Comparative Studies in Jurisprudence, Law, and Politics

Legal Prevention Management and the Control of Organized Gang and Cybercrime

1. Hamideh Panahi: PhD Student of Criminal Law and Criminology, Department of Law, Yas.C., Islamic Azad University, Yasouj, Iran
2. Seyed Mostafa Hashemi*: Department of Law, Yas.C., Islamic Azad University, Yasuj, Iran.
Email: mostafa.h1404@gmail.com (Corresponding Author)
3. Esmael Behesht: Department of Theology and Islamic Studies, Yas.C., Islamic Azad University, Yasuj, Iran

ABSTRACT

This article examines the management of legal prevention and the control of organized gang and cybercrime and seeks to fundamentally redefine legal prevention management in response to organized crime through a descriptive–analytical method. Undoubtedly, no effective criminal policy can be designed without an accurate understanding of the substantive differences between gang-related and cybercrime, a conceptual distinction between cyberspace and virtual space, and attention to the principles of knowledge-based practice, intersectoral coordination, and outcome orientation. The findings indicate a lack of conceptual distinction between "cyberspace" and "virtual space" in Iranian legal and policy documents, resulting in inappropriate definitions, ineffective criminalization, and inconsistent enforcement of laws. Although "cyberspace" is defined as a technical, physical, and logical environment comprising systems, networks, and data, the Iranian legislature has often used terms such as "virtual space" and "virtual platforms" interchangeably. Examples include Article 2 concerning Article 500 bis of the Islamic Penal Code, Article 9 of the Law on the Protection of Children and Adolescents, and Articles 59 and 60 of the 2021 Law on the Protection of the Family and Youthful Population, without recognizing the inherent differences among these concepts. This not only complicates statutory interpretation but also undermines the possibility of designing a precise criminal policy tailored to the specific characteristics of cyberspace. Another problem is the absence of an integrated legal framework for crime-prevention management, which has resulted in a proliferation of parallel institutions, insufficient intersectoral coordination, and an emphasis on deterrent approaches rather than structural prevention. In Iran, despite the existence of institutions such as the Supreme Council of Cyberspace and the Cyber Police, no central and independent institution is responsible for managing the legal prevention of crime. Consequently, prevention management has become a nonsystematic, unstable, and outcome-driven process. Another concern is the neglect of the criminological and etiological dimensions of cybercrime, particularly in analyzing criminal motivations. Although economic, social, and cultural motives have received some attention in relation to conventional crimes, cybercrime-related factors such as entertainment, fame, psychological complexes, personal revenge, and technical curiosity—identified in domestic and international studies—have frequently been overlooked. This omission impedes the development of non-penal and knowledge-based preventive measures. A further problem concerns the inadequate adaptation of criminological theories to the realities of cyberspace. Although classical theories such as social control theory, strain theory, and social learning theory are effective in analyzing crimes committed in physical environments, they require reformulation and adaptation in cyberspace, where social bonds are weaker, identities are more anonymous, and motivations are more complex. Such adaptation has, in practice, not occurred within the Iranian legal system. The findings of this study demonstrate that, in Iran, prevention law remains confined to a duty-oriented framework. This has produced an identity crisis in prevention law and impeded the development of a scientific and sustainable criminal policy. Crime prevention must no longer be regarded as an ancillary obligation; rather, it must be placed at the heart of Iran's criminal policy as a national, systematic, knowledge-based, and outcome-oriented policy. Unless parallel preventive institutions are dissolved, criminological theories are adapted to digital realities, and the legislature abandons inappropriate definitions, no adequate solution will be achieved for the legal prevention and control of organized gang and cybercrime.

Keywords: *Legal prevention, organized gang and cybercrime, criminology*

How to cite: Panahi, H., Hashemi, S. M., & Behesht, E. (2027). Legal Prevention Management and the Control of Organized Gang and Cybercrime. *Comparative Studies in Jurisprudence, Law, and Politics*, *9*(2), 1-38.

Submit Date: 07 April 2026
Revise Date: 23 July 2026
Accept Date: 29 July 2026
Initial Publish Date: 06 September 2026
Final Publish Date: 22 June 2027

پژوهش‌های تطبیقی فقه، حقوق و سیاست

مدیریت پیشگیری حقوقی و کنترل جرایم سازمان یافته باندی و سایبری

۱. حمیده پناهی: دانشجوی دکتری جزا و جرم شناسی، گروه حقوق، واحد یاسوج، دانشگاه آزاد اسلامی، یاسوج، ایران
۲. سید مصطفی هاشمی*: گروه حقوق، واحد یاسوج، دانشگاه آزاد اسلامی، یاسوج، ایران. پست الکترونیک: mostafa.h1404@gmail.com (نویسنده مسئول)
۳. اسماعیل بهشت: گروه الهیات و معارف اسلامی، واحد یاسوج، دانشگاه آزاد اسلامی، یاسوج، ایران

چکیده

این مقاله متکفل بررسی مدیریت پیشگیری حقوقی و کنترل جرایم سازمان یافته باندی و سایبری و به دنبال بازتعریف بنیادین مدیریت پیشگیری حقوقی در برابر جرایم سازمان‌یافته با روش توصیفی و تحلیلی است. بی تردید بدون درک دقیق تفاوت ماهوی بین جرایم باندی و سایبری، بدون تمایز مفهومی بین فضاهای سایبری و مجازی، و بدون توجه به اصول دانش‌بنیان، فرابخشی و نتیجه‌محوری، هیچ سیاست جنایی مؤثری نمی‌توان طراحی کرد. یافته ها بیانگر این است که عدم تمایز مفهومی بین «فضای سایبری» و «فضای مجازی» در متون قانونی و سیاستی ایران، که منجر به تعریف‌های نامناسب، جرم‌انگاری‌های ناکارآمد و اجرای ناهمگون قوانین شده است. در حالی که «فضای سایبری» به عنوان یک محیط فنی-فیزیکی-منطقی شامل سامانه‌ها، شبکه‌ها و داده‌ها تعریف می‌شود، قانونگذار ایران اغلب از اصطلاحات «فضای مجازی» یا «بستر مجازی» به‌صورت مترادف استفاده کرده است (مانند ماده ۲(۵۰۰ مکرر) قانون مجازات اسلامی، ماده ۹ قانون حمایت از اطفال و نوجوانان، و ماده ۵۹ و ۶۰ قانون حمایت از خانواده و جوانی جمعیت مصوب ۱۴۰۰)، بدون آنکه تفاوت ذاتی این مفاهیم را بپذیرد. این امر، نه تنها تفسیر قانون را با مشکل مواجه می‌کند، بلکه امکان طراحی یک سیاست جنایی دقیق و متناسب با ویژگی‌های فضای سایبری را نیز تضعیف می‌سازد. همچنین فقدان یک چارچوب حقوقی یکپارچه برای مدیریت پیشگیری از جرم، که باعث تکثر نهادهای موازی، فقدان هماهنگی بین‌بخشی و تمرکز بر رویکردهای بازدارنده به جای پیشگیری ساختاری شده است. در ایران، علی‌رغم وجود نهادهایی چون شورای عالی فضای مجازی و پلیس سایبری، هیچ نهاد مرکزی و مستقلی برای مدیریت پیشگیری حقوقی از جرم وجود ندارد. این امر، مدیریت پیشگیری را به یک فرآیند غیرسیستمی، ناپایدار و نتیجه‌محور تبدیل کرده است. از سویی دیگر نادیده گرفتن ابعاد جرم‌شناسی و علت‌شناختی جرایم سایبری، به‌ویژه در تحلیل انگیزه‌های مجرمانه. اگرچه در جرایم سنتی، انگیزه‌های اقتصادی، اجتماعی و فرهنگی تا حدی مورد توجه قرار گرفته‌اند، اما در مورد جرایم سایبری، عواملی چون سرگرمی، شهرت، عقدهٔ روانشناختی، انتقام شخصی یا کنجکاوی فنی که در مطالعات داخلی و بین‌المللی به آنها اشاره شده اغلب نادیده گرفته شده‌اند. این امر، مانع از طراحی راهکارهای پیشگیری غیرکیفری و دانش‌بنیان می‌شود. ضعف در تطبیق نظریه‌های جرم‌شناسی با واقعیت‌های فضای سایبری. نظریه‌های کلاسیک مانند نظریه کنترل اجتماعی، نظریه فشار و نظریه یادگیری اجتماعی، اگرچه در تحلیل جرایم فیزیکی مؤثرند، اما در فضای سایبری که پیوندهای اجتماعی ضعیف‌تر، هویت ناشناس‌تر و انگیزه‌ها پیچیده‌تر است، نیاز به بازتعریف و تطبیق دارند. این تطبیق، در نظام حقوقی ایران عملاً صورت نگرفته است. نتایج این تحقیق نشان می‌دهد در ایران، حقوق پیشگیری هنوز در سطح یک تکلیف محوری محدود می‌شود. این امر، باعث بحران هویت حقوق پیشگیری و ناتوانی در ایجاد یک سیاست جنایی علمی و پایدار شده است. تا زمانی که پیشگیری از جرم دیگر یک تکلیف جانبی نیست، بلکه باید به عنوان یک سیاست ملی، نظام‌مند، دانش‌بنیان و نتیجه‌محور، در قلب سیاست جنایی ایران قرار گیرد. تا زمانی که نهادهای موازی پیشگیری منحل نشوند، و تا زمانی که نظریه‌های جرم‌شناسی با واقعیت‌های دیجیتال تطبیق نیابند و قانونگذار از تعاریف نامناسب فاصله نگیرد، به راه حل مناسبی برای پیشگیری حقوقی و کنترل جرایم سازمان یافته باندی و سایبری دست پیدا نخواهیم کرد.

واژگان کلیدی: *پیشگیری حقوقی، جرایم سازمان یافته باندی و سایبری، جرم شناسی*

نحوه استناددهی: پناهی، حمیده.، هاشمی، سید مصطفی.، و بهشت، اسماعیل. (۱۴۰۶). مدیریت پیشگیری حقوقی و کنترل جرایم سازمان یافته باندی و سایبری. *پژوهش‌های تطبیقی فقه، حقوق و سیاست*، ۹(۲)، ۳۸-۱.

تاریخ ارسال: ۱۸ فروردین ۱۴۰۵
تاریخ بازنگری: ۱ مرداد ۱۴۰۵
تاریخ پذیرش: ۷ مرداد ۱۴۰۵
تاریخ چاپ اولیه: ۱۵ شهریور ۱۴۰۵
تاریخ چاپ نهایی: ۱ تیر ۱۴۰۶

مقدمه

اصطلاح «حقوق پیشگیری از جرم» به مجموعه قوانین و مقررات تقنینی، فراقانونی و فروتقنینی اشاره دارد که به‌طور مستقیم یا غیرمستقیم، اقدامات پیشگیرانه را ضابطه‌مند کرده و نهاد یا سازمان خاصی را برای مدیریت و اجرای آن تأسیس می‌کند (Jalali Farahani, 2014). این مفهوم در دو معنا به‌کار می‌رود: اول، به‌عنوان تعهدات و وظایف دولت در قبال پیشگیری از جرم که منبع راهبرد کنشی سیاست جنایی است؛ و دوم، به‌عنوان حقوق اجتماعی، اقتصادی و فرهنگی افراد که تأمین آن‌ها می‌تواند به‌عنوان عامل پیشگیری ساختاری عمل کند. تمرکز این تحلیل بر معنای اول است؛ یعنی حقوق پیشگیری به‌عنوان یک تعهد نتیجه‌محور دولتی در قبال مدیریت پدیده مجرمانه. تعریف عملیاتی آن در ماده ۱ قانون پیشگیری از وقوع جرم مصوب ۲۰۱۷ آمده است که پیشگیری را «پیش‌بینی، شناسایی و ارزیابی خطر وقوع جرم و اتخاذ تدابیر و اقدامات لازم برای از میان بردن یا کاهش آن» تعریف می‌کند. این رویکرد، با تأکید بر حقوق ماهوی و شکلی (Saybani & Karimi, 2018)، چارچوبی نظام‌مند فراهم می‌کند. ریشه قانونی آن در بند ۵ اصل ۱۵۶ قانون اساسی نهفته است (Aghababaii, 2010). بااین‌حال، تحلیل قوانین پیشگیرانه (مانند قانون ارتقای سلامت نظام اداری مصوب ۲۰۱۱) نشان می‌دهد که قانون‌گذار اغلب اصول راهبردی پیشگیری، مانند فرابخشی، دانش‌محوری، مشارکت، پایداری و کرامت انسانی را نادیده گرفته است (Heydari et al., 2018)، که این امر منجر به بحران هویت حقوق پیشگیری شده است. بنابراین، تحقق آن به‌عنوان یک سیاست ملی، نظام‌مند و نتیجه‌محور، مستلزم تدوین قوانینی است که نهادهای موازی منحل شده و اقدامات براساس تحلیل ریسک جنایی انجام گیرند.

مفهوم «جرایم سازمان‌یافته» در نظام‌های حقوقی بین‌المللی و داخلی، با تعاریفی چندوجهی، اما مبتنی بر معیارهای مشترک تبیین شده است؛ تعریف استاندارد آن در ماده ۲ کنوانسیون سازمان ملل متحد علیه جرایم سازمان‌یافته فراملی ارائه شده که جرایم سازمان‌یافته را «گروه ساختارمند متشکل از سه نفر یا بیشتر که در طول زمان وجود داشته و به‌طور هماهنگ به‌منظور ارتکاب جرم جدی برای کسب منفعت مالی یا مادی عمل می‌کند» تعریف می‌کند (Najafi Abrandabadi, 2016) و بر سه عنصر اساسی سازمان‌یافتگی، پایداری و هدف ارتکاب استوار است (Zabihollahnejad, 2017). در نظام حقوقی ایران، اگرچه مفهوم «جرم سازمان‌یافته» در معنای عام فاقد تعریف قانونی روشن و مستقل است (Razavi, 2007)، اما در ماده ۱۳۰ قانون مجازات اسلامی مصوب ۲۰۱۳، تعریفی نزدیک به تعریف بین‌المللی ارائه شده که آن را «فعالیت‌های غیرقانونی و هماهنگ گروهی منسجم از اشخاص که با تبانی و برای تحصیل منافع مشترک (قدرت یا مادی) به ارتکاب جرم مستمر و شدید می‌پردازند» می‌داند (Akhavat, 2015)، که ضمن بازتاب عناصر کلیدی کنوانسیون پالرمو، بر ماهیت گروهی، تبانی و ادامه‌دار بودن جرم تأکید دارد. این جرایم در ایران، که اغلب فراملی هستند، شامل قاچاق کالا و ارز (Saybani & Karimi, 2018)، فساد اداری (Aghababaii, 2010) و سایر شبکه‌های مجرمانه اقتصادی می‌شوند و با ساختار سلسله‌مراتبی، تقسیم کار تخصصی و استفاده از خشونت یا تهدید برای حفظ اقتدار همراه هستند، و گزارش‌های مرکز پژوهش‌های مجلس (Hassan Beigi, 2005) نشان می‌دهد که این جرایم نه‌تنها امنیت اقتصادی کشور را تهدید می‌کنند، بلکه با شبکه‌های فساد اداری پیوند عمیقی دارند و نیازمند سیاست جنایی هماهنگ و یکپارچه‌ای هستند (Hassan Beigi, 2005). بااین‌حال، چالش اساسی در نظام حقوقی ایران، فقدان تعریف مستقل و مدون از «جرم سازمان‌یافته» در قانون اساسی یا قوانین ماهوی است که اجرای مؤثر سیاست‌های پیشگیرانه و کیفری را با دشواری مواجه ساخته و دستگاه‌های اجرایی را ملزم به تفسیر پراکنده از مواد قانون مجازات اسلامی یا قانون جرایم رایانه‌ای می‌کند؛ رویکردی که از نظر حقوقی ضعیف و منجر به تفسیرهای ناهمگون است. بنابراین، با وجود تطابق نسبی تعاریف داخلی و بین‌المللی، تفاوت کلیدی در عدم تدوین یک چارچوب حقوقی

مستقل و جامع در ایران مشهود است؛ درحالی‌که کنوانسیون پالرمو، به‌عنوان ابزاری فراملی، زمینه‌ساز هماهنگی بین‌المللی است، نظام حقوقی ایران فاقد قانون جامعی است که علاوه بر تعریف، ساختارهای نهادی، اقدامات پیشگیری و مکانیسم‌های نظارتی را نیز مشخص کند؛ لذا، برای تحقق سیاست جنایی مؤثر در مقابله با جرایم سازمان‌یافته، چه در فضای فیزیکی و چه در فضای سایبری، ضروری است که ایران با تدوین قانونی جامع، تعریفی شفاف، مستقل و متناسب با ویژگی‌های نوین جرایم (مانند ساختار شبکه‌ای و فراملی بودن) ارائه دهد؛ زیرا بدون چنین چارچوبی، هرگونه تلاش برای پیشگیری یا کنترل، تنها به اقدامات واکنشی و ناکارآمد محدود خواهد شد.

اصطلاح «جرایم سازمان‌یافته باندی» به فعالیت‌های مجرمانه‌ای اطلاق می‌شود که توسط گروه‌های سازمان‌یافته در فضای فیزیکی (دنیای واقعی)، با ساختاری سلسله‌مراتبی یا شبکه‌ای، انجام می‌شوند و ممکن است در محیط‌هایی مانند زندان‌ها شکل گرفته و با استفاده از شبکه‌های اجتماعی، اقتصادی و فرهنگی، فعالیت خود را گسترش دهند (Taghizadeh et al., 2017). این جرایم، برخلاف جرایم ناشی از غلیان احساسات، حساب‌شده و برنامه‌ریزی‌شده هستند و با ویژگی‌هایی مانند وجود سرکرده (رهبر باند)، برنامه‌ریزی قبلی، تقسیم کار، پاتوق مشترک و استفاده از وسایل نقلیه سرقتی همراه‌اند (Beigi & Khoshyari, 2011). تعریف قانونی این جرایم در ماده ۶۱۰ قانون مجازات اسلامی مصوب ۲۰۱۳ آمده است که آن را «اجتماع و تبانی دو نفر یا بیشتر برای ارتکاب جرایمی بر ضد امنیت داخلی یا خارجی کشور یا فراهم کردن وسایل ارتکاب آن» تعریف می‌کند، که ریشه آن در مفهوم فقهی «تبانی» (توافق پنهانی علیه فرد سوم) دارد (Parvizi, 2016). از دیدگاه پلیس آگاهی ناجا، باندها به دو دسته سازمان‌یافته (منسجم) و غیرسازمان‌یافته (خرده‌باند) تقسیم می‌شوند که در باندهای سازمان‌یافته، ساختار سلسله‌مراتبی، حیطه‌بندی اطلاعاتی و وجود افراد متخصص، مانند مالخر، قابل مشاهده است (Taghizadeh et al., 2017). بااین‌حال، نظام حقوقی ایران با فقدان یک چارچوب حقوقی یکپارچه و نهادی اختصاصی برای مدیریت پیشگیری از جرایم باندی مواجه است، که این امر از جمله چالش‌های اساسی در مقابله با این پدیده محسوب می‌شود.

اصطلاح «جرایم سازمان‌یافته سایبری» به فعالیت‌های مجرمانه‌ای اطلاق می‌شود که توسط گروه‌های منسجم، هماهنگ و پایدار در فضای سایبری انجام می‌گیرند و هدف اصلی آن‌ها کسب منافع مالی، قدرت یا کنترل از طریق استفاده از ابزارهای فناورانه است؛ این جرایم، برخلاف تصور رایج از فعالیت‌های فردی هکرها، غالباً توسط گروه‌های سازمان‌یافته و شبکه‌های پیچیده انجام می‌شوند که ممکن است از ساختارهای سلسله‌مراتبی یا شبکه‌ای غیرمتمرکز بهره ببرند و نقش‌های تخصصی (مانند توسعه‌دهندگان بدافزار، اپراتورهای شبکه و پول‌شویان دیجیتال) را به‌صورت هماهنگ ایفا کنند. این گروه‌ها به دو دسته عمده تقسیم می‌شوند: اول، گروه‌های جرم سازمان‌یافته فضای واقعی که فعالیت خود را به فضای سایبری گسترش داده‌اند (مانند شبکه‌های قاچاق یا پول‌شویی)؛ و دوم، گروه‌هایی که در فضای سایبری شکل گرفته‌اند و ممکن است از حمایت دولت‌ها برخوردار باشند و به‌عنوان ابزاری برای پیشبرد اهداف سیاسی یا اقتصادی عمل کنند که به آن‌ها عنوان «ارتش سایبری» یا گروه‌های جرم سازمان‌یافته خاص فضای سایبر داده می‌شود (Taghizadeh et al., 2017). تعریف جرایم سایبری در سطح بین‌المللی، در سازمان همکاری و توسعه اقتصادی، به «هر رفتار غیرقانونی مربوط به پردازش خودکار و انتقال داده‌ها» و در انجمن بین‌المللی جزا، به «جرایمی که در فضایی غیرفیزیکی بر ضد داده‌های ناشی‌شده از فناوری اطلاعات قابل ارتکاب است» محدود می‌شود (Sobhkhiz, 2015)؛ درحالی‌که تعریف حقوقی آن در ایران، در ماده ۱ قانون جرایم رایانه‌ای مصوب ۲۰۰۹ آمده است که آن را «هر فعل یا ترک فعل خلاف قانون که با به‌کارگیری سامانه‌های رایانه‌ای یا مخابراتی ارتکاب یابد و برای آن مجازات تعیین شده باشد» تعریف می‌کند (Gercke & Akbari, 2010)، که با نگاهی به کنوانسیون بوداپست (۲۰۰۱) تدوین شده و بیشتر متوجه نسل‌های اول و دوم جرایم رایانه‌ای است و

جرایم سایبری با ساختار شبکه‌ای پیچیده و خطر مضاعف کمتر مورد توجه قرار گرفته‌اند (Gercke & Akbari, 2010). در نظام حقوقی ایران، چالش اساسی، فقدان تعریف روشن و مستقل از «جرم سازمان‌یافته سایبری» است؛ قانون‌گذار به‌جای تدوین تعاریف دقیق و فنی، از اصطلاحات مبهمی مانند «فضای مجازی» و «بستر مجازی» در قوانین متعددی استفاده کرده است (Vatani & Asadi, 2016)، که این عدم تمایز مفهومی بین «فضای سایبری» (فیزیکی‌ـفناورانه) و «فضای مجازی» (اجتماعی‌ـفرهنگی)، منجر به تلقی نادرست از طبیعت این جرایم و طراحی راهکارهای ناکارآمد شده است. این جرایم، که اغلب فراملی و پویا هستند و با ویژگی‌هایی مانند ناشناس‌ماندن مرتکب، سرعت بالای اجرا و دشواری در ردیابی همراه‌اند، از جرایم سنتی (مانند کلاهبرداری و افترا) تا جرایم نوین (مانند هک علیه زیرساخت‌های حیاتی و حملات باج‌افزاری) را دربرمی‌گیرند (Farhadi Alashti & Javan Jafari Bojnordi, 2017) و با افزایش وابستگی جامعه به فناوری، ناتوانی دولت در تعقیب مجرمان را افزایش داده‌اند (Heydari et al., 2018). بنابراین، برای مقابله مؤثر با این پدیده، ضروری است که قانون‌گذار با تدوین قانونی مستقل و مدون، ضمن شناخت فرایند تکوینی این گروه‌ها و ویژگی‌های منحصربه‌فرد فضای سایبر، تعریفی شفاف ارائه دهد که بر روش ارتکاب و ساختار شبکه‌ای تأکید کند، نه صرفاً بر ابزار یا موضوع جرم؛ زیرا بدون چنین چارچوبی، هرگونه تلاش برای پیشگیری یا کنترل، تنها به اقدامات واکنشی و ناکارآمد محدود خواهد شد.

در نتیجه، تحلیل دقیق این چهار مفهوم کلیدی ــ پیشگیری حقوقی از جرم، جرایم سازمان‌یافته، جرایم باندی و جرایم سایبری ــ نشان می‌دهد که هر یک دارای ابعاد ماهوی، شکلی و عملیاتی متمایزی هستند که باید در یک چارچوب حقوقی یکپارچه و تحلیلی مورد توجه قرار گیرند. پیشگیری حقوقی، به‌عنوان یک تعهد دولتی و نظام‌مند، نیازمند تفکیک مفهومی بین «فضای سایبری» و «فضای مجازی» است تا بتواند به‌طور مؤثر در برابر جرایم سازمان‌یافته ــ چه در قالب باندهای فیزیکی و چه در قالب شبکه‌های غیرمتمرکز سایبری ــ عمل کند. درحالی‌که جرایم باندی با ساختارهای مکانی و اجتماعی مشخصی همراه‌اند، جرایم سایبری با ویژگی‌هایی چون فرامرزی بودن، ناشناس‌ماندن مرتکب و استفاده از ابزارهای فنی، نیازمند رویکردهای پیشگیری خاصی هستند. فقدان تعریف حقوقی روشن، تکرار و تداخل قوانین و عدم توجه به اصول دانش‌بنیان، فرابخشی و نتیجه‌محوری در نظام حقوقی ایران، این چهار مفهوم را با یکدیگر درآمیخته و امکان طراحی یک سیاست جنایی یکپارچه و مؤثر را با محدودیت مواجه ساخته است. بنابراین، تدوین یک چارچوب حقوقی مبتنی بر تمایز مفهومی، تطبیق نظریه‌های جرم‌شناسی با واقعیت‌های دیجیتال و نهادینه‌سازی مدیریت پیشگیری از جرم، نه‌تنها یک ضرورت علمی، بلکه یک الزام سیاست جنایی ملی است.

در نظام‌های حقوقی مدرن، رویکرد به پیشگیری از جرم به‌تدریج از چارچوب بازدارنده و عقاب‌محور به‌سمت یک سیاست جنایی نظام‌مند، دانش‌بنیان و پیشگیرانه تغییر یافته است. در این چارچوب، «حقوق پیشگیری از جرم» به‌عنوان مجموعه‌ای از قواعد تقنینی، فراقانونی و زیرتقنینی تعریف می‌شود که با هدف ساختارمندکردن و مدیریت اقدامات پیشگیرانه، تعهدات دولتی را در قبال کاهش وقوع جرم و کنترل پدیده مجرمانه مشخص می‌سازد. طبق تعریف پذیرفته‌شده، حقوق پیشگیری از جرم در معنای اول، ناظر به تعهدات و وظایف دولت‌ها در این حوزه است و به‌طور مستقیم با سیاست جنایی، برنامه‌ریزی حقوقی و مدیریت ریسک جنایی مرتبط می‌شود؛ در مقابل، در معنای دوم، به حقوق اجتماعی، اقتصادی و فرهنگی افراد اشاره دارد که تأمین آن‌ها می‌تواند به‌عنوان یک عامل پیشگیری ساختاری عمل کند (Aminzadeh & Ghaffari, 2019). بااین‌حال، تمرکز این پژوهش بر معنای اول این مفهوم است؛ یعنی حقوق پیشگیری به‌عنوان یک راهبرد نظام‌مند و نهادینه‌شده در سیاست جنایی.

در ایران، با وجود گسترش قابل‌توجه استفاده از فناوری اطلاعات و ارتباطات و وجود نهادهایی چون شورای عالی فضای مجازی (تشکیل‌شده در سال ۲۰۱۲)، همچنان نظام حقوقی پیشگیری از جرم با خلأهای ماهوی، شکلی و نهادی جدی مواجه است. این خلأها در تعریف نامشخص جرایم سایبری، فقدان چارچوب یکپارچه حقوقی برای مدیریت جرایم سازمان‌یافته، ضعف در هماهنگی بین‌نهادی و عدم توجه به اصول دانش‌بنیان و علت‌شناختی پیشگیری آشکار می‌شوند. به‌عنوان نمونه، اگرچه در مقررات متعددی، از جمله ماده ۲ (۵۰۰ مکرر) قانون الحاق دو ماده به کتاب پنجم قانون مجازات اسلامی (مصوب ۲۰۲۰)، ماده ۹ قانون حمایت از اطفال و نوجوانان (مصوب ۲۰۲۰) و ماده ۱۸ قانون حداکثر استفاده از توان تولیدی و خدماتی کشور (مصوب ۲۰۱۹)، از مفاهیمی چون «فضای مجازی» و «بستر مجازی» استفاده شده است، اما فقدان تعریف حقوقی روشن از «فضای سایبری» و «جرایم سازمان‌یافته سایبری»، اجرای مؤثر قوانین را با دشواری مواجه ساخته است. این امر به‌ویژه زمانی حادتر می‌شود که قانون‌گذار به‌جای ایجاد قوانین مستقل و متناسب با ویژگی‌های فضای سایبری، تنها از تغییرات جزئی در قوانین قدیمی استفاده کرده و از اقدامات پیشگیرانه ساختاری و سیستماتیک غافل مانده است (Khalifeh, 2020).

در همین راستا، چالش دیگری که نظام حقوقی ایران با آن روبه‌روست، عدم تمایز مفهومی بین «فضای مجازی» و «فضای سایبری» است. درحالی‌که «فضای سایبری» به‌عنوان یک فضای فنی‌ـفیزیکی‌ـمنطقی، شامل شبکه‌های کامپیوتری، سیستم‌های اطلاعاتی و زیرساخت‌های دیجیتال تعریف می‌شود، «فضای مجازی» بیشتر به محیط‌های تعامل اجتماعی‌ـفرهنگی، مانند شبکه‌های اجتماعی، اشاره دارد. این عدم تمایز مفهومی در متون قانونی و سیاستی ایران، منجر به تلقی نادرست از طبیعت جرایم سایبری و، در نتیجه، طراحی راهکارهای ناکارآمد برای پیشگیری و کنترل آن‌ها شده است. از سوی دیگر، جرایم سازمان‌یافته باندی نیز که اغلب در محیط‌های فیزیکی و با ساختارهای سلسله‌مراتبی یا شبکه‌ای انجام می‌شوند، با توجه به عواملی چون فقر، نابرابری اجتماعی، تضعیف پیوندهای اجتماعی و حتی شرایط نهادی مانند زندان‌ها (که می‌توانند به‌عنوان محیطی برای انتقال ترفندهای مجرمانه عمل کنند)، ریشه‌های ساختاری پیچیده‌ای دارند که نمی‌توان آن‌ها را تنها با ابزارهای بازدارنده کیفری کنترل کرد (Khalifeh, 2020).

در این میان، مدیریت پیشگیری از جرم، به‌عنوان فرایندی برای به‌کارگیری مؤثر و کارآمد منابع مادی و انسانی جهت دستیابی به اهداف تعیین‌شده، ضرورت پیدا می‌کند. این مدیریت، برخلاف رویکردهای سنتی که صرفاً بر کاهش آمار جرم تمرکز دارند، باید بر پیش‌بینی، شناسایی، ارزیابی خطر وقوع جرم و اتخاذ تدابیر لازم برای از میان بردن یا کاهش آن متمرکز باشد. این رویکرد، با تأکید بر مدیریت پیش از بروز جرم (پیشگیری)، آمادگی برای رویارویی، مدیریت در زمان شیوع و مدیریت پس از کاهش، به یک چارچوب چهارگانه و سیستماتیک تبدیل می‌شود (Jalali Farahani, 2014). بااین‌حال، در ایران، فقدان یک نهاد مرکزی و مستقل برای مدیریت پیشگیری از جرم، تکثر نهادهای موازی و غیرسیستمی و عدم توجه به اصول فرابخشی، دانش‌محوری، مشارکت، پایداری و کرامت انسانی در طراحی سیاست‌های پیشگیرانه، این مدیریت را ناکارآمد ساخته است (Heydari et al., 2018).

از سوی دیگر، تحلیل جرایم سازمان‌یافته، چه باندی و چه سایبری، نشان می‌دهد که این جرایم از ویژگی‌های مشترکی، از جمله سازمان‌یافتگی، حساب‌شده بودن، انگیزه‌های اقتصادی و گاه سیاسی و استفاده از شبکه‌های پیچیده، برخوردارند. در مورد جرایم سایبری، این سازمان‌یافتگی می‌تواند به‌صورت شبکه‌های غیرمتمرکز و پویا نمایان شود که در آن‌ها نقش‌های تخصصی (مانند توسعه‌دهندگان بدافزار، اپراتورهای شبکه و پول‌شویان دیجیتال) به‌صورت هماهنگ انجام می‌شود. این امر، لزوم تطبیق رویکردهای جرم‌شناسی کلاسیک با شرایط نوین را آشکار می‌سازد. به‌عنوان مثال، کاربست ترکیبی از نظریه‌هایی چون نظریه فشار، نظریه یادگیری اجتماعی و نظریه کنترل می‌تواند در درک انگیزه‌های مجرمانه

در فضای سایبری مؤثر باشد (Tabar & Hosseini, 2021). بااین‌حال، قانون‌گذاری‌های فعلی در ایران اغلب این ابعاد نظری را نادیده گرفته و به‌جای توجه به ریشه‌های اجتماعی و ساختاری جرم، صرفاً بر جرم‌انگاری اقدامات فردی تمرکز داشته‌اند.

در حوزه بین‌المللی نیز، سازمان‌هایی چون سازمان همکاری و توسعه اقتصادی و انجمن بین‌المللی جزا تعاریفی از جرایم سایبری ارائه کرده‌اند که بر غیرقانونی بودن رفتارها در فضای پردازش و انتقال داده‌ها تأکید دارند. این تعاریف، بر لزوم اتخاذ رویکردهای فراملی و هماهنگی بین‌المللی در مقابله با جرایم سازمان‌یافته سایبری دلالت می‌کنند (Li, 2024). بااین‌حال، ایران هنوز در سطح قانونی و سیاستی، به‌طور سیستماتیک از این تجربیات بهره نبرده و فاقد یک سیاست جنایی ملی یکپارچه در مقابله با جرایم سازمان‌یافته سایبری است. این امر، خلأهای قانونی را تشدید کرده و امکان پیگرد کیفری مؤثر و همکاری بین‌المللی را محدود ساخته است (Li, 2024).

همچنین، یکی از چالش‌های بنیادین در نظام حقوقی ایران، عدم توجه به حقوق پیشگیری به‌عنوان یک تعهد نتیجه‌محور دولتی است. درحالی‌که در نظام‌های پیشرفته، دولت‌ها موظف به اثبات اثربخشی اقدامات پیشگیرانه خود هستند، در ایران، این تعهد همچنان در سطح تکلیف‌محوری محدود می‌شود. این امر منجر به بحران هویت حقوق پیشگیری از جرم شده و اساساً امکان تحقق یک سیاست جنایی علمی و نظام‌مند را زیر سؤال می‌برد. به‌عنوان نمونه، ماده ۵۷۰ قانون مجازات اسلامی (بخش تعزیرات)، که به حمایت کیفری از حقوق اساسی ملت می‌پردازد، می‌تواند به‌عنوان طلیعه‌ای برای حقوق پیشگیری تلقی شود، اما بدون تکمیل آن با قواعد شکلی و ماهوی مناسب، نمی‌تواند به‌عنوان پایه‌ای برای یک نظام پیشگیری مؤثر عمل کند (Afshar et al., 2014).

در نتیجه، مسئله اصلی این پژوهش آن است که با توجه به تحولات فناورانه، گسترش جرایم سازمان‌یافته باندی و سایبری و ضعف ساختاری نظام حقوقی پیشگیری در ایران، چگونه می‌توان یک چارچوب حقوقی یکپارچه، تحلیلی و علمی برای مدیریت پیشگیری از این جرایم تدوین کرد که ضمن تمایز مفهومی بین فضاهای سایبری و مجازی، به اصول دانش‌بنیان، علت‌شناختی، نهادینه‌سازی و نتیجه‌محوری توجه کند و هم‌زمان با رفع خلأهای قانونی و نهادی، امکان کنترل مؤثر جرایم سازمان‌یافته را فراهم آورد؟

این مسئله، مستلزم پاسخ‌گویی به پرسش‌های فرعی متعددی است، از جمله:

آیا نظام حقوقی ایران، با توجه به تعاریف نامشخص و قوانین پراکنده، قادر به تشخیص و پیگرد جرایم سازمان‌یافته سایبری است؟

چگونه می‌توان بین رویکردهای کیفری و غیرکیفری (آموزش، آگاهی‌بخشی و خنثی‌سازی فنی) در پیشگیری از جرایم سایبری تعادل ایجاد کرد؟

چه نقشی از نظریه‌های جرم‌شناسی در تبیین رفتار مجرمانه در فضای سایبری ایفا می‌کند؟

چگونه می‌توان ساختارهای نهادی پیشگیری از جرم را از حالت تکلیف‌محور به‌سمت نتیجه‌محور و دانش‌بنیان تحول داد؟

آیا امکان تدوین یک قانون جامع پیشگیری از جرم در ایران وجود دارد و چه اصولی باید در آن گنجانده شود؟

این پژوهش، با بهره‌گیری از روش توصیفی-تحلیلی و با استناد به منابع قانونی داخلی، اسناد بین‌المللی و یافته‌های علوم حقوقی، جرم‌شناسی و فناوری اطلاعات، به‌دنبال تبیین یک مدل نظری و عملیاتی برای مدیریت پیشگیری حقوقی از جرایم سازمان‌یافته باندی و سایبری است که نه‌تنها به چالش‌های موجود پاسخ دهد، بلکه زمینه‌ساز تحول ساختاری در سیاست جنایی ایران باشد.

تعاریف پراکنده جرم سازمان‌یافته در نظام حقوقی ایران

برخلاف کنوانسیون پالرمو که تعریفی جامع و مستقل از جرم سازمان‌یافته ارائه می‌دهد، نظام حقوقی ایران فاقد چنین تعریفی است و به‌جای آن، تعاریف پراکنده و ناسازگاری را می‌توان در قوانین مختلف یافت که هر یک تنها بخشی از پدیده جرم سازمان‌یافته را پوشش می‌دهند.

تعریف در قانون مجازات اسلامی (ماده ۱۳۰): ماده ۱۳۰ قانون مجازات اسلامی مصوب ۲۰۱۳، نزدیک‌ترین تعریف به استانداردهای بین‌المللی را در نظام حقوقی ایران ارائه می‌دهد: «فعالیت‌های غیرقانونی و هماهنگ گروهی منسجم از اشخاص که با تبانی و برای تحصیل منافع مشترک (قدرت یا مادی)، به ارتکاب جرم مستمر و شدید می‌پردازند». این تعریف سه عنصر کلیدی را دربرمی‌گیرد: (۱) گروهی و منسجم‌بودن، (۲) تبانی و هماهنگی، و (۳) ارتکاب جرم مستمر و شدید با انگیزه منفعت مادی یا قدرت.

بااین‌حال، این تعریف دارای محدودیت‌های ساختاری است:

ابهام در مفهوم «منسجم‌بودن»: قانون معیار مشخصی برای تشخیص «منسجم‌بودن» گروه مجرمانه ارائه نمی‌دهد. آیا منسجم‌بودن مستلزم برخورداری از ساختار سلسله‌مراتبی رسمی است یا شبکه‌های غیرمتمرکز نیز مشمول آن می‌شوند؟ این ابهام در مقابله با شبکه‌های مجرمانه سایبری، که اغلب فاقد ساختار رسمی هستند، مشکل‌ساز است (Akbari & Mousavi, 2019).

عدم الزام به پایداری ساختاری: برخلاف کنوانسیون پالرمو که بر «وجود گروه در طول زمان» تأکید دارد، این تعریف صراحتاً به پایداری ساختاری اشاره نمی‌کند. این امر ممکن است به گسترش تفسیر و مشمول‌شدن جرایم گروهی موقتی در تعریف جرم سازمان‌یافته منجر شود (Saybani & Karimi, 2018).

تکیه بر مفهوم فقهی «تبانی»: ریشه این تعریف در مفهوم فقهی «تبانی» ــ توافق پنهانی علیه فرد سوم ــ است که در فقه امامیه به‌عنوان جرم مستقل شناخته می‌شود. بااین‌حال، تبانی در فقه عمدتاً بر روابط دوجانبه متمرکز است و برای تحلیل شبکه‌های پیچیده چندجانبه کافی نیست (Parvizi, 2016).

تعریف در قانون جرایم رایانه‌ای: مقررات مربوط به تشدید مجازات جرایم رایانه‌ای سازمان‌یافته مقرر می‌کنند که هرگاه ارتکاب جرم رایانه‌ای توسط دو یا چند نفر به‌صورت هماهنگ و برنامه‌ریزی‌شده صورت پذیرد، مرتکبان به‌عنوان اعضای گروه مجرمانه رایانه‌ای شناخته می‌شوند و مجازات آنان تشدید می‌گردد. این تعریف، که تنها بر جرایم رایانه‌ای متمرکز است، دارای محدودیت‌های جدی زیر است:

فقدان معیارهای ساختاری: این تعریف تنها به «هماهنگی» و «برنامه‌ریزی» اشاره می‌کند و معیارهای ساختاری، مانند پایداری و تقسیم کار تخصصی، را نادیده می‌گیرد. این امر موجب می‌شود حتی دو نفر که یک‌بار به‌صورت موقت همکاری کرده‌اند، به‌عنوان «گروه مجرمانه رایانه‌ای» شناخته شوند (Akbari & Mousavi, 2019).

نگاه مجازات‌محور: این مقررات صرفاً بر تشدید مجازات تمرکز دارند و هیچ الزامی برای اقدامات پیشگیرانه یا تحلیل ساختار شبکه‌های مجرمانه پیش‌بینی نکرده‌اند. این رویکرد نشان‌دهنده تفکر سنتی حقوق کیفری است که پیشگیری را فرع مجازات می‌داند، نه شاخه‌ای مستقل (Afshar et al., 2014).

ناتوانی در پوشش جرایم سازمان‌یافته سایبری نسل سوم: قانون جرایم رایانه‌ای، که در سال ۲۰۰۹ تدوین شد، عمدتاً بر جرایم رایانه‌ای نسل اول، مانند هک ساده، و نسل دوم، مانند کلاهبرداری آنلاین، متمرکز است و جرایم سازمان‌یافته سایبری نسل سوم را، که با ساختارهای شبکه‌ای

پیچیده، استفاده از فناوری‌های پیشرفته مانند رمزنگاری پیشرفته و بلاک‌چین و همکاری بین‌المللی همراه‌اند، پوشش نمی‌دهد (Ahmadi & Nikpour Qanvani, 2013; Gercke & Akbari, 2010).

تعریف‌های پراکنده در سایر قوانین:

قانون مبارزه با قاچاق کالا و ارز مصوب ۲۰۱۳: ماده ۱ این قانون، قاچاق را «ورود یا خروج کالا یا ارز به‌صورت غیرقانونی» تعریف می‌کند، اما به‌طور صریح به سازمان‌یافتگی شبکه‌های قاچاق اشاره نمی‌کند. بااین‌حال، ماده ۱۰ با اشاره به «شبکه‌های قاچاق»، به‌صورت ضمنی سازمان‌یافتگی این جرایم را به رسمیت می‌شناسد.

قانون ارتقای سلامت نظام اداری و مقابله با فساد مصوب ۲۰۱۱: این قانون، با تمرکز بر فساد اداری، به‌طور ضمنی شبکه‌های سازمان‌یافته فساد را هدف قرار می‌دهد، اما تعریف مستقلی از جرم سازمان‌یافته ارائه نمی‌کند.

قانون جرایم رایانه‌ای مصوب ۲۰۰۹: این قانون، جرم رایانه‌ای را «هر فعل یا ترک فعل خلاف قانون که با به‌کارگیری سامانه‌های رایانه‌ای یا مخابراتی ارتکاب یابد» تعریف می‌کند، اما هیچ اشاره‌ای به سازمان‌یافتگی ندارد (Gercke & Akbari, 2010).

این تکثر تعاریف پراکنده نشان‌دهنده فقدان چارچوب مفهومی یکپارچه‌ای در نظام حقوقی ایران است که به تفسیرهای ناهمگون قضایی و ناتوانی در شناسایی شبکه‌های مجرمانه پیچیده منجر می‌شود.

جایگاه حقوق پیشگیری در نظام حقوقی ایران؛ نقد ساختاری و شناسایی خلأها

قانون پیشگیری از وقوع جرم مصوب ۲۰۱۷، به‌عنوان نخستین تلاش نظام‌مند برای تدوین چارچوب حقوقی پیشگیری در ایران، اگرچه گامی مثبت محسوب می‌شود، دارای خلأهای ساختاری عمیقی است که اثربخشی آن را زیر سؤال می‌برد.

خلأ ساختاری در مقابله با جرایم سازمان‌یافته

تحلیل نظام حقوقی ایران در مقابله با جرایم سازمان‌یافته، خلأهای ساختاری اساسی زیر را آشکار می‌سازد:

خلأ مفهومی: این قانون، پیشگیری را «پیش‌بینی، شناسایی و ارزیابی خطر وقوع جرم و اتخاذ تدابیر لازم برای از میان بردن یا کاهش آن» تعریف می‌کند، اما فاقد تعریف عملیاتی از «خطر جنایی» و «تدابیر لازم» است. این ابهام مفهومی به تفسیرهای گسترده و گاه متناقض دستگاه‌های اجرایی منجر شده است. برای مثال، برخی نهادها پیشگیری را معادل نظارت امنیتی گسترده می‌دانند، درحالی‌که برخی دیگر آن را به آموزش عمومی محدود می‌کنند (Ahmadi et al., 2016).

خلأ تعریفی: نظام حقوقی ایران فاقد تعریف مستقل و جامع از «جرم سازمان‌یافته» است. درحالی‌که کنوانسیون پالرمو مصوب ۲۰۰۰، جرم سازمان‌یافته را بر اساس سه شاخص ساختار پایدار، همکاری گروهی و انگیزه اقتصادی تعریف می‌کند، در ایران این مفهوم تنها به‌صورت پراکنده در قانون مجازات اسلامی و قانون جرایم رایانه‌ای مورد اشاره قرار گرفته است. این فقدان تعریف مستقل به تفسیرهای ناهمگون قضایی و ناتوانی در شناسایی شبکه‌های مجرمانه پیچیده منجر شده است (Bryant, 2021).

خلأ نهادی: این قانون، با وجود ایجاد «شورای عالی پیشگیری از وقوع جرم»، سازوکاری برای حل تعارض میان این شورا و سایر نهادهای موازی، مانند شورای عالی فضای مجازی، پیش‌بینی نکرده است. این امر به تکثر ساختاری و هدررفت منابع منجر شده است.

خلأ ارزیابی: این قانون فاقد سازوکارهای شفاف برای ارزیابی اثربخشی برنامه‌های پیشگیری است. درحالی‌که در کشورهایی مانند انگلستان، هر برنامه پیشگیری موظف به ارائه گزارش سالانه بر اساس شاخص‌های کمّی، مانند نرخ کاهش جرایم هدف‌گذاری‌شده، است، در ایران چنین الزامی وجود ندارد. این خلأ، پیشگیری را از یک «تعهد نتیجه‌محور» به یک «تکلیف فعالیت‌محور» تبدیل کرده است (Moisiienko, 2024).

خلأ تمایز مفهومی میان فضای سایبری و فضای مجازی: یکی از خلأهای حیاتی در نظام حقوقی ایران، استفاده نامناسب و مترادف از اصطلاحات «فضای مجازی» و «بستر مجازی» در قوانین متعدد، از جمله ماده ۲ (۵۰۰ مکرر) قانون مجازات اسلامی، ماده ۹ قانون حمایت از اطفال و نوجوانان و مواد ۵۹ و ۶۰ قانون حمایت از خانواده و جوانی جمعیت مصوب ۲۰۲۱، است. درحالی‌که «فضای سایبری» به‌عنوان بستر فنی‌ـفیزیکی‌ـمنطقی، شامل شبکه‌ها، سرورها و پروتکل‌ها، تعریف می‌شود و حوزه جرایم وابسته به سایبر را تشکیل می‌دهد، «فضای مجازی» محیط اجتماعی‌ـفرهنگی ساخته‌شده بر بستر سایبری، مانند شبکه‌های اجتماعی و متاورس، است که حوزه جرایم تسهیل‌شده به‌وسیله سایبر را دربرمی‌گیرد (Tabar & Hosseini, 2021).

عدم تمایز مفهومی میان این دو، به طراحی راهکارهای پیشگیری ناکارآمد منجر شده است؛ برای مثال، مقررات نظارتی طراحی‌شده برای شبکه‌های اجتماعی، به‌عنوان فضای مجازی، در مقابله با حملات سایبری علیه زیرساخت‌های حیاتی، به‌عنوان بخشی از فضای سایبری، بی‌اثر هستند.

خلأ نهادی در پیشگیری سایبری

با وجود فعالیت پلیس فتا به‌عنوان نهاد اجرایی اصلی در مقابله با جرایم سایبری، ایران فاقد نهادی تخصصی برای پیشگیری از جرایم سازمان‌یافته سایبری است. در کشورهای پیشرفته، مانند انگلستان، مرکز ملی جرایم سایبری، علاوه بر پاسخ‌گویی به حوادث، مسئولیت شناسایی تهدیدات نوظهور و طراحی برنامه‌های پیشگیرانه را نیز بر عهده دارد (Moisiienko, 2024).

در ایران، این مسئولیت به‌صورت پراکنده میان چندین نهاد تقسیم شده و هیچ نهادی مسئولیت کلی مدیریت پیشگیری سایبری را بر عهده ندارد. این خلأها نشان می‌دهند که نظام حقوقی ایران هنوز از گذار از «حقوق پیشگیری به‌عنوان تکلیف فرعی» به «حقوق پیشگیری به‌عنوان سیاست ملی مستقل» عاجز مانده است. تحقق این گذار مستلزم تدوین قانون جامع «مدیریت پیشگیری و کنترل جرایم سازمان‌یافته» است که بر اصول فرابخشی، دانش‌بنیانی و نتیجه‌محوری استوار باشد.

تحلیل مفهومی ـ تطبیقی ساختار سازمانی جرایم سازمان‌یافته سایبری و جرایم باندی

جدول زیر تفاوت‌های کلیدی ساختار سازمانی در دو نوع جرم را نشان می‌دهد:

جدول ۱. تفاوت‌های کلیدی ساختار سازمانی

ویژگی ساختاری	جرایم باندی (فیزیکی)	جرایم سازمان‌یافته سایبری
الگوی ساختاری	سلسله‌مراتبی یا شبکه‌ای متمرکز	شبکه‌ای غیرمتمرکز و پویا
ثبات اعضا	اعضای ثابت با وفاداری بلندمدت	اعضای موقتی با همکاری پروژه‌محور
محل هماهنگی	پاتوق فیزیکی (مکان مشخص)	پلتفرم‌های دیجیتال رمزنگاری‌شده
تقسیم کار	بر اساس نقش‌های سنتی (رهبر، مالخر، اجراکننده)	بر اساس تخصص فنی (توسعه‌دهنده، اپراتور، پول‌شوی)
پایداری	پایداری هم‌زمان ساختار و عملیات	پایداری ساختار در مقابل پویایی عملیات
چالش شناسایی	شناسایی مکان فیزیکی و ارتباطات	شناسایی هویت واقعی در فضای ناشناس

این تحلیل نشان می‌دهد که رویکرد سنتی شناسایی جرایم سازمان‌یافته، که بر یافتن ساختار سلسله‌مراتبی و اعضای ثابت متمرکز است، در مقابله با جرایم سایبری ناکارآمد است. نظام حقوقی ایران، که در ماده ۱۳۰ قانون مجازات اسلامی بر «گروهی و منسجم‌بودن» تأکید دارد، فاقد معیارهای شفاف برای شناسایی ساختارهای شبکه‌ای غیرمتمرکز است (Akhavat, 2015). این خلأ موجب می‌شود بسیاری از شبکه‌های مجرمانه سایبری، به‌دلیل فقدان ساختار رسمی، به‌عنوان جرم سازمان‌یافته شناخته نشوند.

ساختار سازمانی شبکه‌های مجرمانه سایبری بر سه رکن استوار است: شبکه‌ای‌بودن غیرمتمرکز که پویایی و انعطاف‌پذیری عملیاتی را فراهم می‌آورد؛ تقسیم کار تخصصی فنی که کارایی عملیاتی را افزایش می‌دهد؛ و وجود گروه‌های حمایت‌شده توسط دولت‌ها (ارتش‌های سایبری) که اهداف سیاسی ـ استراتژیک را دنبال می‌کنند. این ویژگی‌ها، شبکه‌های مجرمانه سایبری را از باندهای فیزیکی متمایز می‌سازند و نشان می‌دهند که راهکارهای پیشگیری از جرایم سایبری باید بر تقویت امنیت سایبری فنی (رمزنگاری و نظارت شبکه‌ای)، همکاری بین‌المللی در ردیابی سرورها و تبادل اطلاعات تهدیدات و هدایت استعدادهای فنی جوان به مسیرهای قانونی متمرکز باشند. بدون درک این ویژگی‌های ساختاری، هرگونه تلاش برای مقابله با جرایم سازمان‌یافته سایبری صرفاً به اقدامات واکنشی و ناکارآمد محدود خواهد شد.

شاخص انگیزه‌های ارتکاب

انگیزه‌های ارتکاب به دلایل و عواملی اشاره دارند که گروه مجرمانه را به ارتکاب جرم سوق می‌دهند. درحالی‌که در جرایم سازمان‌یافته سنتی، انگیزه اقتصادی غالب است، در جرایم سایبری طیف گسترده‌تری از انگیزه‌ها، از جمله انگیزه‌های روان‌شناختی و اجتماعی دیجیتال، مشاهده می‌شود.

انگیزه‌های ارتکاب در جرایم باندی

انگیزه‌های ارتکاب جرایم سازمان‌یافته باندی را نمی‌توان صرفاً به عوامل فردی یا روان‌شناختی محدود کرد؛ بلکه این انگیزه‌ها در بافتی ساختاری شکل می‌گیرند که در آن، تعامل پیچیده‌ای میان شرایط اقتصادی، نابرابری‌های اجتماعی، هنجارهای فرهنگی محلی و فرصت‌های ساختاری جرم‌زا، فرد را به‌سمت عضویت در باند سوق می‌دهد. در این بند، با تحلیل سه دسته از انگیزه‌های کلیدی اقتصادی، قدرت و پیوندهای اجتماعی ـ فرهنگی و بررسی علل ساختاری زمینه‌ساز آن‌ها، چارچوبی تحلیلی برای درک عمیق‌تر ریشه‌های جرایم سازمان‌یافته باندی ارائه می‌شود.

۱. انگیزه اقتصادی محض: این انگیزه، که ریشه در فقر ساختاری، بیکاری و نابرابری اقتصادی دارد، شایع‌ترین انگیزه در جرایم باندی است. باندهای قاچاق کالا، مواد مخدر و فساد مالی عمدتاً با هدف کسب درآمد غیرقانونی فعالیت می‌کنند. مطالعات نشان می‌دهند که ۷۸ درصد باندهای فعال در ایران، انگیزه اقتصادی را به‌عنوان عامل اصلی فعالیت خود ذکر می‌کنند (Taghizadeh et al., 2017). بااین‌حال، تفسیر این انگیزه صرفاً به «گرایش به کسب درآمد غیرقانونی» محدود نمی‌شود؛ بلکه در بافتی ساختاری شکل می‌گیرد که در آن، سه عامل کلیدی هم‌زمان تأثیرگذارند:

فقر ساختاری و بیکاری مزمن: تحلیل نقشه‌های جرم‌زایی شهر تهران در سال ۲۰۲۳ نشان می‌دهد که ۷۳ درصد پاتوق‌های شناسایی‌شده باندهای فعال در محلاتی با شاخص‌های زیر قرار دارند:

نرخ بیکاری بالاتر از ۲۰ درصد، در مقابل میانگین شهری ۱۲ درصد؛

تراکم جمعیتی بالا، بیش از ۱۵۰ نفر در هکتار؛

فاصله بیش از دو کیلومتر از مراکز اشتغال‌زایی و خدمات دولتی.

این شاخص‌ها نشان‌دهنده «فقر ساختاری» هستند؛ یعنی وضعیتی که در آن، فرد به‌دلیل محدودیت‌های سیستمی، مانند دسترسی نابرابر به آموزش، بازار کار بسته و فقدان سرمایه اولیه، از مسیرهای قانونی کسب درآمد محروم می‌شود (Beigi & Khoshyari, 2011). در چنین شرایطی، عضویت در باند نه به‌عنوان انتخابی عقلانی برای ثروتمندشدن، بلکه به‌عنوان «راه‌حلی اجباری برای بقا» تلقی می‌شود.

نابرابری اقتصادی و تبعیض ساختاری: مطالعات جرم‌شناختی نشان می‌دهند که نابرابری اقتصادی، نه فقر مطلق، عامل کلیدی در جرم‌زایی است. شاخص جینی در مناطق پرجرم تهران (۰/۵۸) به‌طور معناداری بالاتر از میانگین ملی (۰/۴۲) است. این نابرابری، احساس محرومیت نسبی را در جوانان ایجاد می‌کند؛ یعنی احساسی که در آن، فرد با مشاهده درآمدهای بالای دیگران در رسانه‌ها یا محیط اطراف، خود را محروم و بی‌ارزش می‌بیند (Vatani & Asadi, 2016). این احساس، زمینه‌ساز پذیرش ارزش‌های ضداجتماعی باندها می‌شود.

فرصت‌های ساختاری جرم‌زا: در مناطق محروم، فرصت‌های قانونی کسب درآمد محدودند، اما فرصت‌های غیرقانونی، مانند شبکه‌های قاچاق کالا و مواد مخدر یا فساد اداری، به‌دلیل ضعف نظارتی و فساد نهادی فراوان هستند. این ترکیب از «محدودیت فرصت‌های مشروع» و «فراوانی فرصت‌های نامشروع»، محیطی را فراهم می‌آورد که در آن، عضویت در باند به‌عنوان «راه‌حلی منطقی» برای جوانان بی‌سرمایه تلقی می‌شود (Najafi Abrandabadi, 2016).

۲. انگیزه قدرت و نفوذ: برخی باندها، به‌ویژه در حوزه فساد اداری و سیاسی، فراتر از کسب درآمد، به‌دنبال ایجاد نفوذ در ساختارهای قدرت هستند. این انگیزه اغلب با شبکه‌سازی در میان مقامات اداری و قضایی همراه است و هدف آن، ایجاد حیطه نفوذی است که فعالیت‌های مجرمانه را از پیگرد قضایی مصون نگه دارد (Yar et al., 2011).

۳. انگیزه‌های اجتماعی ـ فرهنگی: در برخی جوامع محلی، عضویت در باند به‌عنوان نماد مردانگی، شجاعت یا وفاداری به گروه قومی ـ خانوادگی تلقی می‌شود. این انگیزه، که ریشه در هنجارهای محلی دارد، به‌ویژه در باندهای فعال در حاشیه شهرها و مناطق محروم مشاهده می‌شود (Beigi & Khoshyari, 2011).

انگیزه‌های ارتکاب در جرایم سازمان‌یافته سایبری

انگیزه‌های ارتکاب جرایم سازمان‌یافته سایبری، در مقایسه با جرایم سازمان‌یافته باندی، طیف گسترده‌تر و پیچیده‌تری دارند که ریشه در ماهیت غیرمکانی، ناشناس و فرامرزی فضای سایبری دارد. برخلاف باندهای فیزیکی که عمدتاً با انگیزه اقتصادی یا قدرت فعالیت می‌کنند، شبکه‌های مجرمانه سایبری از ترکیبی از انگیزه‌های اقتصادی، سیاسی ـ ایدئولوژیک و روان‌شناختی دیجیتال بهره می‌برند که هر یک نیازمند رویکرد پیشگیرانه مجزایی هستند. با تحلیل سه دسته انگیزه کلیدی مالی، سیاسی ـ ایدئولوژیک و روان‌شناختی دیجیتال و بررسی کاربست نظریه‌های جرم‌شناختی در تبیین این انگیزه‌ها، چارچوبی تحلیلی برای درک عمیق‌تر ریشه‌های جرایم سازمان‌یافته سایبری ارائه می‌شود.

۱. انگیزه مالی، مشابه جرایم باندی: کلاهبرداری‌های بانکی، سرقت اطلاعات کارت‌های اعتباری و باج‌افزارها عمدتاً با انگیزه مالی ارتکاب می‌یابند. بااین‌حال، تفاوت کلیدی در سازوکار کسب درآمد است: درحالی‌که باندهای فیزیکی از طریق فروش کالاهای قاچاق درآمدزایی می‌کنند، گروه‌های سایبری از طریق ارزهای دیجیتال و شبکه‌های پیچیده پول‌شویی، درآمد خود را پنهان می‌کنند (Yarovenko & Rogkova, 2022).

۲. انگیزه سیاسی و ایدئولوژیک: گروه‌هایی مانند هکتیویست‌ها، از جمله گروه آنونیموس، یا گروه‌های حمایت‌شده توسط دولت‌ها، مانند گروه‌های سایبری روسیه یا چین، با انگیزه‌های سیاسی و ایدئولوژیک فعالیت می‌کنند. این گروه‌ها اغلب به‌دنبال افشای اطلاعات محرمانه، تضعیف دشمنان سیاسی یا ایجاد بحران در کشورهای هدف هستند (Radoglou-Grammatikis et al., 2021). این انگیزه در تعریف کنوانسیون پالرمو، که بر انگیزه اقتصادی تأکید دارد، جای نمی‌گیرد.

۳. انگیزه‌های روان‌شناختی دیجیتال: این دسته از انگیزه‌ها، که ویژه فضای سایبری است، شامل موارد زیر می‌شود:

شهرت دیجیتال: برخی مجرمان سایبری، به‌ویژه جوانان، به‌دنبال کسب شهرت در جوامع تخصصی دارک‌نت هستند. این شهرت ممکن است از طریق افشای آسیب‌پذیری‌های امنیتی بزرگ یا هک سامانه‌های معروف کسب شود (Bryant, 2021).

سرگرمی و چالش فنی: برخی هکرها فعالیت‌های مجرمانه را به‌عنوان چالشی فنی و نوعی سرگرمی در نظر می‌گیرند و انگیزه مالی برای آنان در مرتبه دوم اهمیت قرار دارد.

انتقام شخصی: این انگیزه شامل حملات سایبری علیه افراد یا سازمان‌های خاصی است که ریشه در تنش‌های شخصی یا حرفه‌ای دارند.

این انگیزه‌ها، که در جرایم سنتی کمتر دیده می‌شوند، نشان می‌دهند که تحلیل جرایم سایبری مستلزم درک فرهنگ دیجیتال و روان‌شناسی کاربران فضای سایبری است.

جدول ۲. تحلیل تطبیقی انگیزه‌های ارتکاب

نوع انگیزه	جرایم باندی	جرایم سایبری	پیامد برای سیاست پیشگیری
اقتصادی	غالب (۷۸ درصد)	غالب در جرایم مالی	نیاز به مبارزه با ریشه‌های ساختاری فقر و بیکاری
قدرت و نفوذ	شایع، به‌ویژه در فساد اداری	محدود، به‌جز حملات دولتی	نیاز به شفاف‌سازی در نظام اداری
سیاسی و ایدئولوژیک	نادر	شایع در هکتیویسم و جنگ سایبری	نیاز به رویکرد بین‌المللی و دیپلماسی سایبری
روان‌شناختی دیجیتال	نامرتبط	شایع، مانند شهرت و سرگرمی	نیاز به آموزش اخلاق دیجیتال و هدایت استعدادهای فنی

این تحلیل نشان می‌دهد که سیاست‌های پیشگیری از جرایم سایبری نمی‌توانند صرفاً بر مبارزه با انگیزه اقتصادی متمرکز باشند؛ بلکه باید به انگیزه‌های روان‌شناختی و فرهنگی دیجیتال نیز توجه کنند. نظام حقوقی ایران، که در ماده ۱۳۰ قانون مجازات اسلامی تنها به «منافع مشترک (قدرت یا مادی)» اشاره می‌کند، فاقد چارچوبی برای تحلیل انگیزه‌های نوین سایبری است.

بستر وقوع باندهای فیزیکی در مقابل شبکه‌های سایبری

جدول ۳. تفاوت‌های کلیدی بستر وقوع

بُعد تحلیلی	جرایم سازمان‌یافته باندی (فیزیکی)	جرایم سازمان‌یافته سایبری	پیامد برای سیاست پیشگیری
الگوی ساختاری	سلسله‌مراتبی رسمی و ثابت	شبکه‌ای غیرمتمرکز و پویا	برای باندها، شناسایی مکان فیزیکی و ساختار سلسله‌مراتبی؛ برای جرایم سایبری، تحلیل داده‌های شبکه و ردیابی تراکنش‌های دیجیتال
ثبات اعضا	اعضای ثابت با وفاداری بلندمدت	اعضای موقتی با همکاری پروژه‌محور	برای باندها، شکستن وفاداری گروهی؛ برای جرایم سایبری، استفاده از معافیت‌ها و تخفیف‌های قضایی برای جلب همکاری اعضای موقتی
مکان هماهنگی	پاتوق فیزیکی و مشخص	پلتفرم‌های دیجیتال رمزنگاری‌شده	برای باندها، گشت‌زنی فیزیکی و دوربین‌های مداربسته؛ برای جرایم سایبری، نظارت فنی شبکه و تحلیل ترافیک داده‌ها
انگیزه اقتصادی	ریشه در فقر ساختاری و بقا	ریشه در بازدهی بالا و هزینه پایین	برای باندها، مقابله با فقر ساختاری و ایجاد فرصت‌های اشتغال؛ برای جرایم سایبری، ایجاد فرصت‌های شغلی فنی برای جوانان مستعد

انگیزه قدرت	نفوذ محلی و کنترل فیزیکی	شهرت دیجیتال و تأثیر فنی	برای باندها، تقویت پیوندهای اجتماعی متعارف؛ برای جرایم سایبری، ایجاد مجاری مشروع کسب شهرت فنی، مانند مسابقات امنیت سایبری
پیوندهای اجتماعی	خانوادگی، قومی و مبتنی بر هنجارهای محلی	هویت دیجیتال و تخصص فنی	برای باندها، بازتوانی اجتماعی و تقویت خانواده؛ برای جرایم سایبری، آموزش اخلاق دیجیتال و هدایت استعدادهای فنی
ماهیت بستر	فضای فیزیکی ـ مکانی با مختصات جغرافیایی مشخص	فضای غیرمکانی و پراکنده در سراسر جهان	برای باندها، قوانین محلی و ملی؛ برای جرایم سایبری، همکاری بین‌المللی و تطبیق قوانین با استانداردهای جهانی
قابلیت نظارت	نظارت فیزیکی از طریق گشت‌زنی و دوربین	نظارت صرفاً از طریق ابزارهای فنی	برای باندها، پلیس انتظامی و امنیتی؛ برای جرایم سایبری، نهاد تخصصی امنیت سایبری دارای اختیارات فنی و بین‌المللی
نقش زندان	زندان به‌عنوان «مدرسه جرم» و فضای شبکه‌سازی	تأثیر محدود زندان بر شبکه‌های سایبری	برای باندها، جداسازی مجرمان سازمان‌یافته و برنامه‌های بازپروری تخصصی؛ برای جرایم سایبری، محدودسازی دسترسی به اینترنت و ابزارهای فنی در زندان

این تحلیل نشان می‌دهد که راهکارهای پیشگیری از جرایم باندی نمی‌توانند صرفاً بر مقابله با بستر فیزیکی متمرکز باشند؛ بلکه باید به پیوندهای اجتماعی ـ فرهنگی و علل ساختاری جرم‌زایی نیز توجه کنند. نظام حقوقی ایران، که در ماده ۱۳۰ قانون مجازات اسلامی تنها به «گروهی و منسجم‌بودن» اشاره می‌کند، فاقد چارچوبی برای تحلیل این بسترهای تکوینی است.

بستر وقوع جرایم سازمان‌یافته باندی، که شامل زندان، محلات محروم و شبکه‌های خانوادگی ـ قومی است، نقشی تعیین‌کننده در تکوین و تداوم این جرایم ایفا می‌کند. زندان‌ها، به‌جای بازپروری، به «مدارس جرم» تبدیل شده‌اند که در آن‌ها، تکنیک‌های مجرمانه و شبکه‌های سازمانی جدید شکل می‌گیرند. محلات محروم، با ویژگی‌هایی مانند فقر ساختاری، بیکاری بالا و نظارت اجتماعی ضعیف، فضایی مناسب برای شکل‌گیری پاتوق‌ها و تداوم فعالیت باندها فراهم می‌کنند. شبکه‌های خانوادگی ـ قومی نیز از طریق سازوکارهای یادگیری اجتماعی و وفاداری گروهی، جوانان را به‌سمت عضویت در باندها سوق می‌دهند. سیاست‌های پیشگیری مؤثر باید هم‌زمان در سه سطح مداخله کنند: (۱) اصلاح ساختار زندان‌ها و جداسازی مجرمان سازمان‌یافته؛ (۲) احیای فضاهای شهری محروم و افزایش نظارت اجتماعی؛ و (۳) تقویت پیوندهای اجتماعی سنتی و ایجاد فضاهای امن برای تعامل جوانان. بدون این رویکرد تلفیقی، هرگونه تلاش برای مقابله با جرایم سازمان‌یافته باندی صرفاً به اقدامات واکنشی و ناکارآمد محدود خواهد شد.

تطبیق و تمایز جرایم باندی و سایبری

درک عمیق جرایم سازمان‌یافته مستلزم تحلیل هم‌زمان اشتراکات و تمایزات میان اشکال مختلف آن است. جرایم سازمان‌یافته باندی (فیزیکی) و جرایم سازمان‌یافته سایبری، باوجود تفاوت‌های ساختاری و بستری عمیق، دارای اشتراکات ماهوی هستند که پایه‌ای برای طراحی سیاست جنایی یکپارچه فراهم می‌آورند. درعین‌حال، تمایزات آن‌ها مستلزم اتخاذ رویکردهای تخصصی‌شده در سطح اجرایی است. این بحث، با تحلیل تطبیقی اشتراکات و تمایزات، چارچوبی تحلیلی برای طراحی سیاست پیشگیری یکپارچه، اما تفکیک‌پذیر، ارائه می‌دهد.

اشتراکات: سازمان‌یافتگی، انگیزه اقتصادی ـ قدرت و فراملی‌بودن

تحلیل تطبیقی جرایم سازمان‌یافته باندی و سایبری نشان می‌دهد که این دو دسته جرم سه اشتراک ماهوی اساسی دارند که آن‌ها را از جرایم گروهی موقتی و تک‌نفره متمایز می‌سازد: سازمان‌یافتگی ساختاری، انگیزه اقتصادی ـ قدرت و گرایش به فراملی‌شدن. این اشتراکات، پایه‌ای برای تدوین سیاست جنایی یکپارچه در سطح راهبردی فراهم می‌آورند.

سازمان‌یافتگی ساختاری؛ هسته ماهوی جرایم سازمان‌یافته

سازمان‌یافتگی ساختاری، که در کنوانسیون پالرمو مصوب ۲۰۰۰ بر اساس سه شاخص پایداری ساختار، هماهنگی گروهی و انگیزه اقتصادی تعریف شده است، هسته ماهوی مشترک جرایم سازمان‌یافته باندی و سایبری است که آن‌ها را از جرایم گروهی موقتی متمایز می‌سازد.

الف) پایداری ساختار در دو الگوی متفاوت: در جرایم باندی، پایداری ساختار معمولاً به‌صورت سلسله‌مراتبی رسمی و ثابت ظاهر می‌شود و اعضا در طول زمان، معمولاً سال‌ها، در سطوح مختلف، مانند رهبر، سرپرست محله‌ای و اعضای اجرایی، فعالیت می‌کنند (Beigi & Khoshyari, 2011). در جرایم سایبری، پایداری ساختار به‌صورت شبکه‌ای غیرمتمرکز و پویا شکل می‌گیرد؛ یعنی خود شبکه، برای مثال یک فروم تخصصی در دارک‌نت یا کانال رمزنگاری‌شده، پایدار می‌ماند، اما ترکیب اعضا و نوع عملیات در هر مرحله تغییر می‌کند (Gkoktsis et al., 2023). این تفاوت در نحوه تجلی پایداری، ذات پایداری ساختاری را تغییر نمی‌دهد؛ هر دو نوع جرم دارای ساختاری پایدارند که فراتر از همکاری موقت است.

ب) هماهنگی گروهی برنامه‌ریزی‌شده: هم باندهای فیزیکی و هم شبکه‌های سایبری بر هماهنگی گروهی برنامه‌ریزی‌شده استوارند. در باندهای فیزیکی، این هماهنگی از طریق جلسات در پاتوق‌ها و تقسیم کار تخصصی، مانند رهبری، مالخری و اجرا، صورت می‌گیرد (Beigi & Khoshyari, 2011). در شبکه‌های سایبری، هماهنگی از طریق پلتفرم‌های رمزنگاری‌شده و تقسیم کار تخصصی فنی، مانند توسعه‌دهنده بدافزار، اپراتور شبکه و پول‌شوی دیجیتال، انجام می‌شود (Gkoktsis et al., 2023). این تفاوت در ابزار هماهنگی، ماهیت هماهنگی گروهی را تغییر نمی‌دهد؛ هر دو نوع جرم نتیجه همکاری برنامه‌ریزی‌شده گروهی هستند، نه تجمیع اقدامات فردی.

ج) انگیزه اقتصادی به‌عنوان هسته مشترک: کنوانسیون پالرمو جرم سازمان‌یافته را بر اساس «انگیزه اقتصادی یا مادی» تعریف می‌کند. این انگیزه در هر دو نوع جرم حضور دارد. در جرایم باندی، انگیزه اقتصادی عامل اصلی فعالیت بسیاری از باندهاست (Taghizadeh et al., 2017). در جرایم سایبری نیز بخش مهمی از جرایم سازمان‌یافته سایبری به کلاهبرداری‌های بانکی و مالی مربوط می‌شود (Akbari & Mousavi, 2019). این اشتراک، پایه‌ای برای تطبیق تعریف کنوانسیون پالرمو با جرایم سایبری فراهم می‌آورد؛ زیرا باوجود تفاوت در سازوکارهای کسب درآمد، یعنی فروش کالای قاچاق در مقابل پول‌شویی دیجیتال، هسته انگیزه اقتصادی مشترک است.

انگیزه قدرت و نفوذ

فراتر از انگیزه اقتصادی محض، هر دو نوع جرم دارای انگیزه قدرت و نفوذ هستند که در دو سطح ظاهر می‌شود:

الف) نفوذ در ساختارهای قدرت: باندهای فیزیکی با شبکه‌سازی در میان مقامات اداری و قضایی به‌دنبال ایجاد حیطه‌ای هستند که فعالیت‌های مجرمانه آن‌ها را از پیگرد قضایی مصون نگه دارد (Sobhkhiz, 2015). شبکه‌های سایبری نیز، به‌ویژه گروه‌های حمایت‌شده توسط دولت‌ها، با نفوذ به سامانه‌های حساس، مانند بانکداری و زیرساخت‌های حیاتی، به‌دنبال ایجاد قدرت سایبری هستند که امکان اعمال فشار سیاسی یا اقتصادی را فراهم می‌آورد (Li, 2024).

ب) نماد قدرت در جامعه محلی یا دیجیتال: در باندهای فیزیکی، عضویت در باند به‌عنوان نماد «مردانگی» و «قدرت» در جامعه محلی تلقی می‌شود (Beigi & Khoshyari, 2011). در شبکه‌های سایبری، کسب شهرت دیجیتال در جوامع تخصصی دارک‌نت به‌عنوان نماد قدرت فنی و اجتماعی عمل می‌کند. این اشتراک نشان می‌دهد که جرایم سازمان‌یافته، چه فیزیکی و چه سایبری، فراتر از کسب درآمد، به‌دنبال ایجاد «حیطه نفوذ» هستند که در آن، گروه مجرمانه به‌عنوان قدرتی واقعی تلقی می‌شود.

گرایش به فراملی‌شدن؛ چالش مشترک برای سیاست جنایی

یکی از ویژگی‌های مشترک جرایم سازمان‌یافته باندی و سایبری، گرایش ذاتی به فراملی‌شدن است که ریشه در ماهیت اقتصاد جهانی و فناوری دیجیتال دارد.

الف) شبکه‌های قاچاق فراملی: باندهای فیزیکی فعال در حوزه قاچاق کالا و ارز، از شبکه‌های فراملی برای انتقال کالاها از کشورهای تولیدکننده به کشورهای مصرف‌کننده استفاده می‌کنند (Taghizadeh et al., 2017).

ب) شبکه‌های سایبری فراملی: شبکه‌های مجرمانه سایبری، به‌دلیل ماهیت فرامرزی فضای سایبری، به‌راحتی فراملی می‌شوند. در این جرایم، ممکن است دست‌کم یکی از اعضا، سرورها یا قربانیان در خارج از مرزهای کشور محل وقوع نتیجه مجرمانه قرار داشته باشد (Farhadi Alashti & Javan Jafari Bojnordi, 2017).

ج) چالش‌های مشترک برای سیاست جنایی: این گرایش به فراملی‌شدن، چالش‌های مشترک زیر را برای سیاست جنایی ایجاد می‌کند:

چالش حاکمیت: کدام کشور حق تعقیب قضایی دارد؟

چالش همکاری بین‌المللی: فرایندهای قضایی سنتی، مانند درخواست کمک قضایی متقابل، به‌دلیل کندی ذاتی، برای مقابله با جرایم فراملی ناکارآمد هستند.

چالش اجرای حکم: حتی در صورت صدور حکم قضایی، اجرای آن در کشورهای دیگر، به‌دلیل تفاوت‌های حقوقی و سیاسی، با دشواری مواجه است (Sobhkhiz, 2015).

این چالش‌های مشترک، ضرورت طراحی سیاست جنایی بین‌المللی یکپارچه برای مقابله با جرایم سازمان‌یافته، اعم از فیزیکی و سایبری، را آشکار می‌سازند.

تمایزات ساختاری، انگیزه‌ای و بستری و تأثیر آن‌ها بر سیاست جنایی پیشگیری

درحالی‌که اشتراکات ماهوی جرایم سازمان‌یافته باندی و سایبری پایه‌ای برای طراحی سیاستی یکپارچه در سطح راهبردی فراهم می‌آورند، تمایزات عمیق آن‌ها در سطوح ساختاری، انگیزه‌ای و بستری مستلزم اتخاذ رویکردهای تخصصی‌شده در سطح اجرایی است. این تمایزات، که ریشه در ماهیت فضاهای فیزیکی و سایبری دارند، سه پیامد کلیدی برای سیاست جنایی پیشگیری ایجاد می‌کنند: (۱) ناتوانی راهکارهای یکسان در پوشش هر دو نوع جرم؛ (۲) نیاز به نهادهای مسئول تخصصی‌شده با اختیارات متناسب؛ و (۳) ضرورت تدوین شاخص‌های ارزیابی مجزا برای سنجش اثربخشی. در این قسمت، با تحلیل دقیق این تمایزات و ارائه جدول تحلیلی ـ تطبیقی جامع، چارچوبی عملیاتی برای طراحی سیاست پیشگیری «یکپارچه در راهبرد و تفکیک‌پذیر در اجرا» ارائه می‌شود.

تمایزات ساختاری؛ سلسله‌مراتب ثابت در مقابل شبکه پویا

ساختار سازمانی جرایم سازمان‌یافته باندی و سایبری دارای تفاوت‌های بنیادینی است که مستقیماً بر راهکارهای شناسایی و کنترل آن‌ها تأثیر می‌گذارد.

الگوی ساختاری؛ سلسله‌مراتب رسمی در مقابل شبکه غیرمتمرکز

باندهای فیزیکی: باندهای فیزیکی عمدتاً بر ساختار سلسله‌مراتبی رسمی استوارند که در آن، تصمیم‌گیری از بالا به پایین جریان دارد و نقش‌ها به‌صورت مشخص و تثبیت‌شده تعریف شده‌اند. این ساختار سه سطح را دربرمی‌گیرد: رهبر باند در سطح رهبری، سرپرست محله‌ای در سطح

میانی و اعضای اجرایی در سطح پایینی. ثبات این ساختار در طول زمان، معمولاً طی سال‌ها، و وضوح نقش‌ها، شناسایی ساختار مجرمانه را، هرچند دشوار، امکان‌پذیر می‌سازد (Taghizadeh et al., 2017).

شبکه‌های سایبری: شبکه‌های مجرمانه سایبری عمدتاً بر ساختار شبکه‌ای غیرمتمرکز استوارند که در آن:

اعضا ثابت نیستند و ممکن است ترکیب آن‌ها در هر عملیات تغییر کند؛

نقش‌ها بر اساس تخصص فنی، مانند توسعه بدافزار، عملیات شبکه و پول‌شویی دیجیتال، تعریف می‌شوند، نه بر اساس موقعیت سلسله‌مراتبی؛

هماهنگی از طریق پلتفرم‌های رمزنگاری‌شده، مانند پیام‌رسان‌های رمزگذاری‌شده، تور و دارک‌وب، صورت می‌گیرد که شناسایی هویت واقعی را به‌شدت دشوار می‌سازد (Nguyen & Sikal, 2021).

این تفاوت ساختاری پیامد عملیاتی عمیقی دارد: در باندهای فیزیکی، حذف رهبر معمولاً ساختار سازمانی را از بین می‌برد؛ درحالی‌که در شبکه‌های سایبری، حذف یک گره لزوماً به فروپاشی کل شبکه منجر نمی‌شود؛ زیرا سایر گره‌ها می‌توانند ارتباطات را بازسازی کنند.

ثبات اعضا؛ وفاداری بلندمدت در مقابل همکاری پروژه‌محور

باندهای فیزیکی: اعضای باندهای فیزیکی معمولاً دارای وفاداری بلندمدت به گروه هستند که از طریق سازوکارهایی مانند تهدید فیزیکی، پیوندهای خانوادگی ـ قومی و سود اقتصادی مستمر شکل می‌گیرد. خودداری اعضا از افشای اطلاعات در مراحل اولیه تحقیقات، نشانه‌ای از اثربخشی سازوکارهای وفاداری گروهی است (Taghizadeh et al., 2017).

شبکه‌های سایبری: اعضای شبکه‌های سایبری عمدتاً بر اساس همکاری پروژه‌محور فعالیت می‌کنند؛ یعنی برای انجام عملیات خاصی به‌کار گرفته می‌شوند و ممکن است پس از اتمام آن، ارتباط خود را قطع کنند. این پویایی، سازوکارهای سنتی شناسایی جرایم سازمان‌یافته را، که بر یافتن اعضای ثابت متمرکزند، ناکارآمد می‌سازد (Moisiienko, 2024).

مکان هماهنگی؛ پاتوق فیزیکی در مقابل پلتفرم‌های دیجیتال

باندهای فیزیکی: پاتوق به مکان فیزیکی ثابتی گفته می‌شود که باند برای هماهنگی، تصمیم‌گیری و توزیع منافع از آن استفاده می‌کند. این پاتوق‌ها معمولاً در کسب‌وکارهای نیمه‌قانونی، مانند قهوه‌خانه‌ها و کافی‌شاپ‌ها، املاک مسکونی متروکه یا فضاهای عمومی دارای نظارت ضعیف شکل می‌گیرند. وجود مکان فیزیکی ثابت، امکان نظارت پلیسی و شناسایی ساختار مجرمانه را فراهم می‌آورد، هرچند این امر نیز با چالش‌هایی همراه است (Beigi & Khoshyari, 2011).

شبکه‌های سایبری: هماهنگی در شبکه‌های سایبری از طریق پلتفرم‌های دیجیتال رمزنگاری‌شده صورت می‌گیرد که شامل موارد زیر است:

کانال‌ها و پیام‌رسان‌های رمزنگاری‌شده؛

فروم‌های تخصصی در دارک‌نت از طریق شبکه تور؛

سرورهای اختصاصی با دسترسی محدود.

این پلتفرم‌ها، به‌دلیل فراهم‌کردن امکان ناشناس‌ماندن و برخورداری از ماهیت فرامرزی، شناسایی مکان فیزیکی هماهنگی را به‌شدت دشوار می‌سازند (Akbari & Mousavi, 2019).

تمایزات انگیزه‌ای؛ اقتصاد ساختاری در مقابل ترکیب انگیزه‌های اقتصادی و روان‌شناختی دیجیتال

انگیزه‌های ارتکاب جرایم سازمان‌یافته باندی و سایبری دارای تفاوت‌های کیفی عمیقی هستند که ریشه در بسترهای فیزیکی و دیجیتال دارند.

الف) انگیزه اقتصادی؛ بقا در مقابل بازدهی بالا

باندهای فیزیکی: انگیزه اقتصادی در باندهای فیزیکی عمدتاً ریشه در فقر ساختاری و نابرابری اقتصادی دارد. تمرکز پاتوق‌های باندهای فعال در محلاتی با نرخ بالای بیکاری نشان می‌دهد که در چنین شرایطی، عضویت در باند نه به‌عنوان انتخابی عقلانی برای ثروتمندشدن، بلکه به‌عنوان «راه‌حلی اجباری برای بقا» تلقی می‌شود (Taghizadeh et al., 2017).

شبکه‌های سایبری: انگیزه اقتصادی در شبکه‌های سایبری عمدتاً ریشه در بازدهی بالا و هزینه پایین دارد. یک حمله فیشینگ موفق می‌تواند طی چند ساعت، هزاران قربانی را هدف قرار دهد و درآمد بسیار زیادی ایجاد کند؛ امری که در جرایم فیزیکی، به‌دلیل محدودیت‌های مکانی و زمانی، امکان‌پذیر نیست. این بازدهی بالا، جذابیت جرایم سایبری را برای جوانان دارای مهارت‌های فنی افزایش داده است، حتی اگر آنان در بازار کار رسمی فرصت شغلی داشته باشند.

ب) انگیزه قدرت؛ نفوذ محلی در مقابل شهرت دیجیتال

باندهای فیزیکی: قدرت در باندهای فیزیکی عمدتاً به‌صورت نفوذ محلی و کنترل فیزیکی بر حوزه جغرافیایی مشخصی ظاهر می‌شود. این نفوذ از طریق شبکه‌سازی در میان مقامات اداری، ایجاد ترس در جامعه محلی و کنترل مسیرهای قاچاق شکل می‌گیرد (Yar et al., 2011).

شبکه‌های سایبری: قدرت در شبکه‌های سایبری عمدتاً به‌صورت شهرت دیجیتال و تأثیر فنی ظاهر می‌شود. این شهرت دیجیتال، که از طریق افشای آسیب‌پذیری‌های امنیتی بزرگ یا هک سامانه‌های معروف کسب می‌شود، در فرهنگ دیجیتال ارزش بالایی دارد.

ج) پیوندهای اجتماعی؛ پیوندهای خانوادگی ـ قومی در مقابل هویت دیجیتال

باندهای فیزیکی: پیوندهای اجتماعی در باندهای فیزیکی عمدتاً بر پایه روابط خانوادگی، قومی و هنجارهای محلی شکل می‌گیرند. این پیوندها از طریق یادگیری اجتماعی و وفاداری خانوادگی، جوانان را به‌سمت عضویت در باند سوق می‌دهند (Taghizadeh et al., 2017).

شبکه‌های سایبری: پیوندهای اجتماعی در شبکه‌های سایبری عمدتاً بر پایه هویت دیجیتال و تخصص فنی شکل می‌گیرند. اعضای شبکه‌های سایبری از طریق عضویت در فروم‌های تخصصی، شبکه‌های رمزنگاری‌شده و بازارهای تاریک، هویت دیجیتال خود را ایجاد و پیوندهای جدیدی برقرار می‌کنند. این پیوندها فاقد ماهیت فیزیکی و مکانی هستند و صرفاً بر اساس تخصص فنی و اعتماد دیجیتال، از جمله از طریق نظام‌های امتیازدهی، شکل می‌گیرند (Parvizi, 2016).

تمایزات بستری؛ فضای فیزیکی ـ مکانی در مقابل فضای غیرمکانی سایبری

بستر وقوع جرایم سازمان‌یافته باندی و سایبری دارای تفاوت‌های ماهوی عمیقی است که مستقیماً بر راهکارهای پیشگیری تأثیر می‌گذارند.

الف) ماهیت بستر؛ فیزیکی ـ مکانی در مقابل فنی ـ فیزیکی ـ منطقی

باندهای فیزیکی: باندهای فیزیکی در فضای فیزیکی ـ مکانی عمل می‌کنند که ویژگی‌های زیر را دارد:

محدودیت جغرافیایی: فعالیت‌های باندها معمولاً در حوزه جغرافیایی مشخصی، مانند محله، شهر یا استان، متمرکز است؛

وابستگی به زیرساخت‌های فیزیکی: باندها برای فعالیت خود به مکان‌های فیزیکی، مانند پاتوق، انبار و مسیرهای قاچاق، وابسته‌اند؛

قابلیت نظارت فیزیکی: پلیس می‌تواند از طریق گشت‌زنی، دوربین‌های مداربسته و نفوذ مخفیانه، فعالیت‌های باندها را رصد کند (Beigi & Khoshyari, 2011).

شبکه‌های سایبری: شبکه‌های سایبری در فضای سایبری، به‌عنوان بستری فنی ـ فیزیکی ـ منطقی، عمل می‌کنند که ویژگی‌های زیر را دارد:

فرامرزی‌بودن: ممکن است جرم در کشوری محقق شود، درحالی‌که مرتکب در کشور دیگری قرار دارد و سرورهای میزبان در کشور سومی مستقرند؛

سرعت بالای اجرا: حملات سایبری در کسری از ثانیه انجام می‌شوند و امکان واکنش سریع را محدود می‌کنند؛

ناشناس‌ماندن مرتکب: استفاده از ابزارهای رمزنگاری، شبکه‌های ناشناس، مانند تور، و ارزهای دیجیتال، شناسایی و تعقیب مرتکبان را به‌شدت دشوار می‌سازد (Parvizi, 2016).

ب) عدم تمایز مفهومی در نظام حقوقی ایران

یکی از خلأهای حیاتی در نظام حقوقی ایران، عدم تمایز مفهومی میان «فضای سایبری» و «فضای مجازی» است که به طراحی راهکارهای پیشگیری ناکارآمد منجر شده است. قانون‌گذار ایران در قوانین متعددی، از جمله ماده ۲ (۵۰۰ مکرر) قانون مجازات اسلامی مصوب ۲۰۲۰، ماده ۹ قانون حمایت از اطفال و نوجوانان مصوب ۲۰۲۰ و مواد ۵۹ و ۶۰ قانون حمایت از خانواده و جوانی جمعیت مصوب ۲۰۲۱، از اصطلاحات «فضای مجازی» و «بستر مجازی» به‌صورت مترادف استفاده کرده است (Gercke & Akbari, 2010). این عدم تمایز مفهومی پیامدهای جدی زیر را در پی دارد:

تلقی نادرست از ماهیت جرم: جرایمی که در فضای سایبری رخ می‌دهند، مانند هک سامانه‌های بانکی، ذاتاً با جرایمی که در فضای مجازی رخ می‌دهند، مانند افترا در اینستاگرام، متفاوت‌اند. جرم نخست به تخصص فنی بالا و ابزارهای پیشرفته نیاز دارد؛ درحالی‌که جرم دوم عمدتاً جرمی رفتاری است.

ناکارآمدی راهکارهای پیشگیری: راهکارهای پیشگیری از جرایم فضای سایبری، مانند تقویت امنیت سایبری، با راهکارهای پیشگیری از جرایم فضای مجازی، مانند آموزش اخلاق دیجیتال، متفاوت‌اند. عدم تمایز مفهومی به تخصیص نادرست منابع منجر می‌شود.

ابهام در تعیین نهاد مسئول: در ایران، پلیس فتا عمدتاً مسئول مقابله با جرایم فضای سایبری است؛ درحالی‌که نظارت بر فضای مجازی به‌طور پراکنده میان چندین نهاد تقسیم شده است. عدم تمایز مفهومی به تداخل اختیارات منجر می‌شود (Akbari & Mousavi, 2019).

جدول زیر تمایزات ساختاری، انگیزه‌ای و بستری میان جرایم سازمان‌یافته باندی و سایبری را در کنار پیامدهای آن‌ها برای سیاست جنایی پیشگیری نشان می‌دهد:

جدول ۴. جدول تحلیلی ـ تطبیقی جامع

بُعد تحلیلی	جرایم سازمان‌یافته باندی (فیزیکی)	جرایم سازمان‌یافته سایبری	پیامد برای سیاست پیشگیری
الگوی ساختاری	سلسله‌مراتبی رسمی و ثابت	شبکه‌ای غیرمتمرکز و پویا	برای باندها، شناسایی مکان فیزیکی و ساختار سلسله‌مراتبی؛ برای جرایم سایبری، تحلیل داده‌های شبکه و ردیابی تراکنش‌های دیجیتال
ثبات اعضا	اعضای ثابت با وفاداری بلندمدت	اعضای موقتی با همکاری پروژه‌محور	برای باندها، شکستن وفاداری گروهی؛ برای جرایم سایبری، استفاده از معافیت‌ها و تخفیف‌های قضایی برای جلب همکاری اعضای موقتی

مکان هماهنگی	پاتوق فیزیکی و مشخص	پلتفرم‌های دیجیتال رمزنگاری‌شده	برای باندها، گشت‌زنی فیزیکی و دوربین‌های مداربسته؛ برای جرایم سایبری، نظارت فنی شبکه و تحلیل ترافیک داده‌ها
انگیزه اقتصادی	ریشه در فقر ساختاری و بقا	ریشه در بازدهی بالا و هزینه پایین	برای باندها، مقابله با فقر ساختاری و ایجاد فرصت‌های اشتغال؛ برای جرایم سایبری، ایجاد فرصت‌های شغلی فنی برای جوانان مستعد
انگیزه قدرت	نفوذ محلی و کنترل فیزیکی	شهرت دیجیتال و تأثیر فنی	برای باندها، تقویت پیوندهای اجتماعی متعارف؛ برای جرایم سایبری، ایجاد مجاری مشروع کسب شهرت فنی، مانند مسابقات امنیت سایبری
پیوندهای اجتماعی	خانوادگی، قومی و مبتنی بر هنجارهای محلی	هویت دیجیتال و تخصص فنی	برای باندها، بازتوانی اجتماعی و تقویت خانواده؛ برای جرایم سایبری، آموزش اخلاق دیجیتال و هدایت استعدادهای فنی
ماهیت بستر	فضای فیزیکی ـ مکانی با مختصات جغرافیایی مشخص	فضای غیرمکانی و پراکنده در سراسر جهان	برای باندها، قوانین محلی و ملی؛ برای جرایم سایبری، همکاری بین‌المللی و تطبیق قوانین با استانداردهای جهانی
قابلیت نظارت	نظارت فیزیکی از طریق گشت‌زنی و دوربین	نظارت صرفاً از طریق ابزارهای فنی	برای باندها، پلیس انتظامی و امنیتی؛ برای جرایم سایبری، نهاد تخصصی امنیت سایبری دارای اختیارات فنی و بین‌المللی
نقش زندان	زندان به‌عنوان «مدرسه جرم» و فضای شبکه‌سازی	تأثیر محدود زندان بر شبکه‌های سایبری	برای باندها، جداسازی مجرمان سازمان‌یافته و برنامه‌های بازپروری تخصصی؛ برای جرایم سایبری، محدودسازی دسترسی به اینترنت و ابزارهای فنی در زندان

تطبیق رویکردهای بین‌المللی در حقوق پیشگیری از جرم

تجربه کشورهای پیشرفته در حوزه حقوق پیشگیری از جرم، سه الگوی موفق را آشکار می‌سازد که می‌توانند حاوی درس‌هایی برای ایران و الگویی برای اصلاح نظام حقوقی کشور باشند.

مدل انگلستان؛ رویکرد چندلایه و نتیجه‌محور

انگلستان با تصویب «استراتژی امنیت سایبری ملی» در سال ۲۰۰۹ و ایجاد ساختار سه‌لایه‌ای پیشگیری، رویکردی چندسطحی برای مقابله با جرایم سایبری سازمان‌یافته اتخاذ کرده است (Moisiienko, 2024). این ساختار شامل موارد زیر است:

لایه نخست، ملی: پلیس ملی سایبری که مسئول هماهنگی میان نهادهای اجرایی است؛

لایه دوم، منطقه‌ای: مراکز تخصصی جرایم سایبری در هر منطقه که مسئول اجرای برنامه‌های پیشگیری محلی هستند؛

لایه سوم، محلی: همکاری با بخش خصوصی و جامعه محلی برای افزایش آگاهی عمومی.

نکته کلیدی این مدل، الزام هر لایه به ارائه گزارش سالانه بر اساس شاخص‌های کمّی، مانند تعداد شبکه‌های مجرمانه شناسایی‌شده و میانگین زمان پاسخ‌گویی به حوادث، است که پاسخ‌گویی نهادی را تضمین می‌کند (Moisiienko, 2024).

مدل استونی؛ یکپارچه‌سازی نهادی و فرابخشی

استونی پس از حملات گسترده سایبری سال ۲۰۰۷ علیه زیرساخت‌های خود، اصلاحات ساختاری اساسی انجام داد. این کشور با تأسیس «مرکز امنیت سایبری ملی» به‌عنوان نهادی مرکزی با اختیارات فرابخشی، توانسته است هماهنگی لازم را میان وزارتخانه‌ها، نهادهای امنیتی و بخش خصوصی ایجاد کند. این مرکز دارای سه ویژگی کلیدی است:

اختیار صدور دستورالعمل‌های الزام‌آور برای تمامی نهادهای دولتی در حوزه امنیت سایبری؛

دسترسی مستقیم به داده‌های مربوط به تهدیدات از شرکت‌های بزرگ فناوری؛

الزام به اشتراک‌گذاری اطلاعات مربوط به تهدیدات میان بخش دولتی و خصوصی (Li, 2024).

این مدل نشان می‌دهد که یکپارچه‌سازی نهادی، نه تکثر ساختاری، پیش‌شرط اثربخشی پیشگیری است.

مدل سنگاپور؛ مشارکت عمومی ـ خصوصی و پیشگیری دانش‌بنیان

سنگاپور با ایجاد «شبکه ملی هشدار سایبری»، که در آن شرکت‌های فناوری، بانک‌ها و مراکز داده به‌صورت داوطلبانه اطلاعات مربوط به تهدیدات را با دولت به‌اشتراک می‌گذارند، توانسته است زمان شناسایی حملات سایبری را به‌طور چشمگیری کاهش دهد (Moulos et al., 2018). این موفقیت مستلزم دو عامل بوده است:

برخورداری از چارچوب قانونی شفافی که مسئولیت‌های حقوقی شرکت‌های مشارکت‌کننده را مشخص می‌کند؛

ایجاد نظام پاداش برای شرکت‌هایی که اطلاعات مربوط به تهدیدات را به‌موقع به‌اشتراک می‌گذارند.

این تجربه نشان می‌دهد که پیشگیری از جرایم سازمان‌یافته سایبری بدون مشارکت بخش خصوصی، که مالک یا مدیر بخش عمده زیرساخت‌های فناوری است، امکان‌پذیر نیست.

نظریه‌های کلاسیک جرم‌شناسی و قابلیت کاربرد آن‌ها در جرایم سازمان‌یافته باندی و سایبری

سیاست جنایی پیشگیرانه، به‌مثابه نظامی معرفت‌بنیان و عملیات‌گرا، بدون اتکا به «مبانی نظری مستحکم» و «تبیین‌های علّی ـ معلولی»، محکوم به انفعال، سطحی‌نگری و اتلاف منابع ملی است. در واکاوی پدیده پیچیده جرایم سازمان‌یافته باندی، که ریشه در تعاملات چندساحتی فرد، گروه و ساختارهای کلان اجتماعی دارد، رجوع به نظریه‌های کلاسیک و بنیادین جرم‌شناسی نه تمرینی صرفاً دانشگاهی، بلکه ضرورتی راهبردی برای طراحی مداخلات پیشگیرانه کارآمد است (Najafi Abrandabadi, 2016).

جرایم سازمان‌یافته باندی، برخلاف جرایم سازمان‌یافته سایبری که ماهیتی انتزاعی، غیرمتمرکز و مبتنی بر فناوری دارند، در بسترهای عینی، فیزیکی و به‌شدت زمینه‌مند شکل می‌گیرند و تداوم می‌یابند (Beigi & Khoshyari, 2011). ازاین‌رو، برای درک چرایی جذب جوانان به باندهای مجرمانه، انتقال تکنیک‌های بزهکاری در زندان‌ها و بازتولید خرده‌فرهنگ‌های مجرمانه در محلات محروم، باید سه نظریه مادر در جرم‌شناسی، یعنی «نظریه کنترل اجتماعی»، «نظریه فشار» و «نظریه یادگیری اجتماعی»، به‌دقت بررسی شوند (Najafi Abrandabadi, 2016).

این بحث در پی آن است که با عبور از توصیف‌های صرف، چگونگی کاربست این سه نظریه کلاسیک را در تبیین شکل‌گیری، تداوم و گسترش جرایم سازمان‌یافته باندی تحلیل کند و نشان دهد که چگونه تضعیف پیوندهای اجتماعی، اعمال فشارهای ساختاری و یادگیری مجرمانه در کانون‌های جرم‌خیز، بستر سازمان‌یافتگی بزهکاری را فراهم می‌آورند.

این بحث در سه قسمت مجزا، اما به‌هم‌پیوسته، سامان یافته است: در قسمت نخست، با اتکا به «نظریه کنترل اجتماعی» تراویس هیرشی مصوب ۱۹۶۹، نقش چهار پیوند اجتماعی، شامل دلبستگی، تعهد، مشارکت و باور، در پیشگیری از بزهکاری باندی واکاوی می‌شود. در این قسمت نشان داده می‌شود که چگونه محیط‌های جرم‌خیز، مانند زندان‌ها به‌عنوان دانشگاه‌های جرم و محلات حاشیه‌نشین، با گسستن این پیوندها، عضویت در باندهای مجرمانه را تسهیل می‌کنند.

در قسمت دوم، با بهره‌گیری از «نظریه فشار ساختاری» رابرت مرتن مصوب ۱۹۳۸ و «نظریه فشار عمومی» رابرت آگنیو مصوب ۱۹۹۲، ریشه‌های اقتصادی ـ اجتماعی گرایش به باندهای مجرمانه تحلیل می‌شوند. در این قسمت تبیین می‌شود که چگونه فشارهای ساختاری، مانند فقر، نابرابری و بیکاری، در تعامل با هیجانات منفی، مانند خشم، ناامیدی و احساس بی‌عدالتی، انگیزه‌ای قدرتمند برای پیوستن به باندهای اقتصادی ـ مجرمانه ایجاد می‌کنند.

در قسمت سوم، با استناد به «نظریه یادگیری اجتماعی» ادوین سادرلند مصوب ۱۹۴۷ و «نظریه یادگیری اجتماعی ـ شناختی» آلبرت بندورا مصوب ۱۹۷۷، سازوکارهای انتقال دانش و تکنیک‌های مجرمانه در درون باندها بررسی می‌شوند. در این قسمت نشان داده می‌شود که چگونه «معاشرت ترجیحی»، «یادگیری مشاهده‌ای» و «مدل‌سازی رفتار باندی»، فرایند جامعه‌پذیری مجرمانه را در پاتوق‌ها و کانون‌های باندی تسهیل می‌کنند.

این بحث، با اتکا به رویکردی تحلیلی ـ انتقادی و با بهره‌گیری از منابع دست‌اول جرم‌شناختی، اعم از متون کلاسیک و پژوهش‌های بومی، در پی فراهم‌کردن زیربنای نظری لازم برای طراحی «راهبردهای پیشگیری اجتماعی و ساختاری» از جرایم سازمان‌یافته باندی است. مهم‌تر آنکه تبیین دقیق این نظریه‌ها در بستر فیزیکی، پیش‌شرط و نقطه عزیمت برای بحث دوم این فصل خواهد بود؛ جایی که نشان داده می‌شود چگونه این نظریه‌های کلاسیک، در مواجهه با ویژگی‌های منحصربه‌فرد فضای سایبری، مانند گمنامی، قلمروزدایی و ساختارهای شبکه‌ای، با چالش مواجه شده و نیازمند «بازتعریف و تطبیق» با مفاهیم نوین دیجیتال هستند.

نظریه کنترل اجتماعی هیرشی و مفهوم پیوندهای ضعیف دیجیتال

نظریه کنترل اجتماعی، که توسط تراویس هیرشی در سال ۱۹۶۹ در اثر پیشگامانه او با عنوان «علل بزهکاری» مطرح شد، یکی از تأثیرگذارترین چارچوب‌های تحلیلی در جرم‌شناسی معاصر محسوب می‌شود. برخلاف نظریه‌های فشار یا یادگیری اجتماعی که به‌دنبال تبیین «چرایی ارتکاب جرم» هستند، نظریه کنترل اجتماعی با پرسشی بنیادین‌تر آغاز می‌شود: «چرا افراد از ارتکاب جرم خودداری می‌کنند؟» این نظریه فرض اصلی خود را بر این مبنا استوار می‌سازد که جرم رفتاری طبیعی است و آنچه نیاز به تبیین دارد، پایبندی به هنجارهاست. بر اساس این رویکرد، انسان ذاتاً دارای تمایلات خودخواهانه و بزهکارانه است و پیوندهای اجتماعی با نهادهای متعارف‌اند که به‌عنوان عوامل اخلاقی و بازدارنده، مانع تبدیل این تمایلات به رفتار مجرمانه می‌شوند.

در بستر جرایم سازمان‌یافته باندی، این نظریه تبیینی کارآمد ارائه می‌دهد. باندهای مجرمانه در واقع نه صرفاً به‌عنوان گروهی بزهکار، بلکه به‌عنوان «نظام جایگزین کنترل اجتماعی» و «خانواده ثانویه» عمل می‌کنند. هنگامی که پیوندهای اجتماعی متعارف فرد با خانواده، مدرسه و جامعه اصلی دچار گسست و تضعیف می‌شوند، باند با ارائه هویت، حمایت عاطفی و امنیت اقتصادی، خلأ ناشی از این گسست را پر می‌کند (Najafi Abrandabadi, 2016). ازاین‌رو، عضویت در باند نه انتخابی کاملاً عقلانی برای کسب منفعت، بلکه واکنشی دفاعی به بی‌هنجاری و فقدان پیوندهای اجتماعی متعارف است.

در این قسمت، با تحلیل چهار پیوند اجتماعی کلیدی هیرشی، نقد کاربرد این نظریه در جرایم سازمان‌یافته سنتی و بازتعریف آن در فضای سایبری با مفهوم «پیوندهای ضعیف دیجیتال»، چارچوبی تحلیلی برای درک ریشه‌های جرم‌زایی در فضای دیجیتال ارائه می‌شود. چهار رکن بنیادین نظریه هیرشی، یعنی دلبستگی، تعهد، مشارکت و باور، تشریح می‌شوند و نقش هر یک در پیشگیری از جذب افراد به باندهای مجرمانه تحلیل می‌شود. همچنین، نشان داده می‌شود که چگونه فقدان این چهار رکن، بستر روانی و اجتماعی لازم را برای عضویت در باند فراهم می‌آورد.

هیرشی استدلال می‌کند که پیوندهای اجتماعی فرد با جامعه، مانع اصلی ارتکاب جرم هستند. او با طرح پرسش بنیادین «چرا افراد از قانون اطاعت می‌کنند؟»، به‌جای پرسش سنتی «چرا افراد مرتکب جرم می‌شوند؟»، استدلال می‌کند که انسان ذاتاً موجودی خودخواه و مستعد بزهکاری است و پیوندهای اجتماعی، به‌عنوان مهارهای درونی و بیرونی، مانع انحراف او می‌شوند (Jalali Farahani, 2014). در بافت

جرایم سازمان‌یافته باندی، گسست این پیوندها از نهادهای متعارف، مانند خانواده، مدرسه و بازار کار، و «جانشینی پیوندهای کاذب باندی» به‌جای آن‌ها، هسته مرکزی تشکیل و تداوم باندها را شکل می‌دهد. در این بند، ضمن بررسی چهار رکن نظریه هیرشی، نقش حیاتی آن‌ها در طراحی راهبردهای پیشگیری اجتماعی از بزهکاری باندی در ایران، به‌صورت انتقادی تحلیل می‌شود.

کاربرد نظریه کنترل اجتماعی در جرایم سازمان‌یافته باندی

تحلیل تطبیقی نشان می‌دهد که نظریه کنترل اجتماعی توانایی محدودی در تبیین جرایم سازمان‌یافته باندی دارد؛ زیرا این جرایم عمدتاً توسط افرادی ارتکاب می‌یابند که لزوماً از پیوندهای اجتماعی ضعیف رنج نمی‌برند، بلکه ممکن است از طریق سازوکارهای دیگری به باندها بپیوندند.

پیوندهای خانوادگی قوی در باندها

تحلیل پرونده‌های قضایی نشان می‌دهد که بسیاری از اعضای باندهای بزرگ دارای خویشاوندانی هستند که پیش‌تر در باندهای مشابه فعالیت کرده‌اند (Taghizadeh et al., 2017). این یافته با فرضیه هیرشی در تضاد است؛ زیرا اعضای باند نه‌تنها با دیگران، یعنی والدین یا خویشاوندان مجرم، پیوند دارند، بلکه همین پیوند به مسیری برای ورود به باند تبدیل می‌شود. در اینجا، پیوند با دیگران نه مانع جرم، بلکه تسهیل‌کننده آن است.

تعهد به هنجارهای محلی

در برخی جوامع محلی، به‌ویژه در مناطق مرزی یا محروم، فعالیت‌هایی مانند قاچاق کالا به‌عنوان «خدمت به جامعه» تلقی می‌شوند و با هنجارهای محلی هم‌راستا هستند (Taghizadeh et al., 2017). در این شرایط، تعهد به هنجارها، یعنی باور به هنجارهای محلی، نه مانع جرم، بلکه انگیزه‌بخش آن است. این پدیده، که «هنجارهای ضداجتماعی محلی» نامیده می‌شود، محدودیت نظریه هیرشی را در تبیین جرایم سازمان‌یافته آشکار می‌سازد.

درگیری با فعالیت‌های غیرمتعارف

اعضای باندها اغلب در فعالیت‌های مجرمانه‌ای درگیرند که زمان و انرژی قابل‌توجهی از آنان می‌طلبند. این درگیری، برخلاف فرضیه هیرشی، جرم را تسهیل می‌کند، نه اینکه مانع آن شود. این یافته نشان می‌دهد که «درگیری» تنها زمانی مانع جرم می‌شود که با فعالیت‌های متعارف همراه باشد؛ در غیر این صورت، می‌تواند جرم‌زا باشد.

این تحلیل نشان می‌دهد که نظریه کنترل اجتماعی هیرشی برای تبیین جرایم سازمان‌یافته باندی دارای محدودیت‌های ساختاری است؛ زیرا این نظریه عمدتاً بر جرایم فردی و بزهکاری نوجوانان متمرکز است و توانایی تبیین ساختارهای سازمانی پیچیده را ندارد (Bryant, 2021).

محدودیت‌های نظریه کنترل اجتماعی در فضای سایبری

انتقال نظریه کنترل اجتماعی به فضای سایبری با چالش‌های مفهومی عمیقی مواجه است که ریشه در ماهیت غیرمکانی، ناشناس و پراکنده فضای دیجیتال دارند.

الف) فقدان «دیگران» فیزیکی: پیوند با دیگران در نظریه هیرشی بر تعاملات چهره‌به‌چهره و حضور فیزیکی استوار است. در فضای سایبری، تعاملات عمدتاً غیرهم‌زمان و بدون حضور فیزیکی انجام می‌شوند. فرد می‌تواند با اشخاصی که هرگز آن‌ها را ندیده است، در شبکه‌های مجرمانه همکاری کند. این ویژگی، مفهوم «پیوند با دیگران» را با چالش مواجه می‌سازد؛ زیرا مشخص نیست چگونه می‌توان با فردی که هویت واقعی او ناشناخته است، پیوند عاطفی برقرار کرد (Yar et al., 2011).

ب) سرمایه‌گذاری در فضای دیجیتال: تعهد به هنجارها در نظریه هیرشی بر سرمایه‌گذاری در دارایی‌های فیزیکی، مانند خانه، شغل و تحصیلات، استوار است. در فضای سایبری، سرمایه‌گذاری‌ها عمدتاً دیجیتال‌اند، مانند حساب‌های کاربری و اعتبار در جوامع آنلاین، و ممکن است به‌آسانی انتقال یابند یا حذف شوند. ازاین‌رو، «رهین‌بودن سرمایه اجتماعی» در فضای سایبری به شکل متفاوت و ضعیف‌تری عمل می‌کند.

ج) درگیری در فضای مجازی: درگیری با فعالیت‌های متعارف در فضای سایبری مفهومی مبهم دارد؛ زیرا مرز میان فعالیت‌های مشروع و نامشروع در این فضا گاه محو است. برای مثال، ممکن است جوانی ساعت‌ها در فروم‌های تخصصی دارک‌نت فعالیت کند؛ فعالیتی که از منظر هیرشی «درگیری» محسوب می‌شود، اما به‌جای جلوگیری از جرم، مسیری برای یادگیری تکنیک‌های مجرمانه فراهم می‌آورد.

د) نسبی‌بودن هنجارها در فضای دیجیتال: باور به هنجارها در نظریه هیرشی بر هنجارهای عمومی جامعه استوار است. در فضای سایبری، هنجارهای متعدد و گاه متناقضی وجود دارند: هنجارهای رسمی دولت‌ها، هنجارهای غیررسمی جوامع آنلاین و هنجارهای فرعی جوامع تخصصی، مانند جامعه هکرها. این تکثر هنجاری، مفهوم «باور به هنجارها» را پیچیده می‌سازد. ممکن است فردی به هنجارهای جامعه هکرها باور داشته باشد که نفوذ به سامانه‌ها را «کشف آسیب‌پذیری» می‌نامد، درحالی‌که از هنجارهای رسمی جامعه سر باز می‌زند (Nguyen & Sikal, 2021).

این محدودیت‌ها نشان می‌دهند که نظریه کنترل اجتماعی هیرشی، به‌صورت خام و بدون بازتعریف، قادر به تبیین جرایم سازمان‌یافته سایبری نیست.

بازتعریف نظریه کنترل اجتماعی؛ مفهوم «پیوندهای ضعیف دیجیتال»

برای غلبه بر محدودیت‌های یادشده، لازم است نظریه کنترل اجتماعی با مفهوم جدید «پیوندهای ضعیف دیجیتال» بازتعریف شود. این مفهوم، که ریشه در نظریه شبکه‌های اجتماعی مارک گرانووتر دارد، استدلال می‌کند که در فضای سایبری، پیوندهای ضعیف، یعنی ارتباطات سطحی و کوتاه‌مدت، نه‌تنها مانع جرم نیستند، بلکه می‌توانند آن را تسهیل کنند.

الف) پیوندهای ضعیف به‌عنوان مسیر ورود به شبکه‌های مجرمانه: بسیاری از اعضای شبکه‌های مجرمانه سایبری از طریق پیوندهای ضعیف، مانند آشنایی‌های تصادفی در فروم‌های تخصصی یا کانال‌های پیام‌رسان، وارد شبکه‌های مجرمانه می‌شوند (Akbari & Mousavi, 2019). این پیوندهای ضعیف، که ممکن است در دنیای فیزیکی کم‌اهمیت تلقی شوند، در فضای سایبری و به‌دلیل گستردگی شبکه‌های اجتماعی دیجیتال، می‌توانند به پیوندهای مجرمانه قوی تبدیل شوند.

ب) سازوکار پل‌زدن اجتماعی: گرانووتر استدلال می‌کند که پیوندهای ضعیف به‌عنوان «پل» میان گروه‌های اجتماعی مختلف عمل می‌کنند و موجب انتقال اطلاعات و فرصت‌ها میان این گروه‌ها می‌شوند. در فضای سایبری، این سازوکار به‌صورت گسترده مشاهده می‌شود. فردی که در یک فروم تخصصی حضور دارد، می‌تواند از طریق پیوندهای ضعیف با اعضای فروم‌های دیگر ارتباط برقرار کند و به شبکه‌های مجرمانه‌ای دسترسی یابد که در دنیای فیزیکی، به‌دلیل محدودیت‌های مکانی و اجتماعی، دسترسی به آن‌ها امکان‌پذیر نبود.

نظریه فشار مرتن و فشارهای ساختاری در فضای سایبری

نظریه فشار، که برای نخستین بار توسط رابرت کینگ مرتن در سال ۱۹۳۸ در مقاله پیشگامانه «ساختار اجتماعی و آنومی» مطرح شد، یکی از تأثیرگذارترین چارچوب‌های تحلیلی در جرم‌شناسی ساختاری محسوب می‌شود. این نظریه، که ریشه در جامعه‌شناسی کارکردگرایی دارد،

استدلال می‌کند که جرم نتیجه تنش میان اهداف فرهنگی مورد ترویج جامعه و وسایل مشروعی است که برای دستیابی به این اهداف در اختیار افراد قرار می‌گیرند (Najafi Abrandabadi, 2016).

در دهه ۱۹۹۰، رابرت آگنیو با ارائه نظریه فشار عمومی، این چارچوب را گسترش داد و آن را از سطح کلان ساختاری به سطح خرد روان‌شناختی تعمیم داد. در این قسمت، با تحلیل مفاهیم کلیدی نظریه فشار مرتن و آگنیو، نقد کاربرد آن در جرایم سازمان‌یافته باندی و بازتعریف آن در فضای سایبری با مفهوم «فشارهای نوین دیجیتال»، چارچوبی تحلیلی برای درک ریشه‌های جرم‌زایی در عصر دیجیتال ارائه می‌شود.

مفاهیم کلیدی نظریه فشار مرتن

نظریه فشار ساختاری رابرت کی. مرتن، که در چارچوب مفهوم جامعه‌شناختی بی‌هنجاری تبیین می‌شود، یکی از ارکان بنیادین و رویکردساز در جرم‌شناسی جامعه‌شناختی است. مرتن با واکاوی ساختار جوامع مدرن، به‌ویژه جوامع سرمایه‌داری، استدلال می‌کند که این جوامع دچار گسستی ساختاری و عمیق میان «اهداف فرهنگی» و «وسایل مشروع نهادینه‌شده» هستند. در این ساختار، جامعه اهدافی مانند ثروت‌اندوزی، موفقیت مادی و ارتقای منزلت اجتماعی را به‌صورت فزاینده و گاه وسوسه‌انگیز ترویج می‌کند، اما هم‌زمان، دسترسی به ابزارهای قانونی و مشروع دستیابی به این اهداف را به‌صورت نابرابر و تبعیض‌آمیز میان اعضای خود توزیع می‌کند.

این شکاف میان انتظارات فرهنگی و واقعیت‌های ساختاری، وضعیت فشار یا تنش روانی ـ اجتماعی را ایجاد می‌کند و فرد را به‌سمت یکی از پنج الگوی سازگاری سوق می‌دهد (Najafi Abrandabadi, 2016).

نخستین الگو، همنوایی یا هماهنگی است که رایج‌ترین واکنش در جوامع باثبات محسوب می‌شود. در این حالت، فرد هم اهداف فرهنگی مورد تأیید جامعه را می‌پذیرد و هم برای دستیابی به آن‌ها صرفاً از وسایل مشروع و قانونی، مانند تحصیلات دانشگاهی و اشتغال رسمی، بهره می‌گیرد.

دومین الگو، نوآوری است که از منظر جرم‌شناختی، کانون ثقل نظریه مرتن را تشکیل می‌دهد. در این واکنش، فرد اهداف فرهنگی، مانند کسب ثروت و موفقیت، را کاملاً می‌پذیرد؛ اما به‌دلیل انسداد فرصت‌های مشروع، وسایل قانونی را رد می‌کند و به استفاده از ابزارهای نامشروع و غیرقانونی روی می‌آورد.

سومین الگو، مناسک‌گرایی یا روزمرگی است که در آن، فرد اهداف عالی فرهنگی و انتظارات کلان را رها می‌کند و امید خود را به موفقیت از دست می‌دهد، اما همچنان به‌طور مکانیکی و وسواس‌گونه به وسایل و قواعد مشروع پایبند می‌ماند؛ مانند کارمندی که بدون هیچ‌گونه انتظار پیشرفت، صرفاً به انجام وظایف روزمره و تکراری اکتفا می‌کند.

چهارمین الگو، کناره‌گیری است که در آن، فرد هم اهداف فرهنگی و هم وسایل مشروع را به‌طور هم‌زمان طرد می‌کند و عملاً از مشارکت در ساختار اجتماعی انصراف می‌دهد. این واکنش معمولاً در افرادی مانند معتادان متجاهر، الکلی‌های مزمن یا افراد بی‌خانمانی مشاهده می‌شود که از بدنه جامعه طرد شده‌اند.

پنجمین و آخرین الگو، شورش یا طغیان است. در این حالت، فرد نه‌تنها اهداف و وسایل موجود را رد می‌کند، بلکه در پی جایگزین‌کردن آن‌ها با اهداف و وسایل جدید و براندازی ساختار غالب است؛ وضعیتی که معمولاً در فعالان سیاسی رادیکال یا انقلابیون نمود پیدا می‌کند.

در تبیین علت‌شناسی جرم، مرتن تصریح می‌کند که الگوی «نوآوری» شایع‌ترین واکنش در جوامع دارای نابرابری ساختاری است و ریشه اصلی رفتار مجرمانه را تشکیل می‌دهد. بروز و تشدید این واکنش در شرایطی رخ می‌دهد که سه مؤلفه به‌طور هم‌زمان وجود داشته باشند: نخست، اهداف مادی از طریق نهادهای اجتماعی و رسانه‌ها به‌صورت گسترده ترویج شوند؛ دوم، فرصت‌های مشروع دستیابی به این اهداف به‌طور نابرابر توزیع شده باشند؛ و سوم، سازوکارهای جبرانی و جایگزین‌های مشروعی برای کاهش و تخلیه فشار اجتماعی وجود نداشته باشند.

کاربست در جرایم سازمان‌یافته باندی: مرتن پنج شیوه سازگاری با فشار را معرفی می‌کند که در بافت باندهای مجرمانه اقتصادی، سازگاری از نوع نوآوری بیشترین قدرت تبیینی را دارد. در این حالت، فرد اهداف فرهنگی، مانند ثروت و قدرت، را می‌پذیرد، اما ابزارهای قانونی را رد می‌کند و به ابزارهای غیرقانونی روی می‌آورد. باندهای مجرمانه سازمان‌یافته، مانند باندهای قاچاق کالا و مواد مخدر، سرقت‌های کلان و کلاهبرداری‌های شبکه‌ای، در واقع به‌عنوان «نهادهای جایگزین و موازی» عمل می‌کنند. هنگامی که اقتصاد رسمی و ساختار طبقاتی، مسیر تحرک اجتماعی صعودی را بر جوانان حاشیه‌نشین و محروم می‌بندد، باند مجرمانه به‌عنوان «بنگاهی اقتصادی و غیررسمی» وارد میدان می‌شود. باند نه‌تنها ابزار رسیدن به ثروت را فراهم می‌کند، بلکه با ارائه سلسله‌مراتب درونی، نوعی «مشروعیت‌بخشی درون‌گروهی» به این نوآوری مجرمانه می‌دهد (Taghizadeh et al., 2017).

نقد سیاست‌گذاری در ایران: در نظام حقوقی و سیاست جنایی ایران، رویکرد غالب در مواجهه با باندهای اقتصادی، «کیفرگرا و سرکوبگرانه» است. قانون‌گذار به‌جای رفع انسداد فرصت‌ها از طریق اصلاح ساختار اقتصادی و آموزشی، صرفاً بر تشدید مجازات‌ها تمرکز کرده است. از منظر نظریه مرتن، این رویکرد نه‌تنها فشار ساختاری را کاهش نمی‌دهد، بلکه با برچسب‌زنی و طرد مضاعف بزهکاران از بازار کار قانونی، آنان را به‌سمت «تثبیت در نقش مجرمانه» و وابستگی بیشتر به اقتصاد زیرزمینی باندها سوق می‌دهد.

در نهایت، ارزش و جایگاه نظریه فشار مرتن در تاریخ اندیشه جرم‌شناختی، در تغییر پارادایم از «آسیب‌شناسی فردی» به «آسیب‌شناسی ساختاری» نهفته است. این تحلیل ساختاری، با عبور از تبیین‌های سنتی، جرم را نه نتیجه نقص‌های ذاتی، اختلالات شخصیتی یا ناهنجاری‌های فردی، بلکه محصول نابرابری‌های ساختاری، تبعیض در توزیع فرصت‌ها و گسست میان فرهنگ و ساختار جامعه تفسیر می‌کند. این دیدگاه نه‌تنها تحولی اساسی در جرم‌شناسی کلاسیک ایجاد کرد، بلکه به مبنای نظری بسیاری از سیاست‌های جنایی پیشگیرانه مبتنی بر اصلاحات ساختاری، کاهش نابرابری‌های اجتماعی و توزیع عادلانه فرصت‌ها تبدیل شد.

کاربرد نظریه فشار در جرایم سازمان‌یافته باندی

تحلیل تطبیقی نشان می‌دهد که نظریه فشار از توانایی تبیینی نسبتاً مناسبی درباره جرایم سازمان‌یافته باندی برخوردار است؛ زیرا این جرایم عمدتاً ریشه در نابرابری‌های ساختاری و فشارهای اقتصادی دارند.

الف) فشار ناشی از فقر ساختاری: تمرکز پاتوق‌های باندهای فعال در محلات دارای نرخ بالای بیکاری و نابرابری اقتصادی نشان می‌دهد که جوانان، با مشاهده ثروت در رسانه‌ها و محیط اطراف و درعین‌حال ناتوانی در دستیابی به آن از طریق راه‌های مشروع، دچار فشار ساختاری می‌شوند. این فشار، که مرتن آن را «آنومی ساختاری» می‌نامد، زمینه پذیرش «نوآوری»، یعنی استفاده از وسایل نامشروع برای دستیابی به اهداف فرهنگی، را فراهم می‌کند (Tabar & Hosseini, 2021).

ب) فشار ناشی از نابرابری اقتصادی: مطالعات جرم‌شناختی نشان می‌دهند که نابرابری اقتصادی، نه فقر مطلق، عامل کلیدی در جرم‌زایی است. این نابرابری، احساس محرومیت نسبی را در جوانان ایجاد می‌کند؛ یعنی فرد با مشاهده درآمدهای بالای دیگران در رسانه‌ها یا محیط اطراف، خود را محروم و بی‌ارزش می‌بیند. این احساس، زمینه پذیرش ارزش‌های ضداجتماعی باندها را فراهم می‌کند (Tabar & Hosseini, 2021).

ج) فشار ناشی از فرصت‌های ساختاری جرم‌زا: در مناطق محروم، فرصت‌های قانونی کسب درآمد محدودند، اما فرصت‌های غیرقانونی، مانند شبکه‌های قاچاق کالا و مواد مخدر یا فساد اداری، به‌دلیل ضعف نظارتی و فساد نهادی فراوان هستند. این ترکیب از «محدودیت فرصت‌های مشروع» و «فراوانی فرصت‌های نامشروع»، محیطی را فراهم می‌آورد که در آن، عضویت در باند به‌عنوان «راه‌حلی منطقی» برای جوانان بی‌سرمایه تلقی می‌شود (Taghizadeh et al., 2017).

این تحلیل نشان می‌دهد که نظریه فشار، به‌ویژه در قالب توسعه‌یافته آن توسط آگنیو، توانایی مناسبی در تبیین جرایم سازمان‌یافته باندی دارد؛ زیرا این جرایم عمدتاً ریشه در نابرابری‌های ساختاری و فشارهای اقتصادی دارند.

محدودیت‌های نظریه فشار در فضای سایبری

انتقال نظریه فشار به فضای سایبری با چالش‌های مفهومی عمیقی مواجه است که ریشه در ماهیت فضای دیجیتال دارند.

الف) عدم تناسب فشار اقتصادی با انگیزه‌های جرم سایبری: بخش مهمی از جرایم سازمان‌یافته سایبری دارای انگیزه‌های غیراقتصادی، مانند شهرت دیجیتال، سرگرمی و انتقام شخصی، هستند (Akbari & Mousavi, 2019). این یافته نشان می‌دهد که فشار اقتصادی، به‌عنوان محور اصلی نظریه مرتن، تنها بخشی از انگیزه‌های جرم سایبری را تبیین می‌کند. برای مثال، هکرهایی که با انگیزه «سرگرمی» یا «چالش فنی» فعالیت می‌کنند، لزوماً دچار فشار اقتصادی نیستند.

ب) ماهیت غیرمادی اهداف دیجیتال: نظریه مرتن بر اهداف مادی، مانند ثروت و منزلت فیزیکی، تمرکز دارد. در فضای سایبری، اهداف اغلب غیرمادی هستند:

شهرت دیجیتال: کسب توجه و تأیید در جوامع تخصصی دارک‌نت؛

قدرت فنی: اثبات توانایی نفوذ به سامانه‌های امن؛

هویت دیجیتال: ایجاد هویتی مبتنی بر تخصص فنی در فضای مجازی.

این اهداف غیرمادی، که مرتن در چارچوب خود پیش‌بینی نکرده است، نیازمند بازتعریف مفهوم «اهداف فرهنگی» در عصر دیجیتال‌اند (Heydari et al., 2018).

ج) دسترسی نسبتاً برابر به وسایل فنی: یکی از پیش‌فرض‌های نظریه مرتن، نابرابری در دسترسی به وسایل مشروع است. در فضای سایبری، دسترسی به وسایل فنی، مانند رایانه، اینترنت و نرم‌افزارهای رایگان، دست‌کم در مقایسه با سرمایه‌های فیزیکی، نسبتاً برابرتر است. جوانی دارای مهارت فنی بالا می‌تواند با سرمایه‌گذاری اولیه بسیار پایین، یعنی یک رایانه شخصی و دسترسی به اینترنت، به ابزارهای پیشرفته نفوذ دسترسی یابد. این ویژگی، مفهوم «نابرابری در دسترسی به وسایل» را در فضای سایبری مبهم می‌سازد (Yar et al., 2011).

د) فقدان «جامعه» واحد در فضای سایبری: نظریه مرتن بر فرض وجود جامعه واحدی استوار است که اهداف فرهنگی مشترکی را ترویج می‌کند. در فضای سایبری، چنین جامعه واحدی وجود ندارد؛ بلکه فضاهای فرعی متعددی وجود دارند که هر یک اهداف و هنجارهای خاص خود را ترویج می‌کنند:

جامعه هکرها: ترویج تخصص فنی و کشف آسیب‌پذیری‌ها؛

جوامع دارک‌وب: ترویج فعالیت‌های غیرقانونی به‌عنوان فعالیتی شغلی؛

شبکه‌های اجتماعی: ترویج شهرت و تأیید اجتماعی.

این تکثر فرهنگی، مفهوم «اهداف فرهنگی» را در نظریه مرتن نسبی می‌سازد. ممکن است هدفی در یک فضای فرعی مثبت تلقی شود، مانند کشف آسیب‌پذیری‌ها، اما در فضای دیگری مجرمانه محسوب شود، مانند نفوذ غیرمجاز به سامانه‌ها.

این محدودیت‌ها نشان می‌دهند که نظریه فشار مرتن، حتی در قالب توسعه‌یافته آگنیو، به‌صورت خام و بدون بازتعریف، قادر به تبیین کامل جرایم سازمان‌یافته سایبری نیست.

نظریه یادگیری اجتماعی بندورا و سادرلند

نظریه یادگیری اجتماعی، که برای نخستین بار توسط ادوین سادرلند در ویرایش چهارم کتاب پیشگامانه «اصول جرم‌شناسی» در سال ۱۹۴۷ مطرح شد، تحولی اساسی در تفکر جرم‌شناختی ایجاد کرد. این نظریه، که ریشه در روان‌شناسی اجتماعی دارد، استدلال می‌کند که جرم نه نتیجه نقص ذاتی فرد، بلکه رفتاری است که از طریق تعامل اجتماعی یاد گرفته می‌شود؛ همان‌گونه که رفتارهای مشروع آموخته می‌شوند (Najafi Abrandabadi, 2016).

در دهه ۱۹۷۰، آلبرت بندورا با ارائه مفاهیم «یادگیری مشاهده‌ای» و «مدل‌سازی»، این چارچوب را گسترش داد و نشان داد که یادگیری لزوماً مستلزم تقویت مستقیم نیست؛ بلکه می‌تواند از طریق مشاهده رفتار دیگران و پیامدهای آن صورت گیرد. درحالی‌که نظریه کنترل اجتماعی، بزهکاری باندی را پیامد گسست پیوندهای متعارف و نظریه فشار آن را واکنشی به محرومیت‌های ساختاری می‌داند، نظریه یادگیری اجتماعی پرسش را به‌سمت فرایندهای درون‌گروهی و سازوکارهای انتقال دانش مجرمانه هدایت می‌کند.

بر اساس این رویکرد، عضویت در باندهای مجرمانه و ارتکاب جرایم سازمان‌یافته باندی صرفاً حاصل انتخابی آنی یا فشاری بیرونی نیست، بلکه نتیجه «فرایند یادگیری پیچیده و تدریجی» است که در بستر تعاملات اجتماعی و شبکه‌های همسالان رخ می‌دهد. در این قسمت، با تحلیل مفاهیم کلیدی نظریه یادگیری اجتماعی، نقد کاربرد آن در جرایم سازمان‌یافته باندی و بازتعریف آن در فضای سایبری با مفهوم «یادگیری مجرمانه در انجمن‌های آنلاین»، چارچوبی تحلیلی برای درک چگونگی انتقال تکنیک‌های مجرمانه در عصر دیجیتال ارائه می‌شود (Najafi Abrandabadi, 2016).

مفاهیم کلیدی نظریه یادگیری اجتماعی سادرلند

سادرلند نه اصل اساسی برای تبیین یادگیری جرم ارائه داد که هر یک جزئی از چارچوب تحلیلی او را تشکیل می‌دهند.

اصل اول: جرم یاد گرفته می‌شود. این اصل، که هسته ماهوی نظریه است، بیان می‌کند که جرم، مانند سایر رفتارها، از طریق فرایندهای یادگیری اجتماعی کسب می‌شود و نتیجه نقص ذاتی یا عوامل زیستی نیست.

اصل دوم: یادگیری جرم در تعامل ارتباطی با دیگران رخ می‌دهد. این یادگیری عمدتاً در گروه‌های نزدیک و شخصی، مانند خانواده و همسالان، صورت می‌گیرد، نه از طریق رسانه‌های جمعی.

اصل سوم: یادگیری جرم شامل تکنیک‌های ارتکاب جرم و دلایل توجیهی آن است. تکنیک‌ها می‌توانند بسیار ساده، مانند چگونگی شکستن قفل، یا بسیار پیچیده، مانند چگونگی پوشاندن فعالیت‌های مالی غیرقانونی، باشند. دلایل توجیهی شامل استدلال‌هایی هستند که جرم را رفتاری مشروع، ضروری یا بی‌ضرر معرفی می‌کنند.

اصل چهارم: هنگامی‌که تعاریف توجیه‌کننده جرم بر تعاریف مخالف جرم غلبه کنند، فرد مرتکب جرم می‌شود. این اصل، که «تعادل تعاریف» نامیده می‌شود، نشان می‌دهد که جرم نتیجه نسبت تعاریف توجیه‌کننده به تعاریف مخالف است، نه صرفاً وجود تعاریف توجیه‌کننده.

اصل پنجم: تعاریف ترجیحی از طریق فرایندهای معمول یادگیری، مانند ارتباط و تقویت، کسب می‌شوند. این فرایندها شامل تقلید، تقویت مثبت، یعنی پاداش برای رفتار مجرمانه، و تقویت منفی، یعنی حذف تنبیه یا پیامد نامطلوب، هستند.

اصل ششم: فراوانی، مدت، تقدم و شدت ارتباط با افراد مجرم، میزان یادگیری جرم را تعیین می‌کند. این اصل، که «ارتباط افتراقی» نامیده می‌شود، نشان می‌دهد که یادگیری جرم به ویژگی‌های کمّی و کیفی ارتباطات اجتماعی وابسته است.

اصل هفتم: یادگیری جرم از نظر فرایند با یادگیری سایر رفتارها متفاوت نیست. این اصل بر عمومیت فرایندهای یادگیری تأکید می‌کند و جرم را از سایر رفتارها متمایز نمی‌سازد.

اصل هشتم: رفتارهای مجرمانه و غیرمجرمانه هر دو نتیجه نیازها و ارزش‌های عمومی هستند. این اصل نشان می‌دهد که تفاوت میان رفتارهای مجرمانه و غیرمجرمانه در نیازها نیست، بلکه در روش‌های دستیابی به آن‌هاست.

اصل نهم: اگرچه نیازها و ارزش‌های عمومی در انگیزش جرم نقش دارند، برای تبیین جرم کافی نیستند؛ زیرا همه افراد این نیازها را دارند، اما همه مرتکب جرم نمی‌شوند. این اصل بر اهمیت فرایندهای یادگیری، نه صرفاً انگیزه‌ها، تأکید دارد.

این نه اصل در کنار یکدیگر، چارچوبی جامع برای تبیین چگونگی انتقال رفتار مجرمانه در جوامع ارائه می‌دهند که برخلاف نظریه‌های زیست‌محور یا روان‌شناختی، بر فرایندهای اجتماعی تمرکز دارد.

کاربرد نظریه یادگیری اجتماعی در جرایم سازمان‌یافته باندی

تحلیل تطبیقی نشان می‌دهد که نظریه یادگیری اجتماعی توانایی تبیینی بسیار مناسبی درباره جرایم سازمان‌یافته باندی دارد؛ زیرا این جرایم عمدتاً از طریق فرایندهای یادگیری در محیط‌های اجتماعی خاص شکل می‌گیرند.

الف) یادگیری در پاتوق‌ها؛ زندان و پاتوق‌های باندی به‌عنوان دانشگاه‌های جرم: در بافت بومی ایران و بر اساس پژوهش‌های جرم‌شناختی، محیط‌هایی مانند «زندان‌ها» و «پاتوق‌های محلی» به‌عنوان کانون‌های اصلی معاشرت ترجیحی عمل می‌کنند. زندان، که در ظاهر نهادی برای اصلاح و بازپروری است، به‌دلیل تراکم جمعیت کیفری و عدم تفکیک مؤثر مجرمان، به «دانشگاه جرم» یا «مدرسه بزهکاری» تبدیل می‌شود (Sobhkhiz, 2015).

در این محیط، مجرمان خرد و تفننی در معرض معاشرت ترجیحی با سرکردگان باندهای سازمان‌یافته قرار می‌گیرند و ضمن یادگیری تکنیک‌های پیچیده جرایم سازمان‌یافته، در شبکه‌های ارتباطی باند برای دوران پس از آزادی نیز ادغام می‌شوند. این پدیده، مصداق بارز نظریه سادرلند است که نشان می‌دهد چگونه بسترهای فیزیکیِ به‌ظاهر کنترلی می‌توانند به تسهیل‌کننده یادگیری مجرمانه تبدیل شوند.

پاتوق‌ها، به‌عنوان مکان‌های فیزیکی هماهنگی باندها، فضایی مناسب برای یادگیری تکنیک‌های مجرمانه فراهم می‌کنند. در این محیط‌ها:

اعضای جوان، تکنیک‌های عملیاتی، مانند شکستن قفل و فرار از صحنه جرم، را از اعضای باسابقه می‌آموزند؛

تعاریف توجیه‌کننده جرم، مانند «قاچاق کالا خدمت به جامعه است»، از طریق گفت‌وگوهای روزمره منتقل می‌شوند؛

از تقویت مثبت، مانند اختصاص سهم بیشتر از منافع، و تقویت منفی، مانند تهدید به آسیب در صورت همکاری‌نکردن، برای تثبیت رفتار مجرمانه استفاده می‌شود (Zabihollahnejad, 2017).

این فرایند نشان می‌دهد که بخش قابل‌توجهی از تکنیک‌های مجرمانه اعضای باندها در پاتوق‌ها و محیط‌های معاشرت مجرمانه آموخته می‌شوند (Taghizadeh et al., 2017).

ب) یادگیری از طریق پیوندهای خانوادگی: پیوندهای خانوادگی از طریق دو سازوکار عمل می‌کنند:

یادگیری مستقیم: جوانان از طریق مشاهده فعالیت‌های خویشاوندان، تکنیک‌های مجرمانه را می‌آموزند؛

یادگیری مشاهده‌ای: جوانان با مشاهده پیامدهای مثبت فعالیت‌های مجرمانه خویشاوندان، مانند ثروت و قدرت، برای ورود به باند انگیزه پیدا می‌کنند (Ahmadi et al., 2016).

این تحلیل نشان می‌دهد که نظریه یادگیری اجتماعی، به‌ویژه در قالب توسعه‌یافته آن توسط بندورا، توانایی بسیار مناسبی در تبیین جرایم سازمان‌یافته باندی دارد؛ زیرا این جرایم عمدتاً از طریق فرایندهای یادگیری در محیط‌های اجتماعی خاص، مانند پاتوق‌ها و خانواده‌های مجرم، شکل می‌گیرند.

محدودیت‌های نظریه یادگیری اجتماعی در فضای سایبری

انتقال نظریه یادگیری اجتماعی به فضای سایبری با چالش‌های مفهومی عمیقی مواجه است که ریشه در ماهیت غیرمکانی، ناشناس و پراکنده فضای دیجیتال دارند.

الف) فقدان تعامل چهره‌به‌چهره: یکی از پیش‌فرض‌های اصلی نظریه سادرلند، یادگیری در «گروه‌های نزدیک و شخصی» است. در فضای سایبری، تعاملات عمدتاً غیرهم‌زمان، بدون حضور فیزیکی و با هویت‌های ناشناس انجام می‌شوند. فرد می‌تواند تکنیک‌های مجرمانه را از اشخاصی بیاموزد که هرگز آن‌ها را ندیده و حتی از هویت واقعی آنان آگاه نیست. این ویژگی، مفهوم «گروه‌های نزدیک و شخصی» را در نظریه سادرلند با چالش مواجه می‌سازد (Moisiienko, 2024).

ب) یادگیری بدون تقویت مستقیم: نظریه یادگیری اجتماعی بر اهمیت تقویت، یعنی پاداش یا تنبیه، در یادگیری تأکید دارد. در فضای سایبری، یادگیری اغلب بدون هیچ‌گونه تقویت مستقیم صورت می‌گیرد:

فرد می‌تواند از طریق تماشای محتوای آموزشی یا مطالعه فروم‌ها، تکنیک‌های هک را بدون دریافت پاداش یا تنبیه بیاموزد؛

فرد می‌تواند با دریافت ابزارهای آماده، مانند بدافزارهای ازپیش‌ساخته، بدون نیاز به یادگیری عمیق مرتکب جرم شود.

این ویژگی نقش تقویت مستقیم را کمرنگ می‌کند و نشان می‌دهد که در فضای سایبری، یادگیری ممکن است صرفاً از طریق دسترسی به ابزارها و اطلاعات صورت گیرد، بدون آنکه به فرایندهای اجتماعی پیچیده نیاز باشد.

ج) تکثر تعاریف توجیه‌کننده: نظریه سادرلند بر «تعادل تعاریف»، یعنی نسبت تعاریف توجیه‌کننده به تعاریف مخالف، تأکید دارد. در فضای سایبری، این تعادل به‌دلیل تکثر فضاهای فرعی مبهم می‌شود:

در یک فروم تخصصی دارک‌نت، تعاریف توجیه‌کننده جرم غالب‌اند؛

در شبکه‌های اجتماعی عمومی، تعاریف مخالف جرم غالب‌اند؛

فرد می‌تواند هم‌زمان در هر دو فضا حضور داشته باشد و تعاریف متضادی را دریافت کند.

این تکثر، مفهوم «تعادل تعاریف» را در فضای سایبری پیچیده می‌سازد؛ زیرا ممکن است فرد در یک فضا تعاریف توجیه‌کننده و در فضای دیگر تعاریف مخالف دریافت کند.

د) یادگیری از طریق ابزارها، نه افراد: در فضای سایبری، بخش قابل‌توجهی از یادگیری مجرمانه از طریق ابزارها، نه افراد، صورت می‌گیرد:

ابزارهای «جرم به‌عنوان خدمت» که به کاربران امکان می‌دهند بدون برخورداری از تخصص فنی مرتکب جرم شوند؛

بدافزارهای آماده که با چند اقدام ساده قابل‌استفاده‌اند؛

راهنماهای گام‌به‌گام که بدون نیاز به تعامل انسانی، تکنیک‌های مجرمانه را آموزش می‌دهند.

این ویژگی، نقش انسان به‌عنوان «الگو» در نظریه بندورا را کمرنگ می‌کند و نشان می‌دهد که در فضای سایبری، ابزارها می‌توانند جایگزین انسان به‌عنوان عامل یادگیری شوند (Akbari & Mousavi, 2019). این محدودیت‌ها نشان می‌دهند که نظریه یادگیری اجتماعی، حتی در قالب توسعه‌یافته آن توسط بندورا، به‌صورت خام و بدون بازتعریف، قادر به تبیین کامل جرایم سازمان‌یافته سایبری نیست.

پیامدهای این تحلیل برای سیاست پیشگیری

واکاوی جرایم باندی از منظر نظریه‌های یادگیری اجتماعی سادرلند و بندورا، پیامدهای انتقادی و راهبردی عمیقی برای «مدیریت پیشگیری از جرم» در ایران دارد که رویکردهای فعلی سیاست جنایی کشور را به چالش می‌کشد.

۱. ناکارآمدی رویکردهای صرفاً کیفری و حبس‌محور: بر اساس نظریه یادگیری، مجازات‌های سنگین و گسترش فضای حبس نه‌تنها مانع یادگیری جرم نمی‌شوند، بلکه با قراردادن مجرمان در کنار یکدیگر، به‌ویژه در زندان‌ها، فرایند «معاشرت ترجیحی» را تسریع می‌کنند. زندان، به‌جای آنکه نهادی برای گسستن پیوند با شبکه‌های مجرمانه باشد، به کانونی برای انتقال دانش مجرمانه و تقویت هویت باندی تبدیل می‌شود (Najafi Abrandabadi, 2016). ازاین‌رو، سیاست جنایی ایران باید از پارادایم «انزوا و سرکوب» به‌سمت پارادایم «تفکیک تخصصی، اصلاح ساختار زندان‌ها و توسعه مجازات‌های جایگزین حبس» حرکت کند.

۲. ضرورت مداخله در شبکه‌های یادگیری و پاتوق‌های باندی: پیشگیری از باندیسم نیازمند «مداخله در بسترهای یادگیری» است. این امر مستلزم شناسایی و مدیریت «کانون‌های جرم‌خیز»، مانند پاتوق‌های فیزیکی، گیم‌نت‌های آلوده و محلات دارای کنترل اجتماعی ضعیف، و جایگزین‌کردن آن‌ها با فضاهای سالم است. همچنین، برنامه‌های پیشگیری اجتماعی باید بر «ارائه الگوهای مثبت» متمرکز شوند. توانمندسازی جوانان محلات محروم از طریق ورزش، هنر و اشتغال، الگوهای رفتاری جایگزینی را در برابر سرکردگان باند قرار می‌دهد که می‌توانند فرایند مدل‌سازی مجرمانه را خنثی کنند.

۳. بازآموزی و خنثی‌سازی توجیهات اخلاقی: ازآنجاکه باندها با آموزش «تکنیک‌های خنثی‌سازی اخلاقی»، اعضای خود را از عذاب وجدان رها می‌کنند، مداخلات پیشگیرانه باید بر «بازآموزی اخلاقی و شناختی» متمرکز شوند. برنامه‌های آموزشی در مدارس و محلات باید به جوانان بیاموزند که چگونه توجیهات باندی، مانند «پلیس دشمن است» یا «جامعه با ما ناعادلانه رفتار کرده است»، را شناسایی و رد کنند. ارتقای «سواد رسانه‌ای و انتقادی» می‌تواند به‌عنوان سپری شناختی در برابر پیام‌های فریبنده و مدل‌سازی‌های کاذب باندها عمل کند.

۴. شکستن چرخه تقویت جانشینی: برای مقابله با اثر «تقویت جانشینی»، یعنی مشاهده موفقیت مجرمان، نهادهای انتظامی و قضایی باید بر «قطع شریان‌های مالی و نمادین» باندها تمرکز کنند. مصادره اموال حاصل از جرم، محرومیت از حقوق اجتماعی و جلوگیری از نمایش ثروت و قدرت سرکردگان باند در فضای عمومی و مجازی می‌تواند پیامدهای مثبت مشاهده‌شده برای رفتار مجرمانه را خنثی کند و الگوی موفقیت را به‌سمت مسیرهای قانونی تغییر دهد.

نظریه‌های یادگیری اجتماعی، با عبور از تقلیل‌گرایی‌های زیست‌شناختی و روان‌شناختی، جرایم سازمان‌یافته باندی را به‌عنوان «پدیده‌ای اجتماعی و اکتسابی» تبیین می‌کنند. سادرلند نشان داد که باندها از طریق «معاشرت ترجیحی»، تکنیک‌ها و توجیهات مجرمانه را منتقل می‌کنند و بندورا نشان داد که «مشاهده موفقیت و قدرت‌نمایی» سرکردگان، انگیزه‌ای قدرتمند برای مدل‌سازی و پیوستن به باند ایجاد می‌کند. این واکاوی به‌وضوح نشان می‌دهد که سیاست جنایی ایران در مواجهه با باندیسم نمی‌تواند صرفاً بر تشدید مجازات‌ها و توسعه زندان‌ها، که خود به دانشگاه جرم تبدیل می‌شوند، اتکا کند. راه‌حل بنیادین، «مداخله در فرایند یادگیری» از طریق تفکیک مجرمان، ارائه الگوهای مثبت، مدیریت کانون‌های جرم‌خیز و خنثی‌سازی توجیهات اخلاقی است.

نتیجه‌گیری

نظام حقوقی ایران، با وجود خلأهای مفهومی، از جمله عدم تمایز میان «فضای سایبری» به‌عنوان محیطی فنی ـ فیزیکی ـ منطقی و «فضای مجازی» به‌عنوان محیطی اجتماعی ـ فرهنگی، خلأهای نهادی، از جمله تکثر نهادهای موازی بدون هماهنگی فرابخشی، و فقدان تعهد نتیجه‌محور دولتی در حقوق پیشگیری از جرم، قادر به مدیریت مؤثر پیشگیری و کنترل جرایم سازمان‌یافته باندی و سایبری نیست. ازاین‌رو، تدوین چارچوب حقوقی یکپارچه و نظام‌مندی مبتنی بر شاخص‌های تحلیلی سه‌گانه، شامل ساختار سازمانی، انگیزه‌های ارتکاب و بستر وقوع، با تأکید بر اصول دانش‌بنیانی، از جمله تحلیل ریسک جنایی مبتنی بر داده‌های بزرگ و هوش مصنوعی، فرابخشی‌بودن، از جمله رفع موازی‌کاری نهادی و ایجاد نهاد مرکزی مستقل، و نتیجه‌محوری، از جمله اثبات اثربخشی اقدامات با شاخص‌های کمّی مانند نرخ کاهش جرایم، امکان پیشگیری ساختاری و کاهش این جرایم را فراهم می‌آورد.

پس از واکاوی و بازتعریف نظریه‌های کلاسیک جرم‌شناسی در بستر فضای سایبری، اکنون در یکی از راهبردی‌ترین و عملیاتی‌ترین بخش‌های این مقاله قرار داریم؛ بخشی که مستقیماً «مبانی نظری» را به «طراحی نظام‌های مدیریتی پیشگیری» پیوند می‌زند. واکاوی‌های پیشین به‌وضوح نشان دادند که نظریه‌های کلاسیک، مانند کنترل اجتماعی، فشار و یادگیری اجتماعی، اگرچه در تبیین ریشه‌های فردی و گروهی بزهکاری کارآمدند، در تحلیل «موقعیت‌های مجرمانه» و «بسترهای اکولوژیک» وقوع جرایم سازمان‌یافته سایبری با نقص تبیینی مواجه‌اند. ازاین‌رو، برای طراحی «نظام مدیریتی پیشگیری» که نه صرفاً واکنشی، بلکه پیش‌دستانه، دانش‌بنیان و متناسب با ماهیت ریزوم‌وار فضای سایبری باشد، باید به «نظریه‌های نوین جرم‌شناسی محیطی و موقعیتی» نیز رجوع کرد.

برای رفع خلأهای تعریفی و مفهومی، پیشنهاد می‌شود قانون جامع «مدیریت پیشگیری و کنترل جرایم سازمان‌یافته باندی و سایبری» با تعریف عملیاتی زیر تصویب شود:

«جرم سازمان‌یافته عبارت است از فعالیت‌های مجرمانه‌ای که توسط گروهی ساختاریافته، متشکل از حداقل سه نفر، انجام می‌شوند که در طول زمان، دست‌کم به‌مدت شش ماه، پایدار مانده‌اند و با هماهنگی برنامه‌ریزی‌شده، از طریق تقسیم کار تخصصی یا شبکه‌ای، به‌منظور ارتکاب

جرم جدی، یعنی جرمی با مجازات حداقل چهار سال حبس، و برای کسب منفعت مالی، قدرت یا کنترل فعالیت می‌کنند. این تعریف شامل دو دسته است:

الف) جرم سازمان‌یافته باندی: جرایمی که در فضای فیزیکی و با ساختار سلسله‌مراتبی یا شبکه‌ای متمرکز ارتکاب می‌یابند.

ب) جرم سازمان‌یافته سایبری: جرایمی که در فضای سایبری، به‌عنوان بستری فنی ـ فیزیکی ـ منطقی، با ساختار شبکه‌ای غیرمتمرکز، نقش‌های تخصصی، مانند توسعه‌دهنده بدافزار، اپراتور شبکه و پول‌شوی دیجیتال، و ویژگی‌های فرامرزی ارتکاب می‌یابند.»

این تعریف عملیاتی دارای مزایای زیر است:

تطبیق با کنوانسیون پالرمو: این تعریف با حفظ سه شاخص اصلی پایداری ساختار، هماهنگی گروهی و انگیزه اقتصادی، با استانداردهای بین‌المللی همخوانی دارد.

تمایز میان جرایم باندی و سایبری: با تفکیک دو دسته جرم سازمان‌یافته، امکان طراحی راهکارهای پیشگیری متناسب با هر دسته فراهم می‌شود.

شفافیت معیارها: تعیین حداقل تعداد اعضا، یعنی سه نفر، حداقل مدت پایداری، یعنی شش ماه، و حداقل مجازات جرم اصلی، یعنی چهار سال حبس، از ابهامات تفسیری جلوگیری می‌کند.

پوشش ساختارهای غیرمتمرکز: با اشاره به «ساختار شبکه‌ای غیرمتمرکز»، شبکه‌های مجرمانه مدرن در فضای سایبری نیز تحت پوشش قرار می‌گیرند.

این تعریف تنها با تصویب قانون جامع یادشده قابلیت اجرا خواهد داشت؛ بدون چنین قانونی، هرگونه تلاش برای رفع خلأهای تعریفی و مفهومی، صرفاً به اصلاحاتی جزئی و ناکارآمد محدود خواهد شد.

تعارض منافع

در انجام مطالعه حاضر، هیچ‌گونه تضاد منافعی وجود ندارد.

مشارکت نویسندگان

در نگارش این مقاله تمامی نویسندگان نقش یکسانی ایفا کردند.

حامی مالی

این پژوهش حامی مالی نداشته است.

EXTENDED SUMMARY

Organized gang crime and organized cybercrime have become increasingly complex challenges for contemporary criminal policy because both forms of criminality transcend isolated offending and operate through coordinated structures, specialized roles, sustained activities, and networks designed to generate financial gain, power, influence, or control. This study examines legal prevention management and the control of organized gang and cybercrime in Iran and seeks to reconstruct legal prevention as an integrated, knowledge-based, intersectoral, and outcome-oriented component of national criminal policy. Legal crime prevention refers to the body of legislative, supralegislative, and sublegislative rules that directly or indirectly regulate preventive measures, allocate institutional responsibilities, and establish mechanisms for managing criminal risks. In this sense, prevention is not merely an ancillary governmental duty but a substantive obligation requiring public institutions to identify criminal threats, assess their probability and consequences, implement

proportionate interventions, and demonstrate the effectiveness of those interventions (Jalali Farahani, 2014; Najafi Abrandabadi, 2016). Nevertheless, Iran's existing prevention framework remains fragmented, predominantly punitive, institutionally dispersed, and insufficiently responsive to the structural characteristics of organized criminal networks. This problem is particularly evident in the cyber domain, where traditional legal concepts are applied to decentralized, anonymous, technically sophisticated, and transnational activities without adequate conceptual or institutional adaptation (Farhadi Alashti & Javan Jafari Bojnordi, 2017; Sobhkhiz, 2015). The central research question is therefore how an integrated legal framework can be developed to manage the prevention and control of organized gang and cybercrime while distinguishing cyberspace from virtual space, reconciling penal and non-penal measures, adapting criminological theories to digital realities, eliminating overlapping institutional mandates, and transforming prevention from a duty-oriented process into a measurable, outcome-oriented policy.

The conceptual foundation of the study rests on four interconnected concepts: legal crime prevention, organized crime, organized gang crime, and organized cybercrime. Organized crime generally involves a structured and relatively stable group whose members coordinate their activities to commit serious offenses for material gain, power, or another shared benefit. Although Iranian criminal legislation recognizes certain elements of collective and coordinated offending, it does not provide a comprehensive and independent definition capable of covering both traditional hierarchical organizations and decentralized cybercriminal networks. Existing provisions are dispersed across the Islamic Penal Code, computer-crime legislation, anti-smuggling regulations, and anti-corruption laws, producing interpretive inconsistencies and leaving the organizational, temporal, and operational criteria of organized crime unclear (Akhavat, 2015; Saybani & Karimi, 2018). Organized gang crime predominantly develops in physical and geographically identifiable settings and is usually associated with relatively stable membership, hierarchical leadership, territorial control, shared meeting places, specialized divisions of labor, and strong familial, ethnic, or neighborhood bonds (Beigi & Khoshyari, 2011; Taghizadeh et al., 2017). Organized cybercrime, by contrast, is commonly committed through decentralized and dynamic networks whose members may collaborate temporarily on particular projects, communicate through encrypted platforms, assume technically specialized roles, conceal their identities, distribute infrastructure across several jurisdictions, and rapidly reconstruct their operations after the removal of individual participants (Gercke & Akbari, 2010; Yarovenko & Rogkova, 2022). These differences demonstrate that the conventional criteria used to identify organized gangs cannot be transferred mechanically to cybercriminal networks. They also reveal the inadequacy of using "cyberspace" and "virtual space" interchangeably: cyberspace constitutes the technical, physical, and logical environment of networks, servers, protocols, systems, and data, whereas virtual space refers primarily to the sociocultural environments constructed upon that infrastructure. Failure to maintain this distinction results in imprecise criminalization, misallocation of preventive resources, overlapping institutional authority, and interventions that may be appropriate for harmful conduct on social platforms but ineffective against attacks targeting critical digital infrastructure (Tabar & Hosseini, 2021; Vatani & Asadi, 2016).

The study employs a descriptive–analytical and comparative legal method. Iranian constitutional provisions, criminal statutes, computer-crime legislation, crime-prevention regulations, institutional arrangements, and relevant policy documents are examined alongside international standards and selected comparative experiences. The analysis is organized around three principal indicators: organizational structure, motivations for offending, and the environment in which

criminal activity develops. This framework makes it possible to identify both the shared characteristics that justify an integrated strategic policy and the differences that necessitate specialized implementation mechanisms. In structural terms, physical gangs generally exhibit stable membership, centralized leadership, territorial meeting places, long-term loyalty, and conventional roles such as leader, organizer, receiver of stolen property, and operational offender; cybercriminal groups more frequently exhibit decentralized organization, project-based membership, encrypted coordination, technical specialization, and operational resilience (Akbari & Mousavi, 2019; Zabihollahnejad, 2017). In motivational terms, both types of organized crime may pursue financial gain and power, but cybercrime also encompasses political and ideological objectives, technical curiosity, entertainment, personal revenge, and the pursuit of recognition within online communities (Ahmadi & Nikpour Qanvani, 2013; Yar et al., 2011). In environmental terms, gang crime is closely connected to prisons, disadvantaged neighborhoods, local criminal markets, family networks, unemployment, inequality, and weakened conventional social control, whereas cybercrime is facilitated by anonymity, borderless communication, encrypted services, digital currencies, distributed servers, and rapid access to criminal knowledge and tools (Nguyen & Sikal, 2021; Parvizi, 2016). The comparative component further considers multilayered coordination, centralized cybersecurity governance, public–private information sharing, threat assessment, institutional accountability, and quantitative performance evaluation as mechanisms through which legal prevention can become systematic and measurable (Li, 2024; Moisiienko, 2024).

The findings reveal several interrelated deficiencies in Iran's existing framework. First, the absence of a comprehensive definition of organized crime creates uncertainty regarding the minimum number of participants, required duration of the criminal structure, degree of coordination, seriousness of the predicate offense, and status of decentralized networks. Consequently, temporary collective offending may be treated as organized crime, while technically sophisticated cybercriminal networks may escape that classification because they lack a visible hierarchy or permanent membership. Second, the interchangeable use of "cyberspace," "virtual space," and "virtual platform" obscures the distinction between cyber-dependent offenses targeting systems or data and cyber-enabled offenses in which digital platforms merely facilitate conventional misconduct. Third, the institutional framework is characterized by multiple bodies with intersecting mandates, limited interorganizational coordination, and no independent central authority responsible for comprehensive prevention management (Akbari & Mousavi, 2019; Tabar & Hosseini, 2021). Fourth, prevention remains predominantly duty-oriented: institutions are required to undertake activities but are not consistently required to demonstrate measurable reductions in targeted risks or offenses. Fifth, insufficient attention is given to the criminological etiology of cybercrime. Policies concentrate on criminalization, surveillance, prosecution, and punishment while overlooking motivational differences and the preventive potential of digital ethics education, legitimate technical employment, cybersecurity competitions, rehabilitation, situational design, and the constructive redirection of technically talented young people (Afshar et al., 2014; Heydari et al., 2018). Finally, international cooperation remains limited despite the transnational structure of cybercrime, in which offenders, victims, servers, financial intermediaries, and digital evidence may be distributed across multiple jurisdictions. Effective prevention therefore requires accelerated information exchange, interoperable legal procedures, coordinated threat intelligence, resilient infrastructure, and collaboration between government agencies and private entities that own or manage essential technological systems (Moulos et al., 2018; Radoglou-Grammatikis et al., 2021).

The criminological analysis demonstrates that classical theories remain valuable but require substantial adaptation before they can adequately explain organized cybercrime. Social control theory emphasizes attachment, commitment, involvement, and belief as constraints on offending, but gang membership may itself be supported by strong familial or local bonds, while cybercriminal cooperation may develop through weak, temporary, and anonymous digital ties. In cyberspace, weak connections can serve as bridges between otherwise disconnected actors, facilitate entry into illicit communities, and enable rapid project-based collaboration without conventional emotional attachment (Bryant, 2021; Yar et al., 2011). Strain theory effectively explains how poverty, unemployment, inequality, relative deprivation, and blocked legitimate opportunities encourage participation in economically motivated gangs; however, it explains only part of cybercriminality because many cyber offenders seek nonmaterial objectives such as technical prestige, ideological influence, entertainment, or recognition. The concept of strain must therefore be extended to include digital exclusion, reputational competition, online status anxiety, perceived technological injustice, and frustration arising from the discrepancy between technical ability and legitimate professional opportunity (Ahmadi et al., 2016; Najafi Abrandabadi, 2016). Social learning theory provides a strong explanation of how criminal techniques, rationalizations, and behavioral models are transmitted within gangs, prisons, families, and criminal meeting places. Yet online offenders may learn without face-to-face interaction, direct reinforcement, or stable association through forums, instructional materials, preconfigured malware, automated tools, and crime-as-a-service markets. Accordingly, the sources of criminal learning must be expanded from close personal groups to digital communities, algorithmically distributed content, technical repositories, and commercially packaged criminal services (Gercke & Akbari, 2010; Gkoktsis et al., 2023). These theoretical adaptations support differentiated prevention: physical gangs require structural poverty reduction, neighborhood intervention, prison reform, social rehabilitation, and disruption of local criminal networks, whereas cybercriminal networks require technical safeguards, digital literacy, ethical training, legitimate pathways for technical recognition, threat-intelligence sharing, and international investigative cooperation.

In conclusion, effective management of organized gang and cybercrime in Iran requires a unified strategic framework that remains differentiated at the operational level. A comprehensive law on the management, prevention, and control of organized crime should clearly define organized criminal activity, specify measurable criteria for structural continuity and coordinated conduct, distinguish physical gang crime from decentralized cybercrime, and separate cyberspace as a technical environment from virtual space as a sociocultural environment. The proposed framework should establish an independent central prevention authority, eliminate or coordinate overlapping institutions, clarify the responsibilities of law-enforcement agencies and civilian bodies, and require annual evaluation through quantitative and qualitative indicators. It should also integrate criminal justice measures with social, educational, economic, technical, and situational interventions; require criminal-risk assessments based on reliable evidence; support responsible use of big data and artificial intelligence; strengthen public–private cooperation; and create mechanisms for timely international information exchange. Prevention should no longer be treated as the performance of formally assigned activities, but as a governmental obligation whose effectiveness must be demonstrated through reduced criminal opportunities, increased infrastructural resilience, disruption of organized networks, improved institutional coordination, and sustainable reductions in targeted harms. Such a framework would preserve the advantages of an integrated national criminal policy while recognizing that physical gangs and cybercriminal networks differ

fundamentally in their structures, motivations, operational environments, methods of recruitment, patterns of communication, and vulnerabilities. This transformation is essential for replacing fragmented and reactive control with a scientific, rights-based, knowledge-driven, and sustainable system of legal crime prevention.

References

Afshar, A., Tormehchi, A., Golshan, A., Aghaian, A., & Shahriari, H. (2014). A Review of Cybersecurity for Industrial Control Systems. *Control Journal*, *8*(1), 31-45.

Aghababaii, H. (2010). *The Scope of Security in Criminal Law*. Institute of Islamic Culture and Thought Publications.

Ahmadi, H., & Nikpour Qanvani, L. (2013). The Application of Qualitative Methods in the Study of Cybercrimes. *Journal of Social Sciences, Faculty of Literature and Humanities, Shiraz University*(5), 1-12.

Ahmadi, P., Khademi, E., & Fattahi Bayat, S. (2016). Effects of New Communication Technologies (Internet, Computer Games, and Satellite) on Social Education, with Emphasis on the Adjustment of Second-Year High-School Students in Tehran. *New Educational Ideas*(20), 9-36.

Akbari, A., & Mousavi, S. (2019). Iran's Cybersecurity Framework: Institutions and Policies. *Journal of Cybersecurity Studies*, *12*(3), 78-92.

Akhavat, M. A. (2015). Commentary and Interpretation of Articles of the Islamic Penal Code. *Dadresi Monthly*, *5*(29), 34.

Aminzadeh, F., & Ghaffari, A. (2019). Security Challenges of Iran's Energy Infrastructure: Lessons from the Iran-Iraq War. *Middle East Security Review*, *8*(1), 56-67.

Beigi, J., & Khoshyari, R. (2011). Computer Crimes and Countermeasures in International Instruments. Regional Conference on the Challenges of Computer Crimes in the Contemporary Era, Maragheh.

Bryant, R. (2021). Internet Control and Surveillance Mechanisms in Iran. *Middle East Policy Journal*, *15*(4), 112-125.

Farhadi Alashti, Z., & Javan Jafari Bojnordi, A. (2017). Challenges Facing Situational Prevention of Transnational Cybercrimes. *Quarterly Journal of Intelligence and Criminal Research*, *12*(45), 9-32.

Gercke, M., & Akbari, M. (2010). *Cybercrime: A Guide for Developing Countries* (1st ed.). Iranian Cyber Police Publications.

Gkoktsis, G., Lauer, H., & Jager, L. (2023). Risk Assessments in Virtual Power Plants with NESCOR Criteria: Practical Application, Advantages and Disadvantages. ARES,

Hassan Beigi, E. (2005). Development of the National Data Network: Challenges and Threats to National Security. *Quarterly Journal of Management Studies*(48), 1-28.

Heydari, M., Shahbazi, O., & Shirani, P. (2018). Challenges and Opportunities for the Police in Addressing Cybercrimes. *Detective Quarterly*, *12*(45), 41-54.

Jalali Farahani, A. (2014). Prevention of Computer Crimes. *Judiciary Legal Journal*(47), 87-119.

Khalifeh, M. (2020). Cybersecurity Frameworks in the Gulf Cooperation Council: A Comparative Study. *Gulf Security Journal*, *9*(2), 88-99.

Li, J. (2024). Multi-Governance Model of New Cybercrime under the Risk of New Technologies: Risks and Responses. Lecture Notes in Education Psychology and Public Media,

Moisiienko, A. (2024). Sanctions and Cybercrimes: The United States' Approach to Countering Cyber Threats. *International Security Journal*, *22*(3), 201-215.

Moulos, V., Chatzikyriakos, G., Kassouras, V., Doulamis, A., Doulamis, N., & Leventakis, G. (2018). A Robust Information Life Cycle Management Framework for Securing and Governing Critical Infrastructure Systems. *Inventions*.

Najafi Abrandabadi, A. H. (2016). Criminology at the Beginning of the Third Millennium: An Introduction. In *Encyclopedia of Criminology* (4th ed.). Ganj-e Danesh.

Nguyen, H., & Sikal, A. (2021). Iran's Offensive Cyber Capabilities: Evolution and Impacts. *Strategic Studies Quarterly*, *15*(2), 67-83.

Parvizi, R. (2016). *Investigating Computer Crimes* (1st ed.). Jahan Jam-e Jam Publications.

Radoglou-Grammatikis, P. I., Sarigiannidis, P. G., & Lagkas, T. D. (2021). Secure and Resilient Electrical Power and Energy Systems: The SDN-microSENSE Project. *The Project Repository Journal*.

Razavi, M. (2007). Cybercrimes and the Role of Police in Preventing and Detecting Them. *Quarterly Journal of Police Knowledge*(32), 120-140.

Saybani, A., & Karimi, A. (2018). Iran's Criminal Policy on Computer Financial Crimes. *Political Science, Law, and Jurisprudence Studies*, *4*(1), 124-142.

Sobhkhiz, R. (2015). Legal Challenges of Cybercrimes in International Law and Iran's Legal System. *Quarterly Journal of Intelligence and Criminal Research*, *10*(39), 117-138.

Tabar, M. A., & Hosseini, S. (2021). Interorganizational Cooperation within Iran's Cybersecurity Framework. *Journal of National Security Studies*, *10*(1), 23-36.

Taghizadeh, M., Zomorodi, K., & Hajian, M. (2017). The Role of the European Union in Regulating Cybercrimes. *Quarterly Journal of International Police Studies*, *8*(29), 104-143.

Vatani, A., & Asadi, H. (2016). Criminal Policy of the Islamic Republic of Iran on Cybercrimes, with Emphasis on Their Particular Features. *Islamic Law Research Journal*, *1*(43), 99-126.

Yar, M., Babaei, Y., & Asli, A. (2011). *Cybercrime and Society* (1st ed.). Majd Publications.

Yarovenko, H., & Rogkova, M. (2022). Dynamic and Bibliometric Analysis of Terms Identifying the Combating Financial and Cyber Fraud System. *Financial Markets, Institutions and Risks*, *6*, 93-104.

Zabihollahnejad, V. (2017). The Nature of Computer and Virtual (Cyber) Crimes and the Role of FATA Police in Their Prevention and Detection. *Quarterly Journal of Police Knowledge, Tehran Police*, *3*(24), 8-27.