Comparative Studies in Jurisprudence, Law, and Politics

Reactive Measures against the Crime of Treason from the Perspective of Imami Jurisprudence and Iranian Criminal Law

1. Hamidreza Haghshenas: Department of Law, KI.C., Islamic Azad University, Kish, Iran
2. Heydar Ali Jahanbakhshi*: Department of Theology and Islamic Studies, Isl.C., Islamic Azad University, Islamshahr, Iran. Email: jahanbakhshi@iau.ac.ir (Corresponding Author)
3. Fatemeh Ghanad: Department of Criminal Law and Criminology, University of Science and Culture, Tehran, Iran

ABSTRACT

Treason is one of the most serious offenses against national security and the fundamental interests of the state, as it may threaten independence, territorial integrity, defense capacity, security secrets, and other vital national interests. Despite the significance of this offense, Iranian criminal law does not provide a fully independent and coherent criminal title for treason. Instead, related conduct is criminalized under offenses such as espionage, disclosure of classified information, cooperation with hostile governments, unauthorized entry into protected places, and transmission of security information. Using a descriptive-analytical method, the present study examines the foundations and reactive measures applicable to treason from the perspectives of Imami jurisprudence and Iranian criminal law. The findings indicate that although treason in its modern legal sense is not formulated as an independent offense in Imami jurisprudence, principles such as the prohibition of betrayal, the obligation to preserve entrusted information, the prohibition of assisting an enemy, and the necessity of protecting collective security provide sufficient normative foundations for criminal response. In many contemporary cases, ta'zir constitutes the most appropriate reactive mechanism, with its severity determined according to the offender's status, the nature and sensitivity of the information, the degree of cooperation with the enemy, criminal intent, and the extent of actual or potential harm. The analysis of Iranian criminal law further reveals several challenges, including fragmented legislation, ambiguity in key concepts, insufficient distinction between treason and espionage, and difficulties in applying traditional provisions to cyber espionage and technological information transfer. Accordingly, structural legislative reform, a more precise definition of treason, graded sanctions, and technology-neutral legal rules could contribute to a more coherent, proportionate, and effective criminal justice framework.

Keywords: *Treason; Imami Jurisprudence; Iranian Criminal Law; Espionage; National Security; Ta'zir.*

How to cite: Haghshenas, H., Jahanbakhshi, H. A., & Ghanad, F. (2027). Reactive Measures against the Crime of Treason from the Perspective of Imami Jurisprudence and Iranian Criminal Law. *Comparative Studies in Jurisprudence, Law, and Politics, 9*(6), 1-22.

Submit Date: 18 May 2026
Revise Date: 29 August 2026
Accept Date: 05 September 2026
Initial Publish Date: 08 September 2026
Final Publish Date: 20 February 2028

پژوهش‌های تطبیقی فقه، حقوق و سیاست

اقدامات واکنشی جرم خیانت به کشور از منظر فقه امامیه و حقوق کیفری ایران

۱. حمیدرضا حق شناس: گروه حقوق، واحد بین المللی کیش، دانشگاه آزاد اسلامی، کیش، ایران
۲. حیدر علی جهانبخشی*: گروه الهیات و معارف اسلامی، واحد اسلامشهر، دانشگاه آزاد اسلامی، اسلامشهر، ایران.
پست الکترونیک: jahanbakhshi@iau.ac.ir (نویسنده مسئول)
۳. فاطمه قناد: گروه حقوق کیفری و جرم شناسی، دانشگاه علم و فرهنگ، تهران، ایران

چکیده

خیانت به کشور از مهم‌ترین جرایم علیه امنیت و منافع بنیادین دولت است که می‌تواند استقلال، تمامیت ارضی، قدرت دفاعی، اسرار امنیتی و سایر منافع حیاتی کشور را در معرض تهدید قرار دهد. با وجود اهمیت این جرم، در حقوق کیفری ایران عنوان مستقل و منسجمی برای خیانت به کشور پیش‌بینی نشده و رفتارهای مرتبط با آن در قالب جرایمی مانند جاسوسی، افشای اطلاعات محرمانه، همکاری با دولت‌های متخاصم، ورود به اماکن ممنوعه و انتقال اطلاعات امنیتی جرم‌انگاری شده‌اند. پژوهش حاضر با روش توصیفی ـ تحلیلی و با هدف تبیین مبانی و اقدامات واکنشی نسبت به جرم خیانت به کشور از منظر فقه امامیه و حقوق کیفری ایران انجام شده است. یافته‌ها نشان می‌دهد که در فقه امامیه، اگرچه خیانت به کشور با مفهوم مدرن آن به‌عنوان یک عنوان مستقل کیفری مطرح نشده است، اصولی مانند حرمت خیانت، وجوب حفظ امانت، ممنوعیت یاری‌رساندن به دشمن و ضرورت حمایت از امنیت جامعه، مبانی لازم برای واکنش کیفری را فراهم می‌کنند. در بسیاری از مصادیق معاصر، تعزیر مناسب‌ترین سازوکار واکنشی محسوب می‌شود و شدت آن باید بر اساس وضعیت مرتکب، نوع و حساسیت اطلاعات، میزان همکاری با دشمن، قصد مجرمانه و شدت خسارت تعیین شود. بررسی حقوق کیفری ایران نیز نشان می‌دهد که مهم‌ترین چالش‌ها شامل پراکندگی مقررات، ابهام برخی مفاهیم، عدم تفکیک کامل خیانت از جاسوسی و دشواری انطباق مقررات سنتی با جاسوسی سایبری و انتقال اطلاعات فناورانه است. بر این اساس، اصلاح ساختاری مقررات، تعریف دقیق‌تر خیانت به کشور، درجه‌بندی ضمانت اجراها و تدوین قواعد فناوری‌خنثی می‌تواند به ایجاد نظامی منسجم‌تر، متناسب‌تر و کارآمدتر منجر شود.

واژگان کلیدی: *خیانت به کشور؛ فقه امامیه؛ حقوق کیفری ایران؛ جاسوسی؛ امنیت ملی؛ تعزیر.*

نحوه استناددهی: حق شناس، حمیدرضا.، جهانبخشی، حیدر علی.، و قناد، فاطمه. (۱۴۰۶). اقدامات واکنشی جرم خیانت به کشور از منظر فقه امامیه و حقوق کیفری ایران. *پژوهش‌های تطبیقی فقه، حقوق و سیاست*، ۹(۶)، ۲۲-۱.

تاریخ ارسال: ۲۸ اردیبهشت ۱۴۰۵
تاریخ بازنگری: ۷ شهریور ۱۴۰۵
تاریخ پذیرش: ۱۴ شهریور ۱۴۰۵
تاریخ چاپ اولیه: ۱۷ شهریور ۱۴۰۵
تاریخ چاپ نهایی: ۱ اسفند ۱۴۰۶

مقدمه

امنیت ملی یکی از بنیادی‌ترین ارزش‌هایی است که استمرار حیات سیاسی، اجتماعی و حقوقی هر جامعه به آن وابسته است. هر نظام سیاسی برای حفظ موجودیت خود ناگزیر از حمایت کیفری در برابر رفتارهایی است که استقلال، تمامیت ارضی، اسرار اساسی، توان دفاعی، ساختار حاکمیت یا منافع حیاتی کشور را در معرض مخاطره قرار می‌دهند. در میان این رفتارها، خیانت به کشور از جایگاهی خاص برخوردار است؛ زیرا برخلاف بسیاری از جرایم عادی که زیان آن‌ها متوجه اشخاص یا منافع محدود اجتماعی است، خیانت می‌تواند مستقیماً اساس حاکمیت و امنیت عمومی را هدف قرار دهد. در ادبیات حقوقی کشورهای مختلف نیز خیانت همواره در زمره شدیدترین جرایم علیه دولت و امنیت سیاسی طبقه‌بندی شده است و تحولات تاریخی این مفهوم نشان می‌دهد که مرزهای آن متناسب با تحول مفهوم دولت، تابعیت، جنگ، امنیت و وفاداری سیاسی تغییر یافته است. بررسی تاریخی مفهوم treason در حقوق انگلستان نشان می‌دهد که این عنوان از یک مفهوم بسیار گسترده در حمایت از شخص پادشاه به مفهومی محدودتر و مرتبط با امنیت بنیادین دولت تحول پیدا کرده است (Boyer & Nicholls, 2024). چنین تحولی مؤید آن است که خیانت را نمی‌توان صرفاً با برداشت‌های سنتی از همکاری با دشمن در جنگ تعریف کرد، بلکه باید آن را در پرتو ساختارهای جدید تهدید علیه امنیت ملی بازشناسی کرد.

در نظام حقوقی ایران، برخلاف برخی نظام‌های کیفری که عنوان مستقل و نسبتاً منسجمی برای «خیانت به کشور» پیش‌بینی کرده‌اند، رفتارهایی که ماهیتاً واجد وصف خیانت‌آمیز هستند در قالب عناوین کیفری متعدد مورد جرم‌انگاری قرار گرفته‌اند. جاسوسی، تسلیم اسناد و اطلاعات محرمانه به بیگانگان، همکاری با دولت‌های متخاصم، ورود به اماکن ممنوعه با هدف کسب اطلاعات، افشای اسرار امنیتی و نظامی و برخی اشکال همکاری اطلاعاتی با بیگانگان از مهم‌ترین مصادیقی هستند که می‌توان آن‌ها را در چهارچوب گسترده خیانت به کشور بررسی کرد. رحمدل، در بررسی رابطه جاسوسی و خیانت به کشور، بر پیوند مفهومی این دو رفتار و در عین حال ضرورت تفکیک دقیق قلمرو آن‌ها در حقوق کیفری تأکید کرده است (Rahmdel, 2020). ساریخانی نیز خیانت به کشور و جاسوسی را از مهم‌ترین جرایم علیه امنیت داخلی و خارجی معرفی کرده و تحلیل آن‌ها را منوط به توجه هم‌زمان به ماهیت رفتار، هدف مرتکب و رابطه وی با کشور دانسته است (Sarikhani, 1999). بنابراین، یکی از نخستین چالش‌های حقوق کیفری ایران در این زمینه، فقدان یک مفهوم قانونی جامع از خیانت به کشور و پراکندگی مصادیق آن در عناوین مجرمانه متعدد است.

اهمیت موضوع زمانی بیشتر می‌شود که اقدامات واکنشی نظام کیفری در برابر این جرم مورد توجه قرار گیرد. واکنش کیفری صرفاً به معنای تعیین یک مجازات شدید نیست، بلکه مجموعه‌ای از تدابیر قانونی، قضایی و کیفری را در بر می‌گیرد که پس از ارتکاب رفتار مجرمانه یا احراز خطر ناشی از آن به اجرا درمی‌آید. این واکنش‌ها می‌تواند شامل مجازات‌های سالب حیات یا آزادی در موارد بسیار شدید، حبس‌های طولانی‌مدت، مجازات‌های تعزیری، محرومیت از برخی حقوق اجتماعی، انفصال از خدمات عمومی یا نظامی، مصادره یا ضبط ابزار و عواید جرم و نیز تدابیر محدودکننده مرتبط با دسترسی به اطلاعات محرمانه باشد. سیاست کیفری ایران نسبت به جرایم امنیتی همواره گرایش به شدت واکنش داشته است؛ با این حال، تحلیل کارآمدی این سیاست نیازمند توجه به تناسب میان نوع تهدید و شدت ضمانت اجراست. مطالعات مربوط به سیاست جنایی ایران در قبال جرایم علیه امنیت نشان می‌دهد که جاسوسی و رفتارهای مشابه به دلیل تأثیر مستقیم بر منافع حیاتی دولت در زمره مهم‌ترین حوزه‌های مداخله کیفری قرار دارند (Mazaheri, 2019). بررسی دیگری نیز بر این نکته تأکید می‌کند که

جرایم امنیتی، از جمله جاسوسی و ورود غیرمجاز به اماکن حساس، در سیاست کیفری ایران با واکنش‌های شدید و مبتنی بر حفاظت از ساختار سیاسی و دفاعی مواجه شده‌اند (Mazhari, 2019).

با این حال، شدت مجازات به‌تنهایی تضمین‌کننده کارآمدی نظام واکنشی نیست. در حوزه جرایم علیه امنیت، یکی از مهم‌ترین مسائل، تعیین دقیق حدود جرم‌انگاری است؛ زیرا توسعه بیش از اندازه مفاهیمی همچون جاسوسی، همکاری با دشمن یا افشای اطلاعات ممکن است اصل قانونی بودن جرایم و مجازات‌ها را تضعیف کند و از سوی دیگر، تعریف بیش از اندازه محدود این عناوین می‌تواند نظام کیفری را در برابر اشکال جدید خیانت ناکارآمد سازد. بررسی نارسایی‌های تقنینی جرم جاسوسی در حقوق ایران نشان داده است که تعدد مقررات، پراکندگی عناصر قانونی و ابهام در برخی اصطلاحات، امکان ایجاد اختلاف در تفسیر و اجرای قوانین را فراهم می‌کند (Aghigh, 2023). این مسئله در ارتباط با خیانت به کشور اهمیتی مضاعف پیدا می‌کند، زیرا ماهیت این جرم با مفاهیمی همچون دشمن، دولت متخاصم، اسرار، اطلاعات طبقه‌بندی‌شده، منافع ملی و قصد ضربه زدن به امنیت کشور پیوند خورده است و هر یک از این مفاهیم می‌تواند محل تفسیر متفاوت باشد.

تحول فناوری نیز مفهوم سنتی خیانت و ابزارهای ارتکاب آن را دگرگون کرده است. در گذشته، دستیابی به اسناد نظامی یا انتقال اطلاعات به دولت بیگانه غالباً مستلزم حضور فیزیکی مرتکب در مراکز حساس، تماس مستقیم با مأموران اطلاعاتی یا جابه‌جایی فیزیکی اسناد بود؛ در حالی که امروزه حجم عظیمی از اطلاعات راهبردی در قالب داده‌های الکترونیکی نگهداری می‌شود و انتقال آن‌ها می‌تواند در زمانی بسیار کوتاه و بدون حضور مرتکب در محل صورت گیرد. جرم جاسوسی سایبری یکی از مصادیق روشن این تحول است و حقوق کیفری ایران نیز با ضرورت تطبیق ساختارهای سنتی جرم‌انگاری با فضای سایبری مواجه شده است (Hamidi, 2024). در تعریف‌های جدید امنیت سایبری نیز جاسوسی سایبری به فعالیت‌هایی اطلاق می‌شود که از طریق نفوذ دیجیتال برای دسترسی مخفیانه به اطلاعات حساس دولتی، نظامی، اقتصادی یا فناورانه انجام می‌گیرد (SentinelOne, 2025). در نتیجه، اگر مفهوم خیانت به کشور به همکاری عامدانه با قدرت خارجی در جهت آسیب به منافع حیاتی کشور گره زده شود، بسیاری از اشکال جدید جاسوسی سایبری نیز قابلیت تحلیل در چهارچوب آن را خواهند داشت.

پیچیدگی مسئله تنها به فناوری محدود نیست. امنیت ملی امروز علاوه بر ابعاد نظامی و سیاسی، شامل امنیت اقتصادی، علمی، فناورانه، انرژی و زیرساخت‌های حیاتی نیز می‌شود. جاسوسی اقتصادی و صنعتی می‌تواند موجب انتقال دانش فنی، اسرار تجاری یا فناوری‌های راهبردی به رقبا شود و در سطحی گسترده‌تر توان اقتصادی و استقلال کشور را تضعیف کند. ناشسی نشان می‌دهد که جاسوسی اقتصادی و صنعتی در نظام رقابت جهانی جدید به یکی از ابزارهای جدی دستیابی به مزیت اقتصادی و فناورانه تبدیل شده است (Nashesi, 2022). همچنین، مباحث جدید امنیت پژوهش و سرمایه‌گذاری خارجی بر ضرورت حمایت از دانش، زیرساخت علمی و اطلاعات حساس در برابر نفوذ و انتقال غیرمجاز تأکید دارند (Walker-Munro, 2024). از این منظر، واکنش کیفری به خیانت نباید تنها بر الگوی کلاسیک همکاری نظامی با دشمن متمرکز باشد، بلکه باید توان پاسخ‌گویی به انتقال اطلاعات راهبردی اقتصادی، علمی و فناورانه را نیز داشته باشد.

در کنار حقوق کیفری موضوعه، فقه امامیه یکی از مهم‌ترین مبانی هنجاری نظام حقوقی جمهوری اسلامی ایران محسوب می‌شود و بررسی اقدامات واکنشی نسبت به خیانت به کشور بدون مطالعه مبانی فقهی آن ناقص خواهد بود. در منابع فقهی، اگرچه اصطلاح «خیانت به کشور» با مفهوم مدرن حقوق کیفری به شکل مستقل و نظام‌مند مطرح نشده است، مفاهیمی مانند خیانت، افشای اسرار مسلمانان، اعانت دشمن، تجسس، جاسوسی برای دشمن، بغی، محاربه و همکاری‌ای که سبب تقویت دشمن و تضعیف جامعه اسلامی شود، ظرفیت قابل توجهی برای

تحلیل رفتارهای امروزی دارند. البته انطباق این مفاهیم با جرایم جدید باید با احتیاط انجام شود، زیرا هر مفهوم فقهی دارای عناصر، شرایط و آثار خاص خود است و نمی‌توان صرف شباهت ظاهری یک رفتار را مبنای تسری حکم شدیدتر قرار داد. مطالعه ادله قرآنی و روایی مرتبط با تجسس نیز نشان می‌دهد که فقه اسلامی میان تجسس ممنوع در امور خصوصی و اقداماتی که با هدف کشف جرایم شدید یا حمایت از مصالح اساسی جامعه صورت می‌گیرند، نیازمند تمایزگذاری دقیق است (Sarikhani et al., 2022).

مسئله اساسی این پژوهش آن است که اقدامات واکنشی مناسب در برابر خیانت به کشور از منظر فقه امامیه بر چه مبانی استوار است و حقوق کیفری ایران تا چه اندازه توانسته است این مبانی را در قالب یک نظام منسجم، متناسب و کارآمد منعکس کند. همچنین باید بررسی شود که آیا جرم‌انگاری‌های پراکنده موجود می‌توانند همه اشکال نوین خیانت را پوشش دهند یا نیاز به بازنگری تقنینی وجود دارد. هدف اصلی مقاله، تبیین مبانی فقهی و حقوقی واکنش به جرم خیانت به کشور، شناسایی مهم‌ترین ضمانت اجراهای قابل اعمال و ارزیابی تناسب و کارآمدی آن‌ها در حقوق کیفری ایران است. روش تحقیق، توصیفی ـ تحلیلی است و با بهره‌گیری از منابع فقهی و حقوق کیفری، سیاست تقنینی ایران در قبال مهم‌ترین رفتارهای خیانت‌آمیز تحلیل می‌شود. فرض اساسی پژوهش این است که هرچند در فقه امامیه ظرفیت هنجاری کافی برای برخورد قاطع با رفتارهایی که آگاهانه امنیت جامعه اسلامی را در معرض خطر اساسی قرار می‌دهند وجود دارد و حقوق کیفری ایران نیز ضمانت اجراهای متعددی برای مصادیق چنین رفتارهایی پیش‌بینی کرده است، پراکندگی عناوین مجرمانه، نبود تعریف روشن از خیانت به کشور و عدم تناسب کامل میان برخی مصادیق و ضمانت اجراها، ضرورت تدوین رویکردی منسجم‌تر را آشکار می‌سازد.

مبانی مفهومی و فقهی جرم خیانت به کشور

خیانت در معنای عمومی متضمن نقض اعتماد، عهد یا تکلیفی است که بر عهده شخص قرار گرفته و در نتیجه آن، منفعت یا حق دیگری در معرض آسیب قرار می‌گیرد. هنگامی که این مفهوم به سطح روابط فرد و دولت منتقل می‌شود، خیانت به کشور به رفتاری تبدیل می‌شود که از طریق نقض تکلیف بنیادین وفاداری، منافع اساسی جامعه سیاسی را در معرض خطر قرار می‌دهد. این تعریف، خیانت را از هر نوع مخالفت، انتقاد یا رفتار غیرهمسو با دولت متمایز می‌سازد. صرف مخالفت سیاسی، اعتراض یا بیان دیدگاه انتقادی، مادامی که واجد عناصر رفتار مجرمانه و قصد تعرض به منافع بنیادین امنیتی نباشد، نباید تحت مفهوم خیانت قرار گیرد. تاریخ حقوق کیفری نیز نشان می‌دهد که یکی از مهم‌ترین تحولات در جرم خیانت، حرکت از تعاریف موسع و سیاسی به سمت تعاریف محدودتر و مبتنی بر رفتارهای مشخص علیه موجودیت دولت بوده است (Boyer & Nicholls, 2024). چنین رویکردی با اصل قانونی بودن جرایم و مجازات‌ها و ضرورت جلوگیری از توسعه نامحدود جرایم امنیتی سازگارتر است.

یکی از عناصر مهم در مفهوم خیانت، وجود رابطه‌ای است که بر اساس آن از شخص انتظار وفاداری به جامعه سیاسی وجود دارد. در معنای کلاسیک، این رابطه معمولاً از تابعیت ناشی می‌شود؛ بنابراین، تبعه‌ای که عامدانه با دشمن کشور همکاری می‌کند، اطلاعات حساس را در اختیار آن قرار می‌دهد یا امکانات لازم برای ضربه زدن به کشور را فراهم می‌سازد، نمونه روشن خیانت محسوب می‌شود. با این حال، تحولات معاصر موجب پیچیده‌تر شدن این معیار شده است. ممکن است شخص فاقد تابعیت، به سبب سمت دولتی، قرارداد امنیتی، دسترسی ویژه یا تعهد حرفه‌ای، دارای تکلیفی نسبت به حفظ اسرار کشور باشد. در چنین مواردی، رفتار وی ممکن است از نظر حقوقی جاسوسی، افشای اسرار یا همکاری با دولت خارجی باشد، هرچند از منظر مفهومی نتوان همه آثار خیانت مبتنی بر تابعیت را بر آن بار کرد. رحمدل در تفکیک جاسوسی و خیانت نشان می‌دهد که این دو عنوان اگرچه در بسیاری از موارد هم‌پوشانی دارند، از نظر عناصر و وضعیت مرتکب الزاماً یکسان

نیستند (Rahmdel, 2020). این تمایز در تعیین واکنش کیفری اهمیت اساسی دارد، زیرا شدت پاسخ باید متناسب با سطح نقض تعهد و میزان خطری باشد که رفتار ایجاد کرده است.

جاسوسی از نزدیک‌ترین مفاهیم به خیانت به کشور است. جاسوسی معمولاً با تحصیل، جمع‌آوری، انتقال یا در دسترس قرار دادن اطلاعاتی مرتبط است که به دلیل اهمیت امنیتی، سیاسی یا نظامی تحت حفاظت قرار گرفته‌اند. در برخی موارد، شخص جاسوس اساساً تبعه کشور هدف نیست و به‌عنوان مأمور دولت خارجی فعالیت می‌کند؛ در این وضعیت، استفاده از مفهوم خیانت به معنای دقیق دشوار است، زیرا تکلیف وفاداری مبتنی بر تابعیت وجود ندارد. در مقابل، هنگامی که تبعه یک کشور اطلاعات محرمانه آن را آگاهانه در اختیار قدرت خارجی قرار می‌دهد، رفتار او می‌تواند هم واجد وصف جاسوسی و هم متضمن ماهیت خیانت‌آمیز باشد. سادات در تحلیل نظری جاسوسی و خیانت، این جرایم را از مهم‌ترین ابزارهای تعرض پنهان به امنیت دولت دانسته و بر تفاوت میان ساختار عملیات جاسوسی و موقعیت حقوقی مرتکب تأکید کرده است (Sadat, 2019). بنابراین، در تحلیل حقوقی باید میان عنوان فنی جرم و وصف ارزشی خیانت تفاوت گذاشت.

عنصر دیگری که در تشخیص خیانت نقش دارد، ماهیت منفعت مورد تعرض است. هر افشای اطلاعاتی را نمی‌توان خیانت دانست. اطلاعات باید به نحوی با امنیت، استقلال، قدرت دفاعی، روابط خارجی، زیرساخت‌های راهبردی یا سایر منافع حیاتی کشور ارتباط داشته باشند. گسترش حوزه امنیت ملی سبب شده است که امروزه اطلاعات اقتصادی و فناورانه نیز در برخی شرایط اهمیت راهبردی پیدا کنند. جاسوسی اقتصادی ممکن است به انتقال فناوری‌هایی منجر شود که مستقیماً در توان دفاعی یا رقابت راهبردی کشور نقش دارند (Nashesi, 2022). از سوی دیگر، حمایت از امنیت پژوهش، فناوری و سرمایه‌گذاری خارجی در بسیاری از کشورها به بخشی از سیاست امنیت ملی تبدیل شده است؛ زیرا انتقال برخی دانش‌ها و فناوری‌های حساس می‌تواند پیامدهای امنیتی فراتر از زیان اقتصادی مستقیم داشته باشد (Walker-Munro, 2024). بر این اساس، معیار مناسب آن است که اهمیت اطلاعات و آثار واقعی یا بالقوه انتقال آن بر منافع اساسی کشور مورد ارزیابی قرار گیرد.

در حقوق کیفری ایران، مصادیق نزدیک به خیانت به کشور در قالب مقررات متنوع مطرح شده‌اند و همین امر سبب شده است که تعریف جامع و یکپارچه‌ای از آن شکل نگیرد. برخی مقررات ناظر بر در اختیار گذاشتن اسناد و اسرار به اشخاص فاقد صلاحیت یا بیگانگان هستند، برخی همکاری با دولت متخاصم را جرم می‌دانند و گروهی دیگر بر ورود به اماکن ممنوعه یا تصویربرداری و کسب اطلاعات تأکید دارند. پژوهش درباره جرم جاسوسی در حقوق ایران نشان می‌دهد که تعدد مقررات و تفاوت در عناصر جرم می‌تواند موجب دشواری در تعیین دقیق قلمرو هر عنوان شود (Aghigh, 2023). هدایتی چنانی نیز در بررسی جاسوسی در حقوق بین‌الملل و حقوق کیفری نیروهای مسلح، بر اهمیت وضعیت مرتکب، نوع اطلاعات و ارتباط رفتار با امنیت نظامی تأکید کرده است (Hedayati Chenani, 2021). این پراکندگی، ضرورت ارائه معیاری مفهومی برای تشخیص رفتارهای واقعاً خیانت‌آمیز را تقویت می‌کند.

از منظر فقه امامیه، نخستین مبنای تحلیل خیانت، حرمت خود خیانت و لزوم وفای به عهد و امانت است. در نظام اخلاقی و فقهی اسلام، امانت تنها شامل اموال خصوصی نیست و هر چیزی که بر اساس اعتماد در اختیار شخص قرار گیرد می‌تواند موضوع تعهد به حفظ باشد. اسرار مربوط به مصالح عمومی و امنیت جامعه نیز از این حیث قابلیت تحلیل دارند. شخصی که به سبب منصب، عضویت در ساختارهای نظامی یا اداری، حرفه یا اعتماد عمومی به اطلاعات حساس دسترسی پیدا می‌کند، از منظر مبانی فقهی نمی‌تواند آن‌ها را برخلاف مصلحت

مشروع جامعه در اختیار دشمن یا افراد فاقد صلاحیت قرار دهد. در چنین وضعیتی، نقض تعهد محرمانگی افزون بر تخلف از ضابطه اداری یا قانونی، واجد وصف خیانت در امانت معنوی و عمومی خواهد بود.

مبنای دوم، حرمت یاری رساندن به دشمن در اقداماتی است که علیه جامعه اسلامی صورت می‌گیرد. اگر رفتاری به‌طور آگاهانه سبب تقویت دشمن در تجاوز، عملیات نظامی، خرابکاری، نفوذ یا اخلال جدی در امنیت شود، نمی‌توان آن را صرفاً یک تخلف عادی دانست. در چنین مواردی، آثار رفتار و قصد مرتکب در تعیین عنوان فقهی اهمیت دارد. ممکن است در شرایطی رفتار به سطح اعانت بر ظلم یا معاونت در جرم برسد و در وضعیت شدیدتر، حسب عناصر خاص، قابلیت بررسی تحت عناوین دیگری مانند محاربه یا بغی پیدا کند. با این حال، توسعه عناوین فقهی شدید باید محدود به مواردی باشد که تمام شرایط آن عنوان وجود داشته باشد. این امر از یک سو مانع بی‌پاسخ ماندن رفتارهای تهدیدکننده می‌شود و از سوی دیگر، از تسری غیرموجه مجازات‌های شدید به رفتارهای فاقد عناصر لازم جلوگیری می‌کند.

موضوع تجسس در فقه امامیه نیز با بحث جاسوسی ارتباطی پیچیده دارد. اصل منع تجسس در امور خصوصی افراد، یکی از قواعد مهم حمایت از حریم اشخاص است، اما نمی‌توان آن را به نحوی تفسیر کرد که هر نوع اقدام اطلاعاتی دولت برای مقابله با تهدید جدی امنیتی ممنوع تلقی شود. بررسی ادله قرآنی و روایی منع تجسس نشان می‌دهد که میان تجسس ناروا در زندگی خصوصی اشخاص و اقدامات ضروری برای کشف برخی جرایم شدید می‌توان تمایز قائل شد، هرچند این تمایز باید تحت ضوابط و محدودیت‌های مشخص قرار گیرد (Sarikhani et al., 2022). از همین منظر، مقابله با خیانت و جاسوسی نمی‌تواند مجوزی نامحدود برای نقض حقوق افراد ایجاد کند، بلکه اقدامات کشفی و امنیتی باید بر ضرورت، تناسب و وجود ظن معتبر یا قرائن قابل اتکا استوار باشند.

در فقه کیفری امامیه، واکنش به رفتارهای آسیب‌زننده به امنیت لزوماً در قالب یک مجازات ثابت برای عنوان «خیانت» تنظیم نشده است. برخلاف حدود که نوع و میزان مجازات آن‌ها در شرع تعیین شده است، بسیاری از رفتارهای جدید امنیتی در قلمرو تعزیرات قرار می‌گیرند. این ویژگی امکان انطباق سیاست کیفری با شرایط متغیر اجتماعی و فناوری را فراهم می‌کند. اگر یک رفتار جاسوسی یا همکاری اطلاعاتی با دشمن واجد عنوان حدی مستقل نباشد، حاکم اسلامی می‌تواند با رعایت ضوابط تعزیر، برای آن مجازاتی متناسب مقرر کند. این انعطاف از اهمیت زیادی برخوردار است؛ زیرا شیوه‌های خیانت در عصر اطلاعات با اشکال سنتی تفاوت بنیادین دارند و بخش مهمی از آن‌ها در فضای دیجیتال رخ می‌دهد. تحلیل جاسوسی سایبری در حقوق ایران و افغانستان نیز نشان می‌دهد که ابزار و محیط ارتکاب جرم تغییر کرده است، اما ماهیت تعرض به اطلاعات حساس همچنان باقی است (Hamidi, 2024).

تحول مفهوم «اسرار» نیز در این زمینه قابل توجه است. در گذشته، مفهوم اسرار امنیتی بیشتر با نقشه‌های نظامی، برنامه‌های عملیاتی و اسناد دیپلماتیک پیوند داشت؛ اما در محیط جدید، داده‌های رایانه‌ای، کلیدهای دسترسی، پایگاه‌های اطلاعاتی، سامانه‌های زیرساختی، فناوری‌های حساس و اطلاعات علمی راهبردی نیز می‌توانند همان اهمیت را داشته باشند. جرم جاسوسی سایبری می‌تواند بدون برداشتن سند فیزیکی و تنها از طریق کپی داده، نفوذ از راه دور یا ایجاد دسترسی برای شخص ثالث تحقق یابد (SentinelOne, 2025). از همین رو، مبانی فقهی مرتبط با خیانت نباید به شکل و قالب مادی اطلاعات محدود شوند، بلکه آنچه اهمیت دارد ماهیت امانت، ارزش امنیتی اطلاعات و قصد مرتکب در انتقال یا فراهم کردن دسترسی غیرمجاز است.

در نهایت، مبانی مفهومی و فقهی خیانت به کشور بر سه محور استوار است: وجود منفعت اساسی و مشروع عمومی، وجود رفتاری عامدانه که این منفعت را در معرض خطر قابل توجه قرار می‌دهد و وجود نوعی نقض تعهد یا همکاری آگاهانه با عامل تهدیدکننده. هرچه رابطه

مرتکب با کشور نزدیک‌تر، اطلاعات یا امکانات مورد انتقال حساس‌تر و قصد آسیب‌رسانی روشن‌تر باشد، وصف خیانت‌آمیز رفتار تقویت می‌شود. در مقابل، باید میان خیانت واقعی و رفتارهایی که صرفاً با سیاست‌های رسمی اختلاف دارند تمایز صریح برقرار شود. چنین تفکیکی برای مشروعیت اقدامات واکنشی ضروری است؛ زیرا واکنش شدید کیفری زمانی توجیه‌پذیر است که رفتار مرتکب نه صرفاً نامطلوب یا مخالف، بلکه متضمن تعرض جدی و عامدانه به امنیت بنیادین کشور باشد.

اقدامات واکنشی در برابر خیانت به کشور از منظر فقه امامیه

واکنش به جرم در فقه امامیه تابع مجموعه‌ای از اصول است که در کنار ضرورت حمایت از نظم و مصالح جامعه، بر محدود بودن مجازات به موارد مشروع و اثبات‌شده تأکید دارد. در این چهارچوب، هر رفتار آسیب‌زننده به امنیت کشور الزاماً دارای مجازات ثابت شرعی نیست و باید ابتدا عنوان فقهی دقیق آن مشخص شود. این مسئله در مورد خیانت به کشور اهمیت ویژه‌ای دارد، زیرا عنوان امروزی خیانت ممکن است در عمل شامل مجموعه‌ای از رفتارها از افشای اطلاعات محرمانه تا همکاری عملیاتی با دشمن باشد و شدت این رفتارها یکسان نیست. بنابراین، نمی‌توان برای همه آن‌ها واکنشی واحد در نظر گرفت. در برخی موارد، رفتار در قلمرو تعزیر باقی می‌ماند و در برخی دیگر ممکن است واجد شرایط عنوان شدیدتری شود. اصل اساسی آن است که نوع واکنش باید تابع ماهیت واقعی رفتار، قصد مرتکب، آثار ایجادشده و میزان تهدید علیه جامعه باشد.

تعزیر مهم‌ترین ظرفیت فقه امامیه برای پاسخ‌گویی به رفتارهای خیانت‌آمیز جدید است. بسیاری از اشکال جاسوسی، افشای داده‌های محرمانه، همکاری اطلاعاتی با بیگانگان یا انتقال فناوری حساس، عنوان حدی مستقلی ندارند، اما این امر به معنای فقدان واکنش کیفری نیست. ماهیت انعطاف‌پذیر تعزیر اجازه می‌دهد که قانون‌گذار بر اساس مصالح عمومی و شدت خطر، مجازات مناسب تعیین کند. این ویژگی در حوزه امنیتی اهمیت فراوان دارد؛ زیرا تهدیدها در گذر زمان تغییر می‌کنند و جرم‌انگاری باید توانایی پاسخ به شیوه‌های جدید را داشته باشد. افزایش اهمیت جاسوسی سایبری نمونه‌ای از چنین تحولی است؛ بررسی تطبیقی این جرم در حقوق ایران و افغانستان نشان می‌دهد که انتقال فعالیت‌های جاسوسی به فضای دیجیتال، ساختارهای سنتی جرم‌انگاری را با ضرورت بازتعریف موضوع جرم و شیوه ارتکاب روبه‌رو کرده است (Hamidi, 2024). بنابراین، ظرفیت تعزیر می‌تواند مبنایی برای واکنش متناسب به این اشکال نوین باشد.

تناسب در مجازات یکی از مهم‌ترین اصولی است که باید در تعیین واکنش تعزیری مورد توجه قرار گیرد. خیانت به کشور دامنه‌ای وسیع از رفتارها را در بر می‌گیرد و نمی‌توان فردی را که اطلاعاتی با اهمیت محدود را بدون قصد آسیب جدی افشا کرده است با شخصی که آگاهانه اطلاعات عملیاتی حساس را در اختیار دشمن در حال مخاصمه قرار داده و زمینه وارد شدن خسارات گسترده را فراهم ساخته است، در یک سطح قرار داد. سیاست کیفری مؤثر باید میان میزان حساسیت اطلاعات، وضعیت مرتکب، درجه همکاری با طرف خارجی، نوع قصد و نتیجه رفتار تفکیک ایجاد کند. پژوهش‌های مرتبط با جرایم علیه امنیت در ایران نیز نشان می‌دهند که سیاست کیفری موجود با طیفی از رفتارهای بسیار متفاوت روبه‌رو است و همین امر ضرورت درجه‌بندی واکنش را آشکار می‌سازد (Mazaheri, 2019). واکنش فقهی مبتنی بر تعزیر نیز باید همین منطق را دنبال کند و مجازات را بر اساس شدت واقعی تهدید تعیین نماید.

در شدیدترین حالت‌ها ممکن است رفتار خیانت‌آمیز با عناوینی مانند محاربه ارتباط پیدا کند، اما چنین ارتباطی نیازمند احراز تمام عناصر آن عنوان است. صرف همکاری با بیگانه یا انتقال اطلاعات را نمی‌توان خودبه‌خود محاربه دانست. محاربه در ساختار فقهی دارای شرایط خاصی است و تسری آثار آن به رفتاری که فاقد این شرایط باشد، با اصول احتیاط در دماء و مجازات‌های شدید سازگار نیست. اگر فعالیت مرتکب

بخشی از عملیات مسلحانه یا اقدام سازمان‌یافته‌ای باشد که امنیت مردم را به شکل موردنظر در عنوان محاربه هدف قرار می‌دهد، امکان بررسی موضوع در آن چهارچوب وجود دارد؛ اما در غیر این صورت، باید از ظرفیت تعزیر استفاده کرد. اهمیت این تفکیک از آن جهت است که در جرایم امنیتی، گرایش به تفسیر موسع می‌تواند به افزایش غیرضروری شدت مجازات منتهی شود.

همین ملاحظه درباره بغی نیز وجود دارد. بغی در فقه امامیه دارای شرایطی مرتبط با خروج سازمان‌یافته و مسلحانه علیه حاکمیت مشروع است و هر نوع مخالفت یا همکاری با دولت خارجی به‌تنهایی مصداق آن نیست. خیانت ممکن است در عمل بخشی از یک فعالیت شورشی سازمان‌یافته باشد و در چنین صورتی عنوان فقهی رفتار باید با توجه به مجموعه شرایط بررسی شود. با این حال، اگر رفتار به انتقال اطلاعات یا تسهیل فعالیت دشمن محدود باشد، بدون آنکه عناصر بغی وجود داشته باشد، استفاده از عنوان تعزیری صحیح‌تر است. این رویکرد هم امکان واکنش قاطع را حفظ می‌کند و هم مانع خلط عناوین و اعمال مجازات‌های شدید بدون تحقق عناصر لازم می‌شود.

یکی دیگر از مبانی واکنش فقهی، توجه به وضعیت خاص مرتکب است. کارمند دستگاه امنیتی، نظامی یا اداری که به دلیل موقعیت خود به اسرار کشور دسترسی دارد، در مقایسه با فرد عادی دارای تعهد مضاعفی به حفظ اطلاعات است. نقض این تعهد می‌تواند از حیث سرزنش‌پذیری شدیدتر ارزیابی شود؛ زیرا مرتکب نه‌تنها امنیت عمومی را تهدید کرده بلکه اعتماد خاصی را که به سبب سمت او شکل گرفته نقض کرده است. هدایتی چنانی در بررسی جرم جاسوسی در حوزه نیروهای مسلح به اهمیت دسترسی سازمانی مرتکب به اطلاعات حساس و موقعیت ویژه کارکنان نظامی اشاره می‌کند (Hedayati Chenani, 2021). از منظر فقهی نیز چنین موقعیتی می‌تواند در تعیین درجه تعزیر و ارزیابی شدت خیانت مؤثر باشد.

افشای اسرار نظامی و دفاعی از مهم‌ترین حوزه‌هایی است که واکنش شدید را توجیه می‌کند. اطلاعات مربوط به ساختار دفاعی، برنامه‌های عملیاتی، تجهیزات خاص، نقاط آسیب‌پذیر یا قابلیت‌های راهبردی می‌توانند در صورت انتقال به دشمن آثار مستقیم بر جان افراد و امنیت جامعه داشته باشند. مطالعه سیاست کیفری ایران در زمینه جاسوسی هسته‌ای نیز بر ضرورت توجه ویژه به فناوری و ماهیت اطلاعات در تعیین واکنش تأکید کرده است (Meshkat, 2019). در چهارچوب فقهی، هرچه احتمال ایجاد زیان شدید و فوری بیشتر باشد، ضرورت واکنش بازدارنده نیز تقویت می‌شود. البته همین شدت خطر اقتضا می‌کند که اثبات جرم با دقت بالاتر صورت گیرد، زیرا آثار محکومیت در چنین پرونده‌هایی معمولاً سنگین است.

مجازات تعزیری می‌تواند اشکال مختلفی داشته باشد و لزوماً به حبس محدود نیست. در موارد متناسب، محرومیت از مشاغل حساس، منع دسترسی به اطلاعات طبقه‌بندی‌شده، انفصال از منصب، محدودیت در فعالیت‌های خاص و ضبط عواید حاصل از جرم می‌تواند مکمل مجازات اصلی باشد. این تدابیر از منظر سیاست کیفری دارای کارکرد پیشگیرانه ویژه‌ای هستند، زیرا هدف آن‌ها فقط پاسخ به رفتار گذشته نیست، بلکه کاهش احتمال تکرار جرم نیز هست. اگر شخصی از موقعیت سازمانی خود برای انتقال اطلاعات استفاده کرده است، باقی ماندن او در همان موقعیت می‌تواند زمینه استمرار خطر را ایجاد کند. بنابراین، محرومیت حرفه‌ای متناسب می‌تواند در کنار مجازات اصلی مشروعیت و کارآمدی بیشتری داشته باشد.

در مقابل، اعمال واکنش‌های محدودکننده باید با اصل شخصی بودن مسئولیت کیفری سازگار باشد. خیانت به کشور، به دلیل بار منفی شدید اجتماعی، ممکن است آثار غیررسمی گسترده‌ای بر خانواده و نزدیکان مرتکب ایجاد کند، اما از منظر عدالت کیفری، مسئولیت باید محدود به شخصی باشد که عناصر جرم درباره او اثبات شده است. وابستگی خانوادگی، دوستی یا ارتباط حرفه‌ای با مرتکب، بدون اثبات مشارکت یا

معاونت آگاهانه، نمی‌تواند مبنای مجازات قرار گیرد. این قاعده به‌ویژه در جرایم امنیتی مهم است، زیرا روابط اجتماعی و شبکه‌ای ممکن است گسترده باشد و توسعه مسئولیت بر اساس صرف ارتباط، با اصول اساسی مسئولیت شخصی تعارض پیدا کند.

در حوزه کشف و اثبات جرم نیز فقه امامیه محدودیت‌هایی بر اقدامات واکنشی و امنیتی تحمیل می‌کند. مقابله با خیانت و جاسوسی معمولاً مستلزم روش‌های پنهان اطلاعاتی، کنترل ارتباطات یا مراقبت از افراد مظنون است، اما ضرورت امنیتی نباید به مجوزی نامحدود برای تجسس تبدیل شود. بررسی فقهی ادله منع تجسس بیانگر آن است که ورود به حریم خصوصی اشخاص نیازمند توجیه قوی و وجود ضرورت معتبر است (Sarikhani et al., 2022). بر این اساس، هرچه مداخله شدیدتر باشد، باید ارتباط آن با تهدید مشخص امنیتی روشن‌تر و نظارت قانونی بر آن دقیق‌تر باشد. چنین رویکردی ضمن حفظ قابلیت کشف جرایم مهم، مانع آن می‌شود که عنوان امنیت ملی به پوششی برای مداخلات نامتناسب تبدیل شود.

توبه، ندامت و همکاری مرتکب با مقامات نیز در برخی نظام‌های تعزیری می‌تواند در تعیین میزان واکنش مؤثر باشد. اگر مرتکب پیش از تحقق نتیجه زیان‌بار از ادامه همکاری با دشمن منصرف شود، اطلاعات لازم برای جلوگیری از خسارت را در اختیار مقامات قرار دهد یا زمینه خنثی‌سازی عملیات را فراهم سازد، سیاست کیفری می‌تواند این رفتار را در تعیین مجازات لحاظ کند. این امر به معنای بی‌اهمیت دانستن جرم نیست، بلکه از منظر مصلحت عمومی ممکن است تشویق مرتکبان به توقف همکاری و کاهش خسارت، ارزش عملی بیشتری داشته باشد. در جرایم اطلاعاتی، گاه اطلاعاتی که مرتکب پس از بازگشت ارائه می‌دهد می‌تواند برای جلوگیری از خسارات گسترده‌تر حیاتی باشد. نظام تعزیری به دلیل انعطاف خود ظرفیت مناسبی برای لحاظ کردن چنین عوامل کاهنده دارد.

از سوی دیگر، استفاده از مجازات‌های بسیار شدید صرفاً با استناد به عنوان کلی امنیت ملی می‌تواند با فلسفه تعزیر ناسازگار باشد. فلسفه تعزیر بر امکان تنظیم واکنش بر اساس مصلحت و درجه سرزنش‌پذیری استوار است و همین امر اقتضا می‌کند که میان مرتکب حرفه‌ای مرتبط با سرویس اطلاعاتی بیگانه و فردی که بدون آگاهی کامل از ماهیت اطلاعات مرتکب افشا شده است، تفاوت وجود داشته باشد. تحلیل نظری جاسوسی و خیانت نیز بر اهمیت عنصر قصد و آگاهی در ارزیابی کیفری این جرایم تأکید می‌کند (Sadat, 2019). بنابراین، علم مرتکب به حساسیت اطلاعات و اطلاع او از هویت یا هدف دریافت‌کننده باید در تعیین واکنش نقش مرکزی داشته باشد.

تهدیدهای جدید همچنین ضرورت بازاندیشی در واکنش‌های فقهی ـ تقنینی را ایجاد کرده‌اند. در فضای سایبری، ممکن است مرتکب با نصب بدافزار، ارائه رمز عبور، ایجاد درِ پشتی در یک سامانه یا انتقال پایگاه داده به طرف خارجی، نقشی در جاسوسی ایفا کند بدون آنکه هیچ سند فیزیکی را جابه‌جا کند. ابزارهای مدرن جاسوسی سایبری امکان دسترسی مستمر و پنهان به حجم عظیمی از اطلاعات را فراهم کرده‌اند (SentinelOne, 2025). از منظر فقهی، شکل فنی رفتار نباید مانع توجه به ماهیت آن شود. اگر شخص آگاهانه امکان دسترسی دشمن به اطلاعات حیاتی را فراهم کند، ماهیت رفتارش می‌تواند همان نقض امانت و اعانت زیان‌بار باشد، حتی اگر ابزار آن کاملاً دیجیتال باشد.

جاسوسی اقتصادی نیز نمونه دیگری از ضرورت انعطاف واکنش است. همه اطلاعات اقتصادی دارای ارزش امنیتی یکسان نیستند، اما برخی فناوری‌ها، طرح‌های صنعتی یا داده‌های زیرساختی می‌توانند مستقیماً با استقلال و قدرت راهبردی کشور مرتبط باشند. ناشسی نشان می‌دهد که جاسوسی صنعتی در محیط رقابت بین‌المللی می‌تواند ابزار انتقال غیرقانونی مزیت‌های فناورانه و اقتصادی باشد (Nashesi, 2022). در چنین مواردی، تعیین واکنش باید بر مبنای اهمیت واقعی موضوع، آثار انتقال و میزان ارتباط آن با امنیت ملی انجام گیرد. جرم‌انگاری بیش از

اندازه گسترده اطلاعات اقتصادی خطر توسعه نامحدود مفهوم خیانت را دارد، در حالی که نادیده گرفتن اطلاعات واقعاً راهبردی نیز خلأ حمایتی ایجاد می‌کند.

در مجموع، فقه امامیه امکان ایجاد نظامی چندسطحی برای واکنش به خیانت به کشور را فراهم می‌کند. در سطح نخست، رفتارهایی که خطر محدودتری دارند می‌توانند با تعزیر متناسب پاسخ داده شوند. در سطح بالاتر، رفتارهای عمدی و سازمان‌یافته‌ای که آسیب شدید به امنیت ایجاد می‌کنند مستوجب تعزیرات سنگین‌تر و محرومیت‌های تکمیلی خواهند بود. تنها در شرایطی که رفتار تمام عناصر یکی از عناوین حدی یا خاص فقهی را دارا باشد، امکان اعمال آثار آن عنوان وجود دارد. چنین مدلی از یک سو پاسخ‌گویی قاطع به تهدیدهای واقعی را ممکن می‌سازد و از سوی دیگر، از تبدیل مفهوم خیانت به عنوانی گسترده و نامحدود جلوگیری می‌کند.

اقدامات واکنشی جرم خیانت به کشور در حقوق کیفری ایران و ارزیابی فقهی آن

حقوق کیفری ایران برای مقابله با رفتارهایی که می‌توان آن‌ها را در مفهوم گسترده خیانت به کشور قرار داد، از مجموعه‌ای از عناوین مجرمانه استفاده کرده است. این رویکرد در ظاهر امکان پوشش رفتارهای متنوع را فراهم می‌کند، اما در عمل سبب شده است که عنوان «خیانت به کشور» از انسجام مفهومی مستقلی برخوردار نباشد. جاسوسی، در اختیار قرار دادن اسرار به اشخاص فاقد صلاحیت، همکاری با دولت‌های خارجی متخاصم، ورود به اماکن نظامی یا امنیتی برای کسب اطلاعات و برخی رفتارهای مشابه هر یک تحت مقررات متفاوتی قرار می‌گیرند. رحمدل با بررسی جاسوسی و خیانت به کشور، نشان می‌دهد که پراکندگی مفهومی میان این دو عنوان می‌تواند موجب دشواری در تعیین قلمرو دقیق مسئولیت کیفری شود (Rahmdel, 2020). از منظر سیاست تقنینی، این وضعیت ایجاب می‌کند که یک نظام طبقه‌بندی روشن میان خیانت، جاسوسی و سایر جرایم امنیتی ایجاد شود.

یکی از مهم‌ترین واکنش‌های حقوق کیفری ایران در این حوزه، مجازات حبس است. در بسیاری از مصادیق جاسوسی و افشای اطلاعات امنیتی، قانون‌گذار از حبس به‌عنوان ضمانت اجرای اصلی استفاده کرده است. انتخاب حبس با توجه به شدت بالقوه خسارت این جرایم قابل توجیه است، اما مسئله اساسی تناسب میزان حبس با درجه خطر و تقصیر است. سیاست کیفری نباید به گونه‌ای باشد که رفتارهایی با سطح زیان متفاوت، صرفاً به دلیل قرار گرفتن تحت عنوان کلی جرم امنیتی، با واکنش‌های مشابه مواجه شوند. مطالعات مربوط به جایگاه جرایم علیه امنیت در سیاست جنایی ایران بر شدت واکنش نسبت به جاسوسی و دیگر رفتارهای تهدیدکننده امنیت تأکید کرده‌اند (Mazaheri, 2019). با وجود این، شدت باید با تفکیک میان رفتارهای مقدماتی، انتقال واقعی اطلاعات و همکاری مؤثر با دشمن همراه شود.

در برخی موارد، وضعیت خاص مرتکب موجب تشدید واکنش می‌شود. کارکنان نظامی، امنیتی و برخی مقامات دولتی به دلیل دسترسی گسترده به اطلاعات طبقه‌بندی‌شده، در موقعیتی قرار دارند که سوءاستفاده از آن می‌تواند آثار به‌مراتب گسترده‌تری نسبت به رفتار یک فرد عادی ایجاد کند. مطالعه جاسوسی در حقوق کیفری نیروهای مسلح نشان می‌دهد که نظام کیفری نسبت به افشای اطلاعات نظامی و همکاری اطلاعاتی اشخاص دارای موقعیت سازمانی حساسیت ویژه‌ای دارد (Hedayati Chenani, 2021). این رویکرد از منظر فقهی نیز قابل دفاع است، زیرا دسترسی ناشی از اعتماد و منصب، تعهد مرتکب را به حفظ امانت افزایش می‌دهد و نقض آگاهانه چنین تعهدی درجه سرزنش‌پذیری را بالا می‌برد.

با این حال، یکی از مسائل مهم، تعریف موضوع جرم است. مفاهیمی مانند «اسرار»، «اسناد سری»، «اطلاعات طبقه‌بندی‌شده» یا «دولت متخاصم» باید به اندازه کافی روشن باشند تا اشخاص بتوانند محدوده رفتار ممنوع را تشخیص دهند. ابهام در این مفاهیم می‌تواند هم در مرحله تعقیب

و هم در مرحله قضاوت مشکل ایجاد کند. آغیق در بررسی نارسایی‌های تقنینی جاسوسی در حقوق ایران به ابهامات موجود در ساختار جرم‌انگاری و ضرورت بازنگری در برخی عناصر قانونی اشاره کرده است (Aghigh, 2023). از منظر اصل قانونی بودن، هرچه مجازات شدیدتر باشد، ضرورت صراحت عنصر قانونی نیز بیشتر است.

یکی از زمینه‌هایی که ضعف قوانین سنتی را آشکار کرده، جاسوسی سایبری است. ساختار بسیاری از مقررات کلاسیک بر تصور دسترسی فیزیکی به سند یا محل حساس استوار بوده، در حالی که در محیط سایبری شخص می‌تواند از هزاران کیلومتر فاصله به داده‌های حساس دسترسی پیدا کند. حمیدی با بررسی جرم جاسوسی سایبری در حقوق ایران و افغانستان بر ضرورت تطبیق قواعد موجود با ویژگی‌های جرایم رایانه‌ای تأکید کرده است (Hamidi, 2024). در جاسوسی سایبری، مرتکب ممکن است بدون تصاحب فیزیکی داده، تنها نسخه‌ای از آن ایجاد کند یا دسترسی پنهانی و مستمر برای طرف خارجی فراهم سازد. بنابراین، عنصر مادی جرم باید به نحوی تعریف شود که «دسترسی غیرمجاز»، «نسخه‌برداری»، «انتقال»، «فراهم کردن امکان دسترسی» و «تغییر یا استخراج داده» را متناسب با ماهیت رفتار پوشش دهد.

اهمیت این موضوع در بخش نظامی و دفاعی بیشتر است. جاسوسی سایبری می‌تواند متوجه سامانه‌های فرماندهی، اطلاعات نیروها، زیرساخت‌های دفاعی یا فناوری‌های حساس باشد و در این صورت خسارت بالقوه آن بسیار فراتر از افشای یک سند معمولی خواهد بود. مقاله مرتبط با پیشگیری از جاسوسی سایبری نیروهای مسلح بر نقش حمایت کیفری از امنیت اطلاعات در تضمین حق بر امنیت تأکید کرده است (Fatahi Zafarkandi, 2019). از این منظر، واکنش حقوق کیفری باید در کنار مجازات مرتکب، شامل تدابیری برای کاهش دسترسی مجدد و جلوگیری از تکرار سوءاستفاده از موقعیت سازمانی نیز باشد.

جاسوسی هسته‌ای و انتقال اطلاعات فناورانه حساس نیز یکی از حوزه‌هایی است که نشان می‌دهد تقسیم‌بندی سنتی میان اطلاعات نظامی و غیرنظامی دیگر کافی نیست. برخی فناوری‌های علمی و صنعتی مستقیماً در توان راهبردی کشور اثرگذارند. بررسی راهبرد کیفری ایران در برابر جاسوسی هسته‌ای نشان داده است که قوانین باید به ماهیت فناورانه موضوع و شیوه‌های نوین تحصیل اطلاعات توجه کنند (Meshkat, 2019). این تحلیل را می‌توان به سایر حوزه‌های حساس مانند صنایع دفاعی، هوش مصنوعی راهبردی، زیرساخت انرژی یا فناوری‌های دوکاربردی نیز تعمیم داد. معیار اصلی نباید صرفاً عنوان اداری سند باشد، بلکه آثار افشای آن بر منافع حیاتی کشور نیز باید مورد توجه قرار گیرد.

گسترش مفهوم امنیت به حوزه اقتصادی نیز واکنش کیفری را با چالش جدید روبه‌رو کرده است. جاسوسی اقتصادی ممکن است متوجه اسرار تجاری یک شرکت خصوصی باشد که در حالت عادی بیشتر جنبه اقتصادی دارد، اما اگر موضوع مربوط به فناوری ملی حساس یا زیرساخت حیاتی باشد، ابعاد امنیتی پیدا می‌کند. ناشسی جاسوسی اقتصادی و صنعتی را پدیده‌ای معرفی می‌کند که می‌تواند در رقابت میان دولت‌ها و شرکت‌ها نقش راهبردی داشته باشد (Nashesi, 2022). در نتیجه، قانون‌گذار باید میان جاسوسی تجاری عادی و انتقال اطلاعاتی که واقعاً با امنیت ملی مرتبط است تفاوت قائل شود. توسعه نامحدود مفهوم امنیت ملی به همه اسرار تجاری با اصل ضرورت مداخله کیفری سازگار نیست.

تحولات مربوط به امنیت پژوهش نیز همین ضرورت را نشان می‌دهد. همکاری‌های علمی بین‌المللی، سرمایه‌گذاری خارجی و انتقال دانش بخش ضروری توسعه علمی هستند و نمی‌توان هر ارتباط پژوهشی خارجی را با نگاه امنیتی تحلیل کرد. در عین حال، برخی حوزه‌های پژوهشی حساس ممکن است هدف انتقال برنامه‌ریزی‌شده دانش یا فناوری قرار گیرند. Walker-Munro در تحلیل امنیت ملی،

سرمایه‌گذاری خارجی و امنیت پژوهش بر چالش ایجاد تعادل میان همکاری علمی و حفاظت از منافع راهبردی تأکید می‌کند (Walker-Munro, 2024). بنابراین، واکنش کیفری باید بر رفتار عمدی و غیرمجاز متمرکز باشد، نه بر ارتباط علمی مشروع.

مفهوم دولت یا طرف متخاصم نیز نیازمند وضوح حقوقی است. روابط بین‌الملل در جهان معاصر غالباً میان حالت جنگ و صلح کامل قرار ندارند و اشکالی مانند درگیری نیابتی، عملیات سایبری، تحریم گسترده، عملیات اطلاعاتی و خصومت سیاسی می‌توانند بدون اعلام رسمی جنگ وجود داشته باشند. آثار توافق‌ها و آرایش‌های سیاسی منطقه‌ای بر امنیت ملی نیز نشان می‌دهد که مفهوم تهدید خارجی همواره تابع تحولات ژئوپلیتیکی است (Shah Rezai, 2024). با این حال، تعیین وصف کیفری نباید صرفاً به برداشت سیاسی متغیر وابسته باشد. اگر همکاری با «دولت متخاصم» موجب مجازات شدید می‌شود، لازم است معیارهای قانونی یا رسمی روشنی برای تشخیص این وضعیت وجود داشته باشد.

علاوه بر مجازات اصلی، محرومیت از حقوق اجتماعی و مشاغل خاص می‌تواند نقش مهمی در پاسخ به خیانت داشته باشد. شخصی که از منصب عمومی یا دسترسی امنیتی خود سوءاستفاده کرده است، ممکن است پس از تحمل حبس همچنان برای برخی موقعیت‌ها نامناسب باشد. محرومیت متناسب از تصدی مشاغل دارای دسترسی امنیتی می‌تواند کارکرد پیشگیرانه داشته باشد. با این حال، این محرومیت باید از نظر مدت و دامنه مشخص باشد و به حذف دائمی شخص از همه عرصه‌های اجتماعی منجر نشود، مگر آنکه قانون در شرایط استثنایی و با توجیه کافی چنین اثری را مقرر کرده باشد. اصل بازاجتماعی کردن محکوم نیز اقتضا می‌کند که مجازات تکمیلی به اندازه‌ای اعمال شود که ضرورت امنیتی آن ایجاب می‌کند.

ضبط ابزار و منافع حاصل از جرم نیز در جرایم اطلاعاتی می‌تواند اهمیت داشته باشد. خیانت یا جاسوسی ممکن است با دریافت پول، امتیاز یا حمایت از طرف خارجی همراه باشد. در چنین حالتی، باقی ماندن منافع جرم در اختیار مرتکب با اهداف عدالت کیفری ناسازگار است. از سوی دیگر، ابزارهایی که صرفاً به طور اتفاقی در جرم استفاده شده‌اند نباید بدون ضابطه ضبط شوند. تمایز میان ابزار اختصاص‌یافته به ارتکاب جرم و اموال عادی مرتکب برای حفظ تناسب ضروری است.

شدت واکنش نباید جایگزین کیفیت اثبات شود. پرونده‌های امنیتی به دلیل محرمانه بودن برخی دلایل و اطلاعات، چالش خاصی در زمینه دادرسی عادلانه ایجاد می‌کنند. دولت ممکن است دلایل موجهی برای عدم افشای عمومی برخی اسناد داشته باشد، اما متهم نیز باید امکان مؤثر دفاع در برابر اتهام را داشته باشد. مشروعیت واکنش کیفری زمانی تقویت می‌شود که محکومیت بر ادله معتبر و قابل ارزیابی قضایی استوار باشد. در غیر این صورت، حتی مجازاتی که از نظر ماهوی برای خیانت واقعی قابل توجیه است، در صورت فقدان فرایند اثبات قابل اعتماد مشروعیت خود را از دست می‌دهد.

مسئله تجسس و نظارت نیز در اینجا اهمیت پیدا می‌کند. کشف جاسوسی معمولاً بدون عملیات اطلاعاتی دشوار است، اما کنترل ارتباطات و دسترسی به اطلاعات خصوصی باید محدود و قانونمند باشد. بررسی فقهی امکان تجسس برای کشف برخی جرایم شدید نشان می‌دهد که ممنوعیت تجسس را نمی‌توان به صورت مطلق تفسیر کرد، ولی استثنا نیز نیازمند ضرورت و ضابطه است (Sarikhani et al., 2022). از این منظر، حقوق کیفری ایران باید میان نیاز امنیتی و حمایت از حریم خصوصی تعادل ایجاد کند. نظارت هدفمند مبتنی بر مجوز و قرائن مشخص، با نظارت فراگیر و نامحدود تفاوت دارد.

سیاست کیفری در برابر خیانت همچنین باید میان مراحل ارتکاب تفکیک قائل شود. شخصی که صرفاً اقدام مقدماتی دور از مرحله اجرای جرم انجام داده است، نباید الزاماً با همان واکنش کسی مواجه شود که اطلاعات حیاتی را عملاً تحویل داده است. در مقابل، در جرایم امنیتی برخی اقدامات مقدماتی ممکن است به دلیل ماهیت خطرناک خود مستقلاً جرم‌انگاری شده باشند. معیار مناسب آن است که قانون مشخص کند کدام اعمال به اندازه‌ای خطرناک هستند که مداخله زودهنگام کیفری را توجیه می‌کنند. این امر از توسعه بیش از اندازه مفهوم شروع به جرم جلوگیری می‌کند.

عنصر روانی یکی از مهم‌ترین معیارهای تفکیک واکنش‌هاست. رفتار خیانت‌آمیز واقعی معمولاً مستلزم آگاهی مرتکب از ماهیت اطلاعات یا کمک و علم او به طرفی است که از رفتار منتفع می‌شود. اگر شخص بدون اطلاع از ماهیت محرمانه داده‌ها یا بدون آگاهی از ارتباط طرف مقابل با یک دولت خارجی اقدام کرده باشد، سرزنش‌پذیری او با یک مأمور آگاه و حرفه‌ای قابل قیاس نیست. سادات در بررسی چارچوب نظری جاسوسی و خیانت بر نقش هدف و آگاهی مرتکب در تشخیص ماهیت رفتار تأکید دارد (Sadat, 2019). از این رو، قوانین باید میان عمد مستقیم، علم به احتمال قوی نتیجه و سهل‌انگاری در حفاظت از اطلاعات تمایز ایجاد کنند.

موضوع دیگری که در واکنش کیفری باید مورد توجه قرار گیرد، امکان همکاری مرتکب برای جلوگیری از نتیجه یا کشف شبکه جاسوسی است. در برخی پرونده‌ها، ارزش اطلاعاتی همکاری متهم می‌تواند بسیار بیشتر از اجرای حداکثر مجازات باشد. اگر شخص پیش از ورود خسارت اساسی، داوطلبانه فعالیت خود را متوقف و اطلاعات مؤثری برای خنثی‌سازی عملیات ارائه کند، پیش‌بینی سازوکارهای تخفیف می‌تواند از منظر سیاست جنایی مطلوب باشد. چنین سیاستی باید با دقت تنظیم شود تا به مصونیت افراد حرفه‌ای تبدیل نشود، اما می‌تواند انگیزه خروج از شبکه‌های اطلاعاتی را افزایش دهد.

تاریخ تحول جرم خیانت در سایر نظام‌ها نیز نشان می‌دهد که محدود کردن تعریف خیانت و تفکیک آن از سایر جرایم امنیتی برای جلوگیری از سوءاستفاده سیاسی اهمیت دارد (Boyer & Nicholls, 2024). این تجربه برای حقوق ایران نیز قابل استفاده است. اگر قرار باشد عنوان مستقل خیانت به کشور در قانون تعریف شود، باید به رفتارهایی محدود شود که با نقض شدید تکلیف وفاداری و قصد یا علم روشن نسبت به کمک به دشمن یا وارد ساختن آسیب اساسی به کشور همراه هستند. سایر رفتارهای امنیتی می‌توانند تحت عناوین مستقل جاسوسی، افشای اسرار، خرابکاری یا همکاری غیرمجاز باقی بمانند.

از منظر فقه امامیه، بخش مهمی از ساختار کنونی حقوق ایران که رفتارهای جدید امنیتی را در قالب تعزیر جرم‌انگاری می‌کند قابل دفاع است. مزیت این رویکرد آن است که قانون‌گذار می‌تواند متناسب با تحول تهدیدها، اشکال جدید رفتار را پوشش دهد. با این حال، مشروعیت تعزیر مشروط به رعایت عدالت، تناسب، وضوح و ضرورت است. نمی‌توان صرف استناد به مصلحت امنیتی هر نوع رفتار را جرم یا هر میزان مجازات را مشروع دانست. مصلحت باید واقعی، قابل توضیح و متناسب با ارزش مورد حمایت باشد.

یکی از مهم‌ترین خلأهای تقنینی، نبود معماری منسجم برای جرایم علیه امنیت خارجی است. وجود مقررات پراکنده در قوانین عمومی، نظامی و تخصصی ممکن است به هم‌پوشانی یا تفاوت غیرموجه در مجازات منتهی شود. آغیق نیز در تحلیل کاستی‌های جرم جاسوسی، به ضرورت هماهنگی و شفافیت بیشتر مقررات اشاره کرده است (Aghigh, 2023). اصلاح تقنینی می‌تواند با تعریف دقیق مفاهیم پایه، درجه‌بندی اطلاعات از حیث اهمیت امنیتی، تفکیک مرتکبان بر اساس موقعیت و تعیین مجازات‌های پلکانی انجام شود.

علاوه بر آن، قوانین باید نسبت به فناوری خنثی باشند؛ بدین معنا که جرم‌انگاری به یک ابزار خاص وابسته نباشد. اگر انتقال یک سند کاغذی محرمانه جرم است، انتقال همان محتوا از طریق حافظه ابری یا پیام رمزگذاری‌شده نیز باید قابل پوشش باشد. جاسوسی مدرن به شدت متکی به ابزارهای فناورانه است و عملیات اطلاعاتی معاصر تفاوت چشمگیری با الگوهای جنگ سرد پیدا کرده است (Grey, 2018). بنابراین، تمرکز قانون باید بر دستیابی، تحصیل، انتقال، افشا یا فراهم‌کردن دسترسی غیرمجاز به اطلاعات حساس باشد، نه قالب فیزیکی آن.

روابط بین‌المللی و الزامات امنیت جهانی نیز در این زمینه بی‌تأثیر نیستند. تهدیدهای فرامرزی، جنگ سایبری و شبکه‌های پیچیده اطلاعاتی باعث شده‌اند که امنیت ملی و امنیت بین‌المللی بیش از گذشته به یکدیگر پیوند بخورند. بررسی نقش حقوق بین‌الملل در صلح و امنیت جهانی نشان می‌دهد که دولت‌ها ضمن برخورداری از اختیار حفاظت از امنیت خود، در بستری از قواعد و تعهدات بین‌المللی عمل می‌کنند (Xu, 2024). از این جهت، سیاست کیفری ایران نیز باید به نحوی تنظیم شود که ضمن حمایت مؤثر از کشور، با اصول عام دادرسی منصفانه و مسئولیت فردی سازگار باقی بماند.

در نهایت، ارزیابی حقوق کیفری ایران نشان می‌دهد که مسئله اصلی فقدان واکنش نیست، بلکه پراکندگی و عدم درجه‌بندی کامل واکنش‌هاست. نظام موجود ابزارهای شدید کیفری در اختیار دارد، اما ضرورت دارد این ابزارها در یک ساختار روشن‌تر قرار گیرند. تعریف دقیق رفتار، تفکیک خیانت از جاسوسی، شفاف‌سازی مفهوم دشمن و اطلاعات حساس، توجه به فناوری، درجه‌بندی مجازات بر اساس میزان خطر و پیش‌بینی تدابیر تکمیلی متناسب می‌تواند هم کارآمدی امنیتی و هم مشروعیت حقوقی نظام واکنشی را افزایش دهد.

نتیجه‌گیری

خیانت به کشور از جمله جرایمی است که مستقیماً با بنیادی‌ترین منافع جامعه سیاسی ارتباط پیدا می‌کند و از همین رو، واکنش کیفری نسبت به آن نمی‌تواند مشابه جرایمی باشد که تنها منافع محدود فردی را مورد تعرض قرار می‌دهند. با این حال، اهمیت ارزش مورد حمایت نباید سبب شود که مفهوم خیانت به عنوانی گسترده، مبهم و قابل تسری به هر نوع رفتار سیاسی، اجتماعی یا ارتباط خارجی تبدیل شود. مشروعیت واکنش شدید کیفری در این حوزه بیش از هر چیز به تعریف محدود و روشن جرم، احراز عنصر روانی و اثبات وجود خطر جدی علیه امنیت کشور وابسته است.

تحلیل مفهومی نشان داد که خیانت به کشور را می‌توان در معنای دقیق، نقض آگاهانه و شدید تکلیف وفاداری نسبت به جامعه سیاسی از طریق رفتاری دانست که با هدف یا علم به کمک به دشمن یا آسیب رساندن به منافع بنیادین کشور انجام می‌شود. از این منظر، خیانت با جاسوسی رابطه‌ای نزدیک ولی غیرمترادف دارد. جاسوس ممکن است تبعه کشور هدف نباشد و در نتیجه، رفتار او اگرچه علیه امنیت کشور است، الزاماً متضمن نقض تکلیف وفاداری ناشی از تابعیت نیست. در مقابل، شهروند یا صاحب منصبی که اطلاعات حیاتی کشور را آگاهانه در اختیار دشمن قرار می‌دهد، هم ممکن است مرتکب جاسوسی شود و هم رفتار او از حیث ماهوی وصف خیانت‌آمیز داشته باشد.

در فقه امامیه، اگرچه عنوان مستقل و مدون «خیانت به کشور» به معنای امروزین حقوق کیفری وجود ندارد، مبانی کافی برای مواجهه با مصادیق آن قابل شناسایی است. حرمت خیانت، وجوب رعایت امانت، ممنوعیت یاری رساندن به دشمن در اقدام نامشروع، ضرورت حمایت از جامعه اسلامی و اختیار حکومت در وضع تعزیرات برای رفتارهای زیان‌بار، مهم‌ترین پایه‌های چنین واکنشی هستند. در عین حال، نمی‌توان تمام رفتارهای خیانت‌آمیز را به عناوین حدی مانند محاربه یا بغی تسری داد. هر یک از این عناوین دارای شرایط خاص خود هستند و تنها در صورت تحقق تمام عناصر آن‌ها می‌توان آثار مربوط را اعمال کرد.

مهم‌ترین ظرفیت فقهی برای پاسخ به بیشتر اشکال جدید خیانت، نهاد تعزیر است. انعطاف تعزیر امکان می‌دهد که قانون‌گذار با توجه به تحولات اجتماعی، فناوری و امنیتی، رفتارهایی را که در گذشته وجود نداشته‌اند جرم‌انگاری و برای آن‌ها ضمانت اجرای مناسب تعیین کند. جاسوسی سایبری، انتقال داده‌های طبقه‌بندی‌شده از طریق شبکه، ایجاد دسترسی مخفیانه به سامانه‌های حساس، انتقال فناوری راهبردی یا جاسوسی اقتصادی در حوزه‌های حیاتی نمونه‌هایی هستند که می‌توانند در این چهارچوب قرار گیرند. مزیت این سازوکار در آن است که واکنش می‌تواند متناسب با سطح واقعی خطر تنظیم شود.

بررسی حقوق کیفری ایران نشان داد که قانون‌گذار برای بسیاری از رفتارهایی که ماهیت خیانت‌آمیز دارند مجازات تعیین کرده است، اما این مقررات فاقد انسجام کامل مفهومی هستند. رفتارهای مرتبط با جاسوسی، همکاری با دشمن، افشای اسرار، ورود به اماکن ممنوعه و تحصیل اطلاعات حساس در مقررات گوناگون پراکنده‌اند. این پراکندگی ممکن است موجب هم‌پوشانی عناوین، دشواری تفسیر، تفاوت در مجازات رفتارهای نزدیک و کاهش پیش‌بینی‌پذیری قوانین شود. از این رو، اصلاح ساختاری مقررات جرایم علیه امنیت خارجی ضروری به نظر می‌رسد.

در تدوین چنین اصلاحی، نخست باید مفهوم خیانت به کشور از سایر جرایم امنیتی تفکیک شود. بهتر است خیانت در معنای خاص تنها رفتارهایی را شامل شود که از سوی فرد دارای تکلیف وفاداری انجام گرفته و متضمن کمک عمدی یا آگاهانه به دشمن یا وارد کردن آسیب اساسی به استقلال، تمامیت ارضی، قدرت دفاعی یا منافع حیاتی کشور باشد. جاسوسی می‌تواند عنوان مستقلی باقی بماند و بر تحصیل یا انتقال غیرمجاز اطلاعات حساس تمرکز کند، صرف‌نظر از اینکه مرتکب تبعه کشور است یا خیر. این تفکیک امکان تعیین واکنش متفاوت و عادلانه‌تر را فراهم می‌کند.

دوم، عنصر روانی باید در جرایم مرتبط با خیانت با دقت بیشتری تعریف شود. میان شخصی که آگاهانه با یک سرویس اطلاعاتی خارجی همکاری می‌کند و فردی که بر اثر بی‌احتیاطی اطلاعاتی را افشا می‌کند، تفاوت بنیادین وجود دارد. رفتار دوم ممکن است در مواردی نیازمند ضمانت اجرای کیفری یا اداری باشد، اما نباید با همان شدت رفتار خیانت‌آمیز عمدی پاسخ داده شود. درجه آگاهی، قصد کمک به طرف خارجی، اطلاع از حساسیت اطلاعات و پیش‌بینی آثار رفتار باید در تعیین عنوان و میزان مجازات مؤثر باشند.

سوم، شدت اطلاعات و پیامد افشا باید در درجه‌بندی مجازات نقش مستقیم داشته باشد. اطلاعات مربوط به عملیات نظامی جاری، ساختار دفاعی یا زیرساخت حیاتی با اطلاعات دارای طبقه‌بندی پایین‌تر یکسان نیستند. نظام کیفری مطلوب می‌تواند بر اساس درجه حساسیت اطلاعات و میزان آسیب بالقوه یا بالفعل، طیفی از مجازات‌ها را پیش‌بینی کند. چنین مدلی هم اصل تناسب را بهتر رعایت می‌کند و هم به دادگاه امکان می‌دهد بدون خروج از چهارچوب قانونی، واکنش را با شرایط پرونده هماهنگ سازد.

چهارم، قانون‌گذاری باید نسبت به ابزار ارتکاب خنثی باشد. تحول فناوری نشان داده است که وابستگی جرم‌انگاری به شکل فیزیکی سند یا محل ارتکاب می‌تواند در مدت کوتاهی قانون را ناکارآمد کند. آنچه باید محور جرم باشد، دسترسی، تحصیل، نسخه‌برداری، انتقال، افشا یا فراهم ساختن دسترسی غیرمجاز به اطلاعات حساس است. در این صورت، تفاوتی ندارد که داده روی کاغذ، حافظه الکترونیکی، سرور داخلی یا سامانه ابری قرار داشته باشد.

پنجم، اقدامات واکنشی باید از مجازات اصلی فراتر روند. در مواردی که جرم از طریق سوءاستفاده از موقعیت حرفه‌ای یا دسترسی امنیتی انجام شده است، محرومیت موقت یا بلندمدت از مشاغل حساس می‌تواند ضروری باشد. همچنین، ضبط منافع حاصل از جرم، محدود کردن

دسترسی‌های امنیتی و جلوگیری از تصدی مجدد برخی مناصب می‌تواند در کاهش احتمال تکرار مؤثر باشد. با این حال، این تدابیر نیز باید متناسب، شخصی و محدود به ضرورت واقعی باشند.

ششم، واکنش کیفری شدید باید با تضمین‌های اثباتی قوی همراه شود. حساسیت امنیتی پرونده نباید باعث کاهش استانداردهای دادرسی عادلانه شود. محرمانه بودن برخی اسناد ممکن است محدودیت‌هایی در انتشار عمومی آن‌ها ایجاد کند، اما مرجع قضایی باید امکان ارزیابی واقعی ادله را داشته باشد و متهم نیز باید به میزانی که برای دفاع مؤثر ضروری است از ماهیت اتهام و دلایل آن آگاه شود. مشروعیت سیاست امنیتی در بلندمدت به همان اندازه که به قدرت واکنش وابسته است، به عدالت فرایند نیز وابستگی دارد.

هفتم، اقدامات اطلاعاتی برای کشف خیانت باید تحت محدودیت‌های روشن قرار گیرند. جرم خیانت ماهیتی پنهانی دارد و کشف آن گاه بدون نظارت و مراقبت ممکن نیست، اما این ضرورت نمی‌تواند تجسس بی‌ضابطه را توجیه کند. مداخله در حریم خصوصی باید مبتنی بر قرائن معتبر، ضرورت امنیتی مشخص و نظارت قانونی باشد. چنین رویکردی تعادل میان امنیت جامعه و حقوق فردی را حفظ می‌کند.

هشتم، سیاست جنایی می‌تواند برای توقف داوطلبانه همکاری با دشمن و جلوگیری از خسارت، سازوکارهای تشویقی محدودی پیش‌بینی کند. اگر مرتکب پیش از تحقق نتیجه شدید، فعالیت خود را متوقف کند، اطلاعات لازم برای خنثی‌سازی عملیات را در اختیار مقامات قرار دهد یا به شناسایی شبکه کمک مؤثر کند، امکان تخفیف مجازات می‌تواند کارکرد امنیتی مثبت داشته باشد. البته این سازوکار باید به نحوی طراحی شود که مانع سوءاستفاده شود و تنها در صورت همکاری واقعی و مؤثر اعمال گردد.

در مجموع، نظام مطلوب واکنش به خیانت به کشور باید بر سه اصل بنیادین استوار باشد: قاطعیت در برابر تهدیدهای واقعی، دقت در تعریف و اثبات جرم و تناسب در تعیین مجازات. افراط در هر یک از دو جهت می‌تواند نتیجه‌ای نامطلوب ایجاد کند. واکنش بیش از اندازه موسع ممکن است مرز میان امنیت و حقوق اساسی را مخدوش کند و واکنش بیش از اندازه محدود نیز توان دولت در حفاظت از منافع حیاتی جامعه را کاهش دهد. فقه امامیه از طریق ظرفیت تعزیر و توجه به مصالح عمومی امکان ایجاد تعادلی میان این دو ضرورت را فراهم می‌کند و حقوق کیفری ایران نیز می‌تواند با بازتنظیم مقررات موجود، از این ظرفیت به شکلی منسجم‌تر استفاده کند.

بر این اساس، پیشنهاد می‌شود قانون‌گذار ضمن بازنگری در مجموعه مقررات جرایم علیه امنیت، تعریف دقیق‌تری از خیانت به کشور ارائه کند، مرز آن را با جاسوسی و سایر جرایم امنیتی مشخص سازد، مفهوم اطلاعات حساس و مصادیق راهبردی آن را با معیارهای قابل پیش‌بینی تنظیم کند، جرایم سایبری و فناورانه را به صورت صریح و فناوری‌خنثی تحت پوشش قرار دهد و نظامی پلکانی از مجازات‌ها را بر اساس وضعیت مرتکب، نوع اطلاعات، قصد، میزان همکاری با دشمن و شدت خسارت ایجاد کند. چنین اصلاحی می‌تواند هم با مبانی فقه امامیه هماهنگ باشد و هم اصول بنیادین حقوق کیفری معاصر، به‌ویژه قانونی بودن، شخصی بودن مسئولیت، تناسب و ضرورت مجازات را بهتر تأمین کند. در این صورت، واکنش به خیانت به کشور از یک مجموعه پراکنده و عمدتاً مجازات‌محور به یک سیاست کیفری منسجم، قابل پیش‌بینی و متناسب تبدیل 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

Treason against the country is among the most serious offenses directed against the foundations of political order, national security, territorial integrity, defense capacity, and the vital interests of a state. Unlike ordinary crimes, whose harmful consequences are generally confined to individuals or limited social interests, treason may endanger the continued functioning of the political community itself. Historically, the concept of treason has undergone substantial transformation, particularly in legal systems in which it gradually evolved from a broad offense protecting the sovereign and political authority into a more narrowly defined crime concerning the fundamental security of the state (Boyer & Nicholls, 2024). This historical development is important because it demonstrates that treason should not be equated with political opposition, criticism, ideological dissent, or ordinary violations of law; rather, it should be confined to conduct involving a serious and intentional breach of a duty of loyalty accompanied by assistance to an enemy or substantial harm to the country's fundamental interests. In Iranian criminal law, however, treason has not been formulated as a fully autonomous and coherent criminal title. Instead, conduct that may have a treasonous character is dispersed among different offenses, including espionage, disclosure of classified information, cooperation with hostile governments, unlawful access to protected places, and transmission of military or security information. The conceptual relationship between espionage and treason has therefore become particularly important, since the two offenses may overlap but are not necessarily identical (Rahmdel, 2020). While an espionage agent may be a foreign national who owes no duty of loyalty to the target country, a citizen or public official who intentionally provides sensitive information to a foreign adversary may simultaneously exhibit the essential characteristics of espionage and treason. Iranian scholarship has long emphasized the importance of distinguishing these concepts on the basis of the offender's status, the nature of the protected information, and the purpose of the conduct (Sarikhani, 1999). Accordingly, the principal objective of the present study is to analyze the reactive measures applicable to treason from the perspective of Imami jurisprudence and Iranian criminal law and to determine whether the existing legal framework provides a coherent, proportionate, and effective response to contemporary manifestations of this offense.

From a conceptual perspective, treason may be defined as an intentional and serious violation of a duty of loyalty toward the political community through conduct that knowingly assists a hostile actor or exposes the fundamental interests of the country to substantial danger. The duty of loyalty is traditionally associated with citizenship, but modern security relations have complicated this classic model. Public officials, military personnel, contractors, researchers, and individuals with privileged access to classified systems may acquire special legal obligations even when their position cannot be reduced to nationality alone. This distinction is essential in criminal attribution because the culpability of an insider who abuses entrusted access is significantly different from that of an external actor. The theoretical literature on espionage and treason has emphasized the importance of intent, access, and the relationship between the offender and the protected state interest (Sadat, 2019). Moreover, the subject matter of treason has expanded beyond traditional military documents and diplomatic secrets. Economic, scientific, technological, and infrastructural information may also possess strategic value where its disclosure seriously affects national independence, defense capability, or long-term security. Economic and industrial espionage can facilitate the unauthorized transfer of strategically important knowledge, technology, and competitive advantage (Nashesi, 2022), while contemporary approaches to research security increasingly recognize that sensitive scientific cooperation, foreign investment, and technology transfer may generate national-security

implications in certain sectors (Walker-Munro, 2024). Nevertheless, not every commercial or scientific disclosure should be classified as treason. The decisive criterion must be the degree to which the information concerns genuinely vital national interests. This requirement is especially important in light of the principle of legality, because excessively broad definitions of security offenses may undermine predictability and permit expansive interpretation. Studies of espionage legislation in Iran have identified legislative fragmentation and ambiguity concerning the elements of espionage-related offenses (Aghigh, 2023). Such difficulties support the need for a more precise conceptual framework that clearly distinguishes treason, espionage, unlawful disclosure, and other security offenses.

Imami jurisprudence provides a substantial normative basis for responding to treasonous conduct even though the modern legal expression “treason against the country” does not appear as a single codified classical offense. Several jurisprudential principles are relevant, including the prohibition of betrayal, the obligation to preserve trusts, the prohibition of assisting an enemy in wrongful aggression, the protection of the Muslim community against serious harm, and the authority of legitimate government to impose discretionary punishments for conduct that threatens public order and security. In this framework, sensitive information entrusted to a public official, military officer, or other authorized person may be understood as a form of public trust, and its intentional disclosure to a hostile party may constitute a serious violation of that trust. At the same time, Imami jurisprudence does not justify automatically subsuming every security offense under fixed punishments such as those associated with moharebeh or baghy. These jurisprudential categories have specific constituent elements and cannot be extended merely because an offense is politically or nationally serious. The more appropriate framework for many modern forms of treason is ta'zir, which allows the legislature and competent authority to determine a proportionate response based on the gravity of the conduct, the offender’s intention, the sensitivity of the information, the extent of cooperation with the hostile party, and the actual or potential harm caused. This flexibility is particularly significant in relation to technological transformation. Cyber espionage has altered traditional models of intelligence gathering by enabling offenders to obtain or transmit information without physically entering a restricted site or removing tangible documents (Hamidi, 2024). Modern cyber espionage may involve remote access, credential theft, malware installation, covert data extraction, or the creation of persistent access to sensitive systems (SentinelOne, 2025). From a jurisprudential perspective, the form of the instrument should not determine the legal evaluation; what matters is the intentional creation of unauthorized access, betrayal of entrusted information, and harmful assistance to an adversary. At the same time, methods used to detect such conduct must remain subject to legal and jurisprudential limits. The prohibition of unlawful surveillance and intrusion into private affairs does not necessarily prevent narrowly tailored investigative measures in relation to serious crimes, but such measures require necessity, proportionality, and adequate justification (Sarikhani et al., 2022).

The reactive model derived from Imami jurisprudence is therefore best understood as a graduated system rather than a uniform punitive approach. In less severe cases, where the conduct has limited consequences or the offender’s degree of intent is lower, a moderate discretionary punishment may be sufficient. In more serious cases involving deliberate cooperation with an enemy, disclosure of highly sensitive military information, or facilitation of hostile operations, significantly stronger sanctions may be justified. The offender’s institutional position should also affect the severity of the response, because a person who has obtained access to information through public trust, military office, or security clearance breaches an additional and more serious obligation. Research on

espionage within the context of the armed forces underscores the special importance of the offender's organizational role and access to protected military information (Hedayati Chenani, 2021). Likewise, the development of nuclear, defense, and other strategic technologies demonstrates that modern national-security information may include highly specialized technical knowledge whose disclosure can produce consequences far beyond conventional document theft (Meshkat, 2019). The reactive measures should therefore include not only imprisonment but also proportionate complementary sanctions such as removal from sensitive positions, temporary or permanent restriction of access to classified information, disqualification from certain public offices, and confiscation of criminal proceeds where appropriate. Nevertheless, all such measures must comply with the principle of personal criminal responsibility. Family members, professional associates, or social contacts of an offender cannot be subjected to punitive consequences merely because of their relationship with that person. Similarly, criminal liability should be differentiated according to mens rea. A professional operative who knowingly transfers defense secrets to an intelligence service is not equivalent to a person who negligently mishandles information. Theoretical analyses of espionage have consistently treated knowledge, intention, and awareness of the recipient's status as central elements of culpability (Sadat, 2019). This distinction is indispensable if reactive measures are to remain proportionate rather than merely severe.

Iranian criminal law currently contains multiple legal responses to conduct that may fall within the broader category of treason, but the system remains fragmented. Imprisonment is the principal sanction for many espionage-related and security offenses, while more severe consequences may arise where the conduct overlaps with other criminal titles. Iranian criminal policy has generally adopted a strict approach toward espionage and offenses affecting state security (Mazaheri, 2019), and studies of security crimes have likewise emphasized the central position of espionage and unlawful access to protected information in the national criminal-policy framework (Mazhari, 2019). However, the effectiveness of this approach depends less on the mere existence of severe penalties than on the precision with which offenses are defined and differentiated. Ambiguous concepts such as classified information, hostile government, security secrets, and unlawful cooperation may create inconsistencies in prosecution and sentencing. Legislative criticism of the Iranian offense of espionage has highlighted the need for greater clarity and structural coherence (Aghigh, 2023). The technological environment has further exposed the limitations of provisions originally developed for physical documents and geographical access. Cyber espionage can be committed remotely, through digital copying, unauthorized system access, data exfiltration, or the creation of covert channels, requiring legislation that focuses on the protected interest and prohibited conduct rather than the physical form of the information (Hamidi, 2024). Preventive studies concerning cyber espionage in the armed forces have similarly stressed the importance of protecting information security through a combination of criminal and technical safeguards (Fatahi Zafarkandi, 2019). The same need exists in relation to nuclear and high-technology information, where the strategic importance of technical data may exceed that of conventional military documents (Meshkat, 2019). Contemporary intelligence operations have become increasingly technology-intensive and organizationally complex, further demonstrating the inadequacy of purely traditional legal models (Grey, 2018). Accordingly, Iranian law would benefit from a more coherent architecture for external security offenses, clearer definitions of protected information and hostile cooperation, graded sanctions based on the sensitivity of the information and the offender's status, and technology-neutral formulations capable of covering both physical and digital conduct.

In conclusion, the analysis demonstrates that treason against the country should be treated as a narrowly defined and highly serious offense based on the intentional violation of a duty of loyalty and the creation of substantial danger to the fundamental interests of the state. Imami jurisprudence provides sufficient normative foundations for responding to such conduct through the principles of trust, prohibition of betrayal, prohibition of assistance to hostile actors, protection of collective security, and the discretionary authority to impose ta'zir. At the same time, the jurisprudential framework requires careful differentiation among criminal titles and does not support automatic classification of all security offenses under the most severe fixed punishments. Iranian criminal law has established numerous sanctions for espionage, unlawful disclosure, hostile cooperation, and related conduct, yet these provisions lack complete conceptual and structural coherence. A more effective legal model should distinguish treason from espionage and other security crimes, define the protected national interests with greater precision, differentiate punishment according to the offender's status, degree of intent, sensitivity of the information, nature of the recipient, and extent of actual or potential harm, and expressly accommodate cyber, technological, economic, and research-related forms of strategic information transfer. The system should also combine principal sanctions with proportionate complementary measures, including restrictions on access to sensitive positions and confiscation of criminal proceeds, while preserving personal responsibility, due process, and the right to an effective defense. A coherent reactive policy must therefore avoid two opposite risks: excessive expansion of the concept of treason, which may endanger legality and fundamental rights, and excessive narrowness, which may leave new forms of strategic betrayal outside the scope of effective criminal protection. The most defensible approach is a graded, precise, technology-neutral, and jurisprudentially grounded framework capable of protecting national security while remaining consistent with proportionality, legality, and individual criminal responsibility.

References

Aghigh, R. H. (2023). Legislative inadequacies of the crime of espionage in the Islamic Penal Code compared to the Penal Code of France. *Journal of Scientific Research in Criminal Law and Criminology*(22).

Boyer, A., & Nicholls, M. (2024). *The Rise and Fall of Treason in English History*. Taylor & Francis. https://doi.org/10.4324/9781003052074

Fatahi Zafarkandi, S. (2019). Prevention of the cyber espionage crime of the armed forces and its role in ensuring the right to security. *Islamic human rights studies*, *9*(1).

Grey, S. (2018). *New Spymasters: Inside the Modern World of Espionage from the Cold War to Global Terror* (R. Deputy for & P. Knowledge, Trans.). National University of Intelligence and Security Press.

Hamidi, H. (2024). Cyber Espionage Crime in the Law of Afghanistan and Iran. *Scientific-Research Quarterly of Legal Knowledge*, *10*(4), 157. https://doi.org/10.62134/srqjl/v2.i4.202409.6

Hedayati Chenani, R. (2021). Examining the crime of espionage in international law and the criminal law of the armed forces. *Research and studies of Islamic sciences*, *3*(24).

Mazaheri, A. (2019). The Place of Crimes against Security in Iran's Criminal Policy (Examples: Espionage, Entry into Prohibited Places, Propaganda against the Regime, and Bombing). *Quarterly Journal of Political Science, Law, and Jurisprudence Studies*, *5*(1).

Mazhari, A. (2019). Position of Security Crimes in Iran's Criminal Policy: Espionage, Trespassing, Propaganda Against the Regime, Bombing. *Journal of Political Science, Law, and Jurisprudence*, *5*(1).

Meshkat, M. (2019). Iran's Penal Strategy in Facing Nuclear Espionage: The Need for Tech-Oriented Laws. *Criminal Law and Technology*, *1*(1), 55-78.

Nashesi, H. (2022). *Economic Espionage and Industrial Spying*. Cambridge University Press.

Rahmdel, M. (2020). Espionage and Treason against the Country. *International Law Research Journal*, *8*(28).

Sadat, G. (2019). *Espionage and Treason: Theoretical Frameworks and Countermeasures*. National University of Intelligence and Security Press.

Sarikhani, A. (1999). *Espionage and Treason against the Country*. Islamic Propagation Publications Center.

Sarikhani, A., Hajidehabadi, M. A., & Ghobadian, A. (2022). The Feasibility of Permitting Surveillance to Discover Violent Sexual Crimes in Light of Quranic and Narrative Evidence Prohibiting Espionage, from the Perspective of Iranian Criminal Law. *Ta'ali-ye Hoquq*(1).

SentinelOne. (2025). *What is cyber espionage? Types & examples*. Cybersecurity Magazine.

Shah Rezai, M. H. (2024). *The Impact of the Abraham Accords on the National Security of the Islamic Republic of Iran* Islamic Azad University, Khorasgan Branch.

Walker-Munro, B. (2024). National Security, Foreign Investment & Research Security: The Current State of Art. *Griffith Law Review*, *33*(2), 167-188. https://doi.org/10.1080/10383441.2025.2459007

Xu, K. (2024). Role of International Law for Global Peace and Security.