Criminal Law Doctrines of Islamic Countries
Online ISSN:3041-9964
https://diplic.qom.ac.ir

Criminal Protection of Digital Privacy in Islamic Jurisprudence and Criminal Laws of Islamic Countries

Issa Eshterabeh[1], Marzieh Pilehvar[2], Zabih Motaharikhah[3]

1. PhD student in Theology (Jurisprudence and Fundamentals of Islamic Law), Faculty of Humanities, Islamic Azad University, Hamedan Branch, Iran, Hamedan, Email: 3309574997@iau.ir
2. Associate Professor, Department of Theology (Jurisprudence and Fundamentals of Islamic Law), Faculty of Humanities, Islamic Azad University, Hamedan Branch, Iran, Hamedan, Email: pilehvar@iau.ac.ir
3. Assistant Professor, Department of Theology (Jurisprudence and Fundamentals of Islamic Law), Faculty of Humanities, Islamic Azad University, Hamadan Branch, Iran, Hamadan, Email: zabihmotaharikhah@gmail.com

Abstract

The expansion of communication technologies and the increasing dependence of societies on the digital space has confronted the concept of privacy with new challenges and highlighted the necessity of reconsidering criminal protection mechanisms for personal data in Islamic countries. In such a context, the main question is to what extent Islamic jurisprudence, with emphasis on the common capacities of Islamic schools of thought, is capable of providing criminal protection for digital privacy, and to what extent the criminal laws of Islamic countries have utilized this capacity. The purpose of this research is to analyze the jurisprudential foundations of digital privacy protection, including both Imamiyeh and Sunni jurisprudence, and to compare them with the criminal regulations of Islamic countries. The research method is descriptive-analytical, and the data collection method is library-based, relying on document analysis, laws and comparative studies. The findings indicate that Islamic jurisprudence, based on the common rules of all Islamic schools of thought such as the prohibition of espionage, the principle of no harm, sovereignty over property and the prohibition of disclosing secrets which have been emphasized in the jurisprudential sources of all Islamic schools of thought, has extensive capacity for criminal protection of digital privacy. Although some countries have taken steps toward criminalizing digital violations, but the dispersion of regulations and the lack of independent criminalization of some instances still impede effective criminal protection. Consequently, the systematic utilization of the common capacities of Islamic jurisprudence, which is accepted by all Islamic schools of thought, can provide a coherent framework for strengthening the criminal laws of Islamic countries in the field of digital privacy and pave the way for codifying a unified pattern in the Islamic world.

Keywords: digital privacy, Islamic jurisprudence, criminal protection, the laws of Islamic countries.

Received: 12/03/2026; Revised: 03/04/2026; Accepted: 08/05/2026

How To Cite: Eshterabeh, Issa; Pilehvar, Marzieh & Motaharikhah, Zabih (2026). Criminal Protection of Digital Privacy in Islamic Jurisprudence and Criminal Laws of Islamic Countries, *Criminal Law Doctrines of Islamic Countries, 3 (2), 32-56.* https://www.doi.org/ 10.22091/dclic.2026.15470.1155

Published by: University of Qom **Article type: Research**

آموزه‌های حقوق کیفری کشورهای اسلامی
https://diplic.qom.ac.ir
شاپا الکترونیکی: ۹۹۶۴-۳۰۴۱

حمایت کیفری از حریم خصوصی دیجیتال در فقه اسلامی و قوانین کیفری کشورهای اسلامی

عیسی اِشترابه[۱]، مرضیه پیله‌ور[۲]، ذبیح مطهری خواه[۳]

۱. دانشجوی دکترای الهیات (فقه و مبانی حقوق اسلامی)، دانشکده علوم انسانیِ دانشگاه آزاد اسلامی، واحد همدان، ایران، همدان، رایانامه: 3309574997@iau.ir

۲. دانشیار گروه الهیات (فقه و مبانی حقوق اسلامی)، دانشکده علوم انسانیِ دانشگاه آزاد اسلامی، واحد همدان، ایران، همدان، رایانامه: pilehvar@iau.ac.ir

۳. استادیار گروه الهیات (فقه و مبانی حقوق اسلامی)، دانشکده علوم انسانیِ دانشگاه آزاد اسلامی، واحد همدان، ایران، همدان، رایانامه: zabihmotaharikhah@gmail.com

چکیده

گسترش فناوری‌های ارتباطی و وابستگی روزافزون جوامع به فضای دیجیتال، مفهوم حریم خصوصی را با چالش‌های نوینی مواجه ساخته و ضرورت بازنگری در سازوکارهای حمایت کیفری از داده‌های شخصی را برجسته ساخته است. در چنین بستری، پرسش اصلی آن است که فقه اسلامی با تأکید بر ظرفیت‌های مشترک مذاهب اسلامی تا چه اندازه توانایی حمایت کیفری از حریم خصوصی دیجیتال را دارد و قوانین کیفری کشورهای اسلامی تا چه حد از این ظرفیت بهره‌مند شده‌اند. هدف این پژوهش، تحلیل مبانی فقهی حمایت از حریم خصوصی دیجیتال اعم از فقه امامیه و فقه اهل سنت و مقایسه آن با مقررات کیفری کشورهای اسلامی است. روش تحقیق به صورت توصیفی و تحلیلی بوده و روش گردآوری اطلاعات نیز کتابخانه‌ای و مبتنی بر تحلیل اسناد و قوانین و مطالعات تطبیقی است. یافته‌های پژوهش نشان می‌دهد که فقه اسلامی با تکیه بر قواعد مشترک مذاهب اسلامی همچون حرمت تجسس، لاضرر، سلطنت بر اموال و حرمت افشای اسرار که در منابع فقهی تمام مذاهب اسلامی مورد تأکید قرار گرفته‌اند، ظرفیت گسترده‌ای برای حمایت کیفری از حریم خصوصی دیجیتال دارد. هرچند برخی کشورها گام‌هایی در جهت جرم‌انگاری تعرضات دیجیتال برداشته‌اند، اما همچنان پراکندگی مقررات و فقدان جرم‌انگاری مستقل برخی مصادیق، مانع از تحقق حمایت کیفری مؤثر است. نتیجه آنکه بهره‌گیری نظام‌مند از ظرفیت‌های مشترک فقه اسلامی که مورد قبول تمام مذاهب است می‌تواند چارچوبی منسجم برای تقویت قوانین کیفری کشورهای اسلامی در حوزه حریم خصوصی دیجیتال فراهم آورد و زمینه‌ساز تدوین الگوی واحدی در جهان اسلام باشد.

کلیدواژه‌ها: حریم خصوصی دیجیتال، فقه اسلامی، حمایت کیفری، قوانین کشورهای اسلامی.

تاریخ دریافت: ۱۴۰۴/۱۲/۰۱؛ **تاریخ بازنگری:** ۱۴۰۵/۰۱/۱۴؛ **تاریخ پذیرش:** ۱۴۰۵/۰۲/۱۸

استناد: اِشترابه، عیسی؛ مرضیه، پیله‌ور و مطهری‌خواه، ذبیح (۱۴۰۵). حمایت کیفری از حریم خصوصی دیجیتال در فقه اسلامی و قوانین کیفری کشورهای اسلامی، آموزه‌های حقوق کیفری کشورهای اسلامی، ۳ (۲)، ۵۶-۳۲. https://www.doi.org/10.22091/dclic.2026.15470.1155

ناشر: دانشگاه قم **نوع مقاله:** پژوهشی

مقدمه

گسترش بی‌سابقه فناوری‌های دیجیتال و وابستگی روزافزون جوامع به داده‌های شخصی، مفهوم حریم خصوصی را با چالش‌های عمیق و چندلایه مواجه کرده است؛ چالشی که نه‌تنها ابعاد فردی و اخلاقی دارد، بلکه پیامدهای کیفری و امنیتی گسترده‌ای نیز به همراه آورده است. در دهه اخیر، حجم داده‌های تولید شده توسط کاربران و میزان پردازش اطلاعات شخصی توسط دولت‌ها و شرکت‌های خصوصی به‌گونه‌ای افزایش یافته که نقض حریم خصوصی دیجیتال به یکی از مهم‌ترین تهدیدهای حقوق بشری و امنیت اجتماعی تبدیل شده است (Solove, 2021: 44).

در کشورهای اسلامی این وضعیت با پیچیدگی بیشتری همراه است؛ زیرا از یک سو، آموزه‌های فقه اسلامی بر حرمت تجسس، منع افشای اسرار و رعایت کرامت انسانی تأکید دارند و از سوی دیگر، قوانین کیفری این کشورها در مواجهه با جرائم نوپدید دیجیتال، پراکنده، غیر هم‌سطح و بعضاً فاقد انسجام لازم‌اند (Al-Daraiseh, 2020: 112). در سطح جهانی نیز پژوهش‌های جدید نشان می‌دهد که ضعف در تعریف دقیق داده شخصی، نبود ضمانت اجراهای مؤثر و عدم هماهنگی میان نظام‌های حقوقی، مهم‌ترین موانع تحقق حمایت کیفری کارآمد از حریم خصوصی دیجیتال هستند (Bygrave, 2020: 67). در کشورهای اسلامی، این چالش‌ها با مسئله دیگری نیز گره خورده است: اینکه قوانین کیفری موجود تا چه اندازه با مبانی فقه اسلامی سازگارند و آیا ظرفیت‌های فقهی می‌توانند خلأهای قانونی را پوشش دهند. هرچند برخی کشورها مانند ایران، امارات و مالزی در سال‌های اخیر اصلاحاتی در قوانین جرائم رایانه‌ای انجام داده‌اند، اما مطالعات تطبیقی نشان می‌دهد که این اصلاحات غالباً واکنشی، محدود و فاقد پشتوانه نظری منسجم‌اند (Rahman, 2022: 93). از سوی دیگر، پژوهش‌های فقهی جدید نشان داده‌اند که قواعدی همچون لاضرر، سلطنت، حرمت تجسس و حرمت افشای اسرار، ظرفیت‌های گسترده‌ای برای جرم‌انگاری تعرضات دیجیتال دارند و می‌توانند مبنای نظری محکمی برای حمایت کیفری از داده‌های شخصی فراهم کنند (حسینی، ۱۴۰۰: ۲۵). بااین‌حال، بررسی قوانین کیفری کشورهای اسلامی نشان می‌دهد که این ظرفیت‌ها به‌طور نظام‌مند وارد فرآیند

قانون‌گذاری نشده‌اند و در بسیاری موارد، قوانین فاقد تعریف روشن از داده شخصی، مصادیق تعرض دیجیتال، حدود مسئولیت کیفری و معیارهای اثبات جرم هستند (Khan, 2021: 141).

افزون بر این، رشد فناوری‌های نوین مانند هوش مصنوعی، کلان داده، ردیابی هوشمند و تحلیل رفتار کاربران، ابعاد جدیدی از نقض حریم خصوصی را ایجاد کرده که قوانین سنتی توان پاسخ‌گویی به آن را ندارند (Zuboff, 2019: 211). در سال‌های اخیر، برخی پژوهش‌ها بر ضرورت بازنگری در نظام‌های کیفری کشورهای اسلامی برای مواجهه با این چالش‌ها تأکید کرده‌اند و نشان داده‌اند که بدون بهره‌گیری از مبانی فقهی، قوانین کیفری این کشورها در برابر جرائم دیجیتال دچار گسست نظری و ناکارآمدی عملی خواهند بود (Mansoor, 2023: 54). از سوی دیگر، بدون تحلیل تطبیقی قوانین کشورهای اسلامی، امکان ارائه الگوی واحد و کارآمد برای حمایت کیفری از حریم خصوصی دیجیتال وجود نخواهد داشت. بنابراین، مسئله اصلی این پژوهش آن است که آیا فقه اسلامی می‌تواند چارچوبی نظری و عملی برای حمایت کیفری از حریم خصوصی دیجیتال ارائه دهد و قوانین کیفری کشورهای اسلامی تا چه حد با این چارچوب منطبق‌اند. اهمیت این مسئله از آن جهت است که حریم خصوصی دیجیتال، به‌عنوان یکی از بنیادی‌ترین حقوق بشری در عصر داده‌محور، نیازمند حمایت کیفری مؤثر، منسجم و مبتنی بر مبانی معتبر است؛ حمایتی که بدون پیوند میان فقه اسلامی و نظام‌های کیفری کشورهای اسلامی تحقق نخواهد یافت.

۱. پیشینه شناسی

در این بخش از پژوهش، به مرور پیشینه‌های موجود پرداخته می‌شود تا روشن شود تاکنون چه ابعادی از حریم خصوصی دیجیتال مورد بررسی قرار گرفته است.

سولوو[1] (۲۰۲۱)، در پژوهش خود با عنوان «رخنه شده: چرا قوانین امنیت داده ناکارآمد هستند و چگونه می‌توان آن‌ها را اصلاح کرد»[2] بیان می‌کند که نظام‌های حقوقی موجود در حوزه داده‌های شخصی، به‌ویژه

1. Solove
2. Breached: Why Data Security Law Fails and How to Improve It

در کشورهای غیرغربی، فاقد انسجام مفهومی و ضمانت اجرای کافی برای حمایت از حریم خصوصی دیجیتال هستند.

بایگرو[1] (۲۰۲۰)، در پژوهش خود با عنوان «حقوق حریم خصوصی داده‌ها: چشم‌اندازی بین‌المللی»[2] بیان می‌کند که حمایت کیفری از داده‌های شخصی در سطح جهانی با چالش‌هایی جدی روبه‌روست؛ ازجمله ابهام در تعریف داده شخصی، نبود هماهنگی میان نظام‌های حقوقی و فقدان معیارهای روشن برای جرم‌انگاری رفتارهای مرتبط با نقض حریم خصوصی دیجیتال.

الدرایسه[3] (۲۰۲۰)، در پژوهش خود با عنوان «حریم خصوصی و جرائم سایبری در حقوق اسلامی»[4] بیان می‌کند که فقه اسلامی، از ظرفیت‌های گسترده و منسجمی برای حمایت از حریم خصوصی برخوردار است، اما این ظرفیت‌ها در قوانین کیفری کشورهای اسلامی به‌طور کامل بازتاب نیافته‌اند.

رحمان[5] (۲۰۲۲)، در پژوهش خود با عنوان «قانون‌گذاری جرائم سایبری در کشورهای با اکثریت مسلمان: تحلیلی‌تطبیقی»[6] بیان می‌کند که قوانین جرائم رایانه‌ای در کشورهای اسلامی ازنظر ساختار، دامنه شمول و نوع ضمانت اجرا تفاوت‌های چشمگیری دارند و این عدم هماهنگی، مانعی جدی در مسیر ایجاد یک نظام حمایتی مؤثر برای حریم خصوصی دیجیتال به شمار می‌آید.

خان[7] (۲۰۲۱)، در پژوهش خود با عنوان «حقوق سایبری و حمایت از حریم خصوصی در جهان اسلام»[8] بیان می‌کند که کشورهای اسلامی در مواجهه با تهدیدات دیجیتال، بیشتر رویکردی واکنشی و موردی اتخاذ کرده‌اند تا رویکردی مبتنی بر اصول و چارچوب‌های نظری منسجم.

---

1. Bygrave
2. Data Privacy Law: An International Perspective.
3. Al-Daraiseh
4. Privacy and Cybercrime in Islamic Law.
5. Rahman
6. Cybercrime Legislation in Muslim-Majority Countries: A Comparative Analysis.
7. Khan
8. Cyber Law and Privacy Protection in the Muslim World.

رایت و دهرت[1] (۲۰۲۰)، در پژوهش خود با عنوان «دستنامه پژوهشی حقوق حریم خصوصی و حفاظت از داده‌ها»[2] بیان کرده‌اند که تحول فناوری‌های نوین ابعاد کاملاً جدید و پیچیده‌ای از نقض حریم خصوصی را ایجاد کرده است؛ ابعادی که قوانین سنتی توان پاسخ‌گویی مؤثر به آن‌ها را ندارند.

حسینی (۱۴۰۰)، در پژوهش خود با عنوان «فقه و حقوق حریم خصوصی در فضای مجازی» چنین بیان کرده است که قواعد فقهی مانند لاضرر، سلطنت و حرمت تجسس، ظرفیت‌های گسترده‌ای برای حمایت از حریم خصوصی دیجیتال دارند. یافته‌های این پژوهش نشان می‌دهد که چنین رویکردی در فقه اسلامی نیز قابل تحقق است، زیرا این فقه با برخورداری از قواعدی مانند حرمت تجسس، لاضرر، احترام به کرامت انسانی و حرمت افشای اسرار، ظرفیت ارائه چارچوب نظری مستحکم برای حمایت کیفری از حریم خصوصی دیجیتال را دارا است.

منصور[3] (۲۰۲۳)، در پژوهش خود با عنوان «امنیت سایبری و حمایت از حریم خصوصی در نظام‌های حقوقی اسلامی»[4] بیان می‌کند که نظام‌های حقوقی کشورهای اسلامی در حوزه امنیت سایبری و حریم خصوصی فاقد یک چارچوب واحد، هماهنگ و اصول‌محور هستند و این پراکندگی موجب ضعف جدی در مقابله با تهدیدات دیجیتال شده است.

پژوهش‌های پیشین به موضوعاتی مانند حمایت از داده‌های شخصی، تحلیل قوانین جرائم رایانه‌ای در کشورهای اسلامی، ظرفیت‌های فقهی در حوزه حریم خصوصی یا چالش‌های نوپدید فضای دیجیتال پرداخته درحالی‌که پژوهش حاضر تلاش می‌کند چارچوبی یکپارچه ارائه دهد که در آن، مبانی فقه اسلامی به‌عنوان پشتوانه نظری حمایت کیفری از حریم خصوصی دیجیتال تبیین شده و سپس میزان انطباق و بهره‌گیری قوانین کیفری کشورهای اسلامی از این مبانی بررسی می‌شود.

1. Wright & De Hert
2. Research Handbook on Privacy and Data Protection Law.
3. Mansoor
4. Cybersecurity and Privacy Protection in Islamic Legal Systems.

۲. مفهوم‌شناسی

در این بخش از پژوهش، به بررسی مفهوم‌شناسی خواهیم پرداخت تا مفاهیم بنیادینی مانند حریم خصوصی دیجیتال، داده شخصی، حمایت کیفری و مبانی فقهی مرتبط با آن‌ها به‌صورت دقیق و منسجم تبیین شود. هدف از این بخش، ایجاد چارچوب مفهومی روشن و یکپارچه‌ای است که بتواند مبنای تحلیل‌های فقهی و تطبیقی در ادامه پژوهش قرار گیرد و از هرگونه ابهام در برداشت‌های نظری جلوگیری کند.

۲-۱. حریم خصوصی دیجیتال

حریم خصوصی دیجیتال در ادبیات حقوقی معاصر به مجموعه‌ای از حقوق و آزادی‌های فردی اطلاق می‌شود که به افراد امکان می‌دهد بر گردآوری، پردازش، ذخیره‌سازی و انتشار داده‌های شخصی خود در محیط‌های الکترونیکی کنترل داشته باشند؛ مفهومی که با گسترش فناوری‌های ارتباطی و ظهور پلتفرم‌های داده‌محور، ابعاد پیچیده‌تری یافته و از سطح «حریم فیزیکی» به «حریم داده‌ای» تحول یافته است (Westin, 2020: 19). در نظام‌های حقوقی کشورهای اسلامی، این مفهوم علاوه‌بر مبانی حقوقی، ریشه در اصول فقهی همچون حرمت تجسس، حرمت افشای اسرار و قاعده لاضرر دارد که همگی بر ضرورت صیانت از حیثیت، کرامت و اطلاعات شخصی افراد تأکید می‌کنند (حسینی، ۱۴۰۰: ۳۸). از سوی دیگر، تجسس دیجیتال به هرگونه دسترسی، ردیابی، نظارت یا جمع‌آوری اطلاعات شخصی افراد از طریق ابزارهای الکترونیکی بدون رضایت آنان اطلاق می‌شود؛ رفتاری که در ادبیات حقوق کیفری به‌عنوان یکی از مهم‌ترین مصادیق نقض حریم خصوصی شناخته می‌شود (Lyon, 2021: 52).

این نوع تجسس می‌تواند شامل شنود الکترونیکی، ردیابی موقعیت، تحلیل رفتار کاربران، استخراج کلان داده و نظارت مبتنی بر هوش مصنوعی باشد و به دلیل ماهیت پنهان و گسترده خود، تهدیدی جدی برای آزادی‌های فردی محسوب می‌شود (Zuboff, 2020: 147). در فقه اسلامی، تجسس به‌طور کلی ممنوع دانسته شده و بر اساس آیات و روایات، هرگونه تلاش برای کشف اسرار پنهان افراد بدون مجوز شرعی، تجاوز به حریم خصوصی تلقی می‌شود (موسوی، ۱۳۹۹: ۷۴). بااین‌حال، فقها استثنائاتی را برای این

ممنوعیت قائل شده‌اند که ازجمله آن‌ها می‌توان به نظارت بر کارگزاران حکومتی و مسئولان (برای جلوگیری از فساد و حفظ امانت‌داری)، تجسس در جهت حفظ نظام اسلامی و امنیت عمومی، تحقیقات قضایی با مجوز مرجع صالح و موارد اضطراری برای دفع خطر اشاره کرد (مجلسی، ۱۴۰۳: ج ۶۲، ۲۱۸). این استثنائات نشان می‌دهد که حریم خصوصی در فقه اسلامی، مطلق و بدون قید نیست و در مواردی که مصلحت بالاتر اسلامی اقتضا کند، محدودیت‌هایی بر آن اعمال می‌شود. در حقوق کیفری کشورهای اسلامی نیز هرچند تلاش‌هایی برای جرم‌انگاری رفتارهای مرتبط با تجسس دیجیتال صورت گرفته، اما همچنان ابهام در تعریف داده شخصی، گستره نظارت مجاز و حدود مسئولیت کیفری، مانع از تحقق حمایت کیفری مؤثر است (Bygrave, 2021: 63). بنابراین، مفهوم‌شناسی دقیق این دو واژه نه‌تنها برای تحلیل فقهی و حقوقی ضروری است، بلکه مبنای ارزیابی تطبیقی قوانین کشورهای اسلامی در حوزه حریم خصوصی دیجیتال نیز محسوب می‌شود.

۲-۲. تجسس دیجیتال

تجسس دیجیتال به هرگونه رصد، پایش، گردآوری، تحلیل یا استخراج اطلاعات شخصی افراد از طریق ابزارهای الکترونیکی بدون رضایت آگاهانه آنان اطلاق می‌شود؛ مفهومی که با گسترش فناوری‌های هوشمند، ابعاد پیچیده‌تری یافته است (Lyon, 2021: 52). در این نوع تجسس، داده‌های کاربران از طریق ابزارهای مختلف مانند ردیاب‌های موقعیتی، شنود الکترونیکی، تحلیل رفتار آنلاین، الگوریتم‌های پیش‌بینی‌گر و سامانه‌های تشخیص الگو جمع‌آوری می‌شوند. این ابزارها امکان مداخله عمیق و همه‌جانبه در زندگی خصوصی افراد را فراهم می‌کنند. «ردیاب‌های موقعیتی» موقعیت جغرافیایی کاربر را از طریق GPS یا شبکه‌های موبایل ثبت می‌کنند. شنود الکترونیکی هم شامل استراق سمع مکالمات تلفنی، پیامک‌ها و ارتباطات اینترنتی بدون مجوز است. تحلیل رفتار آنلاین نیز به بررسی الگوهای جستجو، مرور وب و تعاملات کاربر در فضای مجازی پرداخته و الگوریتم‌های پیش‌بینی‌گر با تحلیل داده‌های گذشته، رفتار و ترجیحات آینده کاربر را پیش‌بینی می‌کنند، همچنین سامانه‌های تشخیص الگو هم با بهره‌گیری از هوش

مصنوعی، الگوهای رفتاری و ویژگی‌های خاص افراد را شناسایی می‌نمایند (Zuboff, 2020: 147). تجسس دیجیتال یکی از مهم‌ترین مصادیق نقض حریم خصوصی محسوب می‌شود، زیرا نه‌تنها به دسترسی غیرمجاز به داده‌های شخصی منجر می‌شود، بلکه با تحلیل و ترکیب داده‌ها، امکان کشف الگوهای رفتاری، باورها، روابط و حتی گرایش‌های فردی را فراهم می‌سازد (Andrejevic, 2020: 33). بسیاری از نظام‌های حقوقی جهان تلاش کرده‌اند با جرم‌انگاری دسترسی غیرمجاز، شنود الکترونیکی، رهگیری داده‌ها و افشای اطلاعات، با این پدیده مقابله کنند، اما سرعت تحول فناوری موجب شده که قوانین موجود در بسیاری از کشورها ناکافی یا فاقد شفافیت لازم باشند (Bygrave, 2021: 63).

در کشورهای اسلامی، تجسس دیجیتال علاوه‌بر بعد حقوقی، بعد فقهی نیز دارد؛ زیرا بر اساس مبانی فقه اسلامی، هرگونه تلاش برای کشف اسرار پنهان افراد بدون مجوز شرعی، مصداق بارز تجسس و به‌طور مطلق ممنوع است (موسوی، ۱۳۹۹: ۷۴). این ممنوعیت نه‌تنها شامل تجسس فیزیکی، بلکه شامل هر نوع نظارت الکترونیکی، شنود، ردیابی یا تحلیل داده نیز می‌شود، زیرا ملاک حرمت، تجاوز به حریم خصوصی و نقض کرامت انسانی است (حسینی، ۱۴۰۰: ۴۲). بنابراین، تجسس دیجیتال مفهومی چندبعدی است که در تقاطع فناوری، حقوق کیفری و فقه اسلامی قرار می‌گیرد و فهم دقیق آن برای تحلیل حمایت کیفری از حریم خصوصی دیجیتال در کشورهای اسلامی ضروری است.

۲-۳. نظارت دیجیتال

نظارت دیجیتال به مجموعه‌ای از فرایندها و فناوری‌ها و سازوکارهایی اطلاق می‌شود که با هدف جمع‌آوری، پردازش، تحلیل یا پایش داده‌های افراد در محیط‌های الکترونیکی به‌کار می‌رود. تفاوت اساسی نظارت دیجیتال با تجسس دیجیتال در میزان آشکار بودن آن بوده به طوری که نظارت می‌تواند آشکار باشد مانند دوربین‌های مداربسته در اماکن عمومی درحالی‌که تجسس دیجیتال همواره پنهان و بدون اطلاع کاربر صورت می‌گیرد. همچنین، نظارت دیجیتال ممکن است با مجوز قانونی و در چارچوب ضوابط مشخص انجام شود، اما تجسس دیجیتال فاقد مجوز شرعی یا قانونی است. می‌توان گفت نظارت دیجیتال می‌تواند

برای امنیت، مدیریت یا ارائه خدمات باشد، حال آنکه تجسس دیجیتال با هدف کشف اسرار و نقض حریم خصوصی افراد انجام می‌شود. نظارت دیجیتال طیف گسترده‌ای از فعالیت‌ها از قبیل ردیابی موقعیت مکانی کاربران توسط اپلیکیشن‌ها، پایش رفتارهای آنلاین در شبکه‌های اجتماعی، تحلیل الگوریتمی داده‌های کلان، شنود دیجیتال، استخراج الگوهای رفتاری و حتی پیش‌بینی تصمیمات افراد بر اساس ردپای دیجیتال آنان را در برمی‌گیرد.

نظارت دیجیتال زمانی واجد اهمیت کیفری می‌شود که بدون رضایت آگاهانه، بدون مجوز قانونی یا با هدف نقض حریم خصوصی انجام گیرد و به کشف امور پنهان، افشای داده‌های حساس، دستکاری اطلاعات یا ایجاد آسیب‌های حیثیتی و روانی منجر شود (Andrejevic, 2020: 44). در فضای فقهی این مفهوم با اصولی همچون حرمت تجسس، حرمت افشای اسرار و احترام به کرامت انسانی پیوند می‌خورد و از این منظر، هرگونه نظارت پنهان یا غیرمجاز مصداق روشن هتک حرمت و تجاوز به حریم خصوصی تلقی می‌شود. در قوانین کیفری کشورهای اسلامی نیز نظارت دیجیتال در قالب جرم‌انگاری رفتارهایی مانند شنود الکترونیکی، ردیابی غیرمجاز، پایش ارتباطات، دسترسی به داده‌های در حال انتقال و استفاده غیرمجاز از ابزارهای نظارتی مورد توجه قرار گرفته است، هرچند گستره و شدت این جرم‌انگاری در کشورها متفاوت است (Greenleaf, 2021: 73).

اهمیت این مفهوم در آن است که بسیاری از تعرضات نوپدید به حریم خصوصی، نه از طریق نفوذ مستقیم به سامانه‌ها، بلکه از طریق پایش مستمر، تحلیل رفتاری و جمع‌آوری تدریجی داده‌ها رخ می‌دهد؛ به‌گونه‌ای که فرد حتی بدون آگاهی از فرآیند نظارت، در معرض نقض حریم خصوصی قرار می‌گیرد. ازاین‌رو، فهم دقیق نظارت دیجیتال و پیامدهای آن برای حقوق کیفری، فقه اسلامی و سیاست‌گذاری تقنینی کشورهای اسلامی ضروری است؛ زیرا بدون تحلیل این مفهوم، امکان طراحی نظام کیفری کارآمد برای مواجهه با تهدیدات پیچیده عصر داده فراهم نخواهد شد.

۲-۴. نظارت الگوریتمی و ردیابی هوشمند

نظارت الگوریتمی به فرآیند نظام‌مند جمع‌آوری، پردازش و تحلیل داده‌های رفتاری کاربران توسط الگوریتم‌های رایانه‌ای بدون نیاز به دخالت مستقیم انسانی اطلاق می‌شود (لیون، ۲۰۰۷: ۱۴). زوبوف نظارت الگوریتمی را شکل نوینی از سرمایه‌داری نظارتی می‌داند که در آن داده‌های شخصی به ابزار تولید ارزش تبدیل شده و قدرت پیش‌بینی و تأثیرگذاری بر رفتار افراد را فراهم می‌آورد (Zuboff, 2019: 7). سولوو با اشاره به گسترش فناوری‌های دیجیتال، نظارت را تهدیدی جدی برای حریم خصوصی دانسته که نیازمند بازنگری در مفاهیم سنتی حمایت از داده‌ها است (Solove, 2008: 14).

ردیابی هوشمند به معنای پایش مداوم و خودکار موقعیت مکانی، فعالیت‌ها و عادات رفتاری افراد از طریق دستگاه‌های هوشمند، حسگرها و اپلیکیشن‌ها است (نیسن‌بام، ۲۰۱۰: ۱۲۵). ریچاردز ردیابی دیجیتال را نوعی «نظارت دقیق» توصیف می‌کند که امکان دسترسی به جزئی‌ترین جنبه‌های زندگی افراد را فراهم می‌آورد (Richards, 2013: 1894). در فقه اسلامی، مفهوم حریم خصوصی از قواعد «حرمت تجسس» (کلینی، ۱۴۰۷: ج ۵، ۱۰۹) و «لاضرر» (شیخ طوسی، ۱۳۹۰: ۲۱۸) استنباط می‌شود که مبنای فقهی مناسبی برای حمایت از این مفاهیم در فضای دیجیتال فراهم می‌آورد.

۲-۵. تحلیل پیش‌بینانه رفتار کاربران

تحلیل پیش‌بینانه رفتار کاربران به فرآیند استفاده از تکنیک‌های آماری، الگوریتم‌های یادگیری ماشین و روش‌های داده‌کاوی برای تحلیل داده‌های تاریخی و پیش‌بینی رفتار و اقدامات آینده کاربران اطلاق می‌شود (Siegel, 2013: 15). نیل با اشاره به کاربرد گسترده این فناوری در پلتفرم‌های دیجیتال، تحلیل پیش‌بینانه را ابزاری برای پیش‌بینی نتایج آینده بر اساس داده‌های گذشته تعریف می‌کند (O'Neil, 2016: 21). کرنز وراث تأکید می‌کنند که این روش‌ها فراتر از تحلیل ساده آماری عمل کرده و با پردازش حجم انبوه داده‌های کاربران، الگوهای پنهان رفتاری را کشف و رفتار آینده آن‌ها را پیش‌بینی می‌کنند. نویسندگان تحلیل پیش‌بینانه را شکلی از «علم داده‌های بزرگ» می‌دانند که با استخراج الگوهای رفتاری از مجموعه داده‌های

عظیم، امکان پیش‌بینی و دستکاری رفتار جمعی را فراهم می‌آورد (Boyd & Crawford, 2012: 662). برخی دیگر این پدیده را تهدیدی علیه خودمختاری کاربران دانسته که در آن افراد بدون آگاهی از نحوه تصمیم‌سازی الگوریتم‌ها، تحت تأثیر پیش‌بینی‌های نادرست یا تبعیض‌آمیز قرار می‌گیرند (Tufekci, 2014: 42).

۳. حمایت کیفری از حریم خصوصی دیجیتال در فقه اسلامی

در این بخش، به تبیین مبانی فقهیِ مرتبط با صیانت از حریم خصوصی دیجیتال خواهیم پرداخت و نشان می‌دهیم که چگونه اصول و قواعد و نصوص معتبر فقه اسلامی می‌توانند پشتوانه نظری و عملی برای جرم‌انگاری تعرضات نوپدید در فضای مجازی فراهم کنند. همچنین تلاش می‌شود ظرفیت‌ها و حدود این مبانی در مواجهه با فناوری‌های جدید روشن شود تا چارچوبی منسجم برای تحلیل‌های تطبیقی بخش‌های بعدی شکل گیرد.

۳-۱. مبانی قرآنی و روایی حمایت از حریم خصوصی

۳-۲. قواعد فقهی مرتبط با حمایت از حریم خصوصی دیجیتال

مبانی قرآنی و روایی فقه اسلامی، یکی از استوارترین پشتوانه‌های نظری برای حمایت از حریم خصوصی به شمار می‌رود و بر اساس این مبانی، صیانت از اسرار، منع تجسس و احترام به کرامت انسانی از اصول قطعی شریعت محسوب می‌شود. قرآن کریم در آیه «وَلَا تَجَسَّسُوا» به‌صراحت هرگونه تلاش برای کشف امور پنهان افراد را ممنوع کرده و این حکم، به‌عنوان یک قاعده عام، شامل همه انواع نظارت و دسترسی غیرمجاز می‌شود (طباطبایی، ۱۳۷۴: ۳۶۵). افزون بر این، آیه «لَا تَدْخُلُوا بُيُوتًا غَيْرَ بُيُوتِكُمْ» نیز بر ضرورت رعایت حریم خصوصی و کسب رضایت پیش از ورود به حریم دیگران تأکید دارد و فقها این حکم را به هر نوع ورود به حریم اطلاعاتی افراد نیز تسری داده‌اند (مکارم شیرازی، ۱۴۰۰: ۲۱۲). در روایات نیز تأکیدات فراوانی بر حرمت افشای اسرار و نکوهش شدید تجسس وجود دارد؛ ازجمله روایت نبوی که می‌فرماید: «مَن تَتَبَّعَ عَورَةَ المُسلِمِ تَتَبَّعَ اللهُ عَورَتَهُ» که نشان دهنده شدت حرمت تجاوز به حریم خصوصی است (حرعاملی،

۱۴۱۴: ۴۹۸). فقهای معاصر نیز با استناد به این نصوص، تجسس الکترونیکی، شنود، ردیابی و دسترسی غیرمجاز به داده‌ها را مصداق روشن نقض حریم خصوصی دانسته‌اند و آن را مشمول قواعدی مانند لاضرر و حرمت ایذاء می‌دانند (Sachedina, 2018: 74). بنابراین، مبانی قرآنی و روایی فقه اسلامی ظرفیت گسترده‌ای برای حمایت کیفری از حریم خصوصی دیجیتال فراهم می‌کند و می‌تواند پشتوانه‌ای نظری برای جرم‌انگاری تعرضات نوپدید در فضای مجازی باشد.

قواعد فقهی در فقه اسلامی نقش بنیادینی در تبیین حدودوثغور حمایت از حریم خصوصی دیجیتال دارند و می‌توانند مبنای جرم‌انگاری رفتارهای نوپدید در فضای مجازی قرار گیرند. یکی از مهم‌ترین این قواعد، قاعده حرمت تجسس است که بر اساس آن هرگونه تلاش برای کشف امور پنهان افراد بدون مجوز شرعی ممنوع بوده و فقها این حکم را به نظارت الکترونیکی، شنود، ردیابی و دسترسی غیرمجاز به داده‌ها نیز تسری داده‌اند (نجفی، ۱۴۰۲: ۲۸۱). قاعده لاضرر نیز با تأکید بر منع هرگونه ضرر و زیان ناروا، هر نوع تعرض به داده‌های شخصی را که موجب آسیب حیثیتی، مالی یا روانی شود، ممنوع می‌داند و این قاعده ظرفیت گسترده‌ای برای حمایت کیفری از داده‌های دیجیتال فراهم می‌کند (انصاری، ۱۴۱۵ق: ۳۴۵).

قاعده سلطنت که بر مالکیت و اختیار انسان بر مال و حقوق خود تأکید دارد، در عصر دیجیتال به‌گونه‌ای تفسیر شده که داده‌های شخصی نیز نوعی «حق اختصاص» محسوب می‌شوند و هرگونه تصرف بدون رضایت، تجاوز به سلطنت فرد بر اطلاعاتش است (شهیدی، ۱۳۹۷: ۹۹). همچنین قاعده احترام که بر حرمت جان، مال و آبروی مؤمن تأکید دارد، به‌طور مستقیم نقض حریم خصوصی دیجیتال را مصداق هتک حرمت می‌داند (فاضل لنکرانی، ۱۴۲۱ق: ۲۲۱). افزون بر این، قاعده منع ایذاء نیز هرگونه آزار و اذیت را ممنوع می‌سازد و می‌تواند مبنای جرم‌انگاری رفتارهای نوین باشد (Sachedina, 2018: 81). مجموع این قواعد نشان می‌دهد که فقه اسلامی ظرفیت گسترده و منسجمی برای حمایت کیفری از حریم خصوصی دیجیتال دارد و می‌تواند پشتوانه‌ای نظری برای قوانین کشورهای اسلامی باشد.

۳-۳. مصادیق تعرض به حریم خصوصی در فضای دیجیتال از منظر فقه اسلامی

از منظر فقه اسلامی، مصادیق تعرض به حریم خصوصی در فضای دیجیتال را می‌توان با تکیه بر اصول و قواعد قطعی شریعت شناسایی کرد؛ زیرا هر رفتاری که منجر به کشف اسرار، هتک حیثیت یا دسترسی غیرمجاز به اطلاعات افراد شود، مشمول عنوان «تجسس» یا «هتک حرمت» قرار می‌گیرد. یکی از مهم‌ترین مصادیق، دسترسی غیرمجاز به داده‌های شخصی است. در فقه اسلامی، هرگونه تصرف در مال یا حق دیگری بدون مجوز شرعی، تجاوز به سلطنت و مالکیت فرد محسوب می‌شود. برخی فقهای معاصر با استناد به قاعده «لاضرر» و «حرمت تجسس»، دسترسی غیرمجاز به داده‌های شخصی را نوعی تجاوز به حق اختصاصی فرد بر اطلاعاتش دانسته‌اند (خوئی، ۱۴۲۲ق: ۳۹۱). شنود و رهگیری الکترونیکی نیز از مصادیق روشن تجسس محسوب می‌شود؛ زیرا مطابق نصوص روایی، استراق سمع مصداق بارز هتک حرمت مؤمن است (کلینی، ۱۴۰۷ق: ۵۸). افشای داده‌ها و انتشار تصاویر خصوصی نیز در فقه اسلامی تحت عنوان «افشاء سرّ» و «هتک عرض» قرار می‌گیرد و فقها آن را از شدیدترین انواع تجاوز به حریم خصوصی دانسته‌اند (موسوی بجنوردی، ۱۴۱۹ ق: ۲۴۴).

ردیابی موقعیت مکانی و تحلیل رفتار دیجیتال نیز با ملاک حرمت تجسس و منع تتبع عورات، ممنوع تلقی می‌شود. استدلال این ممنوعیت آن است که رفتار دیجیتال افراد شامل الگوهای خرید، مرور وب، تعاملات اجتماعی و عادات روزانه بخشی از زندگی خصوصی محسوب می‌شود که افراد قصد پنهان داشتن آن را دارند. همچنین تحلیل این رفتارها از طریق الگوریتم‌ها و داده‌کاوی، نوعی کشف تدریجی و پنهانی امور خصوصی است که بدون اطلاع و رضایت فرد صورت می‌گیرد. نتایج حاصل از این تحلیل‌ها می‌تواند به کشف عادات شخصی، باورها، گرایش‌های سیاسی، مذهبی و جنسی افراد منجر شود که همان «عورات» در اصطلاح فقهی است. بنابراین، ردیابی موقعیت مکانی و تحلیل رفتار دیجیتال بدون رضایت، مصداق تجسس و تتبع عورات محسوب می‌شود (Fadel, 2019: 112). همچنین نفوذ به حساب‌های کاربری، سرقت هویت دیجیتال و دستکاری داده‌ها مصادیقی هستند که فقهای معاصر با استناد به قواعد لاضرر و احترام مال و نفس، آن‌ها را مصداق بارز ظلم و تعدی دانسته‌اند (هاشمی شاهرودی، ۱۴۲۳ق: ۱۸۷). بنابراین، فقه

اسلامی با تکیه بر ملاک‌های کلی و قواعد عام، توانایی شناسایی و جرم‌انگاری مصادیق نوپدید تعرض دیجیتال را دارد و می‌تواند چارچوبی منسجم برای حمایت کیفری از حریم خصوصی در عصر فناوری ارائه دهد.

۳-۴. ظرفیت‌ها و چالش‌های فقه اسلامی در جرم‌انگاری تعرضات دیجیتال

فقه اسلامی در مواجهه با پدیده‌های نوپدید دیجیتال از ظرفیت‌های قابل‌توجهی برخوردار است؛ زیرا قواعد عام و فرازمانی آن امکان تعمیم به مصادیق جدید را فراهم می‌سازد. از مهم‌ترین ظرفیت‌ها، انعطاف‌پذیری قواعد فقهی است؛ قواعدی مانند لاضرر، حرمت تجسس، احترام مال و نفس و قاعده سلطنت، قابلیت آن را دارند که رفتارهای نوینی همچون دسترسی غیرمجاز، شنود الکترونیکی، ردیابی و تحلیل داده را تحت شمول خود قرار دهند (خمینی، ۱۴۰۳ق: ۲۹۱). افزون بر این، توجه فقه اسلامی به کرامت انسانی موجب می‌شود که تعرض به داده‌های شخصی به‌عنوان هتک حرمت و ظلم تلقی شود (مطهری، ۱۳۷۹: ۱۱۲). همچنین اصول عقلایی که در فقه اسلامی پذیرفته شده‌اند، امکان بهره‌گیری از یافته‌های علمی و فناوری را در استنباط احکام فراهم می‌کنند و این امر ظرفیت مهمی برای تنظیم قواعد حمایتی در حوزه دیجیتال است (سبحانی، ۱۴۲۵ق: ۴۵). بااین‌حال، فقه اسلامی در کنار این ظرفیت‌ها با چالش‌هایی نیز روبه‌روست. همچنین ابهام در تعیین ماهیت حقوقی داده‌های شخصی می‌تواند بر تعیین ضمانت اجراهای کیفری تأثیر بگذارد (Fadel, 2021: 67).

چالش دیگر، لزوم بازخوانی مفاهیم سنتی مانند تجسس، افشاء سرّ و هتک عرض در بستر دیجیتال است که نیازمند اجتهاد پویا و هماهنگ با تحولات فناوری است. بنابراین، فقه اسلامی ضمن برخورداری از ظرفیت‌های گسترده برای جرم‌انگاری تعرضات دیجیتال، نیازمند توسعه نظری و اجتهادی برای پاسخ‌گویی دقیق به پیچیدگی‌های عصر داده است.

۴. حمایت کیفری از حریم خصوصی دیجیتال در قوانین کیفری کشورهای اسلامی

در این بخش به تحلیل ساختار تقنینی کشورهای اسلامی در حوزه صیانت از حریم خصوصی دیجیتال خواهیم پرداخت و نشان می‌دهیم که هر نظام حقوقی چگونه از ابزارهای کیفری برای مقابله با تعرضات داده‌ای استفاده کرده است. همچنین تلاش می‌شود با بررسی قوانین موجود، میزان کارآمدی، خلأها و تفاوت‌های رویکردی میان این کشورها روشن شود تا زمینه برای ارزیابی تطبیقی و ارائه الگوی پیشنهادی فراهم گردد.

۴-۱. چارچوب‌های قانونی حمایت از حریم خصوصی دیجیتال

چارچوب‌های قانونی حمایت از حریم خصوصی دیجیتال در کشورهای اسلامی بر پایه مجموعه‌ای از قوانین اساسی، مقررات جرائم رایانه‌ای، قوانین حمایت از داده‌های شخصی و آیین‌نامه‌های مرتبط با ارتباطات الکترونیکی شکل گرفته است و هر کشور با توجه به ساختار حقوقی و سیاست‌های تقنینی خود، سطح متفاوتی از حمایت کیفری را ارائه می‌دهد. در برخی کشورها مانند امارات و عربستان، قوانین جامع حفاظت از داده‌های شخصی تصویب شده که به‌طور مشخص اصولی همچون رضایت، محدودیت پردازش، امنیت داده و مسئولیت‌پذیری را مقرر می‌کند (Alhammadi, 2021: 54). در ایران، چارچوب قانونی بیشتر بر پایه «قانون جرائم رایانه‌ای» (مصوب ۱۳۸۸) و مقررات پراکنده در حوزه ارتباطات و تجارت الکترونیکی استوار است. این قانون رفتارهایی مانند دسترسی غیرمجاز به داده‌ها و سامانه‌های رایانه‌ای (ماده ۱)، شنود غیرمجاز ارتباطات الکترونیکی (ماده ۳)، افشای اطلاعات محرمانه (ماده ۱۱) و اختلال در سامانه‌های رایانه‌ای (ماده ۵) را جرم‌انگاری کرده و مجازات‌های تعزیری برای آن‌ها پیش‌بینی کرده است (جعفری لنگرودی، ۱۳۹۹: ۲۲۱). بااین‌حال، این قانون تعریف مشخصی از «داده شخصی» ارائه نداده و حمایت جامعی از حریم خصوصی دیجیتال به عمل نمی‌آورد.

مالزی نیز با تصویب «قانون حمایت از داده‌های شخصی ۲۰۱۰» یکی از پیشرفته‌ترین نظام‌های حمایتی در جهان اسلام را ایجاد کرده و اصولی مشابه استانداردهای بین‌المللی را پذیرفته است (Hassan, 2020:

87). مصر و قطر نیز با اصلاحات اخیر، مقرراتی درزمینهٔ حفاظت از داده و جرائم سایبری وضع کرده‌اند که به‌طور مستقیم به صیانت از حریم خصوصی دیجیتال می‌پردازد (El-Menshawy, 2022: 133).

با وجود این قوانین، ظرفیت‌های فقه اسلامی می‌تواند در موارد زیر کاربرد داشته باشد: نخست، پر کردن خلأهای قانونی: قوانین موجود عمدتاً از الگوهای غربی الگوبرداری شده‌اند و برخی مصادیق مهم مانند تحلیل پیش‌بینانه، ردیابی هوشمند و نظارت الگوریتمی را پوشش نمی‌دهند. فقه اسلامی با استناد به قواعدی مانند حرمت تجسس و لاضرر می‌تواند مبنای جرم‌انگاری این مصادیق جدید فراهم آورد؛ دوم، تقویت توجیه بومی: بسیاری از این قوانین فاقد پشتوانه فقهی هستند و در صورت بروز اختلاف، استناد به آن‌ها دشوار است. فقه اسلامی مشروعیت شرعی به قوانین می‌بخشد؛ سوم، ایجاد الگوی واحد اسلامی: پراکندگی مقررات در کشورهای اسلامی با بهره‌گیری از اصول مشترک فقهی قابل رفع است؛ چهارم، تقویت ضمانت اجرا: مجازات‌های فقهی مانند تعزیر می‌تواند بازدارندگی بیشتری ایجاد کند؛ پنجم، حمایت از حقوق اقلیت‌های دینی: فقه اسلامی با تکیه بر قاعده «لاضرر» حتی غیرمسلمانان را نیز تحت حمایت قرار می‌دهد (Al-Daraiseh, 2021: 102). بنابراین، چارچوب‌های قانونی کشورهای اسلامی ترکیبی از پیشرفت‌های قابل توجه و خلأهای ساختاری است که نیازمند تحلیل تطبیقی دقیق برای ارائه الگوی واحد حمایت کیفری از حریم خصوصی دیجیتال است.

۴-۲. مصادیق جرم‌انگاری تعرض به حریم خصوصی دیجیتال

نظام‌های کیفری کشورهای اسلامی در سال‌های اخیر تلاش کرده‌اند مصادیق تعرض به حریم خصوصی دیجیتال را در قالب قوانین جرائم رایانه‌ای، مقررات ارتباطات الکترونیکی و قوانین حمایت از داده‌های شخصی جرم‌انگاری کنند و هر کشور با توجه به ساختار تقنینی خود، دامنه متفاوتی از این مصادیق را شناسایی کرده است. یکی از مهم‌ترین مصادیق مشترک، دسترسی غیرمجاز به داده‌ها و سامانه‌های رایانه‌ای است که در قوانین ایران، امارات، مالزی و عربستان به‌عنوان جرم مستقل شناخته شده و برای آن مجازات‌های کیفری تعیین شده است (Al-Mutairi, 2020: 61). شنود و رهگیری الکترونیکی نیز در اغلب کشورهای اسلامی

جرم‌انگاری شده و هرگونه استراق سمع، ضبط یا انتقال غیرمجاز داده‌های در حال انتقال، مشمول مجازات است (Rahman, 2021: 94). افشای غیرمجاز داده‌های شخصی از دیگر مصادیق مهم است که در قوانین ایران، قطر و مالزی به‌طور صریح جرم تلقی شده و حتی در برخی کشورها، مسئولیت کیفری برای کارکنان نهادهای دولتی نیز پیش‌بینی شده است (Hassan, 2020: 112).

نشر تصاویر خصوصی، سرقت هویت دیجیتال و جعل رایانه‌ای نیز در بسیاری از نظام‌های کیفری اسلامی جرم‌انگاری شده و به‌عنوان مصادیق بارز تعرض به حریم خصوصی شناخته می‌شوند (El-Menshawy, 2022: 147). در برخی کشورها مانند امارات و عربستان، ردیابی موقعیت مکانی و پایش رفتار دیجیتال بدون رضایت نیز جرم محسوب می‌شود و این نشان دهنده توسعه‌یافتگی تقنینی در حوزه داده‌محور است (Alhammadi, 2021: 73). با وجود این، نقدهای اساسی بر وضعیت فعلی وارد است: نخست، پراکندگی مقررات: هر کشور قانون جداگانه‌ای با تعاریف متفاوت از داده شخصی دارد و قانون واحد حاکم بر حمایت از حریم خصوصی دیجیتال در جهان اسلام وجود ندارد؛ دوم، ابهام در تعریف داده شخصی: برخی قوانین تنها داده‌های مالی را تعریف می‌کنند و داده‌های سلامت، بیومتریک و ژنتیکی را در بر نمی‌گیرند؛ سوم، ضعف ضمانت اجرا: مجازات‌های تعیین شده در اغلب کشورها بازدارندگی کافی ندارند و جرائم با فناوری بالا با مجازات‌های خفیف‌تری مواجه‌اند؛ چهارم، فقدان نهاد مستقل نظارتی: بسیاری از کشورها فاقد مرجع مستقل برای نظارت بر جمع‌آوری و پردازش داده‌ها هستند؛ پنجم، ناهماهنگی با فقه اسلامی: قوانین عمدتاً از الگوهای غربی الگوبرداری شده‌اند و از ظرفیت‌های فقهی برای توجیه و تقویت این قوانین بهره‌گیری نشده است. این نقدها نشان می‌دهد که نظام‌های کیفری اسلامی نیازمند بازنگری جامع برای تحقق حمایت کیفری مؤثر از حریم خصوصی دیجیتال هستند.

۴-۳. مقایسه تطبیقی رویکرد کشورهای اسلامی در حمایت کیفری از داده‌های شخصی

رویکرد کشورهای اسلامی در حمایت کیفری از داده‌های شخصی، با وجود اشتراک در مبانی ارزشی و اخلاقی، ازنظر ساختار تقنینی و دامنه جرم‌انگاری تفاوت‌های قابل‌توجهی دارد. در کشورهایی مانند مالزی،

قانون حمایت از داده‌های شخصی ۲۰۱۰ چارچوبی جامع و مبتنی بر اصول بین‌المللی ارائه کرده و برای نقض اصولی مانند رضایت، امنیت داده و محدودیت پردازش، ضمانت اجراهای کیفری مشخصی پیش‌بینی کرده است (Hassan, 2020: 134). امارات متحده عربی نیز با تصویب قانون ۲۰۲۱ حفاظت از داده‌ها، یکی از پیشرفته‌ترین نظام‌های داده‌محور در جهان اسلام را ایجاد کرده و برای افشای غیرمجاز داده‌های حساس، مجازات‌های سنگین مقرر کرده است (Alhammadi, 2021: 92). در مقابل، کشورهایی مانند ایران و مصر بیشتر بر قوانین جرائم رایانه‌ای تکیه دارند و حمایت کیفری از داده‌های شخصی را در قالب جرم‌انگاری رفتارهایی مانند دسترسی غیرمجاز، شنود و افشای داده دنبال می‌کنند، بدون آنکه قانون جامع حفاظت از داده داشته باشند (El-Menshawy, 2022: 158).

عربستان سعودی نیز با اصلاحات اخیر، رویکردی سخت‌گیرانه اتخاذ کرده و برای نقض امنیت داده‌ها و افشای اطلاعات حساس، مجازات‌های شدید پیش‌بینی کرده است (Al-Daraiseh, 2021: 119). تفاوت مهم دیگر، تعریف داده شخصی و داده حساس است که در برخی کشورها مانند مالزی و امارات دقیق و مطابق استانداردهای بین‌المللی است، اما در کشورهایی مانند ایران همچنان ابهام دارد (Rahman, 2021: 77). این تفاوت‌ها نشان می‌دهد که کشورهای اسلامی در مسیر حمایت کیفری از داده‌های شخصی، رویکردهای متنوعی اتخاذ کرده‌اند و نیازمند همگرایی تقنینی برای مواجهه مؤثر با تهدیدات دیجیتال هستند.

۴-۴. چالش‌ها و کاستی‌های قوانین کیفری کشورهای اسلامی در مواجهه با نقض حریم خصوصی دیجیتال

قوانین کیفری کشورهای اسلامی در مواجهه با نقض حریم خصوصی دیجیتال، با وجود پیشرفت‌های قابل توجه در سال‌های اخیر، همچنان با چالش‌ها و کاستی‌های ساختاری روبه‌رو هستند که کارآمدی حمایت کیفری را محدود می‌کند. یکی از مهم‌ترین چالش‌ها، ابهام در تعریف داده شخصی و داده حساس است. در بسیاری از کشورها، این مفاهیم به‌صورت دقیق و منسجم تعریف نشده و همین امر موجب تفسیرهای متفاوت و گاه متعارض در فرآیند رسیدگی کیفری می‌شود (Al-Khater, 2020: 41). چالش دیگر، پراکندگی تقنینی است؛ به‌گونه‌ای که در کشورهایی مانند ایران و مصر، مقررات مرتبط با حریم خصوصی

دیجیتال در چندین قانون پراکنده است و نبود یک قانون جامع حفاظت از داده، انسجام نظام کیفری را تضعیف می‌کند (El-Desouki, 2021: 93). همچنین، ضعف ضمانت اجراهای کیفری در برخی کشورها موجب شده که مجازات‌ها بازدارندگی کافی نداشته باشند، به‌ویژه در حوزه افشای داده‌های حساس یا ردیابی غیرمجاز (Rahman, 2021: 112). از سوی دیگر، نبود نهادهای مستقل ناظر بر داده در برخی نظام‌های حقوقی، اجرای مؤثر قوانین را با مشکل مواجه کرده و وابستگی نظارت به ساختارهای دولتی، استقلال و بی‌طرفی فرآیند نظارتی را کاهش می‌دهد (Al-Suwaidi, 2022: 67).

چالش مهم دیگر، عدم هماهنگی قوانین کیفری با استانداردهای بین‌المللی است؛ بسیاری از کشورها هنوز اصولی مانند رضایت آگاهانه، محدودیت پردازش و حق دسترسی را به‌طور کامل در قوانین خود نپذیرفته‌اند (Haque, 2020: 58). مجموع این کاستی‌ها نشان می‌دهد که کشورهای اسلامی برای ایجاد نظام کیفری کارآمد در حوزه حریم خصوصی دیجیتال، نیازمند اصلاحات تقنینی، نهادسازی و همگرایی با استانداردهای جهانی هستند.

نتیجه‌گیری

تحولات گسترده در عرصه فناوری اطلاعات و گسترش تعاملات دیجیتال، مفهوم حریم خصوصی را از یک حق سنتی و محدود به فضای فیزیکی، به یک حق پیچیده، چندلایه و داده‌محور تبدیل کرده است؛ حقی که امروز بیش از هر زمان دیگری در معرض تهدیدهای نوپدید قرار دارد. بررسی تطبیقی انجام شده در این پژوهش نشان داد که فقه اسلامی و قوانین کیفری کشورهای اسلامی، هرچند از دو مسیر متفاوت-یکی مبتنی بر نصوص و قواعد فقهی و دیگری مبتنی بر تقنین مدرن- حرکت می‌کنند، اما در هدف نهایی یعنی صیانت از کرامت انسانی و جلوگیری از تعرض به حریم خصوصی دیجیتال، اشتراکات بنیادینی دارند. در بخش فقهی، روشن شد که فقه اسلامی با تکیه بر مبانی قرآنی و روایی، اصولی مانند حرمت تجسس، لاضرر، سلطنت، احترام مال و نفس و منع ایذاء را در اختیار دارد که همگی ظرفیت تعمیم به فضای دیجیتال را دارند.

این قواعد، با وجود آنکه در عصر پیشامدرن شکل گرفته‌اند، به دلیل ماهیت عقلایی و فرازمانی خود، توانایی پاسخ‌گویی به مسائل نوپدیدی مانند دسترسی غیرمجاز، شنود الکترونیکی، افشای داده، ردیابی موقعیت و تحلیل رفتاری را دارا هستند. همچنین، فقه اسلامی با تأکید بر کرامت انسانی و حرمت هتک عرض، چارچوبی اخلاقی و حقوقی فراهم می‌کند که می‌تواند پشتوانه‌ای قوی برای جرم‌انگاری تعرضات دیجیتال باشد. بااین‌حال، چالش‌هایی مانند نبود نصوص خاص درباره فناوری‌های نوین، ابهام در ماهیت حقوقی داده‌ها و ضرورت بازخوانی مفاهیم سنتی در بستر دیجیتال، نشان می‌دهد که فقه اسلامی نیازمند توسعه نظری و اجتهاد پویا برای مواجهه دقیق‌تر با پیچیدگی‌های عصر داده است. در بخش تطبیقی نیز روشن شد که کشورهای اسلامی در مسیر حمایت کیفری از حریم خصوصی دیجیتال، رویکردهای متفاوتی اتخاذ کرده‌اند. برخی کشورها مانند مالزی، امارات و عربستان با تصویب قوانین جامع حفاظت از داده‌های شخصی، ساختارهای پیشرفته و نزدیک به استانداردهای بین‌المللی ایجاد کرده‌اند.

این کشورها اصولی مانند رضایت آگاهانه، محدودیت پردازش، امنیت داده و مسئولیت‌پذیری را به‌طور دقیق تنظیم کرده و برای نقض آن‌ها ضمانت اجراهای کیفری مشخصی پیش‌بینی کرده‌اند. در مقابل، کشورهایی مانند ایران و مصر بیشتر بر قوانین جرائم رایانه‌ای تکیه دارند و حمایت کیفری از داده‌های شخصی را در قالب جرم‌انگاری رفتارهای خاص دنبال می‌کنند، بدون آنکه قانون جامع داده‌محور داشته باشند. این تفاوت‌ها نشان می‌دهد که جهان اسلام در مرحله گذار از «حمایت کیفری پراکنده» به «حمایت کیفری نظام‌مند» قرار دارد. تحلیل تطبیقی نشان داد که چالش‌های مشترکی نیز میان کشورهای اسلامی وجود دارد؛ ازجمله ابهام در تعریف داده شخصی و داده حساس، پراکندگی تقنینی، ضعف ضمانت اجراها، نبود نهادهای مستقل ناظر بر داده و عدم هماهنگی با استانداردهای بین‌المللی. این چالش‌ها موجب شده که حمایت کیفری از حریم خصوصی دیجیتال در برخی کشورها ناکافی، غیرمنسجم یا فاقد بازدارندگی لازم باشد. در مقابل، ظرفیت‌های قابل توجهی نیز وجود دارد؛ ازجمله پشتوانه‌های فقهی غنی، تجربه کشورهای پیشرو در جهان اسلام و امکان همگرایی تقنینی در حوزه داده‌محور.

در مجموع، یافته‌های این پژوهش نشان می‌دهد که ترکیب ظرفیت‌های فقه اسلامی با الگوهای تقنینی کشورهای پیشرو اسلامی می‌تواند به ایجاد یک چارچوب جامع و منسجم و کارآمد برای حمایت کیفری از حریم خصوصی دیجیتال منجر شود. این چارچوب باید بر اصولی مانند کرامت انسانی، منع تجسس، رضایت آگاهانه، امنیت داده، شفافیت پردازش و مسئولیت‌پذیری استوار باشد. همچنین، ایجاد نهادهای مستقل ناظر بر داده، تدوین قوانین جامع حفاظت از داده و هماهنگی با استانداردهای بین‌المللی، از ضرورت‌های اجتناب‌ناپذیر برای ارتقای سطح حمایت کیفری در کشورهای اسلامی است. بنابراین، آینده حمایت کیفری از حریم خصوصی دیجیتال در جهان اسلام، در گرو اجتهاد پویا، تقنین هوشمند و همگرایی منطقه‌ای است؛ مسیری که می‌تواند ضمن حفظ ارزش‌های اسلامی، پاسخگوی چالش‌های پیچیده عصر دیجیتال باشد.

فهرست منابع

انصاری، مرتضی (۱۴۱۵ ق). **المکاسب**. قم: مؤسسه النشر الاسلامی.

جعفری لنگرودی، محمدجعفر (۱۳۹۹). **ترمینولوژی حقوق**. تهران: گنج دانش.

حر عاملی، محمدبن‌حسن (۱۴۱۴ ق). **وسائل الشیعة**. قم: مؤسسه آل‌البیت (ع).

حسینی، محمد (۱۴۰۰). **فقه حریم خصوصی در عصر دیجیتال**. قم: پژوهشگاه فرهنگ و اندیشه اسلامی.

حسینی، محمد (۱۴۰۰). **فقه و حقوق حریم خصوصی در فضای مجازی**. تهران: انتشارات سمت.

حکیم، سید محسن (۱۴۱۸ق). **مستمسک العروة الوثقی**. قم: دارالکتب الإسلامیة.

خوئی، سید ابوالقاسم (۱۴۲۲ق). **مصباح الفقاهة**. قم: مؤسسه احیاء آثار الإمام الخوئی.

سبحانی، جعفر (۱۴۲۵ق). **محاضرات فی اصول الفقه**. قم: مؤسسه امام صادق(ع).

شهیدی، مهدی (۱۳۹۷). **مالکیت و حقوق فردی در فقه امامیه**. تهران: میزان.

طباطبایی، سید محمدحسین (۱۳۷۴). **المیزان فی تفسیر القرآن**. قم: دفتر انتشارات اسلامی.

طوسی، محمد بن حسن (۱۳۹۰ق). **المبسوط**. تهران: مکتبة المرتضویه.

فاضل لنکرانی، محمد (۱۴۲۱ق). **تفصیل الشریعة فی شرح تحریر الوسیلة**. قم: مرکز فقهی ائمه اطهار(ع).

کلینی، محمد بن یعقوب (۱۴۰۷ق). **الکافی**. تهران: دارالکتب الإسلامیة.

مجلسی، محمدباقر بن محمدتقی (۱۴۰۳). **بحار الأنوار الجامعة لدرر أخبار الأئمة الأطهار**. بیروت: دار إحیاء التراث العربی.

مطهری، مرتضی (۱۳۷۹). **انسان و ایمان**. تهران: صدرا.

مکارم شیرازی، ناصر (۱۴۰۰). **تفسیر نمونه**. تهران: دارالکتب الاسلامیه.

موسوی بجنوردی، سید محمد (۱۴۱۹ق). **القواعد الفقهیة**. قم: دارالفقاهة.

موسوی خمینی، روح‌الله (۱۴۰۳). **تحریرالوسیله**. قم: مؤسسه تنظیم و نشر آثار امام خمینی.

موسوی، سید رضا (۱۳۹۹). **بررسی فقهی تجسس و نظارت در عصر دیجیتال**. قم: پژوهشگاه حوزه و دانشگاه.

نجفی، محمدحسن (۱۴۰۲). **جواهرالکلام**. قم: دارالکتب الاسلامیة.

هاشمی شاهرودی، محمود (۱۴۲۳ ق). **بحوث فی شرح العروة الوثقی**. قم: دارالفکر.

هاشمی، محمد (۱۳۹۸). **حقوق اساسی و حریم خصوصی**. تهران: میزان.

References

Al-Daraiseh, Ahmad (2020). **Privacy and Cybercrime in Islamic Law**. Brill.

Alhammadi, Ahmed (2021). **Data Protection Laws in the Gulf States**. Routledge.
Al-Khater, Khalid (2020). **Data Privacy in the Arab World**. Routledge.
Al-Mutairi, Fahad (2020). **Cybercrime Legislation in the Gulf Cooperation Council**. Routledge.
Al-Suwaidi, Fatima (2022). **Digital Governance and Data Protection in the Gulf**. Springer.
Andrejevic, Mark (2020). **Automated Media**. Routledge.
Bygrave, Lee A. (2020). **Data Privacy Law: An International Perspective**. Oxford University Press.
Boyd, D. & Crawford, K. (2012). "Critical Questions for Big Data". Information, **Communication & Society**, 15 (5), 662-679.
El-Desouki, Ahmed (2021). **Cyber Law and Policy in North Africa**. Cambridge University Press.
El-Menshawy, Mohamed (2022). **Cybersecurity Law in the Middle East**. Cambridge University Press.
Fadel, Mohammad (2019). **Islamic Law and Ethics in the Digital Age**. Cambridge University Press.
Greenleaf, Graham (2021). **Global Data Privacy Laws**. Oxford University Press.
Haque, Md. (2020). **Privacy and Data Regulation in Emerging Economies**. Oxford University Press.
Hassan, Fauziah (2020). **Personal Data Protection in Malaysia**. Kuala Lumpur: LexisNexis.
Khan, Imran (2021). **Cyber Law and Privacy Protection in the Muslim World**. Routledge.
Kearns, M. & Roth, A. (2019). **The Ethical Algorithm**. Oxford: Oxford University Press.
Lyon, David (2021). **Surveillance Studies: An Overview**. Polity Press.
Mansoor, Ahmed (2023). **Cybersecurity and Privacy Protection in Islamic Legal Systems**. Oxford University Press.
Nissenbaum, H. (2010). **Privacy in Context. Stanford**: Stanford University Press.
O'Neil, C. (2016). **Weapons of Math Destruction**. New York: Crown.
Rahman, Mohammad Z. (2021). **Cybercrime and Privacy Protection in Muslim-Majority Countries**. Brill.
Rahman, Mohammad Z. (2022). Cybercrime Legislation in Muslim-Majority Countries: A Comparative Analysis. **Journal of Islamic Law and Society**, 29 (2), 85-104.
Richards, N. (2013). "The Dangers of Surveillance". **Harvard Law Review**, 126 (7), 1934-1965.
Sachedina, Abdulaziz (2018). **Islamic Ethics: Fundamental Concepts and Contemporary Applications**. Oxford University Press.
Siegel, E. (2013). **Predictive Analytics**. Hoboken: John Wiley & Sons.
Solove, Daniel J. (2021). **Breached: Why Data Security Law Fails and How to Improve It**. Oxford University Press.
Tufekci, Z. (2014). "Algorithmic Harms Beyond Filter Bubbles". Proceedings of the ACM, 51-58.
Westin, Alan (2020). **Privacy and Freedom in the Digital Age**. New York University Press.
Wright, David & De Hert, Paul (Eds.) (2020). **Research Handbook on Privacy and Data Protection Law**. Edward Elgar Publishing.
Zuboff, Shoshana (2020). **The Age of Surveillance Capitalism**. Harvard University Press.

In Persian and Arabic

Ansari, Murtaza (1415 AH). **Al-Makasib**. Qom: Institute for Islamic Publication [In Arabic].
Fazel-e-Lankrani, Mohammad (1421 AH). **Tafsil al-Sharieh fi Sharh Tahrir al-Wasileh**. Qom: Jurisprudential Center of al-A'imma al-Athar [In Arabic].
Hakim, Sayyed Mohsen (1418 AH). **Mustamsik al-Eurwat al-Wuthqa**. Qom: Darul Kitab Al-Islamiya [In Arabic].
Hashemi Shahroudi, Mahmoud. (1423 AH). **Buhuth fi Sharh al-Eurwat al-Wuthqa**. Qom: Dar al-Fikr [In Arabic].
Hashemi, Mohammad. (2019). **Constitutional Law and Privacy**. Tehran: Mizan.
Hosseini, Mohammad (2021). **Jurisprudence and Privacy Law in Cyberspace**. Tehran: Samt

Publications.
Hosseini, Mohammad (2021). **Jurisprudence of Privacy in the Digital Age**. Qom: Islamic Culture and Thought Research Institute.
Hurr al-Amili, Mohammad ibn Hassan (1414 AH). **Wasail al-Shia**. Qom: Aal al-Bayt Institute [In Arabic].
Jafari Langroodi, Mohammad-Jafar (2020). **Legal Terminology**. Tehran: Ganj-e Danesh.
Khoei, Sayyed Abul-Qasim (1422 AH). **Misbah al-Faqaha**. Qom: Institute for Reviving the Works of Imam al-Khoei [In Arabic].
Kuleyni, Mohammad ibn Ya'qub (1407 AH). **Al-Kafi**. Tehran: Darul Kitab Al-Islamiya [In Arabic].
Majlisi, Muhammad Baqir ibn Muhammad Taqi (2024). **Bihar al-Anwar: Jami' Li-Durar Akhbar al-A'imma al-Athar. Beirut**: Dar Ihya' al-Turath al-Arabi [In Arabic].
Makarem Shirazi, Nasser (2021). **Tafsir-e-Nemooneh**. Tehran: Darul Kitab Al-Islamiya.
Motahari, Morteza (2000). **Human and Faith**. Tehran: Sadra.
Mousavi, Sayyed Reza (2020). **A Jurisprudential Study of Snooping and Surveillance in the Digital Age**. Qom: Research Institute for Hozah and University.
Mousavi Bojnourdi, Sayyed Mohammad (1419 AH). **Al-Qawa'id al-Fiqhiyyah**. Qom: Dar al-Fiqh [In Arabic].
Mousavi Khomeini, Ruhollah (2024). **Tahrir al-Wasileh**. Qom: Institute for Compilation and Publication of Imam Khomeini's Works [In Arabic].
Najafi, Mohammad-Hassan (2023). **Jawahir al-Kalam**. Qom: Darul Kitab Al-Islamiya [In Arabic].
Shahidi, Mehdi (2018). **Ownership and Individual Rights in *Shi'a* Jurisprudence**. Tehran: Mizan.
Subhani, Jafar (1425 AH). **Lectures on Principles of Jurisprudence**. Qom: Imam Sadiq Institute [In Arabic].
Tabatabaei, Sayyed Mohammad-Hosein (1995). **Al-Mizan fi Tafsir al-Qur'an**. Qom: Islamic Publication Office [In Arabic].
Tusi, Muhammad ibn Hasan (1390 AH). **Al-Mabsut**. Tehran: Makta.