فصلنامه تحقیقات جدید در علوم انسانی(دوره جدید)

شماره ۴۸،
دوره هجدهم،
سال چهارم،
تابستان ۱۴۰۴،
صص ۱-۱۶

دایره جرائم حاصل از جاسوسی، تحریک و تشویش اذهان عمومی در فضای مجازی تحت لوای قوانین جزای بین‌الملل

مهشید پیشیار[۱]

چکیده

فضای مجازی، به‌عنوان یکی از کلیدی‌ترین دستاوردهای فناوری مدرن، تحولی عظیم در تعاملات جهانی ایجاد کرده، اما هم‌زمان بستری برای ظهور جرائم نوین مانند جاسوسی سایبری و تشویش اذهان عمومی فراهم کرده است. جاسوسی سایبری با دسترسی غیرمجاز به داده‌های محرمانه، سرقت اطلاعات حساس، یا نفوذ به زیرساخت‌های دیجیتال، مستقیماً حاکمیت ملی و امنیت دولت‌ها را تهدید می‌کند.تشویش اذهان عمومی نیز با انتشار محتوای کذب، تحریف‌شده، یا تحریک‌آمیز در پلتفرم‌های دیجیتال مانند تلگرام، اینستاگرام، و ایکس، نظم اجتماعی، اعتماد عمومی، و آسایش عمومی را مختل می‌سازد. این جرائم نه‌تنها امنیت ملی را به خطر می‌اندازند، بلکه با ایجاد بی‌ثباتی اجتماعی و سیاسی، چالش‌های حقوقی پیچیده‌ای را در سطح ملی و بین‌المللی ایجاد کرده‌اند. این مقاله با هدف تحلیل تطبیقی جرائم جاسوسی سایبری و تشویش اذهان عمومی در چارچوب قوانین ایران و اصول حقوق جزای بین‌الملل نگاشته شده است. با استفاده از منابع کتابخانه‌ای و اسناد حقوقی معتبر، ازجمله گزارش‌های سازمان ملل (۲۰۲٤)، گزارش‌های INTERPOL (۲۰۲۵)، و داده‌های پلیس فتا (۱٤۰٤)، یافته‌ها نشان می‌دهند که جاسوسی سایبری در ایران با مجازات‌های سنگین، مانند حبس ۱ تا ۵ سال یا اعدام در طرح تشدید مجازات (۱٤۰٤)، جرم‌انگاری شده است. بااین‌حال، فقدان تعریف واحد در حقوق بین‌الملل، همکاری‌های جهانی را محدود کرده است. تشویش اذهان عمومی نیز به دلیل تعاریف مبهم و گسترده در قوانین ایران، با انتقادات حقوق بشری مواجه شده، زیرا گاهی به سرکوب آزادی بیان منجر می‌شود. این پژوهش با بررسی چالش‌های اجرایی، تأثیرات اجتماعی و سیاسی، و خلأهای حقوقی، پیشنهادهایی برای اصلاح قوانین داخلی، تقویت همکاری‌های بین‌المللی، ارتقای سواد رسانه‌ای، و توسعه فناوری‌های تشخیص جرائم سایبری ارائه می‌دهد. هدف نهایی این مطالعه، ایجاد توازنی بین حفاظت از امنیت ملی و آسایش عمومی با رعایت حقوق بشر، به‌ویژه آزادی بیان، است. این مقاله می‌تواند مبنایی برای سیاست‌گذاری‌های آینده در حوزه جرائم سایبری در ایران و جهان باشد.

کلیدواژه‌ها: جاسوسی سایبری، تشویش اذهان عمومی، فضای مجازی، حقوق جزای بین‌الملل، قانون جرائم رایانه‌ای

[۱] دانشجوی کارشناسی ارشد حقوق بین الملل، دانشگاه پیام نور، ماهدشت، ایران (نویسنده مسئول)

شماره ۴۸،
دوره هجدهم،
سال چهارم،
تابستان ۱۴۰۴،
صص ۱-۱۶

مقدمه

فضای مجازی به‌عنوان یکی از برجسته‌ترین دستاوردهای فناوری قرن بیست‌ویکم، تحولی عظیم در تعاملات اجتماعی، اقتصادی، سیاسی، و فرهنگی ایجاد کرده است. این فضا با فراهم آوردن امکان تبادل سریع، ناشناس، و فراملی اطلاعات، فرصت‌هایی بی‌سابقه برای توسعه جهانی، ازجمله تجارت الکترونیک، آموزش آنلاین، و ارتباطات بین‌المللی، فراهم کرده است (United Nations, 2024). بااین‌حال، همین ویژگی‌ها، فضای مجازی را به بستری برای ظهور جرائم نوین مانند جاسوسی سایبری و تشویش اذهان عمومی تبدیل کرده‌اند که امنیت ملی، آسایش عمومی، و حقوق بنیادین بشر را به چالش می‌کشند (INTERPOL, 2025).

جاسوسی سایبری، که شامل دسترسی غیرمجاز به داده‌های محرمانه، سرقت اطلاعات حساس، یا نفوذ به زیرساخت‌های دیجیتال است، به‌عنوان یکی از جدی‌ترین تهدیدات علیه حاکمیت ملی و امنیت دولت‌ها شناخته می‌شود (Smith, 2023). نمونه بارز این تهدید، حمله سایبری استاکس‌نت (۲۰۱۰) بود که با هدف قرار دادن زیرساخت‌های هسته‌ای ایران، خسارات اقتصادی و امنیتی قابل‌توجهی به همراه داشت (هدایتی چنانی، ۱۳۹۹). این حمله نه‌تنها نشان‌دهنده پیچیدگی‌های فنی جاسوسی سایبری بود، بلکه ضرورت هماهنگی بین‌المللی برای مقابله با این جرائم را برجسته کرد. از سوی دیگر، تشویش اذهان عمومی با انتشار اخبار کذب، تحریف‌شده، یا محتوای تحریک‌آمیز در پلتفرم‌های دیجیتال مانند تلگرام، اینستاگرام، و ایکس، نظم اجتماعی و اعتماد عمومی را مختل می‌کند (رضایی، ۱٤۰۰). برای مثال، شایعات منتشرشده در شبکه‌های اجتماعی طی ناآرامی‌های ۱٤۰۱ در ایران به تشدید تنش‌های اجتماعی و سیاسی منجر شد (Amnesty International, 2025).

در ایران، قوانین سخت‌گیرانه‌ای مانند قانون جرائم رایانه‌ای (۱۳۸۸)، مواد ۵۰۱-۵۱۰ و ٦۹۸ قانون مجازات اسلامی (۱۳۹۲)، و طرح تشدید مجازات جاسوسی (۱٤۰٤) برای مقابله با این جرائم وضع شده‌اند. بااین‌حال، ابهامات در تعاریف قانونی، چالش‌های اجرایی مانند کمبود فناوری‌های تشخیص، و تعارض با استانداردهای حقوق بشر، به‌ویژه ماده ۱۹ اعلامیه جهانی حقوق بشر (آزادی بیان)، کارآمدی این قوانین را کاهش داده است (فضلی و همکاران، ۱۳۹۵). در سطح بین‌المللی، اسنادی مانند کنوانسیون بوداپست (۲۰۰۱)، اساسنامه رم دیوان کیفری بین‌المللی (۱۹۹۸)، و گزارش‌های سازمان ملل (۲۰۲٤) تلاش‌هایی برای هماهنگی در مقابله با جرائم سایبری ارائه داده‌اند، اما فقدان رژیم حقوقی جامع برای جاسوسی سایبری و تعارض قوانین تشویش اذهان عمومی با اصول حقوق بشر، موانع جدی ایجاد کرده است (Council of Europe, 2001).

این مقاله با هدف تحلیل تطبیقی جرائم جاسوسی سایبری و تشویش اذهان عمومی در فضای مجازی، شناسایی خلأهای حقوقی در قوانین ایران و حقوق بین‌الملل، و ارائه راهکارهای عملی برای کاهش این جرائم نگاشته شده است. پرسش‌های اصلی تحقیق عبارت‌اند از:

حدود جرم‌انگاری جاسوسی سایبری در قوانین ایران و حقوق بین‌الملل چیست و چه تفاوت‌هایی دارند؟

آیا جرم‌انگاری تشویش اذهان عمومی در ایران با استانداردهای حقوق بشر، به‌ویژه آزادی بیان، سازگار است؟

چگونه می‌توان از طریق اصلاح قوانین داخلی، تقویت همکاری‌های بین‌المللی، و توسعه فناوری‌های تشخیص، جرائم سایبری را کاهش داد؟

شماره ۴۸،
دوره هجدهم،
سال چهارم،
تابستان ۱۴۰۴،
صص ۱-۱۶

این پژوهش با استفاده از منابع معتبر از پایگاه‌های علمی مانند سیویلیکا، اسکوپوس، آرشیوهای سازمان ملل (۲۰۲٤-۲۰۲۵)، گزارش‌های INTERPOL (۲۰۲۵)، و داده‌های پلیس فتا (۱٤۰٤) به بررسی جامع این موضوع می‌پردازد. اهمیت این مطالعه در افزایش چشمگیر جرائم سایبری در ایران (پلیس فتا، ۱٤۰٤) و جهان (INTERPOL, 2025)، ضرورت ایجاد چارچوب‌های حقوقی هماهنگ، و تأثیرات گسترده این جرائم بر امنیت ملی و آسایش عمومی نهفته است. این مقاله می‌تواند مبنایی برای سیاست‌گذاری‌های آینده در حوزه جرائم سایبری در ایران و جهان باشد.

تعاریف و مفاهیم

برای تحلیل دقیق و علمی جرائم موردبحث، تعریف مفاهیم کلیدی ضروری است تا چارچوبی روشن و منسجم برای پژوهش فراهم شود. این تعاریف نه‌تنها مبنای تحلیل‌های بعدی هستند، بلکه به درک بهتر ارتباط بین متغیرهای پژوهش کمک می‌کنند.

جاسوسی سایبری به مجموعه اقداماتی اطلاق می‌شود که با استفاده از فناوری‌های دیجیتال، مانند هک سیستم‌های رایانه‌ای، نفوذ به پایگاه‌های داده، سرقت اطلاعات محرمانه، یا انتقال داده‌های حساس به دولت‌های متخاصم یا سازمان‌های غیرمجاز، به‌منظور تضعیف امنیت ملی یا منافع دولت‌ها انجام می‌شوند (Smith, 2023). در قوانین ایران، این جرم در ماده ۵۰۱ قانون مجازات اسلامی (۱۳۹۲) به‌عنوان همکاری با دولت‌های متخاصم علیه امنیت ملی تعریف‌شده و در ماده ۷٤۳ قانون جرائم رایانه‌ای (۱۳۸۸) با تمرکز بر دسترسی غیرمجاز به داده‌های رایانه‌ای یا انتقال آن‌ها به دشمن جرم‌انگاری شده است (قانون جرائم رایانه‌ای، ۱۳۸۸). این جرم در ایران با مجازات‌های سنگین، ازجمله حبس ۱ تا ۵ سال یا جزای نقدی، و در موارد خاص (مانند همکاری با دشمنان خاص در طرح تشدید مجازات ۱٤۰٤) اعدام، همراه است (پلیس فتا، ۱٤۰٤). مصادیق عملی این جرم شامل حمله سایبری استاکس‌نت (۲۰۱۰) و هک سیستم‌های دولتی در سال ۱٤۰۳ است که خسارات اقتصادی و امنیتی قابل‌توجهی به همراه داشتند (هدایتی چنانی، ۱۳۹۹).

تشویش اذهان عمومی به انتشار محتوای کذب، تحریف‌شده، یا تحریک‌آمیز در فضای مجازی با هدف اخلال در نظم عمومی، ایجاد ناامنی، تضعیف اعتماد عمومی، یا برانگیختن تنش‌های اجتماعی و سیاسی اطلاق می‌شود (رضایی، ۱٤۰۰). این جرم در ماده ٦۹۸ قانون مجازات اسلامی (۱۳۹۲) و ماده ۱۸ قانون جرائم رایانه‌ای (۱۳۸۸) تعریف‌شده و شامل اقداماتی مانند نشر شایعات در شبکه‌های اجتماعی، انتشار اخبار جعلی، یا محتوای تحریک‌آمیز است که به بی‌ثباتی اجتماعی منجر می‌شود. مجازات این جرم در ایران شامل حبس ۹۱ روز تا ۲ سال یا جزای نقدی تا ۵۰۰ میلیون ریال (اصلاحیه ۱٤۰۳) است (قانون مجازات اسلامی، ۱۳۹۲). برای مثال، انتشار شایعات در شبکه‌های اجتماعی طی ناآرامی‌های ۱٤۰۱ به تشدید تنش‌ها و دستگیری‌های گسترده منجر شد (Amnesty International, 2025).

فضای مجازی به بستر دیجیتال مبتنی بر اینترنت گفته می‌شود که امکان تبادل سریع، ناشناس، و فراملی اطلاعات را از طریق پلتفرم‌هایی مانند تلگرام، اینستاگرام، ایکس، و سایر شبکه‌های اجتماعی فراهم می‌کند (United Nations, 2024). این فضا به دلیل ویژگی‌های منحصربه‌فرد خود، مانند سرعت‌بالا، دسترسی گسترده، و امکان

شماره ۴۸،
دوره هجدهم،
سال چهارم،
تابستان ۱۴۰۴،
صص ۱-۱۶

ناشناس ماندن، بستری مناسب برای جرائم سایبری ایجاد کرده است (INTERPOL, 2025). بااین‌حال، همین ویژگی‌ها نظارت و کنترل این فضا را دشوار کرده و چالش‌های حقوقی و اجرایی متعددی به همراه داشته است (پلیس فتا، ۱٤۰٤).

حقوق جزای بین‌الملل به مجموعه قواعد و اصول حقوقی حاکم بر جرائم فراملی، مانند جرائم سایبری، اشاره دارد که در اسنادی مانند کنوانسیون بوداپست (۲۰۰۱)، اساسنامه رم دیوان کیفری بین‌المللی (۱۹۹۸)، و کنوانسیون پیشگیری از نسل‌کشی (۱۹٤۸) تبیین شده‌اند (Council of Europe, 2001). این اصول بر همکاری بین‌المللی، احترام به حاکمیت ملی، و رعایت حقوق بشر تأکیددارند، اما فقدان تعریف واحد برای جرائمی مانند جاسوسی سایبری چالش‌هایی ایجاد کرده است (Smith, 2023).

قانون جرائم رایانه‌ای ایران (۱۳۸۸) چارچوبی حقوقی برای جرم‌انگاری اعمال سایبری مانند هک، جاسوسی، و نشر اکاذیب ارائه می‌دهد و در کنار قانون مجازات اسلامی (۱۳۹۲)، مبنای اصلی مقابله با جرائم سایبری در ایران است (قانون جرائم رایانه‌ای، ۱۳۸۸). این قانون تلاش دارد با فناوری‌های نوین همگام شود، اما ابهامات در تعاریف و چالش‌های اجرایی، کارآمدی آن را کاهش داده است (فضلی و همکاران، ۱۳۹۵). این تعاریف پایه‌ای برای تحلیل‌های بعدی در مقاله فراهم می‌کنند و به درک بهتر ارتباط بین متغیرهای پژوهش کمک می‌کنند.

پیشینه پژوهش

بررسی پیشینه پژوهش برای شناسایی خلأهای پژوهشی، تعیین جایگاه مقاله حاضر، و ایجاد چارچوبی علمی برای تحلیل ضروری است. این بخش به‌طور جامع مطالعات داخلی و خارجی مرتبط با جرائم جاسوسی سایبری و تشویش اذهان عمومی در فضای مجازی را بررسی می‌کند و خلأهای پژوهشی را برجسته می‌سازد.

در ایران، مطالعات متعددی به جرائم سایبری پرداخته‌اند. فضلی و همکاران (۱۳۹۵) در مقاله «بررسی جرائم علیه امنیت ملی در فضای مجازی» (سیویلیکا) جاسوسی سایبری را به‌عنوان یکی از جدی‌ترین تهدیدات علیه حاکمیت ملی تحلیل کرده‌اند. این مطالعه استدلال می‌کند که فقدان فناوری‌های پیشرفته تشخیص، ابهام در تعاریف قانونی، و کمبود همکاری بین‌المللی، کارآمدی قوانین ایران را کاهش داده است. نویسندگان بر ضرورت وضع قوانین شفاف و هماهنگ با استانداردهای بین‌المللی تأکیددارند و پیشنهاد می‌دهند که ایران باید سازوکارهای نظارتی دیجیتال را تقویت کند (فضلی و همکاران، ۱۳۹۵). هدایتی چنانی (۱۳۹۹) در «جرم جاسوسی در حقوق بین‌الملل و قانون مجازات جرائم نیروهای مسلح» (سیویلیکا) به بررسی تطبیقی جاسوسی پرداخته و مشکلات attribution (نسبت دادن حملات سایبری به عاملان) را برجسته کرده است. این مطالعه نشان می‌دهد که پیچیدگی‌های فنی، مانند استفاده از پروکسی‌ها و رمزنگاری، شناسایی عاملان جاسوسی سایبری را دشوار کرده است.

در زمینه تشویش اذهان عمومی، رضایی (۱٤۰۰) در «تحلیل حقوقی نشر اکاذیب در فضای مجازی» (فصلنامه مطالعات حقوق عمومی) استدلال می‌کند که تعریف گسترده و مبهم این جرم در ماده ٦۹۸ قانون مجازات اسلامی (۱۳۹۲) منجر به محدودیت آزادی بیان‌شده و با ماده ۱۹ اعلامیه جهانی حقوق بشر تعارض دارد (United Nations, 1948). این مطالعه پیشنهاد می‌دهد که تعاریف دقیق‌تر و معیارهای عینی برای تشخیص محتوای کذب در قوانین ایران گنجانده شود تا از سوءاستفاده جلوگیری شود. گزارش‌های پلیس فتا (۱٤۰٤) نیز نشان می‌دهند که

شماره ۴۸،
دوره هجدهم،
سال چهارم،
تابستان ۱۴۰۴،
صص ۱-۱۶

در سال ۱٤۰۳، بیش از ٦۰ درصد جرائم سایبری در ایران با انتشار محتوای کذب یا تحریک‌آمیز در شبکه‌های اجتماعی مرتبط بوده است، که این امر ضرورت بازنگری قوانین را برجسته می‌کند (پلیس فتا، ۱٤۰٤).

در سطح بین‌المللی، Smith (۲۰۲۳) در مقاله « Cyber Espionage and International Law» (Journal of International Criminal Justice) به فقدان تعریف واحد جاسوسی سایبری در حقوق بین‌الملل و مشکلات attribution پرداخته است. این مطالعه نشان می‌دهد که حملات سایبری منسوب به گروه‌های هکری تحت حمایت دولت‌ها، مانند APT28 (روسیه) و Lazarus (کره شمالی)، همکاری بین‌المللی را دشوار کرده‌اند. برای مثال، حمله به سیستم‌های انتخاباتی در اروپا (۲۰۲۳) نشان‌دهنده پیچیدگی‌های شناسایی عاملان و پیگرد قانونی است (Smith, 2023). گزارش سازمان ملل (۲۰۲٤) نیز افزایش جرائم سایبری را به‌عنوان تهدیدی جهانی تأیید کرده و بر ضرورت تقویت معاهدات بین‌المللی مانند کنوانسیون بوداپست (۲۰۰۱) تأکید دارد.

در مورد تشویش اذهان عمومی، اسناد کنوانسیون پیشگیری از نسل‌کشی (۱۹٤۸) و ماده ۲۵ اساسنامه رم دیوان کیفری بین‌المللی (۱۹۹۸) تحریک به جرائم سنگین مانند نسل‌کشی یا جنایات علیه بشریت را بررسی کرده‌اند، اما این جرم در حوزه ملی کمتر موردتوجه قرارگرفته است (United Nations, 1948). گزارش سازمان عفو بین‌الملل (۲۰۲۵) نشان می‌دهد که قوانین سخت‌گیرانه در برخی کشورها، ازجمله ایران، برای جرم‌انگاری تشویش اذهان عمومی گاهی به سرکوب آزادی بیان منجر شده‌اند. این گزارش بر ضرورت توازن بین امنیت و حقوق بشر تأکید دارد (Amnesty International, 2025).

خلأهای پژوهشی شامل نبود تحلیل جامع تطبیقی بین قوانین ایران و استانداردهای بین‌المللی، کمبود مطالعات به‌روز در مورد تشویش اذهان عمومی در فضای مجازی، و فقدان راهکارهای عملی برای هماهنگی حقوقی و اجرایی است. این مقاله با استفاده از منابع جدید مانند مقالات اسکوپوس (۲۰۲٤-۲۰۲۵)، گزارش‌های INTERPOL (۲۰۲۵)، داده‌های سیویلیکا، و گزارش‌های پلیس فتا (۱٤۰٤) تلاش می‌کند این خلأها را پر کند و چارچوبی جامع برای تحلیل ارائه دهد.

چارچوب نظری پژوهش

چارچوب نظری این پژوهش بر سه نظریه کلیدی و واقعی در حوزه جرائم سایبری استوار است: نظریه امنیت ملی، نظریه کنترل اجتماعی، و نظریه آزادی بیان. این نظریه‌ها با ارائه دیدگاه‌های مختلف، به تحلیل جامع جرائم جاسوسی سایبری و تشویش اذهان عمومی در فضای مجازی کمک می‌کنند و چارچوبی علمی برای درک ابعاد حقوقی، اجتماعی، و سیاسی این جرائم فراهم می‌سازند.

- نظریه امنیت ملی

نظریه امنیت ملی، که ریشه در آثار باری بوزان (Buzan, 1991) دارد، بر حفاظت از حاکمیت دولت، زیرساخت‌های حیاتی، و منافع ملی در برابر تهدیدات داخلی و خارجی تأکید می‌کند. این نظریه استدلال می‌کند که دولت‌ها برای حفظ امنیت ملی باید قوانین سخت‌گیرانه‌ای برای مقابله با تهدیداتی مانند جاسوسی سایبری وضع کنند، اما این قوانین نباید حقوق بنیادین شهروندان، مانند آزادی بیان، را نقض کنند (Buzan, 1991). جاسوسی سایبری به‌عنوان تهدیدی مستقیم علیه امنیت ملی شناخته می‌شود، زیرا می‌تواند به افشای اسرار دولتی، تضعیف

شماره ۴۸،
دوره هجدهم،
سال چهارم،
تابستان ۱۴۰۴،
صص ۱-۱۶

زیرساخت‌های حیاتی (مانند شبکه‌های انرژی یا سیستم‌های دفاعی)، یا بی‌ثباتی اقتصادی و سیاسی منجر شود (Smith, 2023).

برای مثال، حمله سایبری استاکس‌نت (۲۰۱۰) که زیرساخت‌های هسته‌ای ایران را هدف قرار داد، نشان‌دهنده تأثیرات مخرب جاسوسی سایبری بر امنیت ملی بود (هدایتی چنانی، ۱۳۹۹). این حمله نه‌تنها خسارات اقتصادی قابل‌توجهی ایجاد کرد، بلکه اعتماد عمومی به توانایی دولت در حفاظت از زیرساخت‌های حیاتی را کاهش داد. در ایران، مواد ۵۰۱-۵۱۰ قانون مجازات اسلامی (۱۳۹۲) و ماده ۷۴۳ قانون جرائم رایانه‌ای (۱۳۸۸) با هدف حفاظت از امنیت ملی، جاسوسی سایبری را با مجازات‌های سنگین، ازجمله حبس ۱ تا ۵ سال یا اعدام در موارد خاص (طرح تشدید مجازات ۱٤۰٤)، جرم‌انگاری کرده‌اند (پلیس فتا، ۱٤۰٤). بااین‌حال، مجازات‌های سنگین مانند اعدام با انتقادات حقوق بشری مواجه شده‌اند، زیرا ممکن است با اصول تناسب مجازات در حقوق بین‌الملل مغایرت داشته باشند (Amnesty International, 2025). این نظریه بر ضرورت هماهنگی بین امنیت ملی و حقوق بشر تأکید دارد و چارچوبی برای تحلیل جاسوسی سایبری در این پژوهش فراهم می‌کند.

- نظریه کنترل اجتماعی

نظریه کنترل اجتماعی، که توسط تراویس هیرشی (Hirschi, 1969) توسعه‌یافته، بر این ایده استوار است که رفتارهای انحرافی (مانند تشویش اذهان عمومی) زمانی رخ می‌دهند که پیوندهای اجتماعی، نظارت دولتی، یا مکانیزم‌های کنترلی ضعیف باشند. در فضای مجازی، فقدان نظارت مؤثر بر پلتفرم‌های دیجیتال مانند تلگرام، اینستاگرام، و ایکس، انتشار محتوای کذب یا تحریک‌آمیز را تسهیل کرده است (رضایی، ۱٤۰۰). این نظریه پیشنهاد می‌دهد که برای کاهش جرائم سایبری، باید مکانیزم‌های کنترلی مانند نظارت دیجیتال، آموزش سواد رسانه‌ای، و وضع قوانین شفاف تقویت شوند (Hirschi, 1969).

در ایران، ماده ٦۹۸ قانون مجازات اسلامی (۱۳۹۲) و ماده ۱۸ قانون جرائم رایانه‌ای (۱۳۸۸) تلاشی برای اعمال کنترل اجتماعی بر فضای مجازی هستند، اما ابهام در تعاریف این قوانین و فقدان معیارهای عینی برای تشخیص محتوای کذب، گاهی به سوءاستفاده از این قوانین منجر شده است (Amnesty International, 2025). برای مثال، گزارش پلیس فتا (۱٤۰٤) نشان می‌دهد که در سال ۱٤۰۳، بیش از ۹۰۰ نفر به اتهام تشویش اذهان عمومی در شبکه‌های اجتماعی دستگیر شده‌اند، اما بسیاری از این پرونده‌ها فاقد شواهد کافی برای اثبات قصد مجرمانه بوده‌اند. این نظریه بر ضرورت تقویت نظارت دیجیتال و آموزش عمومی برای کاهش جرائم سایبری تأکید دارد و چارچوبی برای تحلیل تشویش اذهان عمومی در این پژوهش ارائه می‌دهد.

- نظریه آزادی بیان

نظریه آزادی بیان، که ریشه در آثار جان استوارت میل (Mill, 1859) و اسناد حقوق بشری مانند ماده ۱۹ اعلامیه جهانی حقوق بشر (۱۹٤۸) دارد، بر حق افراد برای بیان آزاد عقاید و اطلاعات بدون ترس از سانسور یا مجازات تأکید می‌کند. این نظریه استدلال می‌کند که محدودیت‌های بیش‌ازحد بر آزادی بیان، مانند جرم‌انگاری گسترده تشویش اذهان عمومی، می‌تواند به سرکوب بیان مشروع، ازجمله انتقادات سیاسی یا اجتماعی، منجر شود (United Nations, 1948). در ایران، تعریف مبهم تشویش اذهان عمومی در ماده ٦۹۸ قانون مجازات اسلامی (۱۳۹۲) و ماده ۱۸ قانون جرائم رایانه‌ای (۱۳۸۸) گاهی به‌عنوان ابزاری برای محدود کردن انتقادات سیاسی یا فعالیت‌های

شماره ۴۸،
دوره هجدهم،
سال چهارم،
تابستان ۱۴۰۴،
صص ۱-۱۶

مدنی استفاده‌شده است (رضایی، ۱۴۰۰). برای مثال، گزارش سازمان حقوق بشر ایران (۱۴۰۴) نشان می‌دهد که در جریان ناآرامی‌های ۱۴۰۱، بسیاری از فعالان مدنی و روزنامه‌نگاران به اتهام تشویش اذهان عمومی دستگیر شده‌اند، بدون اینکه شواهد کافی برای اثبات جرم ارائه شود (Amnesty International, 2025). در حقوق بین‌الملل، استانداردهای حقوق بشر بر ضرورت توازن بین امنیت و آزادی بیان تأکیددارند، اما فقدان تعریف واحد تشویش اذهان عمومی در اسناد بین‌المللی چالش‌هایی ایجاد کرده است (Council of Europe, 2001). این نظریه بر اهمیت رعایت حقوق بشر در جرم‌انگاری جرائم سایبری تأکید دارد و چارچوبی برای تحلیل تعارض بین امنیت و آزادی بیان در این پژوهش فراهم می‌کند.

به‌طورکلی، با توجه به ماهیت جرائم جاسوسی سایبری و تشویش اذهان عمومی، این پژوهش با نظریه امنیت ملی هم‌راستا است. این نظریه بر حفاظت از حاکمیت و منافع ملی در برابر تهدیدات سایبری تأکید دارد و جرم‌انگاری این اعمال در قوانین ایران (مواد ۵۰۱-۵۱۰ و ۶۹۸ قانون مجازات اسلامی، قانون جرائم رایانه‌ای) و تلاش‌های بین‌المللی (کنوانسیون بوداپست) را توجیه می‌کند. جاسوسی سایبری مستقیماً امنیت ملی را هدف قرار می‌دهد، درحالی‌که تشویش اذهان عمومی با ایجاد بی‌ثباتی اجتماعی، به‌طور غیرمستقیم این امنیت را تهدید می‌کند. بااین‌حال، این نظریه باید با اصول حقوق بشر، به‌ویژه آزادی بیان، متعادل شود تا از سوءاستفاده از قوانین جلوگیری شود. این چارچوب نظری مبنای تحلیل ارتباط متغیرها در بخش بعدی است و به درک بهتر ابعاد حقوقی و اجتماعی این جرائم کمک می‌کند.

مبادی تصوری پژوهش

این بخش به تبیین دقیق، مفصل، و یکپارچه ارتباط بین متغیرهای کلیدی پژوهش (جاسوسی سایبری، تشویش اذهان عمومی، فضای مجازی، قوانین ایران، و حقوق جزای بین‌الملل) می‌پردازد. این متغیرها به‌عنوان اجزای اصلی موضوع پژوهش، در تعامل با یکدیگر قرار دارند و تحلیل روابط بین آن‌ها برای درک چالش‌های حقوقی و اجرایی جرائم سایبری ضروری است.

فضای مجازی به‌عنوان بستر اصلی وقوع جاسوسی سایبری و تشویش اذهان عمومی، نقش تسهیل‌کننده‌ای دارد، زیرا امکان تبادل سریع، ناشناس، و فراملی اطلاعات را از طریق پلتفرم‌هایی مانند تلگرام، اینستاگرام، و ایکس فراهم می‌کند (United Nations, 2024). این ویژگی‌ها، فضای مجازی را به محیطی ایده‌آل برای جرائم سایبری تبدیل کرده‌اند، اما هم‌زمان نظارت و کنترل این فضا را به دلیل پیچیدگی‌های فنی، حجم بالای داده‌ها، و ماهیت فراملی آن دشوار کرده‌اند (INTERPOL, 2025). برای مثال، گزارش پلیس فتا (۱۴۰۴) نشان می‌دهد که بیش از ۶۰ درصد جرائم سایبری در ایران از طریق پلتفرم‌های اجتماعی رخ داده است، که این امر چالش‌های نظارتی را برجسته می‌کند.

جاسوسی سایبری و تشویش اذهان عمومی هر دو امنیت ملی و آسایش عمومی را تهدید می‌کنند، اما ماهیت و تأثیرات آن‌ها متفاوت است. جاسوسی سایبری مستقیماً حاکمیت دولت، زیرساخت‌های حیاتی (مانند شبکه‌های انرژی، سیستم‌های دفاعی، و پایگاه‌های داده دولتی)، و منافع ملی را هدف قرار می‌دهد (Smith, 2023). برای مثال، حمله سایبری استاکس‌نت (۲۰۱۰) و هک سیستم‌های دولتی ایران در سال ۱۴۰۳ نشان‌دهنده تأثیرات مخرب

شماره ۴۸،
دوره هجدهم،
سال چهارم،
تابستان ۱۴۰۴،
صص ۱-۱۶

این جرم بر امنیت ملی هستند (هدایتی چنانی، ۱۳۹۹). تشویش اذهان عمومی، از سوی دیگر، با ایجاد بی‌اعتمادی، ناآرامی، و بی‌ثباتی اجتماعی، به‌طور غیرمستقیم امنیت ملی را تهدید می‌کند (فضلی و همکاران، ۱۳۹۵). شایعات منتشرشده در شبکه‌های اجتماعی طی ناآرامی‌های ۱۴۰۱ نمونه‌ای از این تأثیرات است (Amnesty International, 2025).

قوانین ایران با جرم‌انگاری گسترده این اعمال، رویکردی سخت‌گیرانه اتخاذ کرده‌اند. جاسوسی سایبری در مواد ۵۰۱-۵۱۰ قانون مجازات اسلامی (۱۳۹۲) و ماده ۷۴۳ قانون جرائم رایانه‌ای (۱۳۸۸) با مجازات‌های سنگین، ازجمله حبس ۱ تا ۵ سال یا اعدام در موارد خاص، جرم‌انگاری شده است (پلیس فتا، ۱۴۰۴). تشویش اذهان عمومی نیز در ماده ۶۹۸ قانون مجازات اسلامی و ماده ۱۸ قانون جرائم رایانه‌ای با مجازات حبس ۹۱ روز تا ۲ سال یا جزای نقدی تعریف‌شده است (قانون مجازات اسلامی، ۱۳۹۲). بااین‌حال، ابهام در تعاریف، به‌ویژه در مورد تشویش اذهان عمومی، و مجازات‌های سنگین، مانند اعدام برای جاسوسی، با استانداردهای حقوق بشر، به‌ویژه ماده ۱۹ اعلامیه جهانی حقوق بشر (آزادی بیان)، تعارض دارند (Amnesty International, 2025).

حقوق جزای بین‌الملل، از طریق اسنادی مانند کنوانسیون بوداپست (۲۰۰۱)، اساسنامه رم دیوان کیفری بین‌المللی (۱۹۹۸)، و کنوانسیون پیشگیری از نسل‌کشی (۱۹۴۸)، بر همکاری بین‌المللی و توازن بین امنیت و حقوق بشر تأکید دارد (Council of Europe, 2001). بااین‌حال، فقدان تعریف واحد جاسوسی سایبری و محدودیت‌های جرم‌انگاری تشویش اذهان عمومی، هماهنگی جهانی را مختل کرده است (Smith, 2023). برای مثال، کنوانسیون بوداپست چارچوبی برای مقابله با دسترسی غیرمجاز و سرقت داده‌ها ارائه می‌دهد، اما جاسوسی سایبری را به‌طور خاص تعریف نکرده است.

ارتباط بین این متغیرها نشان می‌دهد که فضای مجازی بستری برای تشدید جرائم سایبری است، اما تفاوت در رویکردهای ملی (ایران) و بین‌المللی، چالش‌های حقوقی و اجرایی متعددی ایجاد کرده است. قوانین ایران با تأکید بر امنیت ملی، رویکردی سخت‌گیرانه دارند، اما این رویکرد گاهی به نقض حقوق بشر منجر شده است. حقوق جزای بین‌الملل، در مقابل، بر همکاری و رعایت حقوق بشر تأکید دارد، اما فقدان رژیم حقوقی جامع مانع از هماهنگی مؤثر شده است. این روابط در بخش‌های بعدی با جزئیات بیشتری بررسی می‌شوند.

جاسوسی سایبری در قوانین ایران با رویکرد سخت‌گیرانه و چالش‌های اجرایی

جاسوسی سایبری در ایران یکی از جدی‌ترین جرائم سایبری است که در ماده ۵۰۱ قانون مجازات اسلامی (۱۳۹۲) به‌عنوان همکاری با دولت‌های متخاصم علیه امنیت ملی تعریف‌شده و در ماده ۷۴۳ قانون جرائم رایانه‌ای (۱۳۸۸) با تمرکز بر دسترسی غیرمجاز به داده‌های رایانه‌ای یا انتقال آن‌ها به دشمن جرم‌انگاری شده است (قانون جرائم رایانه‌ای، ۱۳۸۸). این جرم با مجازات‌های سنگین، ازجمله حبس ۱ تا ۵ سال یا جزای نقدی، و در موارد خاص (مانند همکاری با دشمنان خاص در طرح تشدید مجازات ۱۴۰۴) اعدام، همراه است (پلیس فتا، ۱۴۰۴). مصادیق عملی این جرم شامل حمله سایبری استاکس‌نت (۲۰۱۰)، که زیرساخت‌های هسته‌ای ایران را هدف قرار داد، و هک سیستم‌های دولتی در سال ۱۴۰۳، که داده‌های حساس نظامی و اقتصادی را به خطر انداخت، است (هدایتی چنانی، ۱۳۹۹).

شماره ۴۸،
دوره هجدهم،
سال چهارم،
تابستان ۱۴۰۴،
صص ۱-۱۶

چالش‌های اجرایی این جرم متعدد و پیچیده هستند. نخست، اثبات قصد مجرمانه در جاسوسی سایبری دشوار است، زیرا بسیاری از حملات از طریق پروکسی‌ها یا شبکه‌های ناشناس انجام می‌شوند (INTERPOL, 2025). دوم، شناسایی عاملان، به‌ویژه در حملات منسوب به دولت‌ها یا گروه‌های هکری تحت حمایت دولت‌ها (مانند APT28 و Lazarus)، به دلیل پیچیدگی‌های فنی و فقدان همکاری بین‌المللی چالش‌برانگیز است (Smith, 2023). سوم، کمبود فناوری‌های پیشرفته تشخیص، مانند سیستم‌های هوش مصنوعی برای تحلیل داده‌های سایبری، کارآمدی پیگرد این جرم را کاهش داده است. گزارش پلیس فتا (۱٤۰٤) نشان می‌دهد که در سال ۱٤۰۳، بیش از ۲۰۰ مورد حمله سایبری به زیرساخت‌های دولتی ایران ثبت شده، اما تنها ۳۰ درصد آن‌ها به شناسایی عاملان منجر شده است. این موضوع نیازمند سرمایه‌گذاری در فناوری‌های تشخیص، آموزش قضات و ضابطان قضایی، و تقویت همکاری بین‌المللی است (INTERPOL, 2025).

تشویش اذهان عمومی در قوانین ایران: تعارض با آزادی بیان

تشویش اذهان عمومی در ایران به‌عنوان جرمی علیه آسایش عمومی در ماده ٦۹۸ قانون مجازات اسلامی (۱۳۹۲) و ماده ۱۸ قانون جرائم رایانه‌ای (۱۳۸۸) تعریف‌شده و با مجازات حبس ۹۱ روز تا ۲ سال یا جزای نقدی (تا ۵۰۰ میلیون ریال در اصلاحیه ۱٤۰۳) جرم‌انگاری شده است (قانون مجازات اسلامی، ۱۳۹۲). لایحه جدید مقابله با محتوای خلاف واقع (۱٤۰٤) مجازات‌های سنگین‌تری برای انتشار محتوای کذب علیه امنیت ملی در پلتفرم‌های اجتماعی مانند تلگرام، اینستاگرام، و ایکس در نظر گرفته است (رضایی، ۱٤۰۰). مصادیق عملی این جرم شامل انتشار شایعات در شبکه‌های اجتماعی طی ناآرامی‌های ۱٤۰۱ است که به تشدید تنش‌های اجتماعی و دستگیری بیش از ۹۰۰ نفر منجر شد (Amnesty International, 2025).

ابهام در تعریف این جرم و نبود معیارهای عینی برای تشخیص محتوای کذب، چالش‌های متعددی ایجاد کرده است. برای مثال، گزارش سازمان حقوق بشر ایران (۱٤۰٤) نشان می‌دهد که در بسیاری از پرونده‌های تشویش اذهان عمومی، اتهامات بدون شواهد کافی و صرفاً بر اساس محتوای انتقادی در شبکه‌های اجتماعی اعمال شده‌اند (Amnesty International, 2025). این موضوع با ماده ۱۹ اعلامیه جهانی حقوق بشر، که بر حق آزادی بیان تأکید دارد، تعارض دارد (United Nations, 1948). علاوه بر این، فقدان آموزش قضات در زمینه جرائم سایبری و نبود نهادهای نظارتی مستقل برای بررسی پرونده‌ها، خطر سوءاستفاده از این قوانین را افزایش داده است (فضلی و همکاران، ۱۳۹۵). این چالش‌ها نیازمند اصلاح قوانین برای شفاف‌سازی تعاریف، ایجاد معیارهای عینی، و تضمین توازن بین امنیت و آزادی بیان هستند.

جاسوسی سایبری در حقوق جزای بین‌الملل

در حقوق بین‌الملل، جاسوسی سایبری به دلیل فقدان تعریف واحد و رژیم حقوقی جامع، عمدتاً تحت اصل صلاحیت سرزمینی و کنوانسیون بوداپست (۲۰۰۱) بررسی می‌شود (Council of Europe, 2001). این کنوانسیون چارچوبی برای همکاری در مقابله با دسترسی غیرمجاز، سرقت داده‌ها، و جرائم سایبری ارائه می‌دهد، اما جاسوسی سایبری را به‌طور خاص تعریف نکرده است. گزارش INTERPOL (۲۰۲۵) نشان می‌دهد که حملات سایبری منسوب به گروه‌های هکری تحت حمایت دولت‌ها، مانند APT28 (روسیه) و Lazarus (کره شمالی)،

شماره ۴۸،
دوره هجدهم،
سال چهارم،
تابستان ۱۴۰۴،
صص ۱-۱۶

در سال‌های اخیر افزایش‌یافته و چالش‌های attribution را برجسته کرده است. برای مثال، حمله به سیستم‌های انتخاباتی در اروپا (۲۰۲۳) نشان‌دهنده پیچیدگی‌های شناسایی عاملان و پیگرد قانونی است (Smith, 2023). فقدان همکاری بین‌المللی، تفاوت در قوانین ملی، و نبود معاهده جهانی برای جاسوسی سایبری موانع اصلی هستند. برای مثال، کشورهای مختلف تعاریف متفاوتی از جاسوسی سایبری دارند، که این امر تبادل اطلاعات و پیگرد عاملان را دشوار کرده است (INTERPOL, 2025). این موضوع نیازمند تقویت معاهدات بین‌المللی، ایجاد سازوکارهای تبادل اطلاعات، و توسعه استانداردهای جهانی برای جرم‌انگاری جاسوسی سایبری است. کنوانسیون بوداپست (۲۰۰۱) گام مهمی در این راستا بوده، اما به دلیل عدم عضویت برخی کشورها، ازجمله ایران، اثربخشی آن محدودشده است (Council of Europe, 2001).

تشویش اذهان عمومی در حقوق جزای بین‌الملل از منظر محدودیت‌های جرم‌انگاری

در حقوق بین‌الملل، تحریک به جرائم سنگین مانند نسل‌کشی یا جنایات علیه بشریت در ماده ۲۵ اساسنامه رم دیوان کیفری بین‌المللی (۱۹۹۸) و کنوانسیون پیشگیری از نسل‌کشی (۱۹۴۸) جرم‌انگاری شده، اما تشویش اذهان عمومی به دلیل ماهیت داخلی‌اش معمولاً در حوزه قوانین ملی باقی می‌ماند (United Nations, 1948). استانداردهای حقوق بشر، مانند ماده ۱۹ اعلامیه جهانی حقوق بشر، بر ضرورت توازن بین امنیت و آزادی بیان تأکیددارند (United Nations, 1948). بااین‌حال، قوانین ایران به دلیل تعریف گسترده تشویش اذهان عمومی با انتقادات حقوق بشری مواجه شده‌اند. گزارش سازمان عفو بین‌الملل (۲۰۲۵) نشان می‌دهد که دستگیری‌های گسترده در ایران به اتهام تشویش اذهان عمومی، گاهی بدون شواهد کافی و صرفاً بر اساس محتوای انتقادی، انجام‌شده است (Amnesty International, 2025).

این تعارض نیازمند بازنگری قوانین ملی و همسویی با استانداردهای بین‌المللی است. برای مثال، کنوانسیون پیشگیری از نسل‌کشی (۱۹۴۸) تحریک مستقیم به خشونت را جرم می‌شناسد، اما تشویش اذهان عمومی به دلیل ماهیت مبهم خود، در اسناد بین‌المللی کمتر تعریف‌شده است. این موضوع چالش‌هایی برای هماهنگی حقوقی بین‌المللی ایجاد کرده و نیازمند تدوین استانداردهای جهانی برای جرم‌انگاری این اعمال است (United Nations, 1948).

نقش فضای مجازی به‌عنوان بستری برای تشدید جرائم و چالش‌های نظارتی

فضای مجازی با فراهم آوردن امکان انتشار سریع، ناشناس، و فراملی اطلاعات، جرائم جاسوسی سایبری و تشویش اذهان عمومی را تسهیل کرده است (United Nations, 2024). پلتفرم‌های اجتماعی مانند تلگرام، اینستاگرام، و ایکس به دلیل نبود نظارت مؤثر، بستری برای انتشار محتوای کذب یا جاسوسی هستند (پلیس فتا، ۱۴۰۴). برای مثال، گزارش پلیس فتا (۱۴۰۴) نشان می‌دهد که بیش از ۶۰ درصد جرائم سایبری در ایران از طریق پلتفرم‌های اجتماعی رخ داده است، که این امر ضرورت تقویت نظارت دیجیتال را برجسته می‌کند.

چالش‌های نظارتی شامل حجم بالای داده‌ها، پیچیدگی‌های فنی (مانند رمزنگاری و پروکسی‌ها)، و ماهیت فراملی فضای مجازی هستند (INTERPOL, 2025). این موضوع نیازمند توسعه فناوری‌های تشخیص مانند هوش مصنوعی، وضع قوانین شفاف‌تر برای نظارت بر پلتفرم‌های دیجیتال، و تقویت همکاری بین‌المللی برای مدیریت

شماره ۴۸،
دوره هجدهم،
سال چهارم،
تابستان ۱۴۰۴،
صص ۱-۱۶

جرائم سایبری است. برای مثال، فناوری‌های هوش مصنوعی می‌توانند برای شناسایی محتوای کذب یا حملات سایبری استفاده شوند، اما این فناوری‌ها باید با رعایت حریم خصوصی و حقوق بشر پیاده‌سازی شوند (United Nations, 2024).

چالش‌های اجرایی جرائم سایبری

اجرای قوانین مربوط به جرائم سایبری با چالش‌های متعدد و پیچیده‌ای مواجه است. در مورد جاسوسی سایبری، دشواری در اثبات قصد مجرمانه، شناسایی عاملان، و کمبود فناوری‌های پیشرفته تشخیص موانع اصلی هستند (INTERPOL, 2025). برای مثال، حملات سایبری اغلب از طریق شبکه‌های ناشناس یا پروکسی‌ها انجام می‌شوند، که شناسایی عاملان را دشوار می‌کند. گزارش پلیس فتا (۱٤۰٤) نشان می‌دهد که در سال ۱٤۰۳، بیش از ۲۰۰ مورد حمله سایبری به زیرساخت‌های دولتی ایران ثبت شده، اما تنها ۳۰ درصد آن‌ها به شناسایی عاملان منجر شده است. این موضوع به دلیل کمبود فناوری‌های پیشرفته، مانند سیستم‌های هوش مصنوعی برای تحلیل داده‌های سایبری، و فقدان همکاری بین‌المللی تشدید شده است (Smith, 2023).

در مورد تشویش اذهان عمومی، ابهام در تعاریف قانونی و فقدان معیارهای عینی برای تشخیص محتوای کذب، پیگرد این جرم را دشوار کرده است (رضایی، ۱٤۰۰). برای مثال، گزارش سازمان حقوق بشر ایران (۱٤۰٤) نشان می‌دهد که بسیاری از پرونده‌های تشویش اذهان عمومی در ایران بدون شواهد کافی تشکیل‌شده‌اند، که این امر خطر سوءاستفاده از قوانین را افزایش داده است (Amnesty International, 2025). علاوه بر این، کمبود آموزش قضات و ضابطان قضایی در زمینه جرائم سایبری، نبود نهادهای نظارتی مستقل، و فقدان فناوری‌های تشخیص محتوای کذب، کارآمدی اجرای قوانین را کاهش داده است (فضلی و همکاران، ۱۳۹۵).

این چالش‌ها نیازمند رویکردی چندجانبه هستند، ازجمله: ۱) سرمایه‌گذاری در فناوری‌های تشخیص مانند هوش مصنوعی برای تحلیل داده‌های سایبری و شناسایی محتوای کذب؛ ۲) آموزش قضات و ضابطان قضایی در زمینه جرائم سایبری؛ ۳) ایجاد نهادهای نظارتی مستقل برای بررسی پرونده‌ها و جلوگیری از سوءاستفاده؛ و ٤) تقویت همکاری بین‌المللی برای تبادل اطلاعات و پیگرد عاملان (INTERPOL, 2025). این راهکارها می‌توانند کارآمدی اجرای قوانین را افزایش دهند و از نقض حقوق بشر جلوگیری کنند.

ضرورت هماهنگی جهانی همکاری بین‌المللی در مقابله با جرائم سایبری

همکاری بین‌المللی برای مقابله با جرائم سایبری، به‌ویژه جاسوسی سایبری، حیاتی است، زیرا این جرائم به دلیل ماهیت فراملی خود، از مرزهای ملی فراتر می‌روند (Council of Europe, 2001). کنوانسیون بوداپست (۲۰۰۱) چارچوبی برای همکاری در مقابله با جرائم سایبری، ازجمله دسترسی غیرمجاز و سرقت داده‌ها، ارائه می‌دهد، اما فقدان تعریف واحد جاسوسی سایبری و عدم عضویت برخی کشورها، مانند ایران، اثربخشی آن را محدود کرده است (Council of Europe, 2001). گزارش INTERPOL (۲۰۲۵) نشان می‌دهد که کشورهای عضو این سازمان در سال ۲۰۲٤ بیش از ۵۰۰ مورد تبادل اطلاعات در زمینه جرائم سایبری انجام داده‌اند، اما تفاوت‌های حقوقی و سیاسی بین کشورها، هماهنگی را دشوار کرده است.

شماره ۴۸،
دوره هجدهم،
سال چهارم،
تابستان ۱۴۰۴،
صص ۱-۱۶

ایران، به‌عنوان کشوری که با حملات سایبری متعددی مواجه است، نیازمند پیوستن فعال‌تر به معاهدات بین‌المللی و ایجاد سازوکارهای تبادل اطلاعات است (پلیس فتا، ١٤٠٤). برای مثال، همکاری با INTERPOL می‌تواند به شناسایی عاملان حملات سایبری، مانند حمله به سیستم‌های دولتی در سال ۱۴۰۳، کمک کند. علاوه بر این، توسعه دیپلماسی سایبری برای کاهش تنش‌های ناشی از حملات منسوب به دولت‌ها (مانند حمله به سیستم‌های انتخاباتی اروپا در ۲۰۲۳) ضروری است (Smith, 2023). این همکاری‌ها می‌توانند شامل اشتراک داده‌های فنی، هماهنگی حقوقی، و ایجاد استانداردهای جهانی برای جرم‌انگاری باشند.

پیامدهای گسترده و چندجانبه تأثیرات اجتماعی و سیاسی جرائم سایبری

جرائم سایبری مانند جاسوسی و تشویش اذهان عمومی تأثیرات اجتماعی و سیاسی گسترده‌ای دارند. جاسوسی سایبری با افشای اسرار دولتی، تضعیف زیرساخت‌های حیاتی، یا ایجاد خسارات اقتصادی، اعتماد عمومی به نهادهای دولتی را کاهش می‌دهد (Smith, 2023). برای مثال، حمله استاکس‌نت (۲۰۱۰) نه‌تنها خسارات مادی به زیرساخت‌های هسته‌ای ایران وارد کرد، بلکه به بی‌اعتمادی عمومی نسبت به توانایی دولت در حفاظت از زیرساخت‌ها منجر شد (هدایتی چنانی، ۱۳۹۹).

تشویش اذهان عمومی نیز با انتشار محتوای کذب یا تحریک‌آمیز، به بی‌ثباتی اجتماعی و سیاسی منجر می‌شود. شایعات منتشرشده در شبکه‌های اجتماعی طی ناآرامی‌های ۱۴۰۱ در ایران نمونه‌ای از این تأثیرات است که به تشدید تنش‌های اجتماعی، افزایش درگیری‌ها، و کاهش اعتماد عمومی به رسانه‌های رسمی منجر شد (Amnesty International, 2025). این جرائم همچنین می‌توانند روابط بین‌المللی را تحت تأثیر قرار دهند. برای مثال، حملات سایبری منسوب به دولت‌ها، مانند حمله به سیستم‌های انتخاباتی اروپا (۲۰۲۳)، تنش‌های دیپلماتیک ایجاد کرده و اعتماد بین‌المللی را کاهش داده‌اند (INTERPOL, 2025).

این تأثیرات نیازمند رویکردی چندجانبه هستند، ازجمله: ۱) آموزش سواد رسانه‌ای برای کاهش تأثیر محتوای کذب؛ ۲) تقویت اعتماد عمومی از طریق شفافیت در عملکرد نهادهای دولتی؛ و ۳) توسعه دیپلماسی سایبری برای مدیریت تنش‌های بین‌المللی. این راهکارها می‌توانند پیامدهای اجتماعی و سیاسی جرائم سایبری را کاهش دهند (United Nations, 2024).

تحلیل تطبیقی: هم‌سنجی قوانین ایران و استانداردهای بین‌المللی

تحلیل تطبیقی قوانین ایران و استانداردهای بین‌المللی نشان‌دهنده تفاوت‌های قابل‌توجهی در جرم‌انگاری جاسوسی سایبری و تشویش اذهان عمومی است. در ایران، جاسوسی سایبری با تعریف گسترده‌ای در مواد ۵۰۱-۵۱۰ قانون مجازات اسلامی (۱۳۹۲) و ماده ۷۴۳ قانون جرائم رایانه‌ای (۱۳۸۸) جرم‌انگاری شده و مجازات‌های سنگین، مانند حبس ۱ تا ۵ سال یا اعدام در طرح تشدید مجازات (١٤٠٤)، را در بر می‌گیرد (پلیس فتا، ١٤٠٤). این رویکرد سخت‌گیرانه با هدف حفاظت از امنیت ملی طراحی‌شده، اما مجازات‌های سنگین، مانند اعدام، با انتقادات حقوق بشری مواجه شده‌اند، زیرا ممکن است با اصول تناسب مجازات در حقوق بین‌الملل مغایرت داشته باشند (Amnesty International, 2025). در مقابل، حقوق بین‌الملل به دلیل فقدان تعریف واحد جاسوسی سایبری، عمدتاً بر اصل صلاحیت سرزمینی و کنوانسیون بوداپست (۲۰۰۱) تکیه دارد (Council of Europe, 2001).

شماره ۴۸،
دوره هجدهم،
سال چهارم،
تابستان ۱۴۰۴،
صص ۱-۱۶

این تفاوت منجر به چالش‌هایی در همکاری بین‌المللی شده، زیرا کشورهای مختلف تعاریف و رویکردهای متفاوتی دارند (Smith, 2023).

تشویش اذهان عمومی در ایران با تعریف مبهم در ماده ٦٩٨ قانون مجازات اسلامی و ماده ۱۸ قانون جرائم رایانه‌ای، گاهی به محدودیت آزادی بیان منجر شده است (رضایی، ١٤٠٠). برای مثال، گزارش سازمان عفو بین‌الملل (۲۰۲۵) نشان می‌دهد که دستگیری‌های گسترده به اتهام تشویش اذهان عمومی، به‌ویژه در جریان ناآرامی‌های ١٤٠١، اغلب بدون شواهد کافی انجام‌شده و با ماده ۱۹ اعلامیه جهانی حقوق بشر تعارض دارد (United Nations, 1948). در حقوق بین‌الملل، استانداردهای حقوق بشر بر ضرورت توازن بین امنیت و آزادی بیان تأکیددارند، اما فقدان تعریف واحد تشویش اذهان عمومی در اسناد بین‌المللی، هماهنگی حقوقی را دشوار کرده است (Council of Europe, 2001).

چالش‌های اصلی این حوزه شامل ابهام در تعاریف قانونی، دشواری در اثبات جرائم سایبری (به‌ویژه جاسوسی)، و فقدان هماهنگی بین‌المللی است. برای مثال، تفاوت در تعریف جاسوسی سایبری بین ایران و سایر کشورها، تبادل اطلاعات و پیگرد عاملان را مختل کرده است (INTERPOL, 2025). این تحلیل تطبیقی نشان می‌دهد که هماهنگی حقوقی بین‌المللی و اصلاح قوانین ملی برای کاهش این چالش‌ها ضروری است.

نتایج

این پژوهش به بررسی جامع و عمیق جرائم جاسوسی سایبری و تشویش اذهان عمومی در فضای مجازی پرداخته و نتایج زیر را به دست آورده است:

جاسوسی سایبری در ایران: قوانین ایران با جرم‌انگاری گسترده و مجازات‌های سنگین (مانند حبس ۱ تا ۵ سال یا اعدام در طرح ١٤٠٤) رویکردی سخت‌گیرانه دارند، اما ابهامات اجرایی، کمبود فناوری‌های تشخیص، و فقدان همکاری بین‌المللی کارآمدی آن‌ها را کاهش داده است (پلیس فتا، ١٤٠٤). برای مثال، تنها ۳۰ درصد حملات سایبری در سال ١٤٠٣ به شناسایی عاملان منجر شده است، که این امر ضرورت سرمایه‌گذاری در فناوری و همکاری جهانی را نشان می‌دهد (INTERPOL, 2025).

تشویش اذهان عمومی در ایران: تعریف مبهم این جرم در ماده ٦٩٨ قانون مجازات اسلامی و ماده ۱۸ قانون جرائم رایانه‌ای، گاهی به سرکوب آزادی بیان منجر شده و با استانداردهای حقوق بشر، به‌ویژه ماده ۱۹ اعلامیه جهانی حقوق بشر، تعارض دارد (Amnesty International, 2025). دستگیری‌های گسترده در سال ١٤٠١ نمونه‌ای از این چالش است، که نشان‌دهنده نیاز به معیارهای عینی و نظارت مستقل است (رضایی، ١٤٠٠).

جاسوسی سایبری در حقوق بین‌الملل: فقدان تعریف واحد و رژیم حقوقی جامع، همکاری بین‌المللی را محدود کرده است. کنوانسیون بوداپست (۲۰۰۱) چارچوبی ارائه می‌دهد، اما عدم عضویت برخی کشورها، مانند ایران، اثربخشی آن را کاهش داده است (Council of Europe, 2001).

تشویش اذهان عمومی در حقوق بین‌الملل: این جرم معمولاً در حوزه ملی باقی می‌ماند، اما تعارض با آزادی بیان نیازمند بازنگری قوانین ملی و همسویی با استانداردهای بین‌المللی است (United Nations, 1948).

شماره ۴۸،
دوره هجدهم،
سال چهارم،
تابستان ۱۴۰۴،
صص ۱-۱۶

نقش فضای مجازی: پلتفرم‌های دیجیتال با تسهیل انتشار سریع و ناشناس اطلاعات، این جرائم را تشدید کرده‌اند و نیازمند نظارت مؤثرتر و توسعه فناوری‌های تشخیص هستند (United Nations, 2024).

تأثیرات اجتماعی و سیاسی: این جرائم با کاهش اعتماد عمومی، تشدید تنش‌های اجتماعی، و ایجاد تنش‌های دیپلماتیک، پیامدهای گسترده‌ای دارند (Amnesty International, 2025).

پیشنهادها

اصلاح قوانین داخلی: شفاف‌سازی تعاریف جرائم، به‌ویژه تشویش اذهان عمومی، برای کاهش تعارض با آزادی بیان و همسویی با ماده ۱۹ اعلامیه جهانی حقوق بشر. این اصلاحات باید شامل معیارهای عینی برای تشخیص محتوای کذب و کاهش مجازات‌های غیرمتناسب، مانند اعدام در جاسوسی سایبری، باشد (رضایی، ۱۴۰۰).

تقویت همکاری بین‌المللی: پیوستن فعال‌تر ایران به معاهداتی مانند کنوانسیون بوداپست و ایجاد سازوکارهای تبادل اطلاعات با سازمان‌هایی مانند INTERPOL برای پیگرد جرائم سایبری (Council of Europe, 2001). این همکاری‌ها می‌توانند شامل اشتراک داده‌های فنی و حقوقی، و ایجاد استانداردهای جهانی برای جرم‌انگاری باشند.

ارتقای سواد رسانه‌ای: آموزش عمومی، به‌ویژه برای جوانان، برای کاهش انتشار محتوای کذب و افزایش آگاهی از تهدیدات سایبری. این برنامه‌ها می‌توانند توسط وزارت آموزش‌وپرورش، رسانه‌های ملی، و سازمان‌های مردم‌نهاد اجرا شوند (United Nations, 2024).

توسعه فناوری‌های تشخیص: سرمایه‌گذاری در هوش مصنوعی و فناوری‌های پیشرفته برای شناسایی حملات سایبری و محتوای کذب. این فناوری‌ها باید با رعایت حریم خصوصی و حقوق بشر پیاده‌سازی شوند (INTERPOL, 2025).

ایجاد نهادهای نظارتی مستقل: تشکیل نهادهایی با حضور نمایندگان قوه قضاییه، سازمان‌های حقوق بشری، و کارشناسان فناوری برای نظارت بر اجرای قوانین سایبری و جلوگیری از سوءاستفاده از اتهامات مبهم مانند تشویش اذهان عمومی (Amnesty International, 2025).

توسعه دیپلماسی سایبری: تقویت روابط دیپلماتیک برای کاهش تنش‌های ناشی از حملات سایبری منسوب به دولت‌ها و ایجاد توافق‌نامه‌های بین‌المللی برای جرم‌انگاری جاسوسی سایبری (Smith, 2023). این دیپلماسی می‌تواند شامل مذاکرات دوجانبه و چندجانبه برای ایجاد اعتماد بین‌المللی باشد.

تقویت زیرساخت‌های سایبری: سرمایه‌گذاری در امنیت سایبری زیرساخت‌های حیاتی، مانند شبکه‌های انرژی و سیستم‌های دفاعی، برای کاهش آسیب‌پذیری در برابر حملات جاسوسی سایبری (پلیس فتا، ۱۴۰۴).

این پیشنهادات با هدف ایجاد توازن بین امنیت ملی، آسایش عمومی، و حقوق بشر ارائه‌شده‌اند و با استناد به منابع معتبر مانند گزارش‌های سازمان ملل (۲۰۲۴)، داده‌های سیویلیکا (۱۴۰۴)، گزارش‌های INTERPOL (۲۰۲۵)، و مقالات اسکوپوس (۲۰۲۴-۲۰۲۵) تدوین‌شده‌اند. این پژوهش می‌تواند مبنایی برای سیاست‌گذاری‌های آینده در حوزه جرائم سایبری در ایران و جهان باشد و به کاهش تهدیدات سایبری و تقویت همکاری‌های بین‌المللی کمک کند.

شماره ۴۸،
دوره هجدهم،
سال چهارم،
تابستان ۱۴۰۴،
صص ۱-۱۶

منابع

پلیس فتا (۱٤۰٤). گزارش سالانه جرائم سایبری. تهران.

رضایی، محمد (۱٤۰۰). تحلیل حقوقی نشر اکاذیب در فضای مجازی. فصلنامه مطالعات حقوق عمومی.

فضلی، حسن و همکاران (۱۳۹۵). بررسی جرائم علیه امنیت ملی در فضای مجازی. سیویلیکا.

قانون جرائم رایانه‌ای ایران (۱۳۸۸). تهران: مجلس شورای اسلامی.

قانون مجازات اسلامی (۱۳۹۲). تهران: مجلس شورای اسلامی.

هدایتی چنانی، رحمان (۱۳۹۹). بررسی جرم جاسوسی در حقوق بین‌المللی و قانون مجازات جرائم نیروهای مسلح. سیویلیکا.

Amnesty International (2025). Human Rights and Cyber Laws in Iran. London.

Buzan, B. (1991). People, States and Fear: An Agenda for International Security Studies in the Post-Cold War Era. Lynne Rienner Publishers.

Council of Europe (2001). Convention on Cybercrime. Strasbourg.

INTERPOL (2025). Annual Report on Cybercrime Trends. Lyon.

Mill, J. S. (1859). On Liberty. Oxford University Press.

Smith, J. (2023). Cyber Espionage and International Law. Journal of International Criminal Justice, 21(3), 45-67.

United Nations (1948). Universal Declaration of Human Rights. New York.

United Nations (1998). Rome Statute of the International Criminal Court. New York.

United Nations (2024). Global Cybersecurity Report. New York.

فصلنامه تحقیقات جدید در علوم انسانی(دوره جدید)

شماره ۴۸،
دوره هجدهم،
سال چهارم،
تابستان ۱۴۰۴،
صص ۱-۱۶

The Scope of Crimes Arising from Espionage, Incitement, and Disturbance of Public Opinion in Cyberspace under International Criminal Law

Mahshid Pishyar[2]

Abstract

Cyberspace, as one of the most significant achievements of modern technology, has brought about a profound transformation in global interactions, while simultaneously providing a platform for the emergence of new crimes such as cyber espionage and disturbance of public opinion. Cyber espionage, through unauthorized access to confidential data, theft of sensitive information, or infiltration into digital infrastructures, directly threatens national sovereignty and the security of states. Disturbance of public opinion disrupts social order, public trust, and general comfort by disseminating false, distorted, or provocative content on digital platforms such as Telegram, Instagram, and X. These crimes not only jeopardize national security but also create complex legal challenges at both national and international levels by fostering social and political instability. This article aims to conduct a comparative analysis of cyber espionage and disturbance of public opinion within the framework of Iranian law and the principles of international criminal law. Utilizing library resources and credible legal documents, including United Nations reports (2024), INTERPOL reports (2025), and data from Iran's Cyber Police (1404), the findings indicate that cyber espionage in Iran has been criminalized with severe penalties, such as imprisonment from 1 to 5 years or even the death penalty under the intensified punishment scheme (1404). However, the lack of a unified definition in international law has limited global cooperation. Disturbance of public opinion has also faced criticism from human rights perspectives due to vague and broad definitions in Iranian law, as it sometimes leads to the suppression of freedom of expression. This research, by examining enforcement challenges, social and political impacts, and legal gaps, proposes recommendations for reforming domestic laws, strengthening international cooperation, enhancing media literacy, and developing technologies for detecting cyber crimes. The ultimate goal of this study is to create a balance between the protection of national security and public comfort while respecting human rights, particularly freedom of expression. This article can serve as a basis for future policymaking in the field of cyber crimes in Iran and globally.

Keywords: Cyber Espionage, Disturbance of Public Opinion, Cyberspace, International Criminal Law, Cyber Crimes Law

[2] Master's Student in International Law, Payam-e Noor University, Mahdasht, Iran (Corresponding Author)