Journal of
Comparative Criminal Jurisprudence
www.jccj.ir

Volume 5, Issue 5, 2026

A Comparative Study of the Legitimacy of Searching Digital Evidence and Messaging Applications in Imami Jurisprudence and Iranian Criminal Law

Mahmoud Darvishtorabi [1*]

1. Assistant Professor, Department of Law, Payame Noor University, Tehran, Iran.

ARTICLE INFORMATION

Type of Article: ***Original Research***
Pages: ***405-418***

Corresponding Author's Info
ORCID: *0000-0002-8819-3024*
TELL: *+989113530796*
Email: *darvishtorabi@pnu.ac.ir*

Article history:
Received: *26 Apr 2025*
Revised: *15 May 2025*
Accepted: *12 Jun 2025*
Published online: *20 Feb 2026*

Keywords:
Digital Evidence Searches, Messaging Applications, Prohibition of Tajassus, Imami Jurisprudence, Fair Trial Standards.

ABSTRACT

The transition from physical environments to digital spaces has fundamentally transformed the concepts of privacy and evidentiary searches. This study aims to delineate the boundaries of lawful access to personal data and messaging applications through a comparative analysis of Imami jurisprudence, Iranian criminal law, and international human rights standards governing fair trial. Employing a descriptive-analytical methodology based on documentary research, the study examines the legal and jurisprudential foundations of digital searches. The findings indicate that, while Imami jurisprudence upholds the general prohibition of tajassus (intrusive investigation and surveillance), it recognizes limited exceptions grounded in jurisprudential principles such as the preservation of public order and necessity. These exceptions demonstrate a degree of convergence with the principles of necessity and proportionality recognized under international human rights standards. Nevertheless, Iran's legal framework faces significant challenges, including ambiguity in distinguishing searches of physical devices from access to digital accounts and the absence of effective mechanisms for deleting irrelevant data. These shortcomings may facilitate indiscriminate searches and violations of the right to privacy. The study concludes that reforms to Iran's Criminal Procedure Code and cybercrime legislation are necessary to ensure that access to messaging applications is subject to specific, narrowly tailored judicial warrants and that binding protocols are established for the deletion of irrelevant or excessive data. Such a balanced regulatory framework could enhance the effectiveness of criminal investigations while preventing the dominance of an absolute security-oriented approach over digital privacy, thereby safeguarding individual liberties and maintaining an appropriate balance between security and freedom within the criminal justice system.

This is an open access article under the CC BY license. © 2026 The Authors.

How to Cite This Article: Darvishtorabi, M (2026). "A Comparative Study of the Legitimacy of Searching Digital Evidence and Messaging Applications in Imami Jurisprudence and Iranian Criminal Law". *Journal of Comparative Criminal Jurisprudence*, 5(5): 405-418.

فصلنامه فقه جزای تطبیقی
www.jccj.ir

دوره پنجم، شماره پنجم، اسفند ۱۴۰۴

مطالعه تطبیقی مشروعیت تفتیش ادله دیجیتال و پیام‌رسان‌ها در فقه امامیه و حقوق کیفری ایران

محمود درویش‌ترابی [۱*]

۱. استادیار گروه حقوق، دانشگاه پیام نور، تهران، ایران.

اطلاعات مقاله

نوع مقاله: پژوهشی

صفحات: ۴۱۸-۴۰۵

اطلاعات نویسنده مسؤول

کد ارکید: ۰۰۰۰-۰۰۰۲-۸۸۱۹-۳۰۲۴

تلفن: ۹۸۹۱۱۳۵۳۰۷۹۶+

ایمیل: darvishtorabi@pnu.ac.ir

سابقه مقاله:

تاریخ دریافت: ۱۴۰۴/۰۲/۰۶

تاریخ ویرایش: ۱۴۰۴/۰۲/۲۵

تاریخ پذیرش: ۱۴۰۴/۰۳/۲۲

تاریخ انتشار: ۱۴۰۴/۱۲/۰۱

واژگان کلیدی:

تفتیش اد له دیجی تال، پ یام‌رســـان ها، منع تجسس، فقه امامیه، دادرسی منصفانه.

چکیده

با گذار از فضای فیزیکی به بستر دیجیتال، مفهوم حریم خصوصی و تفتیش ادله نیز دستخوش تحولی بنیادین شده است. پژوهش حاضر با هدف تبیین مرزهای مشروعیت ورود به داده‌های شخصی و پیام‌رسان‌ها، به ارزیابی تطبیقی آموزه‌های فقه امامیه، مقررات کیفری ایران و استانداردهای دادرسی منصفانه پرداخته است. روش تحقیق در این مقاله توصیفی-تحلیلی و مبتنی بر بررسی اسنادی است. یافته‌ها نشان می‌دهد که فقه امامیه ضمن تأکید بر اصل حرمت تجسس، استثنائات محدودی را بر پایه قواعدی همچون حفظ نظام و ضرورت می‌پذیرد که با موازین بین‌المللی دادرسی منصفانه در اصل «ضرورت و تناسب» همگرایی دارد. با این حال، نظام حقوقی ایران با چالش‌هایی نظیر ابهام در تفکیک بازرسی سخت‌افزار از دسترسی به حساب‌های کاربری و فقدان سازوکار امحای داده‌های نامرتبط مواجه است که به تفتیش‌های کور و نقض حریم خصوصی منجر می‌شود. نتیجه این پژوهش بر ضرورت اصلاح قوانین آیین دادرسی کیفری و جرائم رایانه‌ای تأکید دارد؛ به‌نحوی‌که برای هرگونه ورود به پیام‌رسان‌ها، دستور قضایی تفکیک‌شده و محدود اخذ گردد و پروتکل‌های امحای داده‌های اضافی برای صیانت از آزادی‌های فردی شهروندان الزام‌آور شود. این الگوی موازنه می‌تواند ضمن حفظ کارآمدی کشف جرم، از استیلای رویکرد امنیتی مطلق بر حریم خصوصی دیجیتال پیشگیری کند و توازن میان امنیت و آزادی را در نظام عدالت کیفری برقرار سازد. وجه نوآورانه پژوهش، فراتر رفتن از بررسی جداگانه اعتبار ادله یا منع تجسس و ارائه یک الگوی مرحله‌ای برای سنجش مشروعیت تفتیش پیام‌رسان‌هاست که میان دسترسی به دستگاه، حساب کاربری، محتوای پیام‌ها و داده‌های پیرامونی تفکیک می‌کند و تعیین حدود دستور قضایی، حمایت از داده‌های اشخاص ثالث و تعیین تکلیف داده‌های نامرتبط را در یک چارچوب واحد قرار می‌دهد.

خوانندگان این مجله، اجازه توزیع، ترکیب مجدد، تغییر جزئی و کار روی مقاله حاضر به‌صورت غیرتجاری را دارند.

© تمامی حقوق انتشار این مقاله، متعلق به نویسنده می‌باشد.

مقدمه

گسترش فناوری‌های ارتباطی و تبدیل تلفن همراه و پیام‌رسان‌ها به ابزارهای فراگیر زندگی روزمره، مفهوم سنتی مکان و حریم خصوصی را دگرگون ساخته است. تفتیش سنتی عمدتا ناظر بر ورود به مکان یا بازرسی اشیای معین بود؛ اما دسترسی دیجیتال می‌تواند مکاتبات، تصاویر، اطلاعات مکانی و سوابق ارتباطی را آشکار سازد. تلفن همراه بازنمایی فشرده‌ای از روابط و خلوت فردی است و پیام‌رسان‌ها با انباشت محتوا و داده‌های پیرامونی، به مخزنی از اطلاعات شخصی تبدیل شده‌اند. حجم داده‌ها و امکان بازیابی اطلاعات حذف‌شده، تفتیش را از موضوع مورد ظن فراتر می‌برد و حریم اشخاص ثالث را نیز تهدید می‌کند. در این وضعیت، تعارض میان کشف جرم و صیانت از حقوق بنیادین صورتی پیچیده‌تر می‌یابد. داده‌های دیجیتال در شناسایی مرتکب و حمایت از بزه‌دیده مؤثرند؛ اما دسترسی نامتناسب ممکن است اسرار خصوصی را افشا و اطلاعات نامرتبط را آشکار کند. بنابراین، صرف ظن به ارتکاب جرم یا صدور دستور کلی قضایی، لزوما مجوز دسترسی به تمام محتوای تلفن همراه یا حساب پیام‌رسان نیست؛ مشروعیت مداخله باید با موضوع اتهام، ضرورت تحقیق، دامنه داده‌های مورد نیاز و حقوق اشخاص مرتبط تناسب داشته باشد. مسأله، تعیین شرایطی است که دسترسی قضایی به ادله را بدون تبدیل آن به جست‌وجوی فراگیر زندگی خصوصی ممکن سازد.

این مسأله در فقه امامیه نیز اهمیت دارد؛ زیرا منع تجسس، حرمت هتک ستر و لزوم صیانت از اسرار اشخاص، در کنار مباحث حفظ مصالح عمومی و تزاحم حقوق و مصالح، چارچوبی برای سنجش جواز مداخله فراهم می‌آورد. تطبیق این مبانی بر داده‌های دیجیتال نیز نیازمند ضابطه‌ای روشن برای موارد استثنایی است. در حقوق ایران نیز اصول بیست‌ودوم و بیست‌وپنجم قانون اساسی و مقررات تفتیش و توقیف داده‌ها و سامانه‌های رایانه‌ای و مخابراتی، مبانی مهمی برای تحدید اختیار ضابطان و مراجع قضایی‌اند؛ بااین‌حال، انطباق آنها با پیام‌رسان‌ها، تفکیک بازرسی دستگاه از حساب کاربری و تحدید دامنه دستور نیازمند ارزیابی است.

هدف پژوهش، تبیین مبانی و معیارهای مشروعیت تفتیش ادله دیجیتال و پیام‌رسان‌ها با مطالعه تطبیقی فقه امامیه، حقوق کیفری ایران و معیارهای دادرسی منصفانه است. پرسش نخست آن است که حدود مشروعیت فقهی ورود به حریم داده‌ها و ارتباطات خصوصی کجاست؟ فرض بر آن است که اصل اولیه، حرمت تجسس و صیانت از اسرار است و عدول از آن تنها با وجود مصلحت معتبر، احراز ضرورت و رعایت تناسب امکان‌پذیر خواهد بود. پرسش دوم آن است که مقررات کیفری ایران تا چه اندازه تفتیش داده‌های پیام‌رسان‌ها را منضبط کرده‌اند؟

فرضیه آن است که با وجود پیش‌بینی تشریفات قانونی، ابهام در دامنه دستور و تفکیک ناکافی انواع داده و سطوح دسترسی، زمینه تفسیر موسع را باقی گذاشته است. پرسش سوم درباره معیارهای بین‌المللی تفتیش ادله الکترونیکی و نسبت آنها با فقه و حقوق داخلی است. فرض بر آن است که قانون‌مندی، هدف مشروع، ضرورت، تناسب، نظارت مؤثر و تفتیش هدفمند، با منع تجسس و منع مداخله خودسرانه هم‌پوشانی دارند، هرچند حدود استثناها متفاوت است.

پیشینه فارسی، ابعاد جداگانه‌ای از موضوع را بررسی کرده است. باقری حسن‌آبادی (۱۴۰۴) در پژوهش «بررسی اعتبار و قابلیت استناد ابزارهای ارتباطی نوین در فرایند اثبات جرم در نظام حقوقی ایران»، اعتبار پیام‌ها و چالش اصالت و تمامیت آنها را بررسی کرده، نه مشروعیت دسترسی تحقیقی. علیزاده، طاهریان و صوفی زمرد (۱۴۰۲) در پژوهش «مطالعه تطبیقی شرایط تحصیل دلیل، تفتیش و توقیف ادله الکترونیکی در مرحله اقدامات پلیسی در ایران، فرانسه و انگلستان»، مجوز قضایی، محرمانگی و حفاظت از داده‌ها را تحلیل کرده‌اند، اما به مبانی فقهی و ویژگی پیام‌رسان‌ها نپرداخته‌اند. امیری و نامیان (۱۴۰۲) در مقاله «حمایت کیفری از قلمرو حریم خصوصی فضای مجازی در تحقیقات پلیسی با نگاهی به مقررات ایران و اسناد بین‌المللی»، بر حمایت از داده‌ها و مکاتبات خصوصی تأکید کرده‌اند، اما دسترسی به محتوای پیام‌رسان را مستقلا بررسی نکرده‌اند. انارکی‌تودشکی، آقایی بجستانی و روحانی مقدم (۱۳۹۹) در پژوهش «تجسس از منظر

فقه امامیه»، حرمت تجسس و نسبت آن با مصالح عمومی را تحلیل کرده‌اند، اما آن را بر بازرسی دیجیتال تطبیق نداده‌اند. نوآوری پژوهش حاضر، پیوند دادن این سه حوزه و تمرکز بر پیام‌رسان به‌مثابه مجموعه‌ای از داده‌های محتوایی، پیرامونی و اطلاعات اشخاص ثالث است تا معیارهایی برای تحدید تفتیش و تعیین تکلیف داده‌های نامرتبط ارائه شود. روش تحقیق، توصیفی-تحلیلی و تطبیقی است؛ داده‌ها به شیوه کتابخانه‌ای گردآوری و با تحلیل مفهومی و تطبیق معیارها ارزیابی می‌شوند.

۱- مبانی نظری

درک دقیق ابعاد حقوقی و شرعی بازرسی ادله دیجیتال نیازمند واکاوی ویژگی‌های فنی این ادله و تبیین قلمرو نوپدید حریم خصوصی در بستر ارتباطات برخط است که در این بخش به آن پرداخته می‌شود.

۱-۱- ماهیت ادله دیجیتال و پیام‌رسان‌ها

تفتیش فیزیکی و تفتیش دیجیتال، هرچند از حیث هدف کشف و گردآوری دلیل کیفری به یکدیگر شباهت دارند، از نظر موضوع، دامنه و پیامدهای مداخله تفاوتی اساسی دارند. در تفتیش فیزیکی، جست‌وجو معمولا به مکان یا شیئی معین محدود است و حدود آن را می‌توان با مشاهده و تعیین محدوده مکانی نسبتا مشخص کرد؛ اما در تفتیش دیجیتال، دسترسی به یک ابزار یا حساب کاربری ممکن است امکان مشاهده مجموعه‌ای گسترده از اطلاعات را فراهم آورد که از حیث زمان، موضوع و اشخاص مرتبط با اتهام، هیچ پیوندی با موضوع تحقیق ندارند. تلفن همراه، برای مثال، صرفا وسیله‌ای برای نگهداری چند سند یا شیء نیست، بلکه می‌تواند سال‌ها اطلاعات ارتباطی، تصاویر، اسناد، سوابق جست‌وجو، داده‌های مکانی و جزئیات فعالیت‌های روزمره صاحب خود را در برگیرد. ازاین‌رو، ورود به چنین ابزاری، برخلاف بازرسی یک محل محدود، ممکن است به دسترسی گسترده به ابعاد متعدد زندگی خصوصی شخص بینجامد. ویژگی دیگر ادله دیجیتال، وابستگی آن‌ها به ساختارهای فنی و امکان تغییر یا زوال سریع اطلاعات است. برخی داده‌ها با حذف پیام، تغییر تنظیمات برنامه یا گذشت زمان از دسترس خارج می‌شوند؛ در مقابل، بخشی از اطلاعات حذف‌شده ممکن است برای مدتی در حافظه دستگاه یا نسخه‌های پشتیبان باقی بماند. بنابراین، زمان و شیوه تحصیل دلیل در این حوزه اهمیت ویژه‌ای دارد و اقدام شتاب‌زده یا غیرتخصصی می‌تواند هم به از بین رفتن داده‌های مفید و هم به تغییر ناخواسته اطلاعات منجر شود. افزون بر متن پیام‌ها و فایل‌های مبادله‌شده، داده‌های پیرامونی نیز واجد ارزش اثباتی‌اند؛ اطلاعاتی مانند زمان ارسال و دریافت، شناسه فرستنده و گیرنده، ترتیب ارتباطات و موقعیت مکانی می‌توانند روابط میان اشخاص و توالی رویدادها را آشکار کنند. حتی در مواردی که محتوای ارتباط رمزگذاری شده یا در دسترس نیست، همین اطلاعات جانبی امکان بازسازی بخشی از الگوی رفتاری و ارتباطی افراد را فراهم می‌آورد (Jaeckel et al., 2025: 9; Hyder et al., 2024: 11).

اهمیت این ویژگی‌ها هنگامی روشن‌تر می‌شود که پیام‌رسان‌ها نه صرفا ابزار انتقال پیام، بلکه مخزن متراکمی از اطلاعات شخصی تلقی شوند. تاریخچه گفت‌وگوها، تصاویر خانوادگی، پیام‌های عاطفی، مکاتبات کاری، فایل‌های پزشکی و مالی و حتی پیام‌های موقتی، در کنار یکدیگر تصویری نسبتا جامع از روابط، دغدغه‌ها، باورها و عادت‌های فرد ایجاد می‌کنند. چنین مجموعه‌ای ممکن است جنبه‌هایی از زندگی شخص را آشکار سازد که حتی نزدیک‌ترین اطرافیان او نیز از آن آگاه نیستند. به این اعتبار، محتوای پیام‌رسان‌ها با قلمرو خلوت ذهن و زندگی درونی اشخاص پیوند می‌یابد؛ قلمرویی که تعرض به آن، صرفا دسترسی به یک داده یا نوشته نیست، بلکه می‌تواند به آشکار شدن لایه‌های عمیق و ناگفته شخصیت و روابط انسانی بینجامد. قابلیت حذف خودکار پیام‌ها نیز این حساسیت را دوچندان می‌کند؛ زیرا نشان می‌دهد کاربران ممکن است با اتکا به موقتی بودن ارتباط، اطلاعاتی را مبادله کنند که قصد نگهداری دائمی آن را ندارند، هرچند این پیام‌ها در برخی شرایط فنی همچنان قابلیت بازیابی داشته باشند (Heath et al., 2023: 14). در نتیجه، مشروعیت تفتیش دیجیتال را نمی‌توان تنها با مجاز بودن دسترسی به یک دستگاه یا حساب کاربری توجیه کرد. گستردگی داده‌های قابل دسترس و ظرفیت آن‌ها برای آشکار ساختن خصوصی‌ترین ابعاد زندگی اشخاص، ضرورت محدودسازی تفتیش به داده‌های مرتبط، تعیین قلمرو

زمانی و موضوعی آن و جلوگیری از گردآوری اطلاعات نامرتبط را به اقتضایی بنیادین در فرایند کشف جرم تبدیل می‌کند.

۲-۱- چیستی و ابعاد حریم خصوصی دیجیتال

حریم خصوصی دیجیتال را نمی‌توان صرفا به محرمانه ماندن اطلاعات یا جلوگیری از دسترسی اشخاص غیرمجاز به داده‌های ذخیره‌شده محدود کرد؛ این مفهوم، مجموعه‌ای از حقوق و منافع مرتبط با گردآوری، نگهداری، پردازش، انتقال و استفاده از اطلاعات شخصی را در برمی‌گیرد. در فضای دیجیتال، اهمیت حریم خصوصی از آن جهت افزایش می‌یابد که داده‌های پراکنده و ظاهرا کم‌اهمیت، در صورت تجمیع و تحلیل، می‌توانند تصویری دقیق از هویت، روابط، ترجیحات و رفتارهای فرد ایجاد کنند. بنابراین، حمایت از حریم خصوصی نه‌تنها مستلزم جلوگیری از افشای اطلاعات محرمانه، بلکه نیازمند کنترل بر شیوه و زمینه استفاده از آن‌هاست. محرمانگی داده‌ها در این معنا، ناظر بر محدود کردن دسترسی و افشای اطلاعات به اشخاص و مراجع مجاز است؛ بااین‌حال، محرمانگی به‌تنهایی برای تحقق حریم خصوصی کافی نیست. ممکن است داده‌ای بدون افشای عمومی، در اختیار نهادی قرار گیرد و برخلاف هدف اولیه گردآوری یا انتظار معقول صاحب آن، برای تحلیل، دسته‌بندی یا تصمیم‌گیری درباره وی به کار گرفته شود. ازاین‌رو، مشروعیت پردازش اطلاعات باید با توجه به نوع داده، هدف گردآوری، هویت استفاده‌کننده و پیامدهای کاربرد آن سنجیده شود (Ghahremani & Nguyen, 2024: 7).

تمامیت سامانه‌های پردازش نیز بعد مکمل این حمایت به شمار می‌رود. مقصود از تمامیت، حفظ صحت، انسجام و قابلیت اعتماد داده‌ها و جلوگیری از تغییر، حذف، تخریب یا دست‌کاری غیرمجاز آن‌هاست. نقض تمامیت، افزون بر ایجاد اختلال در عملکرد سامانه، می‌تواند به تحریف واقعیت‌های مربوط به اشخاص و شکل‌گیری تصمیم‌های نادرست درباره آنان بینجامد. در فرایند کیفری نیز این موضوع اهمیت مضاعف دارد؛ زیرا دست‌کاری یا تغییر داده‌ها، چه در جریان دسترسی و گردآوری و چه هنگام نگهداری و تحلیل، ممکن است اصالت و قابلیت اعتماد دلیل دیجیتال را مخدوش کند. بدین ترتیب، محرمانگی و تمامیت دو الزام جداگانه اما مرتبط‌اند: نخستین الزام، دسترسی به اطلاعات را محدود می‌کند و دومین الزام، از صحت و سلامت آن‌ها در برابر مداخله ناموجه حمایت می‌کند. در کنار این دو بعد، مفهوم «انتظار متعارف از حریم خصوصی» معیاری برای تشخیص حدود حمایت حقوقی از اطلاعات اشخاص در محیط برخط فراهم می‌کند. بر اساس این معیار، مسأله اصلی صرفا آن نیست که فرد تا چه اندازه اطلاعات خود را محرمانه تلقی می‌کند، بلکه باید بررسی شود که با توجه به ماهیت داده، شیوه دسترسی، زمینه ایجاد و هدف استفاده از آن، آیا شخص به‌طور معقول انتظار داشته است اطلاعات مزبور از دسترس دیگران مصون بماند یا دست‌کم تنها در محدوده‌ای مشخص مورد استفاده قرار گیرد. برای مثال، عمومی بودن یک پیام یا انتشار بخشی از اطلاعات در فضای مجازی، لزوما به معنای رضایت شخص به گردآوری نامحدود، ذخیره‌سازی دائمی یا تحلیل همه‌جانبه آن نیست. به همین ترتیب، امکان فنی دسترسی به داده‌های ارتباطی یا مکانی، به‌خودی‌خود مجوز حقوقی استفاده از آن‌ها را ایجاد نمی‌کند. بنابراین، میان قابلیت دسترسی به اطلاعات و جواز مداخله در حریم خصوصی باید تفکیک کرد (Qarri, 2022: 457–458).

اهمیت این معیار به‌ویژه درباره داده‌های پیرامونی آشکار می‌شود؛ اطلاعاتی که ممکن است به‌تنهایی فاقد محتوای محرمانه به نظر برسند، اما در صورت تجمیع، جزئیاتی از زندگی خصوصی را نمایان کنند. داده‌های مربوط به زمان و مکان حضور فرد، الگوی رفت‌وآمد، ارتباطات مکرر و عادت‌های روزانه، حتی بدون دسترسی به محتوای پیام‌ها، می‌توانند تصویری دقیق از زندگی او بسازند. در نتیجه، محرمانگی نباید تنها به محتوای ارتباطات محدود شود؛ بلکه داده‌هایی که امکان استنباط اطلاعات حساس از زندگی شخص را فراهم می‌کنند نیز شایسته حمایت‌اند. افزون بر این، خطر نقض حریم خصوصی در همه موقعیت‌ها یکسان نیست و ممکن است پیامدهای جسمانی، روانی، اجتماعی، شغلی یا حتی محدودکننده آزادی فرد را در پی داشته باشد. ازاین‌رو، ارزیابی مداخله در حریم خصوصی باید متناسب با نوع داده، زمینه استفاده و پیامدهای احتمالی آن صورت گیرد (Karwatzki et al., 2022: 1126–1127).

بر این مبنا، حریم خصوصی دیجیتال حقی چندبعدی است که هم از اطلاعات در برابر دسترسی و افشای غیرمجاز حمایت می‌کند، هم سلامت و اصالت داده‌ها را مورد توجه قرار می‌دهد و هم اختیار معقول اشخاص در تعیین حدود استفاده از اطلاعاتشان را به رسمیت می‌شناسد. در حوزه تحقیقات کیفری، این برداشت مانع از آن است که صرف وجود اطلاعات در تلفن همراه، حساب کاربری یا بسترهای ارتباطی، مجوز دسترسی نامحدود به تمام محتوای آن‌ها تلقی شود. مشروعیت تفتیش باید با توجه به انتظار متعارف شخص، نوع و حساسیت داده‌ها، هدف مشخص تحقیق و حدود ضرورت دسترسی ارزیابی شود. به این ترتیب، حمایت از حریم خصوصی دیجیتال نه مانعی مطلق در برابر کشف جرم، بلکه ضابطه‌ای برای جلوگیری از تبدیل اختیار قانونی تحقیق به دسترسی فراگیر و نامحدود به زندگی خصوصی اشخاص است.

۲- بنیادهای فقه امامیه در منع تجسس و استثنائات آن

شناخت ابعاد شرعی تفتیش در فضای مجازی مستند به تبیین اصل اولی حرمت تجسس در فقه امامیه و بررسی محدوده استثنائات وارد بر آن است که در ادامه واکاوی می‌شود.

۲-۱- اصل اولی در فقه (حرمت تجسس و اشاعه فحشا)

اصل اولی در منظومه فقهی بر صیانت از حریم خصوصی و حرمت هرگونه ورود غیرمجاز به لایه‌های پنهان زندگی اشخاص استوار است. نهی صریح در آیه شریفه «ولا تجسسوا» تنها یک توصیه اخلاقی نیست، بلکه زیربنای یک قاعده حقوقی الزام‌آور را تشکیل می‌دهد که تتبع در عیوب و احوال پنهانی افراد را به‌طور مطلق منع می‌کند. این ممنوعیت که در احادیث متعددی نیز مورد تأکید قرار گرفته، بیانگر آن است که کشف اسرار و تفحص در اموری که افراد تمایلی به افشای آن‌ها ندارند، اساسا با روح شریعت در تعارض است. در این میان، تفتیش به‌عنوان ابزاری برای یافتن آنچه پنهان است، تنها در موارد استثنایی و با رعایت ضوابط بسیار سخت‌گیرانه مجاز شمرده می‌شود، زیرا اصل بر عدم ولایت اشخاص بر باطن و مراسلات یکدیگر است و هرگونه کنکاش در امور مستور، خروج از مجرای عدالت تلقی می‌گردد (المشکینی الأردبیلی، ۱۳۸۱: ۱۲۸).

بر پایه قاعده «ستر»، شارع بر پوشاندن لغزش‌ها و پنهان ماندن احوال خصوصی افراد تأکید دارد و هرگونه اقدام برای پرده‌دری از این حریم را مصداق اشاعه فحشا و نقض کرامت انسانی می‌داند. از این منظر، حکومت و ضابطان هیچ‌گونه ولایت ذاتی برای جستجو در قلمرو خصوصی اشخاص ندارند و برائت ذمه افراد ایجاب می‌کند که زندگی پنهانی آن‌ها از هرگونه تعرضی مصون بماند. این نگاه فقهی، حق بر خلوت را نه یک امتیاز اعطایی از سوی قدرت، بلکه حقی بنیادین و برخاسته از کرامت ذاتی انسان تلقی می‌کند که سلب آن نیازمند دلیلی قطعی، مشروع و فراتر از ظن و گمان‌های متعارف است (المنتظری، ۱۴۰۹: ۵۳۹).

در تحلیلی نوین از متون کهن، می‌توان عنوان «کتابت و مراسلات مکتوم» را که در فقه سنتی مورد حمایت جدی قرار گرفته، به محتوای پیام‌رسان‌های مجازی تسری داد. اگرچه در گذشته مراسلات بر روی کاغذ و در قالب نامه‌های مهروموم‌شده تحقق می‌یافت، اما با الغای خصوصیت از ابزار مادی و تکیه بر علت منصوص که همان صیانت از پیام‌های خصوصی است، محتوای دیجیتال و تاریخچه گفتگوها نیز مشمول همان حکم حرمت می‌گردند. در واقع، کاغذ یا فضای ابری تنها ظرفی برای انتقال اندیشه و ارتباطات خصوصی هستند و آنچه موضوعیت دارد، محرمانه بودن پیام است که در هر بستری باید محترم شمرده شود (فیاض، ۲۰۲۳: ۸۵). بنابراین، تفاوتی میان نامه فیزیکی و پیامک یا گفتگوی برخط وجود ندارد و هرگونه ورود بدون مجوز به این حریم، نقض مستقیم اصل اولی حرمت تجسس محسوب می‌شود. این رویکرد فقهی نشان می‌دهد که فضای مجازی نه یک منطقه آزاد برای نظارت‌های بی‌پایان، بلکه تداوم همان حریم خصوصی سنتی است که با دقت بیشتری باید از آن پاسداری کرد. استدلال به قیاس منصوص العله ایجاب می‌کند که تمامی حمایت‌های فقهی از نامه‌ها و اسناد مکتوب، عینا در مورد ادله دیجیتال و پلتفرم‌های پیام‌رسان نیز اعمال شود. در نتیجه، هرگونه تفتیش در این فضا بدون وجود ضرورت‌های قطعی و اثبات‌شده، خروج از دایره مشروعیت و گامی در جهت اشاعه فحشا و هتک پوشش مؤمن تلقی می‌گردد که با بنیادهای فقه امامیه در تضاد آشکار است. این مرزبندی میان قلمرو عمومی

و خصوصی، به معنای تعطیلی عدالت نیست، بلکه به معنای مشروط کردن ابزارهای کشف جرم به رعایت کرامت انسانی است تا امنیت اجتماعی به قیمت فروپاشی حصارهای اخلاقی و حقوقی افراد تأمین نگردد.

۲-۲- موارد جواز و استثنائات تجسس در فقه

اگرچه اصل اولیه در فقه بر حرمت تجسس استوار است، اما این قاعده در مواجهه با مصالح عالیه و حقوق بنیادین دیگر، استثنائات دقیقی را برمی‌تابد که مرز میان امنیت و آزادی را ترسیم می‌کنند. یکی از مهم‌ترین این موارد، عرصه حقوق‌الناس و تظلم‌خواهی مجنی‌علیه است؛ در جایی که حق فردی پایمال شده و اثبات آن منوط به تفحص در حریم خصوصی مرتکب باشد، حمایت از مظلوم بر اصل پوشش تقدم می‌یابد. در واقع، تجسس در این مقام نه برای پرده‌دری، بلکه ابزاری برای اجرای عدالت و بازپس‌گیری حق تلقی می‌شود که مشروعیت خود را از لزوم رفع ظلم می‌گیرد (الأحیدب، ۲۰۲۱: ۲۲۰). افزون بر این، در جرائم کلان امنیتی و توطئه‌هایی که کیان جامعه اسلامی را هدف قرار می‌دهند، بر پایه قاعده «حفظ نظام» و ضرورت «دفع مفسده مجبره»، بن‌بست حرمت تجسس شکسته می‌شود. در این چارچوب، اخلال در نظم عمومی و اقدامات براندازانه، مصلحتی برتر ایجاد می‌کند که صیانت از آن، بازرسی و کنکاش در ارتباطات پنهانی توطئه‌گران را توجیه می‌سازد (الحمصی و المصری، ۲۰۲۰: ۱۳۵).

زیربنای نظری این استثنائات غالبا بر قاعده «الضرورات تبیح المحذورات» استوار است، اما اعمال این قاعده هرگز به معنای مجوزی مطلق برای ورود خودسرانه به حریم خصوصی نیست. ضابطه سنجش در اینجا، بر ترازوی تزاحم میان مصلحت امنیتی و مفسده نقض حریم خصوصی قرار دارد؛ به این معنا که تنها در صورت وجود ضرورت قطعی و عدم امکان کشف جرم از طرق دیگر، می‌توان به تفتیش متوسل شد. این ضرورت باید به قدر متیقن اکتفا شود و از مرزهای لازم فراتر نرود، چراکه هرگونه زیاده‌روی در اعمال استثنا، خود به مفسده‌ای بزرگ‌تر تبدیل خواهد شد (الرواحی، ۲۰۱۲: ۴۵).

در تحلیل نهایی، باید میان جرائم حق‌اللهی محض و جرائم سازمان‌یافته یا مرتبط با حقوق‌الناس تفکیک قائل شد. در جرائم اخلاقی که جنبه فردی و حق‌اللهی دارند، سیاست جنایی فقهی بر پایه «درأ» و «ستر» شکل گرفته است؛ بدین معنا که شارع نه تنها مجوزی برای تجسس نداده، بلکه بر تعطیل جستجو و پوشاندن لغزش‌ها تأکید ورزیده است. در مقابل، هنگامی‌که بزهکاری از قالب فردی خارج شده و امنیت عمومی یا حقوق مادی و معنوی دیگران را تهدید می‌کند، لزوم صیانت از حق‌الناس و نظم اجتماعی، تفتیش را از دایره محرمات خارج کرده و به حوزهٔ تکالیف حاکمیتی وارد می‌کند. این رویکرد دوگانه نشان‌دهنده هوشمندی نظام فقهی در تفکیک میان گناهان فردی و جرائم اجتماعی است؛ به‌نحوی‌که در اولی بر بخشش و پوشش تأکید دارد و در دومی بر کشف حقیقت و اجرای مجازات برای پاسداری از سلامت جامعه اصرار می‌ورزد. بنابراین، مشروعیت تفتیش در فقه امامیه، امری عرضی و محدود به ضرورت‌های اجتماعی و صیانت از حقوق ستمدیدگان است و هرگز نباید به قاعده‌ای جاری برای نظارت دائم بر زندگی خصوصی شهروندان تبدیل شود. رعایت این مرز باریک، تضمین‌کننده توازن میان اقتدار حکومت و کرامت انسانی در بستر شریعت است.

۳- چارچوب حقوق کیفری ایران در تفتیش سامانه‌ها و پیام‌رسان‌ها

بررسی نحوه مواجهه حقوق موضوعه با بازرسی ادله الکترونیکی نیازمند واکاوی ضوابط قانونی حاکم بر تفتیش سامانه‌ها و چالش‌های عملی رویه قضایی است که در این بخش تحلیل می‌شود.

۱-۳- اصول حاکم بر بازرسی داده‌ها در قوانین موضوعه

نظام حقوقی ایران در گام نخست، صیانت از حریم خصوصی و امنیت ارتباطات را در عالی‌ترین سطح قانونی، یعنی قانون اساسی، مورد شناسایی قرار داده است. اصول بیست و دوم و بیست و پنجم این قانون، با تأکید بر مصونیت حیثیت، جان، مال و حقوق اشخاص از تعرض، هرگونه استراق سمع، تجسس و تفتیش را ممنوع اعلام کرده‌اند، مگر در مواردی که حکم صریح قانون وجود داشته باشد. این رویکرد بیانگر آن است که

در حقوق کیفری ایران، اصل بر آزادی و محرمانگی است و خروج از این اصل، تنها با رعایت تشریفات دقیق قانونی و در راستای ضرورت‌های قضایی امکان‌پذیر است. در واقع، قانون اساسی مرز میان اقتدار عمومی و آزادی فردی را به گونه‌ای ترسیم کرده که ورود به قلمرو خصوصی شهروندان، نه یک اختیار اداری، بلکه یک استثنای قضایی مقید به قانون تلقی گردد (شاکری و همکاران، ۱۳۹۹: ۵۲).

با ظهور فناوری‌های نوین و دگرگونی ماهیت جرم، قانون‌گذار در مواد ۱۳۲ تا ۱۵۰ قانون جرائم رایانه‌ای، چارچوب اختصاصی برای تفتیش و توقیف داده‌ها و سامانه‌ها تعریف کرده است. این مقررات با درک تفاوت بنیادین میان فضای فیزیکی و محیط دیجیتال، ضوابطی را پیش‌بینی کرده‌اند که بر اساس آن‌ها، بازرسی باید با حداقل مزاحمت برای کاربران و با تمرکز بر داده‌های مرتبط با جرم انجام شود. پیوند میان این مواد و مقررات بخش نهم قانون آیین دادرسی کیفری (مواد ۶۴۷ به بعد) نشان‌دهنده تلاش برای یکپارچه‌سازی نظام ادله الکترونیکی است. بر این اساس، دسترسی به محتوای پیام‌رسان‌ها و حساب‌های کاربری، فراتر از یک بازرسی ساده فیزیکی، نیازمند دستور قضایی مشخصی است که ابعاد زمانی و موضوعی تفتیش را به دقت معین نماید (السان و منوچهری، ۱۳۹۷: ۱۵).

تحلیل قوانین موضوعه حاکی از آن است که تفتیش ادله دیجیتال به دلیل ویژگی‌هایی نظیر فرار بودن و درهم‌تنیدگی داده‌های شخصی با داده‌های مجرمانه، چالش‌های تفسیری متعددی را پیش روی ضابطان و قضات قرار داده است. اگرچه قانون آیین دادرسی کیفری مصوب ۱۳۹۲ با اصلاحات بعدی، سعی در منضبط کردن رویه کشف جرم داشته، اما لزوم رعایت تناسب میان اقدام قضایی و حریم خصوصی اشخاص همچنان به‌عنوان یک اصل لایتغیر باقی مانده است. در مواردی که داده‌ها در محیط‌های ذخیره‌سازی ابری یا خارج از تسلط مستقیم فیزیکی فرد قرار دارند، ضرورت صدور دستورهای قضایی مستدل و محدود، بیش‌ازپیش برجسته می‌شود تا از تبدیل تفتیش هدفمند به نظارت‌های گسترده و بی‌ضابطه جلوگیری گردد (درویشی و رضایی، ۱۴۰۳: ۹۰).

در مجموع، چارچوب قانونی فعلی در ایران بر محور موازنه میان حق بر حریم خصوصی و مصلحت کشف جرم استوار است. با این حال، ماهیت سیال داده‌های دیجیتال ایجاب می‌کند که قضات صادرکننده دستور، از نگاه سنتی به تفتیش عبور کرده و مرزهای بازرسی را به داده‌های مورد نیاز برای اثبات بزه محدود کنند. این رویکرد، مانع از آن می‌شود که ضابطان دادگستری تحت لوای یک دستور کلی، به تمامی ابعاد زندگی دیجیتال متهم دسترسی یابند و بدین ترتیب، اسناد و ارتباطات غیر مرتبط اشخاص از گزند تعرض مصون می‌ماند. صیانت از تمامیت سامانه‌ها و محرمانگی داده‌ها در فرآیند دادرسی، نه تنها یک تکلیف قانونی، بلکه پیش‌شرط تحقق دادرسی منصفانه در عصر دیجیتال است که نیازمند نظارت مستمر بر عملکرد مجریان و پایش دقیق مرزهای مشروعیت در هر مرحله از تحقیق است. رعایت این موازین تضمین می‌کند که اقتدار حاکمیت در مسیر کشف حقیقت، منجر به فروپاشی حصارهای امنیتی شهروندان در فضای مجازی نگردد.

۲-۳- چالش‌های رویه قضایی و ضوابط ورود ضابطان دادگستری

بررسی رویه قضایی حاکی از آن است که دستورهای قضایی صادره برای تفتیش سامانه‌های دیجیتال باید از دقت لازم برخوردار باشند و بر اساس دادنامه شماره ۹۵۰۹۹۷۳۵۳۱۰۰۳۸۴ صادرشده از دادگاه عمومی، هرگونه اقدام فراتر از حدود مقرر قانونی فاقد توجیه قضایی است. در این راستا، تفکیک بازرسی فیزیکی تجهیزات از دسترسی به حساب‌های ابری پیام‌رسان‌ها اهمیتی دوچندان دارد. چالش الزام متهم به گشودن قفل بیومتریک یا رمز عبور با حق سکوت موضوع ماده ۱۹۷ قانون آیین دادرسی کیفری و اصل منع خوداتهامی در تعارض است. با این وجود، بر اساس نظریه مشورتی شماره ۷/۹۹/۱۷۷۹، محتویات به‌دست‌آمده از گوشی حتی در فرض دسترسی غیرمجاز، حسب تشخیص قاضی می‌تواند به‌عنوان قرینه مورد استناد قرار گیرد، هرچند استناد به ادله تحصیل‌شده از طریق تفتیش غیرقانونی بر مبنای آرایی نظیر دادنامه کیفری صادره در سال ۱۳۹۶ با چالش جدی بطلان دلیل مواجه است (تبریزی و همکاران، ۱۴۰۱: ۱۱۵).

فرآیند بازرسی دیجیتال نیازمند نظارت دقیق بر عملکرد ضابطان است تا از تبدیل تفتیش هدفمند به تجسس خودسرانه جلوگیری شود. هنگامی‌که مقام قضایی دستور بازرسی صادر می‌کند، موظف است محدوده زمانی و موضوعی داده‌ها را تفکیک نماید تا از افشای اطلاعات غیر مرتبط جلوگیری به عمل آید (لطیفیان، ۱۳۹۲: ۶۸). اجبار اشخاص به افشای اطلاعات خصوصی در غیاب مستندات قانونی صریح، مرز میان کشف جرم و نقض حقوق بنیادین شهروندان را مخدوش می‌سازد. از این‌رو، ارزیابی قضایی ادله الکترونیکی باید همواره با رعایت اصل تناسب و حمایت از حریم خصوصی همراه باشد تا از اعتبار نظام دادرسی صیانت گردد (تبریزی و همکاران، ۱۴۰۱: ۱۴۰). در تحلیل نهایی، تعادل میان کشف حقیقت و حفظ کرامت انسانی مستلزم انطباق کامل رویه‌های قضایی با استانداردهای حقوقی است. سامانه‌های پیام‌رسان به‌عنوان مخزن خلوت ذهنی و ارتباطی افراد، نباید دست‌خوش بازرسی‌های بدون ضابطه قرار گیرند و هرگونه انحراف از اصول قانونی باید با ضمانت‌اجراهای بازدارنده روبه‌رو شود تا حقوق دفاعی متهمان در برابر اقتدار تحقیق مصون بماند.

۴- استانداردهای بین‌المللی دادرسی منصفانه و حریم خصوصی حقوق بشری

ارزیابی نظام‌مند حمایت از حریم ارتباطات در بستر فناوری نیازمند سنجش موازین اسناد بین‌المللی و آزمون‌های سه‌گانه مشروعیت مداخله است که در این بخش تحلیل می‌گردد.

۴-۱- موازین اسناد بین‌المللی و منطقه‌ای

ماده ۱۷ میثاق بین‌المللی حقوق مدنی و سیاسی به‌عنوان یکی از اسناد بنیادین حقوق بشر، هرگونه مداخله خودسرانه یا غیرقانونی در حریم خصوصی، خانواده، اقامتگاه و مکاتبات اشخاص را به‌شدت ممنوع اعلام کرده و دولت‌ها را به حمایت قانونی در برابر این‌گونه مداخلات ملزم می‌سازد (Ní Loideáin, 2025: 45). کمیته حقوق بشر ملل متحد در نظریه‌های تفسیری خود بر این نکته تأکید می‌کند که مفهوم مکاتبات شامل تمامی ابزارهای ارتباطی نوین و داده‌های ذخیره‌شده در سامانه‌های دیجیتال نیز می‌شود و اعمال هرگونه نظارت، شنود یا تفتیش بر روی آن‌ها باید کاملا مستند به قوانین صریح، شفاف و با رعایت اصول ضرورت و تناسب باشد. در نظام حقوقی اروپایی، ماده ۸ کنوانسیون اروپایی حقوق بشر حق احترام به زندگی خصوصی و ارتباطات را تضمین کرده و رویه قضایی دیوان اروپایی حقوق بشر در آرای شاخصی نظیر پرونده کاپلند علیه بریتانیا، باربولسکو علیه رومانی و کوپکه علیه آلمان مرزهای دقیق نظارت بر ارتباطات دیجیتال را ترسیم نموده است. این آرا تصریح می‌کنند که حتی در بستر ارتباطات کاری یا برخط، کاربران دارای انتظار متعارف از حریم خصوصی هستند و هرگونه بازرسی یا جمع‌آوری داده‌های دیجیتال توسط مراجع عمومی یا کارفرمایان بدون هشدار قبلی، تفکیک دقیق داده‌های شخصی و رعایت اصول دادرسی منصفانه، نقض آشکار حقوق بنیادین محسوب می‌شود (Bernardini, 2023: 330).

در سطح همکاری‌های بین‌المللی، کنوانسیون بوداپست پیرامون جرائم سایبری با هدف ایجاد توازن میان کشف جرائم فرامرزی و صیانت از حقوق بشری اشخاص، استانداردهای مشخصی را برای بازرسی و ضبط داده‌های رایانه‌ای تدوین کرده است. این سند بین‌المللی دولت‌ها را موظف می‌سازد تا در فرآیند دسترسی به داده‌های ذخیره‌شده و سامانه‌های ابری، تشریفات قضایی دقیق، دستورهای مشخص و سازوکارهای نظارتی مستقل را رعایت کنند تا از نظارت‌های انبوه و تفتیش‌های خودسرانه فرامرزی جلوگیری به عمل آید (Gascón Marcén, 2023: 390). تلاقی این استانداردهای بین‌المللی با نظام‌های حقوقی داخلی نشان می‌دهد که ورود به حریم دیجیتال شهروندان نمی‌تواند صرفا به بهانه کشف جرم توجیه شود. الزام به تفکیک داده‌های مربوط به جرم از اطلاعات کاملا شخصی، رعایت اصول سه‌گانه قانون‌مندی، مشروعیت هدف و ضرورت در تمامی مداخلات امنیتی، خط قرمزی است که میان جوامع مبتنی بر حاکمیت قانون و نظام‌های نظارت همه‌جانبه تمایز ایجاد می‌کند.

۴-۲- آزمون‌های سه‌گانه مشروعیت مداخله (Three-Part Test)

از منظر حقوق بشری، ارزیابی مشروعیت هرگونه مداخله در حریم خصوصی و داده‌های دیجیتال اشخاص، نیازمند گذر از

آزمون‌های سه‌گانه قانون‌مندی، مشروعیت هدف و ضرورت و تناسب در جامعه دموکراتیک است. اصل قانون‌مندی دقیق ایجاب می‌کند که هرگونه دسترسی به اطلاعات شخصی و پیام‌رسان‌ها باید مبتنی بر قوانین مدون، قابل دسترس و با پیش‌بینی‌پذیری کافی باشد تا از اقدامات خودسرانه مراجع اجرایی و قضایی جلوگیری به عمل آید (United Nations General Assembly, 2024: 7). این قوانین باید حدود اختیارات ضابطان و نهادهای تحقیق را به روشنی تعیین کنند تا شهروندان بدانند در چه شرایطی ممکن است حریم ارتباطی آنان مورد بازرسی قرار گیرد.

مداخله در داده‌های برخط و سامانه‌های ارتباطی باید صرفا در راستای اهداف مشروعی نظیر حفظ امنیت ملی، نظم عمومی، پیشگیری از وقوع جرم یا حمایت از حقوق دیگران صورت پذیرد. با این وجود، استناد به مفاهیم کلی مانند امنیت عمومی نمی‌تواند مجوزی برای نظارت‌های همه‌جانبه یا دسترسی نامحدود به آرشیو پیام‌رسان‌ها باشد، زیرا گسترش ابزارهای داده‌محور و عملیات‌های کلان نفوذ، خطرات جدی برای یکپارچگی حریم خصوصی ایجاد می‌کند (Oerlemans & Royer, 2023: 440). هرگونه بازرسی باید هدفمند و در ارتباط مستقیم با اتهام مشخص باشد تا از تبدیل تحقیقات کیفری به تفتیش‌های کور و انبوه جلوگیری شود.

در نهایت، رعایت اصل ضرورت و تناسب در جامعه دموکراتیک مستلزم آن است که تفتیش داده‌ها کمترین میزان آسیب را به حقوق بنیادین اشخاص وارد کند و مناسب‌ترین ابزار برای کشف حقیقت باشد. رویه قضایی بین‌المللی بر این باور است که بازرسی انبوه و نگهداری عمومی داده‌های ارتباطی بدون تفکیک اطلاعات مرتبط از غیر مرتبط، با معیارهای دادرسی منصفانه در تضاد است و نظارت قضایی مستقل باید همواره به‌عنوان مانعی در برابر انحرافات احتمالی عمل کند (Mitsilegas et al., 2023: 190). پایبندی به این آزمون‌ها تضمین می‌کند که اقتدار دولت در کشف جرائم سایبری، به بهانه دسترسی به مخازن پیام‌رسان‌ها به استبداد دیجیتال تبدیل نشود و مرز میان امنیت جامعه و آزادی‌های فردی مخدوش نگردد. تنظیم دقیق این موازنه، پیش‌شرط مشروعیت‌بخشی به هرگونه تفتیش الکترونیکی در نظام‌های حقوقی نوین است.

۵- ارزیابی تطبیقی و استخراج الگوی موازنه

نقطه آغاز موازنه، پذیرش این واقعیت است که ضرورت کشف جرم، به‌خودی‌خود مجوز گشودن همه لایه‌های زندگی خصوصی نیست. منع تجسس در فقه امامیه، دست‌کم در قلمرو اسرار بی‌ارتباط با مصالح عمومی، قاعده نخستین است؛ دادرسی منصفانه نیز تفتیش خودسرانه را با حق دفاع و امنیت شخصی ناسازگار می‌داند. این همگرایی در جرائم حق‌اللهی آشکارتر است: تقدم پوشش بر کنجکاوی کیفری، مانع آن می‌شود که مقام تحقیق برای یافتن رفتاری پنهان، ابتدا حریم فرد را بشکند و سپس از حاصل همان تعرض، مبنایی برای تعقیب بسازد (کوشکی و موسوی‌آزاده، ۱۳۹۷: ۱۵۵). بااین‌حال، همسان گرفتن این دو مبنا نیز خطاست. در فقه، حرمت تجسس با تزاحم واقعی با حق دیگران یا مصلحت عمومی مهم می‌تواند محدود شود؛ در معیارهای دادرسی منصفانه، همین مداخله باید از پیش بر پایه قانون روشن، هدف معین و نظارت قضایی قابل سنجش باشد. استثنا، صرفا به دلیل سنگینی اتهام، به اختیار نامحدود تبدیل نمی‌شود: باید نشان داد دلیل موردنظر از راه کم‌تعرض‌تری دست‌یافتنی نیست و دامنه جست‌وجو از نیاز پرونده فراتر نمی‌رود (جعفریان‌سوته و همکاران، ۱۴۰۴: ۱۳۵).

پیام‌رسان‌ها این سنجش را دشوارتر می‌کنند؛ زیرا در کنار گفت‌وگوی مرتبط با اتهام، اطلاعات تماس، زمان و مسیر ارتباط، تصاویر خانوادگی و گفت‌وگوهای اشخاص ثالث را نیز در خود نگه می‌دارند. حریم خصوصی در اینجا فقط محرمانگی متن پیام نیست، بلکه امکان کنترل دسترسی دیگران به مجموعه روابط و عادت‌های فرد نیز هست (بی‌غم باروژ، ۱۴۰۲: ۵۳). مقررات ایران برای تفتیش و توقیف داده‌ها دستور قضایی و تعیین محدوده و نوع داده را پیش‌بینی کرده‌اند، اما برای دسترسی به داده‌های پیرامونی و محتوای پیام‌رسان‌ها، معیار تفکیک‌شده و منسجمی متناسب با حساسیت هر دسته به روشنی مقرر نکرده‌اند.

افزون بر این، قواعد مربوط به استنادپذیری داده‌ها بیشتر بر درستی و تمامیت آنها تمرکز دارند و پیامد روشن و عامی برای

کنار گذاشتن دلیل حاصل از تجاوز به حدود دستور قضایی تعیین نمی‌کنند. در نتیجه، ممکن است داده‌ای از نظر فنی معتبر باشد، اما شیوه دستیابی به آن حق حریم خصوصی را نقض کرده باشد. الگوی عملی موازنه باید از همان متن دستور آغاز شود. بازپرس لازم است شخص یا حساب موردنظر، بازه زمانی، موضوع اتهام، نوع داده و روش جست‌وجو را جداگانه مشخص کند و دسترسی به گوشی را مجوز خودکار ورود به همه حساب‌ها و داده‌های دوردست نداند. ضابط نیز باید نخست داده‌های کم‌تعرض‌تر را بررسی کند، مشاهده محتوای پیام‌ها را به ضرورت مستدل وابسته سازد و داده‌های نامرتبط یا متعلق به اشخاص ثالث را جدا و دور از دسترس پرونده نگه دارد. اگر در جریان بررسی، نشانه جرمی دیگر پیدا شد، گسترش جست‌وجو باید به تصمیم تازه قضایی وابسته باشد. ثبت گام‌های تفتیش، امکان اعتراض مؤثر و تعیین تکلیف داده‌های اضافی، موازنه را از توصیه‌ای اخلاقی به قاعده‌ای قابل نظارت بدل می‌کند؛ قاعده‌ای که هم کشف جرم را ممکن می‌سازد و هم نمی‌گذارد زندگی خصوصی، بهای پیش‌فرض آن باشد.

نتیجه‌گیری

پژوهش حاضر با واکاوی ابعاد فقهی، حقوقی و بین‌المللی تفتیش ادله دیجیتال و پلتفرم‌های پیام‌رسان نشان داد که با گذر جوامع از فضای فیزیکی به بستر رایانه‌ای، مفهوم حریم خصوصی دستخوش تحولی بنیادین شده است. داده‌های ذخیره‌شده در تلفن‌های همراه و حساب‌های کاربری، دیگر صرفا مجموعه‌ای از اطلاعات بی‌روح نیستند، بلکه بازتاب‌دهنده خلوت ذهنی، اندیشه‌ها، روابط عاطفی و اسناد کاملا شخصی شهروندان محسوب می‌شوند. در این میان، چالش اصلی نظام‌های حقوقی همواره ایجاد توازن میان ضرورت کشف جرم، حفظ امنیت عمومی و صیانت از حقوق بنیادین و کرامت انسانی اشخاص بوده است. یافته‌های این پژوهش گویای آن است که نظام حقوق کیفری ایران به رغم تلاش برای پوشش دادن تحولات فناورانه از طریق قانون جرائم رایانه‌ای و قانون آیین دادرسی کیفری، همچنان با خلأهای جدی و ابهاماتی ساختاری در زمینه ضوابط بازرسی داده‌های نوین روبه‌رو است که نیازمند بازنگری و اصلاحات اساسی است.

در سطح مبانی نظری و فقهی، آموزه‌های فقه امامیه با تکیه بر اصولی چون حرمت تجسس، قاعده ستر و اصالت عدم ولایت بر احوال پنهانی اشخاص، خط قرمز روشنی در برابر تفتیش خودسرانه حریم خصوصی ترسیم می‌کنند. با وجود این، فقه پویای امامیه بر مبنای قواعدی همچون حفظ نظام، دفع مفسده مجبره و اضطرار، جواز ورود به حریم خصوصی را در شرایط استثنایی و برای صیانت از مصالح کلان جامعه مجاز می‌شمارد؛ امری که با استانداردهای بین‌المللی دادرسی منصفانه و آزمون‌های سه‌گانه قانون‌مندی، مشروعیت هدف و ضرورت و تناسب در جامعه دموکراتیک دارای همگرایی عمیقی است. هر دو نظام حقوقی و فقهی بر این اصل اتفاق‌نظر دارند که مداخله در حریم خصوصی افراد نباید به‌صورت مطلق، بدون ضابطه و به شیوه نظارت انبوه اعمال شود، بلکه هرگونه بازرسی باید هدفمند، محدود و آخرین راه‌حل در مواجهه با جرائم جدی باشد. با این وجود، رویه عملی مراجع قضایی و ضابطان در ایران گاه به دلیل غلبه رویکرد امنیتی بر رویکرد حقوق بشری، به سمت تفتیش‌های کور، فله‌ای و گسترده متمایل می‌شود که با روح اصول قانون اساسی و موازین شرعی در تضاد است.

یکی از آسیب‌های جدی رویه قضایی کنونی، عدم تفکیک میان بازرسی سخت‌افزار فیزیکی دستگاه و دسترسی به حساب‌های ابری و پیام‌رسان‌های اشخاص است. هنگامی‌که دستوری صادر می‌شود، ضابطان به پشتوانه یک حکم کلی، کل محتوای ارتباطی متهم اعم از اسناد کاری، تصاویر خانوادگی و پیام‌های شخصی غیر مرتبط با پرونده را زیر و رو می‌کنند که این پدیده مصداق بارز تجاوز به حریم خصوصی و نقض قاعده تفتیش هدفمند است. افزون بر این، چالش‌هایی نظیر الزام متهم به افشای رمزهای عبور و قفل‌های بیومتریک، مرز میان همکاری با مقام قضایی و نقض حق سکوت و اصل منع اجبار بر خود متهم‌سازی را مخدوش کرده است. ضمانت‌اجراهای موجود در قوانین داخلی نیز به دلیل ضعف در ضمانت‌اجرای بطلان ادله تحصیل‌شده نامشروع، کارایی لازم را در بازدارندگی از رفتارهای خودسرانه مأموران ندارند و ماده ۳۶ قانون جرائم رایانه‌ای در مقام عمل نیازمند تقویت و شفاف‌سازی است.

برای برون‌رفت از چالش‌های یادشده و انطباق نظام دادرسی کیفری ایران با استانداردهای متعالی فقهی و حقوق بشری، پیشنهادهای مشخصی در حوزه اصلاحات قانون‌گذاری قابل ارائه است. نخست، ضرورت دارد قانون‌گذار در مواد مربوط به تفتیش و توقیف داده‌ها در قانون آیین دادرسی کیفری و قانون جرائم رایانه‌ای، نهاد «دستور قضایی تفکیک‌شده» را به رسمیت بشناسد؛ بدین معنا که صدور اجازه بازرسی سخت‌افزار فیزیکی به‌هیچ‌وجه نباید به معنای جواز دسترسی نامحدود به حساب‌های کاربری، پیام‌رسان‌ها و داده‌های ابری تلقی شود و برای هر بخش باید دلایل، مستندات و حدود دقیق جداگانه‌ای تعیین گردد. دوم، ایجاد سازوکار قانونی دقیق برای «قاعده‌مندسازی امحای داده‌های اضافی» از الزامات غیرقابل انکار است. بازپرسان و ضابطان موظفند پس از پایان بازرسی و استخراج ادله مرتبط با جرم، داده‌های شخصی، خانوادگی و غیر مرتبط انباشته‌شده در پرونده را تحت نظارت مرجع قضایی امحا کنند تا از نشت اطلاعات خصوصی شهروندان جلوگیری شود. اعمال این اصلاحات می‌تواند گامی استوار در جهت صیانت توأمان از کارآمدی نظام عدالت کیفری و پاسداری از حقوق و آزادی‌های مشروع اشخاص در عصر دیجیتال باشد.

ملاحظات اخلاقی: موارد مربوط به اخلاق در پژوهش و نیز امانت‌داری در استناد به متون و ارجاعات به مقاله تماما رعایت گردید.

تعارض منافع: در تدوین این مقاله، هیچ‌گونه تعارض منافعی وجود نداشته است.

سهم نویسندگان: نگارش مقاله توسط نویسندهٔ مسؤول انجام گرفته است.

تشکر و قدردانی: از تمام کسانی که در تهیه این مقاله یاری رسانده‌اند، سپاسگزاریم.

تأمین اعتبار پژوهش: پژوهش حاضر بدون تأمین مالی انجام شده است.

منابع

الف. منابع فارسی و عربی

– الأحیدب، هناء بنت ناصر بن عبد الرحمن (۲۰۲۱). «التجسس بین الزوجین وعلي الأولاد: دراسة فقهیة». *مجلة العلوم الشرعیة*، (۶۱): ۲۶۱–۱۹۹.

– امیری، نجات و نامیان، پیمان (۱۴۰۲). «حمایت کیفری از قلمرو حریم خصوصی فضای مجازی در تحقیقات پلیسی با نگاهی به مقررات ایران و اسناد بین‌المللی». *پژوهش‌های اطلاعاتی و جنایی*، ۱۸(۲): ۱۴۴–۱۱۹.

– انارکی‌تودشکی، محمد، آقایی بجستانی، مریم و روحانی مقدم، محمد (۱۳۹۹). «تجسس از منظر فقه امامیه». *فقه و تاریخ تمدن*، ۱۷(۶۵): ۲۹–۲۴.

– باقری حسن‌آبادی، علیرضا (۱۴۰۴). «بررسی اعتبار و قابلیت استناد ابزارهای ارتباطی نوین در فرایند اثبات جرم در نظام حقوقی ایران». *تمدن حقوقی*، (۲۵): ۳۲۸–۳۰۳.

– بی‌غم باروژ، صیاد (۱۴۰۲). بررسی حریم خصوصی از نگاه اندیشمندان غربی، فقه و حقوق ایران». *قانون‌یار*، (۲۸): ۵۳– ۸۱.

– تبریزی، صادق، الهی‌منش، محمدرضا، عالی‌پور، حسن، طهماسبی، جواد و فضلی، مهدی (۱۴۰۱). «اصل قانون‌مندی توقیف داده و سامانه در فرآیند کیفری؛ جلوه‌ها و تضمین‌ها». *تعالی حقوق*، ۱۳(۲): ۱۴۰–۱۰۹.

– تبریزی، صادق، عالی‌پور، حسن و الهی‌منش، محمدرضا (۱۴۰۱). «اصل تناسب در توقیف داده و سامانه در فرایند کیفری». *مجله حقوقی دادگستری*، ۸۶(۱۱۷): ۱۵۲–۱۳۱.

– جعفریان‌سوته، سید حسن، کلانتری، کیومرث و تدین، عباس (۱۴۰۴). «بازشناسی فقهی حقوقی مفهوم تجسس در کشف جرائم اقتصادی (جواز یا نهی)». *فقه جزای تطبیقی*، ۵(۴): ۱۴۷–۱۳۵.

– الحمصی، فاطمة محمود و المصری، غیداء (۲۰۲۰). «الاطلاع علي المسکن وضوابطه الشرعیة فی التحقیق

الجنائی». *مجلة الجامعة الأسمریة للعلوم الشرعیة*، ۳۳(۲): ۱۵۳-۱۲۲.

- درویشی، صیاد و رضایی، محسن (۱۴۰۳). «چالش‌های پلیس ایران در تفتیش و توقیف داده و سامانه در پیشگیری و کشف جرم». *پژوهشنامه حقوق کیفری*، ۱۵(۱): ۹۸-۸۵

- الرواحی، ساعد بن أحمد بن محمد (۲۰۱۲). *أحکام التجسس فی الفقه الإسلامی* [بحث جامعی، درجة البکالوریوس]. سلطنة عمان: مکتبة مرکز الخدمات العلمیة.

- السان، مصطفی و منوچهری، محمدرضا (۱۳۹۷). «آیین کشف و ابراز دلیل در فضای مجازی». *پژوهشنامه حقوق کیفری*، ۹(۲)؛ ۳۰-۷.

- شاکری، ابوالحسن، گلدوزیان، حسین و رستگار صولتی، محمدسعید (۱۳۹۹). «تفتیش و توقیف ادله الکترونیکی در حقوق کیفری ایران و آمریکا». *کارآگاه*، ۱۳(۵۲): ۶۶-۴۷.

- علیزاده، اکبر، طاهریان، میلاد و صوفی‌زمرد، محسن (۱۴۰۲). «مطالعه تطبیقی شرایط تحصیل دلیل، تفتیش و توقیف ادله الکترونیکی در مرحله اقدامات پلیسی در ایران، فرانسه و انگلستان». *مطالعات بین‌المللی پلیس*، (۵۵): ۱۲۶-۱۰۱.

- فیاض، کاظم جاسب جبار (۲۰۲۳). *التفتیش وأحکامه فی الفقه الإمامی: عرض وتحلیل* [رسالة ماجستیر فی الشریعة والعلوم الإسلامیة]. جامعة کربلاء، کلیة العلوم الإسلامیة، قسم الدراسات القرآنیة والفقه.

- کوشکی، غلامحسن و موسوی‌آزاده، رضا. (۱۳۹۷). «از شناسایی منع تجسس به مثابه قاعده‌ای فقهی تا انعکاس آثار آن در نظام دادرسی کیفری ایران. پژوهشنامه حقوق اسلامی، (۴۷)، ۱۵۵–۱۸۰.

- لطیفیان، سیمین. (۱۳۹۲). «بررسی الزامات قانونی تفتیش و توقیف داده‌ها و سامانه‌های رایانه‌ای در قلمروی جرائم رایانه‌ای [پایان‌نامه کارشناسی ارشد، دانشگاه فردوسی مشهد].

- المشکینی الأردبیلی، علی (۱۳۸۱). *مصطلحات الفقه* (الطبعة الثانیة). قم: انتشارات الهادی. ص. ۱۲۸.

- المنتظری، حسین‌علی (۱۴۰۹). *دراسات فی ولایة الفقیه وفقه الدولة الإسلامیة* (الطبعة الثانیة، الجزء الثانی). قم: نشر تفکر؛ المرکز العالمی للدراسات الإسلامیة.

ب. منابع انگلیسی

- Bernardini, L (2023). "Searches and Seizures in the Digital Age—The Need for a Prior Independent Oversight Among International and European Standards". *Revista de la Facultad de Derecho de México*, 73(287): 309–342.

- Gascón Marcén, A. (2023). "The Push for the International Regulation of Cross-Border Access to Electronic Evidence and Human Rights". *Cuadernos de Derecho Transnacional*, 15(1): 385–402.

- Ghahremani, Shahram, & Nguyen, Uyen Trang. (2024). "Comprehensive Evaluation of Privacy Policies Using the Contextual Integrity Framework". *Security and Privacy*, 7(4): 1-19.

- Heath, Howard, MacDermott, Áine, & Akinbi, Alex. (2023). "Forensic Analysis of Ephemeral Messaging Applications: Disappearing Messages or Evidential Data?" *Forensic Science International: Digital Investigation*, 46(1): 1-17.

- Hyder, Muhammad Faraz, Arshad, Saadia, & Fatima, Tasbiha. (2024). "Toward Social Media Forensics through Development of iOS Analyzers for Evidence Collection and Analysis". *Concurrency and Computation: Practice and Experience*, 36(13): 1-27.

- Jaeckel, Lukas, Spranger, Michael, & Labudde, Dirk. (2025). "Forensic analysis of Telegram Messenger on iOS Smartphones". *Forensic Science International: Digital Investigation*, 52(Supplement): 1-20.

- Karwatzki, Sabrina, Trenz, Manuel, & Veit, Daniel. (2022). "The Multidimensional Nature of Privacy Risks: Conceptualisation, Measurement and Implications for Digital Services". *Information Systems Journal*, 32(6): 1126–1157.

- Mitsilegas, V., Guild, E., Kuskonmaz, E., & Vavoula, N. (2023). "Data Retention and the Future of Large-Scale Surveillance: The Evolution and Contestation of Judicial

Benchmarks". *European Law Journal*, 29(1–2): 176–211.

- Ní Loideáin, N. (2025). *EU Data Privacy Law and Serious Crime: Data Retention and Policymaking*. Oxford University Press.

- Oerlemans, J.-J., & Royer, S. (2023). "The Future of Data-Driven Investigations in Light of the Sky ECC Operation". *New Journal of European Criminal Law*, 14(4): 434–458.

- Qarri, Ana. (2022). "Bringing Section 8 Home: An Argument for Recognizing a Reasonable Expectation of Privacy in Metadata Collected from Smart Home Devices". *Canadian Journal of Law and* Technology, 19(2): 457–473.

- United Nations General Assembly. (2024). *The Right to Privacy in the Digital Age* (A/RES/79/175). United Nations.