Journal of
International Criminal Law
www.iclj.ir

Volume 4, Issue 4, 2026

Criminalization of Privacy Violation in Cyberspace: A Comparative Study in Islamic Criminal Jurisprudence and Contemporary Legal Systems

Fazel Homiry [1*]

1. Department of Criminal Law and Criminology, Persian Gulf International Education Center Branch, Islamic Azad University, Khorramshahr, Iran

ARTICLE INFORMATION

Type of Article: ***Original Research***

Pages: ***45-59***

Corresponding Author's Info:

ORCID: *0000-0000-0000-0000*

TELL: *+98*

Email:

Article History:

Received: *29 May 2026*

Revised: *03 Oct 2026*

Accepted: *23 Nov 2026*

Published online: *22 Dec 2026*

Keywords:

Privacy, Cyberspace, Personal Data, Electronic Evidence, Reasonable Expectation of Privacy, Protection-oriented Design.

ABSTRACT

The expansion of digital platforms and the data economy has transformed the boundaries of "privacy" and created new forms of privacy invasions – from unauthorized access and interception to targeted data disclosure and doxing. This article analyzes, with a comparative approach, the foundations and capacities of Islamic criminal jurisprudence in criminalizing privacy violations alongside the frameworks of contemporary legal systems. In the jurisprudential section, relying on texts (prohibition of surveillance, prohibition of disrobing of the believer) and rules such as non-harm, sovereignty, respect for property and appearance, and preservation of the system, we show that there is a clear normative foundation for criminal protection of information and communication privacy and that punishments are flexible regulatory tools for emerging patterns of harm. In the comparative law section, the legal, material, and psychological elements of privacy-related crimes in European and American law, exceptions based on necessity and proportionality (security, public interest, valid consent), and the position of electronic evidence are examined. The findings indicate the possibility of drawing a "balanced criminalization model" that, while precisely defining criminal behaviors (unauthorized access/interception/disclosure, unauthorized commercial exploitation, defamatory content based on generative technologies), clarifies the boundaries of exceptions with the triad of necessity-proportionality-judicial oversight, and specifies the responsibility of legal entities and the duties of platforms (incident reporting, protection-oriented design). The innovative contribution of the article is the normative connection of jurisprudential rules with modern data governance standards to present a native criminal policy model that is compatible with the requirements of cyberspace.

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

How to Cite This Article: Homiry, F (2026). "Criminalization of Privacy Violation in Cyberspace: A Comparative Study in Islamic Criminal Jurisprudence and Contemporary Legal Systems". *Journal of International Criminal Law*, 4(4): 45-59.

فصلنامه حقوق جزای بین‌الملل

www.iclj.ir

دوره چهارم، شماره چهارم، زمستان ۱۴۰۵

جرم انگاری نقض حریم خصوصی در فضای مجازی: بررسی تطبیقی در فقه جزای اسلامی و نظام‌های حقوقی معاصر

حمیری [۱*]

۱. گروه حقوق کیفری و جرم‌شناسی، واحد مرکز آموزش‌های بین‌المللی خلیج فارس، دانشگاه آزاد اسلامی، خرمشهر، ایران.

اطلاعات مقاله

نوع مقاله: پژوهشی

صفحات: ۵۹-۴۵

اطلاعات نویسنده مسؤول

کد ارکید: ۰۰۰۰-۰۰۰۰-۰۰۰۰-۰۰۰۰

تلفن: +

ایمیل:

سابقه مقاله:

تاریخ دریافت: ۱۴۰۵/۰۳/۰۸

تاریخ ویرایش: ۱۴۰۵/۰۷/۱۱

تاریخ پذیرش: ۱۴۰۵/۰۹/۰۲

تاریخ انتشار: ۱۴۰۵/۱۰/۰۱

واژگان کلیدی:

حریم خصوصی، فضای مجازی، داده‌های شخصی، ادله الکترونیکی، انتظار معقول از خلوت، طراحی صیانت‌محور.

چکیده

گسترش پلتفرم‌های دیجیتال و اقتصاد داده، مرزهای «خلوت» را دگرگون کرده و اشکال تازه‌ای از تعرض به حریم خصوصی –از دسترسی و رهگیری غیرمجاز تا افشاء هدفمند داده‌ها و داکسینگ– را پدید آورده است. این مقاله با رویکردی تطبیقی، مبانی و ظرفیت‌های فقه جزای اسلامی در جرم‌انگاری نقض حریم خصوصی را در کنار چارچوب‌های نظام‌های حقوقی معاصر تحلیل می‌کند. در بخش فقهی، با اتکا به نصوص (نهی از تجسس، حرمت هتک ستر مؤمن) و قواعدی چون لاضرر، سلطنت، احترام مال و عرض و حفظ نظام، نشان می‌دهیم که بنیاد هنجاری روشنی برای حمایت کیفری از حریم اطلاعاتی و ارتباطی وجود دارد و تعزیرات، ابزار انعطاف‌پذیر تنظیمی در قبال الگوهای نوپدید آسیب‌اند. در بخش حقوق تطبیقی، عناصر قانونی، مادی و روانی جرائم مرتبط با حریم خصوصی در حقوق اروپا و آمریکا، استثنائات مبتنی بر ضرورت و تناسب (امنیت، منفعت عمومی، رضایت معتبر) و جایگاه ادله الکترونیکی بررسی می‌شود. یافته‌ها حاکی از امکان ترسیم «الگوی جرم‌انگاری متوازن» است که ضمن تعریف دقیق رفتارهای مجرمانه (دسترسی/رهگیری/افشاء غیرمجاز، بهره‌برداری تجاری غیرمجاز، محتوای هتک‌آمیز مبتنی بر فناوری‌های مولد)، مرز استثنائات را با سه‌گانه‌ی ضرورت–تناسب–نظارت قضایی روشن کرده و مسؤولیت اشخاص حقوقی و تکالیف پلتفرم‌ها (گزارش رخداد، طراحی صیانت‌محور) را تصریح می‌نماید. سهم نوآورانه مقاله، پیوند هنجاری قواعد فقهی با استانداردهای نوین حاکمیت داده برای ارائه‌ی یک مدل سیاست جنایی بومی–همساز با اقتضائات فضای مجازی است.

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

پیشرفت شتابان فناوری اطلاعات و گسترش روزافزون ارتباطات الکترونیکی، حریم خصوصی افراد را در فضای مجازی با چالش‌های نوینی مواجه ساخته است؛ اطلاعات شخصی، ارتباطات خصوصی و داده‌های حساس به‌سرعت قابل جمع‌آوری، پردازش و انتشارند و پیامدهای نقض این حریم می‌تواند اعم از تضعیف کرامت انسانی تا تهدید امنیت روانی و اقتصادی شهروندان باشد. از این‌رو نیاز به چارچوب‌های کیفری روشن برای بازدارندگی و جبران خسارت‌ها آشکار است، اما ابهامات نظری و عملی درباره قلمرو تعریف «حریم خصوصی» در فضای مجازی، معیارهای مشروعت‌بخشی به مصلحت عمومی و نحوه تطبیق اصول فقهی با واقعیت‌های فناورانه، روند جرم‌انگاری را پیچیده می‌سازد. در مقابل، نظام‌های حقوقی معاصر با سنت‌ها و رویکردهای متنوعی از جرم‌انگاری برخوردارند که هر یک نقاط قوت و ضعف خاصی در مواجهه با مسائل فناوری اطلاعات نشان می‌دهند؛ بررسی تطبیقی این رویکردها با آموزه‌های فقه جزایی اسلامی می‌تواند مبنایی برای تدوین مقررات متناسب و قابل اجرا فراهم آورد.

سؤال اصلی تحقیق این است: چه ملاک‌ها و مبانی فقهی در فقه جزای اسلامی و چه مبانی و رویه‌هایی در نظام‌های حقوقی معاصر برای جرم‌انگاری نقض حریم خصوصی در فضای مجازی وجود دارد و چگونه می‌توان میان این رویکردها مدلی تطبیقی عرضه کرد که هم از حیث مشروعیت دینی و هم از نظر اثربخشی کیفری و سازگاری با مقتضیات فناوری‌های نوین قابل اتکا باشد؟

نوآوری این تحقیق در تلفیق تحلیل اصول فقهی مسؤولیت کیفری با مطالعه تطبیقی رویه‌ها و تضمین‌های عملی در نظام‌های معاصر و ارائه الگوی تطبیقی-کاربردی برای جرم‌انگاری نقض حریم خصوصی در فضای مجازی است که ملاک‌های روشن حقوقی، آیین دادرسی مناسب و معیارهای فنی اثبات جرم را به‌صورت یکپارچه در برمی‌گیرد.

۱- روش پژوهش

در این پژوهش از روش کتابخانه‌ای استفاده می‌شود و از ابزار فیش‌برداری جهت گردآوری داده‌ها استفاده شده است.

۲- ادبیات نظری

۲-۱- تعریف و اقسام حریم خصوصی

در ادبیات فارسی حقوق و فقه، «حریم خصوصی» عموما به قلمرویی از زندگی و اطلاعات شخصی اطلاق می‌شود که ورود به آن بدون اذن صاحب آن نارواست و می‌تواند ضمانت‌اجراهای مدنی و کیفری را برانگیزد. در یک جمع‌بندی کارآمد برای فضای مجازی، می‌توان اقسام زیر را از هم تفکیک کرد:

۲-۱-۱- حریم اطلاعاتی

حریم اطلاعاتی یعنی هر نوع داده‌ای که به‌طور مستقیم یا غیرمستقیم به شخص قابل انتساب است؛ از داده‌های هویتی تا سوابق رفتاری و فراداده‌های ارتباطی (اکبری و فلاحیان، ۱۴۰۰؛ جعفری و رهبرپور، ۱۳۹۶).

۲-۱-۲- حریم ارتباطی

حریم ارتباطی یعنی محتوای مکاتبات و مکالمات، ضمائم و لیست مخاطبان؛ تعرض به آن مصداق نقض حریم است (جعفری و رهبرپور، ۱۳۹۶).

۲-۱-۳- حریم مکانی-مجازی

حریم مکانی-مجازی یعنی فضاهای خصوصی در بستر دیجیتال، مثل حساب کاربری، پوشه‌های ابری و پیام‌رسان‌ها که «ورود» به آن‌ها در حکم دخول به «مسکن داده‌ای» است (اکبری و فلاحیان، ۱۴۰۰).

۲-۱-۴- هویت دیجیتال

هویت دیجیتال یعنی نماهای برخط شخصیت، مثل پروفایل، تصویر، صدا و الگوریتم‌های بازشناسی که بهره‌برداری هتک‌آمیز یا تحریف آن‌ها، مانند دیپ‌فیک‌های مخدوش، نقض حریم تلقی می‌شود (جعفری و رهبرپور، ۱۳۹۶).

از منظر مبانی شرعی، نهی از تجسس و تتبع عیوب مؤمن، بنیان هنجاری صیانت از این اقسام را پشتیبانی می‌کند: **«ولا تجسسوا...»** (حجرات/ ۱۲) و تحلیل مفسران درباره تفکیک تجسس از تحسس و نهی از تتبع امور مستور (طباطبایی، ۱۳۷۴)؛ همچنین باب «تحریم تتبع زلات المؤمن ومعایبه» در وسائل‌الشیعه (حر عاملی، بی‌تا).

۲-۲- تمایز «حریم خصوصی» با مفاهیم نزدیک

۲-۲-۱- آبرو و حیثیت

آبرو و حیثیت، ناظر به شأن معنوی شخص است و اعاده حیثیت و جبران لطمه‌های اعتباری را می‌طلبد؛ هر نقض حریم، الزاما توهین به حیثیت نیست، هرچند غالبا ملازم است (جعفری و رهبرپور، ۱۳۹۶).

۲-۲-۲- حق خلوت

حق خلوت، بعد «تنهایی ارادی» و رهایی از تعرض دیداری یا شنیداری است؛ در فقه، با مفاهیمی چون «ستر» و «کراهت تتبع عورات» قرابت دارد (حر عاملی، بی‌تا؛ طباطبایی، ۱۳۷۴).

۲-۲-۳- رازداری حرفه‌ای

رازداری حرفه‌ای، تکلیف ویژه‌ی متصدیان حرفه‌هایی مثل پزشک، وکیل، مددکار که نقض آن می‌تواند عنوان مستقل بیابد (نصرالهی‌نیا، ۱۴۰۱).

۲-۲-۴- اسرار تجاری

اسرار تجاری، متعلق به شخصیت حقوقی و کسب‌وکار است؛ با اینکه «خصوصی» است اما موضوع آن منافع اقتصادی است و نه لزوما حریم شخص انسان؛ تفکیک این دو در تعیین ضمانت‌اجرا اهمیت دارد (نیکخواه سرنقی و همکاران، ۱۴۰۰: ۱۷).

۲-۳- شاخص‌های شناسایی توقع معقول از خلوت در بستر دیجیتال

شاخص‌های شناسایی «توقع معقول از خلوت» در بستر دیجیتال را می‌توان در عناوین زیر دانست:

۲-۳-۱- قرارداد یا اذن معتبر

وجود یا فقدان رضایت آگاهانه، مشخص، قابل‌فهم و قابل رجوع برای جمع‌آوری یا پردازش داده، شاخص اصلی شکل‌گیری «توقع از خلوت» است؛ رضایت‌های صوری و «نمایشی» که بر مبنای عدم‌اطلاع یا اجبار پلتفرمی اخذ می‌شوند، کفایت نمی‌کنند (اکبری و فلاحیان، ۱۴۰۰).

۲-۳-۲- ماهیت فضا

خصوصی‌بودن محیط دیجیتال، مثل پیام مستقیم، فضای ابری شخصی در برابر عمومی‌بودن آن (پست باز) با لحاظ تنظیمات مخاطب و قابلیت پیش‌بینی دسترسی، نقش تعیین‌کننده در احراز انتظار از خلوت دارد (حدادپور، ۱۴۰۱).

۲-۳-۳- حساسیت ذاتی داده

هرچه موضوع داده حساس‌تر باشد، نظیر داده‌های سلامت، گرایش‌ها، زیست‌سنجی و مکان‌نگاری، آستانه حمایت حقوقی/شرعی بالاتر می‌رود و توقع از خلوت تقویت می‌شود (غفاری‌الهی‌کاشانی، ۱۳۹۷).

۲-۳-۴- شیوه تحصیل داده

دستیابی مخفیانه یا فریب‌کارانه، مثل فیشینگ، مهندسی اجتماعی و بدافزار، قرینه قوی بر وجود انتظار از خلوت است و تعرض را تشدید می‌کند (لطیف‌زاده و همکاران، ۱۴۰۲).

۲-۳-۵- حمایت‌های شرعی

نهی قرآنی از تجسس و سنت «ستر» زنجیره‌ای از مناهی همچون سوءظن، تجسس و غیبت را ترسیم می‌کند که حمایت از خلوت برخط را نیز مفروض می‌گیرد؛ بنابراین، اصل بر منع تتبع امور مستور اشخاص است مگر با مجوز معتبر (طباطبایی، ۱۳۷۴؛ حر عاملی، بی‌تا).

۲-۳-۶- مخاطرات باز انتشار

هرچه امکان تکثیر، اسکرین‌شات، فوروارد و نمایه‌سازی بی‌اجازه در یک بستر بیشتر باشد، سطح «توقع معقول از خلوت» بالاتر می‌رود و مقتضی حمایت شدیدتر است (اکبری و فلاحیان، ۱۴۰۰).

۲-۴- ادبیات پژوهش و نقد مطالعات پیشین (فقهی و حقوقی)

ادبیات پژوهش و رویکرد انتقادی به منابع پیشین را می‌توان چنین ترسیم کرد:

۲-۴-۱- رویکرد مبنایی فقهی

پژوهش‌های فقهی با اتکا به نهی از تجسس و قاعده ستر، ضرورت صیانت از حریم را پررنگ کرده‌اند، اما غالبا از «تقسیم‌بندی داده‌محور» و صورت‌بندی عناصر جرم در محیط‌های دیجیتال، کمتر سراغ گرفته‌اند (حدادپور، ۱۴۰۱؛ نیکخواه سرنقی و همکاران، ۱۴۰۰).

۲-۴-۲- رویکرد حقوقی داخلی

مقالاتی مانند اکبری و فلاحیان (۱۴۰۰) در «تمدن حقوقی» ضمن واکاوی مفهوم و مصادیق حریم، به خلأهای سیاستی و قانونی اشاره کرده‌اند؛ مزیت این کارها ترسیم میدان مسأله است، اما در «استانداردسازی شاخص‌های انتظار معقول از خلوت» و «طراحی الگوی هنجاری جرم‌انگاری دیجیتال» هنوز جای کار دارند (اکبری و فلاحیان، ۱۴۰۰).

۲-۴-۳- رویکرد داده‌محور (مسؤولیت مدنی نقض حریم اطلاعات)

جعفری و رهبرپور (۱۳۹۶) با تمرکز بر داده‌ها و فراداده‌ها، بحث «مرگ حریم داده» و «مال‌انگاری حریم اطلاعاتی» را طرح کرده‌اند؛ قوت پژوهش در تبیین مبانی مدنی است، اما پیوند منسجم با «تعزیرات حکومتی دیجیتال» و «ادله الکترونیکی» نیازمند تکمیل است (جعفری و رهبرپور، ۱۳۹۶). کارهای نو در فقه مقارن پزشکی و حقوق بیماران، نشان می‌دهد «اعتماد حرفه‌ای» شاکلهٔ ویژه‌ای از حریم است که باید جداگانه جرم‌انگاری یا ضمانت شود؛ با این حال، نسبت این ادبیات با «معماری پلتفرم» و «جریان داده‌های بیمار در فضای ابری» کمتر بحث شده است (نصرالهی‌نیا، ۱۴۰۱).

بنابراین، بدنه پژوهشی فارسی/عربی، مبانی شرعی و حقوقی نیرومندی برای صیانت از حریم ارائه کرده است، اما در سه حلقه ضعف دارد: ۱) تفکیک دقیق «اقسام حریم» متناسب با معماری‌های نو، مثل ابر، پیام‌رسان و شبکه اجتماعی، ۲) صورت‌بندی عملیاتی «انتظار معقول از خلوت» با شاخص‌های آزمون‌پذیر، ۳) پیوند نظام‌مند قواعد فقهی با عناصر جرم و ادله‌ی دیجیتال، مثل زنجیره حفاظتی، تمامیت و اصالت. این مقاله در ادامه، خلأهای مزبور را هدف می‌گیرد.

۳- مبانی فقه جزای اسلامی در حمایت از حریم خصوصی

۳-۱- نصوص و ادله شرعی

۳-۱-۱- آیات قرآن

نهی صریح از تجسس: **«ولا تجسسوا...»** (حجرات/ ۱۲) که مفسر، آن را منع از تتبع امور مستور مردم دانسته و تفکیک «تجسس/تحسس» را توضیح می‌دهد؛ بر این مبنا، کشف پنهانی اطلاعات بدون اذن، حکم اولی حرمت دارد (طباطبایی، ۱۳۷۴). نهی از دخول بدون اذن و الزام به استیذان و استیناس نیز قلمرو «خلوت» را با ادبیات مکانی/منزلی، تثبیت می‌کند: **«یا أیها الذین آمنوا لا تدخلوا بیوتا غیر بیوتکم حتی تستأنسوا و تسلموا...»** (نور/ ۲۷–۲۹) که در تحلیل المیزان، اصل عدم جواز نفوذ به حوزه خصوصی تا تحقق اذن معتبر و قرائن اطمینان‌بخش تأکید می‌شود. افزون بر این، حرمت اشاعه فحشا (نور/ ۱۹) ناظر به ممنوعیت انتشار محتوای هتک‌آمیز و آبروبر است که با منطق منع افشای اسرار پیوند مستقیم دارد (نور/ ۱۹).

۳-۱-۲- روایات

در ابواب متعددی از حدیث، «حرمت هتک ستر مؤمن»، «نهی از تتبع العورات» و «حرمت افشاء سر» آمده است؛ از جمله: باب «تحریم تتبع زلات المؤمن و معایبه» که بر لزوم ستر و ترک کاوش عیوب مستور دلالت دارد (حر عاملی، بی‌تا: ۱/ ۳۶۶–۳۶۷). همچنین روایات «من ستر مؤمنا ستره الله» مبنایی عام برای ترجیح ستر بر کشف‌های غیرضروری فراهم می‌کند (نوری، بی‌تا).

۳-۲- قواعد فقهی مرتبط

۳-۲-۱- قاعده لاضرر و لاضرار

هر نوع دسترسی، رهگیری یا افشایی که موجب ضرر نوعی یا شخصی بر نفس، عرض یا مال شود، مشمول منع است و می‌تواند مجوز اقدام تعزیری و حکومتی باشد؛ به‌ویژه در تعرضات اطلاعاتی که نتایج حیثیتی و اقتصادی آشکار دارند.

۳-۲-۲- قاعده سلطنت (الناس مسلطون)

تسلط اشخاص بر نفس، اموال و اسرارشان اقتضا می‌کند هر تصرف داده‌ای یا ارتباطی بدون اذن معتبر، ممنوع باشد ولو با دسترسی فنی مقدور گردد (کاتوزیان، ۱۳۷۴).

۳-۲-۳- حرمت تجسس

عنوان اولیه‌ی مستقل بر منع هر نوع تتبع پنهانی در امور مستور اشخاص است؛ در فضای مجازی، «کاوش حساب‌های خصوصی یا ابر شخصی یا پیام‌رسان» مصادیق روشن آن است (حر عاملی، بی‌تا).

۳-۲-۴- احترام مال و نفس و عرض

حریم خصوصی، ذیل «احترام عرض» و گاه «احترام مال داده‌ای» تحلیل‌پذیر است؛ افشای داده‌های هویتی یا زیست‌سنجی یا تصاویر خصوصی، هتک عرض و گاه مقدمه اضرار مالی است (کاتوزیان، ۱۳۹۲).

۳-۲-۵- قاعده احسان

هرگاه دسترسی ناخواسته رخ دهد ولی شخص فورا «ستر» کند و از نشر یا انتفاع بپرهیزد، ضمان و تعزیر می‌تواند تخفیف یابد؛ زیرا «ما علی المحسنین من سبیل» قرینه‌ای برای تفکیک سوءنیت یا سوءرفتار فراهم می‌کند (امام خمینی، ۱۴۱۰ق).

۳-۲-۶- قاعده اذن

رضایت باید «آگاهانه، مشخص و قابل رجوع» باشد؛ رضایت‌های صوری پلتفرمی یا اذن‌های مبهم، مجوز نقض حریم محسوب نمی‌شود (افتخار جهرمی، ۱۳۹۳).

۳-۲-۷- قاعده حفظ نظام

در تعارض صیانت از حریم با مصالح عالیه، مثل امنیت، پیشگیری و تعقیب جرم، اصل بر ضرورت، تناسب و نظارت قضایی است (طباطبایی، ۱۳۷۴؛ امام خمینی، ۱۴۱۰ق).

۳-۳- حدود و قیود شرعی

۳-۳-۱- تفکیک حق‌الله از حق‌الناس

تعرض به حریم خصوصی غالبا «حق‌الناس» است؛ لذا اصل، لزوم جبران و امکان گذشت بزه‌دیده است؛ اما اگر مفسده‌ی عمومی پدید آید (اشاعه فحشا، اختلال امنیت)، وصف حق‌اللهی و عمومی تقویت می‌شود (طباطبایی، ۱۳۷۴؛ امام خمینی، ۱۴۱۰ق).

۳-۳-۲- تزاحم با مصالح عمومی (امنیت و تعقیب جرم)

جواز شنود یا رهگیری محدود، منوط به تحقق «ضرورت واقعی»، «تناسب ابزار با هدف» و «نظارت قاضی» است؛ کشف جرم نمی‌تواند به قاعده‌ای برای تجسس عام و بدون ظن معتبر بدل شود (تبریزی و همکاران، ۱۴۰۱).

۳-۳-۳- اصل ستر و مرزهای کشف جرم

ستر عیب مؤمن، قاعده‌ی غالب است و کشف جرم، استثناء نیازمند دلیل خاص؛ حتی در صورت اطلاع اتفاقی، توسعه‌ی کاوش بدون مجوز معتبر، جایز نیست (نوری، بی‌تا؛ امام خمینی، ۱۴۱۰ق).

۳-۴- آثار جزایی در فقه

۳-۴-۱- عناوین ثانوی و تعزیرات حکومتی

میزان و نوع مجازات بر پایه‌ی ملاکات «شدت اضرار»، «عمومیت انتشار»، «قصد هتک» و «خطر تکرار» تنظیم‌پذیر است (امام خمینی، ۱۴۱۰ق؛ جعفری و رهبرپور، ۱۳۹۶).

۳-۴-۲- ملاکات تشدید یا تخفیف مجازات

تشدید مجازات در مواردی است همچون، عمد خاص در افشاء یا داکسینگ؛ داده‌های بسیار حساس مثل امور مربوط آبرو و نوامیس، امور زیست‌سنجی و سلامت؛ انتشار گسترده یا انتفاع مالی؛ سازمان‌یافتگی یا استفاده از بدافزار (فتحی، ۱۳۹۶).

تخفیف مجازات در مواردی است همچون کشف اتفاقی بدون سوءنیت، اقدام فوری به ستر و حذف، همکاری برای جبران و جلوگیری از باز انتشار (مکارم شیرازی، بی‌تا).

۳-۴-۳- تدابیر تکمیلی یا جایگزین

علاوه بر کیفر مالی یا حبسی، می‌توان به الزام به حذف محتوا، منع موقت فعالیت داده‌محور، آموزش اجباری ستری یا حریم خصوصی و تضمین‌های فنی، مانند تحویل دسترسی‌ها یا کلیدها، حکم کرد؛ این تدابیر با فلسفه تعزیر سازگارند و به «جبران و پیشگیری» نظر دارند (کاتوزیان، ۱۳۹۲؛ جعفری و رهبرپور، ۱۳۹۶).

۴- جرم‌انگاری نقض حریم در نظم‌های حقوقی معاصر (چارچوب تطبیقی)

۴-۱- حقوق اروپا

در نظم اروپایی، حمایت از حریم خصوصی بر دو ستون «حق بنیادین احترام به زندگی خصوصی» و «حفاظت از داده‌های شخصی» استوار است. ستون نخست در ماده ۸ کنوانسیون اروپایی حقوق بشر تضمین شده و هر مداخله را مشروط به سه سنجه می‌داند: قانون‌مندی، هدف مشروع، مثل امنیت ملی، نظم عمومی، رفاه اقتصادی، پیشگیری از جرم، بهداشت و اخلاق و حقوق دیگران و ضرورت و تناسب در جامعه دموکراتیک؛ قید «حاشیه صلاحدید» دولت‌ها نیز در مقدمه و

ساختار کنوانسیون تحت نظارت دیوان اروپایی حقوق بشر پذیرفته شده است (کنوانسیون اروپایی حقوق بشر، ۲۰۲۱). دیوان در رویه خود دامنه «زندگی خصوصی، خانه و مراسلات» را موسع تفسیر کرده و معیارهای سه‌گانه مزبور را به‌صورت سخت‌گیرانه اعمال می‌کند (حیدرقلی‌زاده و همکاران، ۱۳۹۴).

ستون دوم، مقررات عمومی حفاظت از داده‌ها (GDPR 2016/679) است که از ۲۰۱۸ لازم‌الاجرا شد و در حقوق اتحادیه اروپا چهارچوب ماهوی و شکلی جامع برای پردازش داده‌های شخصی ارائه می‌کند (لطیف‌زاده و همکاران، ۱۴۰۲).

اصول و مبانی مشروعیت؛ اصولی مانند قانون‌مندی، محدودیت هدف، به‌علاوه مبانی مشروعیت پردازش، مثل رضایت معتبر، اجرای قرارداد، تکلیف قانونی، منافع حیاتی، مأموریت عمومی، اقتدار رسمی، منافع مشروع، چارچوب رفتاری متولیان داده را تعیین می‌کند (فرجی‌ها و علمداری، ۱۳۹۶).

دسته‌های خاص و ممنوعیت‌های تقویتی؛ پردازش داده‌های شخصی خاص یا حساس، مثل مسائل نژادی یا قومیتی، عقاید سیاسی، باورهای دینی، اتحادیه صنفی، ژنتیک، زیست‌سنجی برای شناسایی یکتا، سلامت، زندگی جنسی یا گرایش خاص، اصولا ممنوع است مگر در استثناهای محدود و با تضمین‌های مضاعف مبتنی بر ارزیابی ریسک (ماده ۹ GDPR)؛ درباره داده‌های مرتبط با محکومیت‌ها و جرائم کیفری نیز نظارت مرجع رسمی و مجوز قانونی تصریح شده است (لطیف‌زاده و همکاران، ۱۴۰۲).

حمایت ویژه از کودکان و رضایت سنی؛ تعیین «حداقل سن برای رضایت معتبر» در خدمات جامعه اطلاعاتی و تقویت شفافیت برای ولی یا قیم از الزامات صریح است (فرجی‌ها و علمداری، ۱۳۹۶). نتایج نهادی و فرایندی. نصب مقام‌های ناظر مستقل، تکلیف به ارزیابی اثرات حفاظت از داده‌ها در پردازش‌های پرخطر و اصل «حفاظت در طراحی و به‌طور پیش‌فرض» از سازوکارهای کلیدی اجرایی است (لطیف‌زاده و همکاران، ۱۴۰۲).

چارچوب اروپایی، حریم خصوصی را در سطح حق بنیادین (ECHR) و نظام داده‌محور (GDPR) توأمان تضمین می‌کند و در بعد کیفری، با تکیه بر استانداردهای شورای اروپا، هسته جرائم تعرض به محرمانگی/تمامیت ارتباطات و داده را هماهنگ می‌سازد؛ در نتیجه، برای نقض حریم برخط، هم مسؤولیت‌های اداری/مدنی شدید و هم جرم‌انگاری هسته‌ای پیش‌بینی شده است (لطیف‌زاده و همکاران، ۱۴۰۲؛ حیدرقلی‌زاده و همکاران، ۱۳۹۴؛ تبریزی و همکاران، ۱۴۰۱).

۴-۲- حقوق ایالات‌متحده

الف) چهارگانه‌ی مسؤولیت‌های حریم خصوصی در کامن‌لا. چارچوب کلاسیک پروسر، چهار شاخه‌ی مسؤولیت مدنی مرتبط با حریم خصوصی را می‌شناسد: «افشای عمومی امور خصوصی»، «تعرض به خلوت»، «انتساب کذب» و «بهره‌برداری از شباهت یا حق بر تصویر»؛ در ادبیات فارسی، بحث حق تصویر/شهرت و نسبت آن با آزادی بیان نیز با همین شاکله تحلیل می‌شود (میرشکاری، ۱۳۹۷؛ شرقی، ۱۳۹۸). در این چارچوب، شرط‌های کلیدی از جمله «انتظار معقول از خلوت» و «رنج یا لطمه حیثیتی» برای احراز مسؤولیت برجسته‌اند (میرشکاری، ۱۳۹۷).

ب) معیار «انتظار معقول از حریم» در محیط ابری یا پلتفرم‌ها. پس از رأی Katz، سنجه‌ی «انتظار معقول از حریم» در تفسیر متمم چهارم، مبنای تمایز میان داده‌هایی که فرد واقعا انتظار صیانت از آنها دارد و داده‌هایی که با واسطه‌ی اشخاص ثالث به اشتراک گذاشته شده‌اند، قرار گرفت. با این‌همه، دکترین «شخص ثالث» در سال‌های اخیر با نقدهای جدی روبه‌رو شده و در حوزه‌ی داده‌های ابری/مکانی، فرض سقوط مطلق انتظار معقول را برنمی‌تابد (ابوالمعالی‌الحسینی و همکاران، ۱۳۹۶). نمونه‌های نوین داده‌های ترافیکی یا مکانی و ذخیره‌سازی‌های کلاد، تقویت‌کننده‌ی این ادعا هستند که رضایت قراردادی‌های صوری «شرایط استفاده»، برای اسقاط حمایت کیفری و آیین‌دادرسی کافی نیست (ابوالمعالی‌الحسینی و همکاران، ۱۳۹۶).

ج) قوانین فدرال/ایالتی در شنود و دسترسی غیرمجاز. در سطح فدرال، «قانون حریم ارتباطات الکترونیکی» (ECPA 1986) سه لایه‌ی اصلی –در دسترسی به ارتباطات ذخیره‌شده و دستورات افشای داده‌های ترافیکی– ترسیم می‌کند و رویه‌ی

قضایی، شروط «اجازه قضایی متناسب» و «خصوصیت نوع داده» را برای مشروعیت بخشی به تحصیل الکترونیکی دلایل برجسته کرده است (میرشکاری، ۱۳۹۷؛ شرقی، ۱۳۹۸). در کنار آن، «قانون کلاهبرداری و سوءاستفاده رایانه‌ای» (CFAA 1986) محور کیفری‌سازی «دسترسی فراتر از مجوز/بدون مجوز» به سامانه‌های حفاظت‌شده است و در تفسیر، مرز میان «تخطی از شروط استفاده‌ی مدنی» و «نفوذ کیفری» اهمیت بنیادین دارد (ابوالمعالی‌الحسینی و همکاران، ۱۳۹۶). ایالات نیز قوانین شنود و رهگیری خویش را دارند که غالبا استانداردهای فدرال را سخت‌گیرانه‌تر می‌کنند (ابوالمعالی‌الحسینی و همکاران، ۱۳۹۶).

۴-۳- حقوق انگلستان

الف) حمایت‌های داده‌ای (فرهمند، ۱۴۰۳).

ب) جرائم رایانه‌ای مرتبط با دسترسی غیرمجاز/مداخله (وحابی، ۱۴۰۴).

ج) رهگیری ارتباطات و اختیارات نظارتی (حیدرقلی‌زاده و همکاران، ۱۳۹۴: ۲۳-۴۱). این چارچوب در کنار استانداردهای DPA 2018، نسبت میان کشف جرم و صیانت از حریم ارتباطی/ترافیک‌داده را با آزمون‌های ضرورت–تناسب محدود می‌کند (فرهمند، ۱۴۰۳).

۴-۴- اسناد و استانداردهای بین‌المللی منتخب

الف) کنوانسیون بوداپست ۲۰۰۱ (شورای اروپا). ترجمه‌ی فارسی مصوب «کنوانسیون جرائم سایبر» و «گزارش توجیهی» نشان می‌دهد که فصل دوم (مواد ۱۳-۲) حداقل‌استانداردهای جرم‌انگاری را در چهار خوشه مقرر می‌کند: «دسترسی غیرقانونی»، «شنود یا رهگیری غیرقانونی»، «جرائم علیه تمامیت داده یا سامانه» و «سوءاستفاده از ابزارها»؛ به‌علاوه جعل یا کلاهبرداری رایانه‌ای و سازوکارهای آیین‌دادرسی ویژه (مواد ۲۱-۱۴) و صلاحیت یا همکاری فراملی (ماده ۲۲ و فصل سوم) را تنظیم می‌نماید. این سند، به‌صراحت بر برقراری توازن با حقوق بشر و آزادی‌ها در اجرای اختیارات الکترونیکی (از جمله شنود محتوا و گردآوری داده‌های در حال انتقال) تأکید می‌کند (مرکز پژوهش‌های مجلس، ۱۳۸۴).

ب) کارکرد تطبیقی برای جرم‌انگاری نقض حریم (فرجی‌ها و علمداری، ۱۳۹۶؛ مرکز پژوهش‌های مجلس، ۱۳۸۴).

۴-۵- جمع‌بندی تطبیق اولیه: نقاط اشتراک و افتراق

در مقایسه‌ی فقه جزای اسلامی و نظم‌های حقوقی معاصر، اشتراک‌ها در چند محور هسته‌ای است: منع تجسس و استراق سمع و افشاء سر در نصوص (اصل صیانت از خلوت مؤمن و ستر عیوب) که در حقوق معاصر با جرم‌انگاری «دسترسی یا رهگیری غیرمجاز» و «افشاء داده‌های خصوصی» متناظر می‌شود؛ و نیز پذیرش آزمون‌های ضرورت–تناسب هنگام تعارض با مصالح عمومی مثل کشف جرم و امنیت که در حقوق اروپایی ذیل ماده ۸ ECHR و در سازوکارهای بوداپست و قوانین داخلی بازتاب دارد (مرکز پژوهش‌های مجلس، ۱۳۸۴؛ جعفری و رهبرپور، ۱۳۹۶). افتراق‌ها بیش‌تر ناظر به مبانی و صورت‌بندی است (لطیف‌زاده و همکاران، ۱۴۰۲). از حیث ضمانت‌اجرا نیز حقوق معاصر تلفیقی از مسؤولیت اداری یا مدنی شدید و جرم‌انگاری هسته‌ای، مثل دسترسی، رهگیری، اخلال یا افشاء را به‌کار می‌گیرد، در حالی‌که فقه در تعزیرات حکومتی و عناوین ثانوی انعطاف‌پذیری بیشتری برای تناسب‌سازی دارد (تبریزی و همکاران، ۱۴۰۱).

۵- تحلیل رکن‌شناسی جرم نقض حریم در بستر دیجیتال

۵-۱- رکن قانونی

انواع رفتار مجرمانه در حقوق تطبیقی معاصر و حقوق ایران عموما در چهار خوشه می‌گنجند:

الف) دسترسی غیرمجاز به حساب یا دستگاه یا ابر (مرکز پژوهش‌های مجلس، ۱۳۸۴). در قوانین ایران نیز ماده ۱ قانون جرائم رایانه‌ای «دسترسی غیرمجاز» را جرم می‌داند (قانون جرائم رایانه‌ای، ۱۳۸۸).

ب) استراق‌سمع یا رهگیری ارتباطات. در بوداپست «شنود غیرقانونی» داده‌های در حال انتقال (مرکز پژوهش‌های مجلس، ۱۳۸۴: ۱۸)، و در قوانین ایران ماده ۲ «شنود غیرمجاز» (قانون جرائم رایانه‌ای، ۱۳۸۸: ماده ۲-۱) و مواد ۵۰-۴۸ در بخش آیین دادرسی درباره شنود و استنادپذیری (قانون جرائم رایانه‌ای، ۱۳۸۸: مواد ۵۰-۴۸).

ج) اخلال در داده یا سامانه. «اختلال در داده‌ها یا سیستم» و «سوءاستفاده از ابزارها» (مرکز پژوهش‌های مجلس، ۱۳۸۴)، متناظر با مواد ۱۰–۸ قانون جرائم رایانه‌ای، درباره حذف یا تخریب یا اخلال و ممانعت از دسترسی (قانون جرائم رایانه‌ای، ۱۳۸۸: ماده ۱–۲).

د) افشاء یا انتشار داده‌ی شخصی و اسرار، داکسینگ و تجاری‌سازی غیرمجاز داده (قانون جرائم رایانه‌ای، ۱۳۸۸: ماده۲). «داکسینگ» –انتشار نظام‌مند شناسه‌ها و اطلاعات شناسایی– عموما ذیل ترکیب افشای اسرار یا هتک حیثیت یا نشر اکاذیب و گاه سرقت داده (ماده ۱۲) قابل انطباق است (قانون جرائم رایانه‌ای، ۱۳۸۸: ماده ۱–۲؛ جعفری و رهبرپور، ۱۳۹۶).

ه) دیپ‌فیک هتک‌آمیز. تغییر یا تحریف تصویر یا صوت و انتشار آن به‌نحوی‌که موجب هتک حیثیت شود، صریحا تحت ماده ۱۶ قابل تعقیب است (قانون جرائم رایانه‌ای، ۱۳۸۸: ماده ۲).

و) نفوذ از طریق بدافزار یا فیشینگ یا مهندسی اجتماعی. حسب وسیله، مشمول مواد دسترسی یا اخلال یا سرقت داده و «سوءاستفاده از ابزار» در بوداپست است (مرکز پژوهش‌های مجلس، ۱۳۸۴؛ قانون جرائم رایانه‌ای، ۱۳۸۸: ماده ۲–۱).

ز) فروش یا تجاری‌سازی غیرمجاز داده. بسته به وضعیت، ممکن است تحت «سرقت داده» (ماده ۱۲) و «افشاء اسرار» یا «نشر اکاذیب یا هتک حیثیت» قرار گیرد؛ تحلیل‌های مسؤولیت مدنی/جزایی نیز این طیف را پوشش می‌دهند (جعفری و رهبرپور، ۱۳۹۶).

یادداشت تطبیقی: فصل دوم کنوانسیون بوداپست ساختار حقوق ماهوی (مواد ۱۳–۲)، آیین دادرسی (۲۱–۱۴) و صلاحیت (۲۲) را یک‌جا تنظیم کرده و به‌روشنی از جرم‌انگاری دسترسی/شنود/اخلال/استفاده از ابزار سخن می‌گوید (مرکز پژوهش‌های مجلس، ۱۳۸۴).

۵–۲– رکن مادی

رفتار مجرمانه می‌تواند از «ورود بدون مجوز»، «رهگیری در حال انتقال»، «حذف یا تخریب یا تغییر»، «انتشار یا افشاء» تا «به‌کارگیری ابزار» امتداد یابد (مرکز پژوهش‌های مجلس، ۱۳۸۴، ۱۹–۱۸؛ قانون جرائم رایانه‌ای، ۱۳۸۸: ماده ۲–۱). وسیله –بدافزار، فیشینگ، مهندسی اجتماعی– در احراز عناصر، دلالت بر سوءنیت و عبور از تدابیر امنیتی دارد (قانون جرائم رایانه‌ای، ۱۳۸۸، ۲–۱؛ جعفری و رهبرپور، ۱۳۹۶). بزه‌دیده می‌تواند شخص حقیقی یا حقوقی باشد؛ قانون جرائم رایانه‌ای، سرقت یا اخلال نسبت به داده‌های متعلق به دیگران را نیز می‌شناسد (قانون جرائم رایانه‌ای، ۱۳۸۸: مواد ۸، ۱۲).

زمان و مکان دیجیتال؛ قانون جرائم رایانه‌ای، در صلاحیت سرزمینی یا فرامرزی معیارهای مکمل دارد (قانون جرائم رایانه‌ای، ۱۳۸۸: ماده ۲۸؛ قانون مجازات اسلامی، ۱۳۹۲: ماده ۴). گستره انتشار؛ در افشاء یا هتک، دامنه انتشار و قابلیت تکثیر بر ارزیابی شدت اثر می‌افزاید (جعفری و رهبرپور، ۱۳۹۶). نتیجه زیان‌بار (مادی یا معنوی)؛ نقض حریم داده غالبا خسارت معنوی می‌آورد، اما در تحلیل‌های «مال‌انگاری داده» نیز بحث شده است؛ مقاله‌ی جعفری و رهبرپور این بحث را نقد می‌کند (جعفری و رهبرپور، ۱۳۹۶).

۵–۳– رکن روانی

اغلب مصادیق، عمدی با «علم به محرمانه‌بودن یا عدم مجوز» هستند (مرکز پژوهش‌های مجلس شورای اسلامی ۱۳۸۴: ۱۸، قانون جرائم رایانه‌ای، مواد ۳–۱، ۱۰–۸). عمد خاص در برخی عناوین شرط است: قصد اضرار یا تشویش در ماده ۱۸ (نشر اکاذیب)، قصد افشاء یا هتک در ماده ۱۷ و قصد تحصیل داده یا مقاصد ناروا در بوداپست (مرکز پژوهش‌های مجلس، ۱۳۸۴؛ قانون جرائم رایانه‌ای، ۱۳۸۸: ماده ۲). انگیزه (مالی یا انتقامی یا کنجکاوی) تأثیر در تشکیل جرم ندارد ولی در تعیین کیفر و سیاست کیفری مؤثر است (جعفری و رهبرپور، ۱۳۹۶).

۵–۴– وضعیت‌های خاص

الف) شروع به جرم و معاونت. حسب قواعد عام تعزیرات و مقررات خاص قانون جرائم رایانه‌ای (مثلا ماده ۲۵ درباره آموزش یا تسهیل برخی جرائم).

ب) تعدد معنوی (یک فعل با چند عنوان). ماده ۱۳۱ قانون مجازات اسلامی ۱۳۹۲ در جرائم تعزیری، رفتار واحد با عناوین متعدد و مجازات اشد (بسامی، ۱۳۹۹).

ج) تکرار. مواد ۱۳۹–۱۳۷قانون ۱۳۹۲، تشدید برای ارتکاب مجدد جرم تعزیری تا درجه‌ی معین (بسامی، ۱۳۹۹).

د) جرم‌پذیری اشخاص حقوقی. مواد ۱۹ و ۲۰ قانون جرائم رایانه‌ای، شرایط انتساب و دامنه مجازات‌های تکمیلی یا انحلال را مقرر می‌کند (قانون جرائم رایانه‌ای، ۱۳۸۸، ماده ۲–۳).

ه) مسؤولیت و تکالیف پلتفرم‌ها و ارائه‌دهندگان خدمات. ماده ۲۱ قانون جرائم رایانه‌ای، تکلیف پالایش و ضمانت‌اجرا در قصور یا تقصیر را پیش‌بینی کرده است (قانون جرائم رایانه‌ای، ۱۳۸۸: ماده ۳).

تعدد نتایج و همپوشانی عناوین در فضای سایبر (مثلا نفوذ واحد منتهی به دسترسی+افشاء+اخلال) با قواعد تعدد مادی/معنوی و جمع مجازات‌ها یا مجازات اشد حل می‌شود (فروغی، ۱۴۰۲).

۵–۵– ادله اثبات الکترونیکی

الف) حجیت و امارات فنی. ادله‌ی الکترونیکی زمانی استنادپذیرند که شرایط صحت انتساب، اصالت و انکارناپذیری رعایت شود؛ راهبردهای فنی مانند رمزنگاری و بیومتریک در ادبیات داخلی به‌عنوان تضمین‌های کلیدی معرفی شده‌اند (مؤذن‌زادگان و همکاران، ۱۳۹۴).

ب) زنجیره حفاظتی. قانون جرائم رایانه‌ای در فصل دادرسی و «استنادپذیری ادله‌ی الکترونیکی» بر حفظ صحت، تمامیت و نگهداری مطابق آیین‌نامه تأکید دارد (مواد ۵۱–۴۹)؛ نیز درباره شنود محتوا، رعایت مقررات خاص مخابراتی و دستور قضایی (ماده ۴۸).

ج) اصالت و تمامیت داده (مؤذن‌زادگان و همکاران، ۱۳۹۴).

د) شنود قانونی و حدود آن (مرکز پژوهش‌های مجلس، ۱۳۸۴).

۶– تزاحم حقوق و استثنائات

۶–۱– آزادی بیان و منفعت عمومی در افشای فساد

اصل تعارض‌زدایی در بستر دیجیتال اقتضا می‌کند میان سه مطالبه‌ی مشروع توازن برقرار شود: آزادی بیان، دسترسی به اطلاعات عمومی و صیانت از حریم خصوصی. در نظام داخلی، «قانون انتشار و دسترسی آزاد به اطلاعات» همزمان دو قاعده را پیش می‌کشد: (الف) اصل دسترسی به اسناد و مکاتبات اداری با شفافیت فرایند پاسخ‌گویی (ماده ۱۴: **«پاسخ باید... شفاف و قابل ردیابی باشد»**)؛ (ب) تفکیک اطلاعات عمومی از اطلاعات مشمول حریم خصوصی و حذف یا بی‌نام‌سازی بخش‌های شخصی پیش از انتشار؛ بدین‌ترتیب «منفعت عمومی افشای فساد» توجیه‌گر نقض حریم خصوصی نیست مگر آن‌جا که با حذف مشخصات فردی، امکان افشا فراهم شود. در نتیجه، استثناء منفعت عمومی باید با معیار حداقلی‌سازی تعارض و «بی‌نام‌سازی یا تفکیک» اجرا شود، نه با انتشار بی‌قید مشخصات شخصی (نیکخواه سرنقی و همکاران، ۱۴۰۰).

۶–۲– امنیت ملی و تعقیب بزه با شنود و پایش هدفمند

استاندارد اروپایی مقابله با جرائم سایبری –در ترجمه رسمی کنوانسیون بوداپست– اختیارات شکلی را فقط با قیود حفاظتی می‌پذیرد. جمع‌آوری هم‌زمان داده‌ی در حال انتقال، شنود محتوا و بازرسی یا توقیف داده و سامانه، منوط به قانون‌مندی، ضرورت و تناسب و کنترل قضایی است (حیدرقلی‌زاده و همکاران، ۱۳۹۴). در حقوق ایران نیز «شنود محتوای در حال انتقال» صراحتا تابع مقررات خاص شنود تلفنی است و دسترسی به محتوای ذخیره‌شده در حکم شنود تلقی می‌شود؛ بنابراین، مأموریت عام برای پایش ترافیک/محتوا بدون مجوز قضایی معتبر مجاز نیست (قانون جرائم رایانه‌ای، ۱۳۸۸: ماده ۴۸). این دو منبع در کنار هم بر پایش هدفمند با مجوز و تناسب ابزار یا هدف، تأکید می‌کنند و «پایش عام» را نفی می‌نمایند.

۶–۳– رضایت یا رضایت نمایشی و امکان رجوع

در محیط‌های پلتفرمی، «رضایت» زمانی شاخص مشروعیت است که آگاهانه، مشخص، قابل‌فهم و قابل رجوع باشد (اکبری و فلاحیان، ۱۴۰۰).

۶–۴– حمایت از داده‌های حساس، کودکان و آسیب‌پذیران

پژوهش‌های فارسی در حقوق حفاظت از داده‌ها بر حساسیت ذاتی دسته‌های خاص –سلامت، زیست‌سنجی برای شناسایی افراد، گرایش‌ها و...– و لزوم تضمین‌های مضاعف، مثل ارزیابی خطر، محدودیت هدف، کمینه‌سازی، امنیت پردازش، تأکید می‌کنند؛ همچنین حمایت افزوده از کودکان و شرط سن یا

رضایت ولی در خدمات جامعه اطلاعاتی برجسته است (نصرالهی‌نیا، ۱۴۰۱).

۶-۵- مرز فضای عمومی آنلاین با انتظار معقول از خلوت

ادبیات داخلی تصریح می‌کند ماهیت فضا مثل خصوصی‌بودن آی دی، ابر شخصی در برابر پست باز و تنظیمات مخاطب و قابلیت پیش‌بینی دسترسی در احراز انتظار معقول از خلوت نقش تعیین‌کننده دارند. عمومیت‌نمایی پروفایل شرط کافی برای زوال حریم نیست؛ کیفیت رضایت، تنظیمات و زمینه‌ی انتشار یا باز انتشار، مرز واقعی عمومی و خصوصی آنلاین را می‌سازند (جعفری و رهبرپور، ۱۳۹۶؛ اکبری و فلاحیان، ۱۴۰۰).

۷- مسؤولیت‌ها، ضمانت‌اجراها و جبران خسارت

۷-۱- کیفرها و تدابیر در فقه جزایی

در فقه امامیه، هر فعل حرام فاقد حد منصوص، در قلمرو «تعزیر» داخل است و تعیین نوع و میزان کیفر، منوط به نظر حاکم شرع به‌منظور حفظ نظم و دفع مفسده است (خمینی، ۱۳۹۲؛ مکارم شیرازی، بی‌تا). در ترجمه تحریرالوسیله با صراحت آمده است که تعزیرات «منوط به نظر حاکم» است و می‌تواند بر حسب حال فاعل و آثار فعل تنظیم شود (خمینی، ۱۳۹۲). از منظر «تدابیر تکمیلی»، فقه سیاسی شیعه امکان اتخاذ اقداماتی مانند منع موقت از برخی فعالیت‌های اجتماعی یا حرفه‌ای را ذیل عنوان «تعزیرات حکومتی» برای صیانت از حقوق عامه می‌پذیرد، مادامی‌که از حد تعزیر فراتر نرود و به مثابه «سیاست شرعی» در خدمت حفظ نظام باشد (امام خمینی، ۱۳۹۲؛ موسوی اردبیلی، بی‌تا).

۷-۲- ضمانت‌اجراهای مدنی و جبران خسارت مادی یا معنوی

در حقوق ایران، زیان‌دیده می‌تواند در کنار پیگیری کیفری، جبران همه خسارات مادی و معنوی ناشی از جرم را مطالبه کند (قانون آیین دادرسی کیفری، ۱۳۹۲: ماده ۱۴، تبصر ه ۱)؛ رویه و دکترین اخیر نیز بر قابلیت جمع جبران مادی و معنوی -جز در تعزیرات منصوص شرعی و دیات- تأکید کرده‌اند (حدادی، ۱۳۹۵). در تئوری مسؤولیت مدنی، سه سنخ زیان قابل‌جبران در نقض حریم خصوصی برجسته است: تلف (از بین‌بردن داده یا محتوا یا فرصت)، تفویت منفعت (مانند از دست رفتن قرارداد یا فرصت شغلی به‌واسطه افشاء)، و هتک حیثیت (لطمه به آبرو و اعتبار) که دومی و سومی غالبا با ادله فنی، شهادت کارشناس و امارات قضایی احراز می‌شود (کاتوزیان، ۱۳۷۴؛ بابایی و آزادبخت ۱۴۰۳).

نکته روشی این است که در دعاوی نقض حریم، جمع خواسته‌ها ممکن است: مطالبه خسارت مالی (هزینه درمان روانی، کاهش درآمد)، حکم به اعاده حیثیت (عذرخواهی رسمی یا الزام به درج حکم) و حکم به توقف تعرض (اقدام تکلیفی غیرمالی). مستند قانونی امکان صدور احکام غیرمالی برای رفع زیان معنوی همان تبصره ۱ ماده ۱۴ است (قانون آیین دادرسی کیفری، ماده ۱۴).

۷-۳- تدابیر غیرکیفری و اداری

در سطح داخلی، فصل «سایر مقررات» و مواد ناظر به محتوا در قانون جرائم رایانه‌ای ۱۳۸۸، مجموعه‌ای از اوامر اداری یا قضایی پشتیبان را پیش‌بینی می‌کند:

الف) حذف یا ممانعت از دسترسی به محتوای مجرمانه (قانون جرائم رایانه‌ای، ۱۳۸۸: مواد ۲۱ و ۲۳).

ب) شنود قانونی و حدود آن (قانون جرائم رایانه‌ای، ۱۳۸۸: ماده ۴۸).

ج) اقدامات حمایتی روی ادله (قانون جرائم رایانه‌ای، ۱۳۸۸: ماده ۴۴)

در سطح تطبیقی، اسناد اتحادیه اروپا (GDPR)، بر طراحی و پیش‌فرض صیانتی (Privacy by Design/Default)، حداقل‌گرایی داده، اعلان رخداد نقض امنیتی و ارزیابی تأثیر تأکید دارند؛ این مجموعه تکالیف پیشگیرانه برای متولیان داده، به‌ویژه درباره داده‌های حساس و کودکان، به‌تفصیل گزارش شده است (لطیف‌زاده و همکاران، ۱۴۰۲). نتیجه اینکه در پرونده‌های نقض حریم، قاضی می‌تواند -علاوه بر مجازات- دستور حذف محتوا، توقف پردازش، هشدار یا تعلیق حساب کاربری و الزام به درج حکم یا عذرخواهی را به‌عنوان تدابیر تکمیلی یا رفع زیان مقرر کند؛ مبنای کیفری و اداری آن در قانون جرائم رایانه‌ای و مبنای مدنی، یعنی اعاده حیثیت در ماده ۱۴ قانون آیین دادرسی کیفری آمده است.

۷-۴- مسؤولیت پلتفرم‌ها و متولیان داده

الف) مسؤولیت کیفری اشخاص حقوقی و مدیران (قانون جرائم رایانه‌ای، ۱۳۸۸: مواد ۲۰-۱۹).

ب) تکلیف همکاری و اعلام (قانون جرائم رایانه‌ای، ۱۳۸۸: تبصره ماده ۲۳).

ج) طراحی و پیش‌فرض صیانتی (قانون جرائم رایانه‌ای، تبصره ماده ۲۳؛ موسوی اردبیلی، بی‌تا).

۸- صلاحیت، تعارض قوانین و همکاری‌های فراملی

۸-۱- صلاحیت سرزمینی، شخصی و مبتنی بر اثر در جرائم آنلاین

در حقوق ایران، «اصل سرزمینی» نقطه آغاز است؛ اما «قانون جرائم رایانه‌ای» به‌طور خاص دامنه صلاحیت را برای وضعیت‌های سایبری گسترش داده است: الف) هرگاه داده‌های مجرمانه یا ابزار ارتکاب، در سامانه یا حامل موجود در قلمرو ایران ذخیره باشد؛ ب) اگر جرم از طریق تارنماهای دارای دامنه مرتبه‌بالای کد کشوری ایران (ir.) ارتکاب یابد. این دو بند، صورت‌بندی روشنی از «صلاحیت مبتنی بر اثر یا ارتباط عینی با قلمرو» در حوزه سایبر ارائه می‌کند (قانون جرائم رایانه‌ای، ۱۳۸۸: ماده ۲۸).

در سطح اسناد بین‌المللی، کنوانسیون بوداپست (ترجمه مرکز پژوهش‌های مجلس) در ماده ۲۲، چهار قاعده صلاحیتی را هم‌زمان پیش‌بینی می‌کند: قلمرو، پرچم کشتی، ثبت هواپیما و برخی موارد صلاحیت حمایتی یا شخصی؛ و نیز هماهنگی میان دولت‌هایی که هم‌زمان ادعای صلاحیت دارند (مرکز پژوهش‌های مجلس شورای اسلامی، ۱۳۸۴: مواد ۲۷-۲۸). این چارچوب، مدل مقبول برای جمع میان صلاحیت‌های موازی و کاهش تعارض مثبت است (مرکز پژوهش‌های مجلس شورای اسلامی، ۱۳۸۴: ماده ۲۲).

در ادبیات داخلی نیز بر ظرفیت اعمال «صلاحیت حمایتی» در برخی جرائم سایبری شدید (مانند تروریسم سایبری) تأکید شده است؛ مبنای آن، لطمه به منافع اساسی کشور فارغ از مکان ارتکاب است (ابوالمعالی‌الحسینی و همکاران، ۱۳۹۶).

۸-۲- تعارض قوانین در داده‌های فرامرزی و ذخیره‌سازی ابری

چالش «محل داده» در رایانش ابری، تعیین قانون حاکم و مرجع صالح را سخت می‌کند؛ قراردادهای ابری غالبا مختلط‌اند و مکان‌استقرار داده یا پردازش، متکثر و سیال است. پژوهش‌های فارسی در حقوق قراردادهای ابری، نشان می‌دهند تکیه صرف بر قالب‌های کلاسیک (اجاره یا ودیعه یا لیسانس) کفایت ندارد و باید به قواعد عام قراردادها (ماده ۱۰ ق.م) و شرط‌گذاری دقیق درباره «محل پردازش یا ذخیره‌سازی یا انتقال» و «انتخاب قانون حاکم» رو آورد (انصاری و کاتب دامغانی، ۱۴۰۱).

از منظر حاکمیت و دسترسی دول خارجی، محل دیتاسنتر و «دسترسی برون‌مرزی» دولت میزبان می‌تواند با اصول حاکمیت و حمایت‌های داخلی از داده شخصی در تعارض افتد؛ این ادبیات بر ضرورت شفاف‌سازی قراردادی، رمزنگاری سراسری و محدودسازی محل استقرار برای کاهش ریسک تعارض مقررات تأکید دارد (صالحی، ۱۳۹۸).

۸-۳- ادله الکترونیکی فرامرزی، انتقال متقابل و معاضدت قضایی

در بخش «همکاری بین‌المللی» کنوانسیون بوداپست، اصول کلی و ابزارهای عملیاتی برای دستیابی فرامرزی به ادله پیش‌بینی شده است: از «حفظ یا توقیف فوری داده‌ها»، «دسترسی و شنود در چهارچوب قانون»، تا «معاضدت قضایی» و «استرداد»؛ همگی با قیود حقوق بشری مواد ۱۴ و ۱۵ مقید شده‌اند (مرکز پژوهش‌های مجلس، ۱۳۸۴: ماده ۲۱).

در حقوق ایران، «قانون جرائم رایانه‌ای» ضمن تصریح بر استنادپذیری ادله الکترونیکی و ضرورت حفظ «صحت، تمامیت، اعتبار و انکارناپذیری» (قانون جرائم رایانه‌ای، مواد ۵۱-۴۰)، وزارت دادگستری را مکلف به پیگیری الحاق به اسناد همکاری و معاضدت دوجانبه/چندجانبه کرده است (قانون جرائم رایانه‌ای، ۱۳۸۸: مواد ۵۲-۴۹). علاوه بر اسناد چندجانبه، ایران معاهدات دوجانبه معاضدت کیفری متعددی دارد؛ به‌عنوان نمونه، «معاهده معاضدت حقوقی دوجانبه در امور کیفری ایران-چین» دامنه گسترده‌ای از همکاری‌ها، مثل ابلاغ، اخذ شهادت، ارائه اسناد و ادله، تفتیش، توقیف، ضبط

ابزار جرم، شناسایی و استرداد عواید ناشی از جرم را با تشریفات مشخص بیان می‌کند (معاهده معاضدت حقوقی دوجانبه در امور کیفری میان ایران و چین، مصوب ۱۳۹۵، مواد ۱۶ و ۲۰-۱۹).

در ادبیات فارسی معاصر نیز «معاضدت درباره ادله الکترونیکی» و اقتضائات نوین آن مانند سرعت، حفاظت زنجیره نگهداری، و قالب‌های استاندارد پاسخ، تشریح و بر لزوم بازمهندسی رویه‌های سنتی نیابت قضایی تأکید شده است (تبریزی و همکاران، ۱۴۰۱).

۸-۴- سیاست‌های همگرایی و الگوهای سازگارسازی با موازین فقهی

در سطح سیاستی، سه محور برای همگرایی پیشنهاد می‌شود:

الف) تقنین همسو با استانداردهای بین‌المللی با «حق‌شرط»های صریح بر بنیان‌های شرعی (مانند صیانت از حریم مؤمن، منع تجسس و ضرورت نظارت قضایی بر شنود). متن فارسی کنوانسیون بوداپست امکان حق‌شرط نسبت به برخی مواد را نیز یادآور شده است (مرکز پژوهش‌های مجلس، ۱۳۸۴، مواد ۴۳-۴۲).

ب) توسعه معاهدات دوجانبه همسو با فقه. تجربه شورای نگهبان در بررسی فقهی معاهدات استرداد و قیود شرعی بر استرداد یا معاضدت، الگوی خوبی برای طراحی شروط «عدم تعارض با نظم عمومی و موازین شرع» در موافقت‌نامه‌های کیفری و ادله الکترونیکی است (فتحی، ۱۳۹۶).

ج) تبیین معیارهای تناسب یا ضرورت یا نظارت قضایی در ابزارهای ادله‌محور (توقیف، دسترسی، شنود). هم‌زمان با ارتقای ظرفیت داخلی برای اجرای معاضدت‌ها و حفاظت از حقوق بزه‌دیدگان و متهمان (قانون آیین دادرسی کیفری، ۱۳۹۲: ماده ۱۴؛ و قانون جرائم رایانه‌ای، ۱۳۸۸: مواد ۴۹-۵۲).

نتیجه‌گیری

مبانی فقه جزایی اسلامی و نظام‌های معاصر در اصول بنیادی حفاظت از حریم خصوصی-مانند منع تجسس، حرمت افشای اسرار و لزوم سنجش مداخلات بر اساس ضرورت و تناسب- اشتراک دارند، اما در زبان و صورت‌بندی متفاوت‌اند؛ فقه بر قواعدی چون ستر، لاضرر و سلطنت افراد تکیه می‌کند و حقوق معاصر مفاهیمی چون «داده شخصی» و «پردازش مشروع» را محور قرار می‌دهد و سازوکارهای اداری، مدنی و کیفری مشخص عرضه می‌کند؛ نظام‌های اروپایی با ترکیب حق بنیادین حریم و کنوانسیون بوداپست چارچوب‌های سخت‌گیرانه‌تری فراهم ساخته‌اند و تجربیات ایالات‌متحده و انگلستان بر انتظار معقول از خلوت و جرم‌انگاری دسترسی بدون مجوز تأکید دارد؛ ادبیات فارسی/عربی مبانی قوی عرضه کرده اما همچنان نیازمند تفکیک اقسام حریم متناسب با معماری‌های نوین، تدوین شاخص‌های آزمون‌پذیر برای انتظار معقول و پیوند نظام‌مند قواعد فقهی با عناصر و ادله دیجیتال است؛ لذا تقنین همسان‌ساز با قیدهای شرعی، الزام پلتفرم‌ها به حریم خصوصی در طراحی و گزارش رخداد، تدوین شاخص‌های آزمون‌پذیر و تقویت معاضدت قضایی و تعیین تکلیف محل نگهداری داده‌ها باید پیگیری شود تا هم عدالت قربانیان تأمین و هم کشف جرم در چارچوب ضرورت، تناسب و نظارت قضایی ممکن گردد.

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

تعارض منافع: تدوین این مقاله، فاقد هرگونه تعارض منافعی بوده است.

سهم نویسندگان: نگارش مقاله به‌صورت انفرادی توسط نویسنده انجام گرفته است.

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

تأمین اعتبار پژوهش: این پژوهش بدون تأمین اعتبار مالی سامان یافته است.

منابع و مآخذ

- قرآن کریم

- ابوالمعالی‌الحسینی، سیدمحمدجواد و فتحی، سیدرضا (۱۳۹۶). «دکترین شخص ثالث و تحصیل دلایل جرائم سایبری». *پژوهش حقوق کیفری*، (۱۸): ۶۴۶-۶۰۶.

– افتخار جهرمی، غلامرضا (۱۳۹۳). «نحوه اعمال صلاحیت دادگاه‌ها در رسیدگی به جرائم فضای مجازی: تحلیل صلاحیت محلی در پرتو مواد ۲۸–۲۹ قانون جرائم رایانه‌ای». *فصلنامه مطالعات حقوقی*، (۳۹): ۷۶–۹۳.

– اکبری، علی و فلاحیان، مهدی (۱۴۰۰). «حریم خصوصی در نظام حقوقی ایران و اسلام». *تمدن حقوقی*، ۴(۹): ۳۸۲– ۳۶۱.

– امام خمینی، روح‌الله (۱۳۹۲). *ترجمه تحریرالوسیله*. تهران: مؤسسه تنظیم و نشر آثار امام خمینی.

– انصاری، باقر و کاتب دامغانی، محمدمهدی (۱۴۰۱). «رژیم حقوقی قراردادهای رایانش ابری». *تحقیقات حقوقی* (دانشگاه شهید بهشتی)، ۹۸(۲۵): ۲۴۴–۲۱۹.

– بابایی، ایرج و آزادبخت، شبیر (۱۴۰۳). «مطالعه تطبیقی مسؤولیت مدنی ناشی از هتک شهرت در حقوق ایران، آمریکا و انگلیس». *مجله حقوقی دادگستری*، ۱۲۵(۸۸): ۳۶۳–۳۹۷.

– بسامی، علیرضا (۱۳۹۹). «تحلیل تعدد معنوی جرم در حقوق کیفری ایران؛ اشاره به ماده ۱۳۱ قانون ۱۳۹۲». *پژوهش حقوق کیفری*، (۴۹): ۴۱–۶۵.

– تبریزی، صادق؛ الهی‌منش، محمدرضا؛ عالی‌پور، حسن؛ طهماسبی، جواد و فضلی، مهدی (۱۴۰۱). «اصل قانونمندی توقیف داده و سامانه در فرآیند کیفری؛ آثار و تضمین‌ها». *تعالی حقوق*، ۱۳(۲): ۱۲۵–۱۳۴.

– جعفری، علی و رهبرپور، محمدرضا (۱۳۹۶). «مسؤولیت مدنی نقض حریم خصوصی داده‌ها در فقه امامیه و حقوق موضوعه». *فصلنامه پژوهش حقوق خصوصی*، ۱۸(۵): ۴۴–۵۲.

– حدادپور، جواد (۱۴۰۱). «حریم خصوصی افراد در فقه امامیه و حقوق موضوعه». *فصلنامه آراء*، (۲): ۵۶–۴۳.

– حدادی، فاضل (۱۳۹۵). «جبران خسارت معنوی از منظر فقه و حقوق». *مجله علمی دانش‌پژوهان*، (۵ و ۶): ۴۲–۲۷.

– حر عاملی، محمدبن‌حسن (بی‌تا). *وسائل‌الشیعة*. قم: مؤسسه آل‌البیت (ع).

– حیدرقلی‌زاده، جعفر؛ عابدینی، غلامرضا و رئیسی، لیلا (۱۳۹۴). «حریم خصوصی و الزام به رعایت آن در رویه قضایی دادگاه اروپایی حقوق بشر». *مطالعات حقوق بشر اسلامی*، ۴(۸): ۲۳–۴۱.

– شرقی، زهرا (۱۳۹۸). «مسؤولیت مدنی ناشی از افترا در کامن‌لا با رویکرد تطبیقی». *پژوهشنامه حقوق خصوصی (علامه)*، (۷۹): ۲۷–۲۵.

– صالحی، جواد (۱۳۹۸). «دسترسی به اطلاعات دیتاسنتر دولت خارجی در تقابل با اصول صلاحیت کیفری سرزمینی و اعمال حاکمیت در حقوق بین‌الملل». *فصلنامه علمی حقوقی بین‌المللی*، ۶۰(۳۶): ۱۸۵–۲۱۰.

– طباطبایی، محمدحسین (۱۳۷۴). *المیزان فی تفسیر القرآن*. قم: جامعه مدرسین.

– غفاری‌الهی‌کاشانی، نجمه (۱۳۹۷). «صلاحیت سرزمینی دادگاه‌های ایران نسبت به جرائم ارتکابی در فضای سایبر». *پژوهش‌های حقوقی*، ۲۱۸–۱۸۵.

– فتحی، یاسر (۱۳۹۶). «گستره و قلمرو حریم خصوصی در فضای مجازی». *دوفصلنامه حقوق و سیاست*، (۴۵): ۹۱–۱۱۸.

– فرجی‌ها، محمد و علمداری، علی (۱۳۹۶). «مطالعه تطبیقی معیارهای جرم‌انگاری در فضای سایبر در ایران و آلمان». *مطالعات حقوق تطبیقی*، ۸(۲): ۶۳۷–۶۵۳.

– فروغی، مهدی (۱۴۰۲). «تعدد نتیجه در جرائم تعزیری براساس قانون مجازات اسلامی ۱۳۹۲؛ دیدگاه‌های حقوقی (تحلیل ماده ۱۳۴ و تفکیک از تعدد معنوی)». *فصلنامه حقوقی مفید*، (۳۵): ۳۲–۵۸.

– فرهمند، فرید (۱۴۰۳). «طرح حمایت و حفاظت از داده و اطلاعات شخصی با مطالعه‌ی تطبیقی مقررات عمومی حفاظت از داده (GDPR)». *حقوق فناوری‌های نوین*، ۹(۵): ۲۵–۱۷.

– کاتوزیان، ناصر (۱۳۷۴). *الزام‌های خارج از قرارداد (مسؤولیت مدنی)*. تهران: دانشگاه تهران.

- کاتوزیان، ناصر (۱۳۹۲). *مسؤولیت مدنی*. تهران: دانشگاه تهران.

- لطیف‌زاده، مهدیه؛ قبولی‌درافشان، سیدمحمدمهدی؛ محسنی، سعید و عابدی، محمد (۱۴۰۲). «چگونگی پردازش داده شخصی خاص در حقوق اتحادیه اروپا و بررسی آن در نظام حقوقی ایران». *فصلنامه JIPM*، ۱(۳۹): ۲۰۰-۱۵۷.

- مکارم شیرازی، ناصر (بی‌تا). *أنوار الفقاهة (کتاب الحدود)*، قم: مدرسه امام علی بن ابیطالب (ع).

- مؤذن‌زادگان، حسنعلی؛ سلیمان‌دهکردی، الهام و یوشی، مهشید (۱۳۹۴). «حفظ صحت و استنادپذیری ادله‌ی الکترونیک با استفاده از بیومتریک و رمزنگاری». *پژوهش حقوق کیفری*، (۱۲): ۶۹-۹۷.

- موسوی اردبیلی، سیدعبدالکریم (بی‌تا). *فقه الحدود و التعزیرات*. قم: کتابخانه نور.

- میرشکاری، محمدحسین (۱۳۹۷). «استثناهای حق تصویر». *مطالعات حقوق تطبیقی*، (۳۹): ۱۶۵-۱۷۴.

- نصرالهی‌نیا، عمار (۱۴۰۱). ح*قوق بیماران؛ حریم خصوصی، محرمانگی و رازداری*. قم: معاونت پژوهش.

- -نوری، حسین (بی‌تا). *مستدرک الوسائل*. قم: مؤسسه آل‌البیت (ع).

- نیکخواه سرنقی، رضا؛ اکرادی، سعید؛ جعفرزاده، سیامک (۱۴۰۰). «حریم خصوصی تابعان و پیوند آن با قضا، فقه، اخلاق و سیاست جنایی». *مطالعات فقه و حقوق اسلامی*، ۱۳(۲۵): ۳۶-۱۱.

- وحابی، زهرا (۱۴۰۴). «جایگاه مأمورین امنیتی انگلستان در کشف جرائم». *دوماهنامه ولایت فقیه و فقه حکومتی*، (۵۱): ۵۸۳-۳۷۳.