attacks in the context of generative artificial intelligence—an experimental study. *International Journal of Cybersecurity Law Review*, 46(4), 399-414.
30. Van Berkel, S., Kleemans, E., and Mooij, A. (2025). Social media and organizing violent crime against persons and properties: a qualitative analysis of online criminal communication between young offenders based on seized telephone information. *Journal of Trends in Organized Crime*, 28(4), 186-212.
31. Vishwakarma, R. (2024). Online Advertising and Fraud Click in Online Advertisement: A Survey. *International Journal of Computer Applications*, 186(1), 1-8.
32. Wang, J., and Zhang, X. (2023). The Reinforcements and Punishments in Social Media Addiction. *Journal of Education Humanities and Social*





Sciences, (8), 1460-1483.

33. Wei, X. (2024). Rule of law or not? A critical evaluation of legal responses to cyberterrorism in the UK. *Journal of Computer Law & Security Review*, (53), 312-330.
34. Wei, S., and Pan, F. (2024). The geographical embeddedness of organised crime in China: A rural–urban divide perspective. *Journal of Criminology & Criminal Justice*, 57(1), 317-343.
35. Whelan, C., Bright, D., and Martin, J. (2023). Reconceptualising organised (cyber)crime: The case of ransomware. *Journal of Criminology*, 57(1), 317-343.