Journal of Governmental Jurisprudence. 2026. Autumn and Winter 10(20): 109-137; DOI:10.30471/MSSH.2025.10907.2635

Research Institute of Hawzah and University

Journal of Governmental Jurisprudence

Journal homepage: https://fh.rihu.ac.ir/

Original Article

Jurisprudential and Legal Foundations of Data Sovereignty in Cyber Armed Conflicts: A Comparative Study of Governmental Jurisprudence and the European Legal System in Protecting Critical Infrastructures (with a focus on the third imposed war)

Seyed Ali Mirlohi[1]

1. PhD student in Jurisprudence and Private Law, Law Department, Faculty of Jurisprudence and Law, Shahid Motahari University and Higher School, Tehran, Iran.

Mirlohi@motahari.ac.ir

Abstract

Introduction and Objectives: The paradigm shift in international hostilities and the transfer of the center of gravity of conflicts to communication infrastructures have confronted the traditional concepts of “sovereignty” and “self-defense” with fundamental challenges. The events of March 2026 (Esfand 1404) and the multi-layered onslaught of the hostile coalition against the nation’s information arteries underscored the necessity of a jurisprudential-legal re-examination of cyber defense. Employing a descriptive-analytical method, this research seeks to elucidate the capacities of Government Jurisprudence (Fiqh al-Hukuma) in safeguarding the National Information Network and managing emerging crises, such as autonomous weaponry and algorithmic contracts.

The findings indicate that, based on principles such as Nafy al-Sabil (Denial of Means/Way), Hifz al-Nizam (Preservation of the System), and La Darar (No Harm), data sovereignty is not merely a technical necessity but a religious obligation (Taklif). In this regard,

Research Institute of Hawzah and University

Journal of Governmental Jurisprudence

Journal homepage: https://fh.rihu.ac.ir/

Original Article

the article, by proposing the innovative construct of "Data as Anfal" (Spoils of War), emphasizes the need to redefine big data ownership during wartime and examines the legal personality of tech hyper-corporations collaborating with enemies under the categories of "Muharib" (Belligerent) and "Baghi" (Rebel). Furthermore, a comparative study with the General Data Protection Regulation (GDPR) reveals a convergence between jurisprudential logic and international law's national security exceptions regarding the application of "algorithmic escape hatches" and intervention in smart contracts. Ultimately, the events of March 2026 necessitate that legislators, by formulating a "Cyber-State of Emergency Legal Regime," move toward establishing a comprehensive system of active defense and damage compensation based on the joint and several liability of the hostiles.

Keywords: Government Jurisprudence, Data Sovereignty, Cyber Warfare, National Information Network, Principle of Nafy al-Sabil, Self-Defense.

Cite this article: Mirlohi, Seyed Ali (2026). Jurisprudential and Legal Foundations of Data Sovereignty in Cyber Armed Conflicts: A Comparative Study of Governmental Jurisprudence and the European Legal System in Protecting Critical Infrastructures (with a focus on the third imposed war). *Journal of Governmental jurisprudence*, 10(20): 109-137.

DOI:10.30471/MSSH.2025.10907.2635 فقه حکومتی، پاییز و زمستان ۱۴۰۴، دوره ۱۰، شماره ۲۰، صص۱۰۹-۱۳۷؛

Research Institute of Hawzah and University

فقه حکومتی

Journal homepage: https://fh.rihu.ac.ir/

نوع مقاله: پژوهشی

مبانی فقهی-حقوقی حاکمیت داده در شرایط مخاصمات سایبری؛ مطالعه تطبیقی رویکرد فقه حکومتی و نظام حقوقی اروپا در صیانت از زیرساخت‌های حیاتی (با محوریت جنگ تحمیلی سوم)

سیدعلی میرلوحی[۱]

۱. دانشـــجوی دکتری فقه و حقوق خصوصی، گروه حقوق، دانشکده فقه و حقوق، مدرسه عالی و دانشگاه شهید مطهری(ره)، تهران، ایران. رایانامه.

Mirlohi@motahari.ac.ir

چکیده

مقدمه و اهداف: تغییر پارادایم مخاصمات بین‌المللی و انتقال ثقل درگیری‌ها به زیرساخت‌های ارتباطی، مفاهیم سنتی «حاکمیت» و «دفاع مشروع» را با چالش‌های بنیادین مواجه ساخته است. رویدادهای اسفند ۱۴۰۴ و هجوم چندلایه ائتلاف متخاصم به شریان‌های اطلاعاتی کشور، لزوم بازخوانی فقهی-حقوقی دفاع سایبری را نمایان کرد. پژوهش حاضر با روش توصیفی-تحلیلی، در پی تبیین ظرفیت‌های فقه حکومتی در صیانت از شبکه ملی اطلاعات و مدیریت بحران‌های مستحدث نظیر تسلیحات خودکار و قراردادهای الگوریتمی است.

یافته‌های تحقیق نشان می‌دهد که با ابتناء بر قواعدی نظیر «نفی سبیل»، «حفظ نظام» و «لا ضرر»،

Research Institute of Hawzah and University

فقه حکومتی

Journal homepage: https://fh.rihu.ac.ir/

نوع مقاله: پژوهشی

حاکمیت داده نه تنها یک ضرورت فنی، بلکه یک تکلیف شرعی است. در این راستا، مقاله با ارائه انگاره نوآورانه «داده به مثابه انفال»، بر لزوم بازتعریف مالکیت کلان‌داده‌ها در زمان جنگ تأکید کرده و شخصیت حقوقی ابرشرکت‌های فناوری همدست با دشمن را ذیل عنوان «محارب و باغی» واکاوی می‌کند. همچنین، مطالعه تطبیقی با مقررات عمومی حفاظت از داده اروپا (GDPR)، حاکی از هم‌گرایی منطق فقهی با استثنائات امنیت ملی در حقوق بین‌الملل برای اعمال «دریچه‌های فرار الگوریتمی» و مداخله در قراردادهای هوشمند است. در نهایت، واقعه اسفند ۱۴۰۴ ایجاب می‌کند تا قانون‌گذار با تدوین «رژیم حقوقی وضعیت فوق‌العاده سایبری»، به سمت استقرار نظام جامع پدافند فعال و جبران خسارات بر مبنای مسئولیت تضامنی متخاصمین حرکت نماید.

واژگان کلیدی: فقه حکومتی، حاکمیت داده، جنگ سایبری، شبکه ملی اطلاعات، قاعده نفی سبیل، دفاع مشروع.

استناد: میرلوحی، سیدعلی (۱۴۰۴). مبانی فقهی-حقوقی حاکمیت داده در شرایط مخاصمات سایبری؛ مطالعه تطبیقی رویکرد فقه حکومتی و نظام حقوقی اروپا در صیانت از زیرساخت‌های حیاتی (با محوریت جنگ تحمیلی سوم). مجله فقه حکومتی ۱۰(۲۰): ۱۰۹-۱۳۷.

مقدمه

تحول بنیادین در ماهیت مخاصمات مسلحانه در دهه سوم قرن بیست و یکم، مفاهیم کلاسیک حاکمیت و دفاع را از ساحت فیزیکی به فضاهای انتزاعی و در عین حال حیاتیِ سایبری منتقل کرده است. در این پارادایم نوین، داده‌ها دیگر صرفاً ابزارهایی برای اطلاع‌رسانی یا تسهیل امور دیوان‌سالارانه نیستند، بلکه به عنوان «دارایی‌های استراتژیک» و «قلمرو نوین حاکمیتی» شناخته می‌شوند که هرگونه خلل در صیانت از آن‌ها، موجودیت سیاسی و امنیتی یک کشور را با تهدیدات موجودیتی مواجه می‌سازد (ضیایی بیگدلی، ۱۴۰۲، ۱۱۲). تجربه تلخ و در عین حال عبرت‌آموز جنگ تحمیلی سوم که در ادبیات سیاسی و نظامی به «جنگ رمضان» شهرت یافت، به وضوح نشان داد که مرزهای دیجیتال ایران در اسفند ۱۴۰۴، هدف نخستین و سنگین‌ترین حملات ائتلاف غربی-صهیونیستی بوده است. در این نبرد ۴۱ روزه، دشمن با بهره‌گیری از پیچیده‌ترین جنگ‌افزارهای الگوریتمی و حملات هدفمند به ستون فقرات شبکه ملی اطلاعات، نه تنها به دنبال از کار انداختن زیرساخت‌های فیزیکی، بلکه در پی «استعمار داده‌ای» و فلج‌سازی کامل قوه مدبره کشور بود (Anderson, 2026, p. 89). واقعه هولناک نهم اسفند و شهادت مظلومانه نخبگان و رهبری نظام، نشان‌دهنده لایه جدیدی از جنایات جنگی است که در آن، اطلاعاتِ مکانی و داده‌های حساس زیرساختی به عنوان ابزار تروریسم دولتی مورد سوءاستفاده قرار گرفتند. از منظر فقه حکومتی، این هجوم چندلایه، مصداق بارز «سبیل» و سلطه غیرقانونی اجانب بر مقدرات جامعه اسلامی است که بر اساس قاعده بنیادین «نفی سبیل»، انسداد تمامی مجاری آن بر آحاد جامعه و به ویژه بر حاکمیت، تکلیفی شرعی و تخلف‌ناپذیر محسوب می‌شود (عمید زنجانی، ۱۳۹۹، ۷۴). دقت در ادله فقهی نشان می‌دهد که شمول قواعدی همچون نفی سبیل در فضای سایبر، صرفاً یک ارجاع کلان نیست، بلکه مبتنی بر تنقیح مناط قطعی از حرمتِ استیلای کفار بر منابع مالی و نظامی است. بر اساس دیدگاه صاحب عناوین، قاعده نفی سبیل بر تمامی عقود و ایقاعاتی که منجر به تضعیف موضع قدرت جامعه اسلامی شود، حاکم (حکومت اصطلاحی) است (مراغی، ۱۴۱۷، ج ۲، ۳۵۰). در شرایط جنگ رمضان، سبیل در لایه پلتفرم و داده رخ داد؛ لذا وجوبِ انسداد این سبیل، از باب مقدمه واجب برای حفظ نظام، الزامی شرعی می‌یابد. با این حال، حدود این مداخله حاکمیتی، محدود به قدر متیقن از ضرورت دفاعی است و بر اساس قاعده الضرورات تبیح المحظورات، به محض رفع خطر تجاوز، اصل

بر بازگشت به مالکیت خصوصی و رعایت حریم شخصیِ داده‌ای شهروندان است؛ چرا که الضروره تُقدّر بقدرها (ابن‌نجیم، ۱۴۱۹، ص ۸۵).در فقه امامیه، صیانت از کیان جامعه اسلامی (بیضه اسلام) همواره به عنوان اوجب واجبات مطرح بوده و در عصر حاضر، شبکه ملی اطلاعات و حاکمیت بر داده‌های ملی، بخشی تفکیک‌ناپذیر از این کیان به‌شمار می‌روند (جوادی آملی، ۱۴۰۱، ج ۲، ۴۱۵). نفوذ دشمن در لایه‌های پنهان داده‌ای در جریان جنگ رمضان، ضرورت بازخوانی مفاهیمی همچون «ثغور اسلام» را ایجاب می‌کند؛ چرا که امروز، مرزبانان کشور همان متخصصانی هستند که در اتاق‌های عملیات سایبری، مانع از دست‌اندازی بیگانگان به حریم داده‌ای شهروندان و نهادهای حاکمیتی می‌شوند.با این حال، چالش اساسی زمانی رخ می‌نماید که تلازم میان «امنیت ملی» و «آزادی‌های فردی» در بستر حقوق عمومی مورد مداقه قرار می‌گیرد. در جریان بحران اسفند ۱۴۰۴، مدیریت متمرکز جریان داده و محدودسازی دسترسی به پلتفرم‌های متخاصم، اگرچه ضرورتی گریزناپذیر برای پدافند سایبری بود، اما نیازمند تبیین دقیق فقهی و حقوقی است تا از شائبه استبداد دیجیتال مبرا گردد.

در این راستا، مطالعه تطبیقی با نظام‌های حقوقی پیشرو، از جمله اتحادیه اروپا، حقایق قابل تأملی را آشکار می‌سازد. مقررات عمومی حفاظت از داده (GDPR)، علیرغم تاکید فراوان بر حریم خصوصی، در ماده ۶ و ۲۳ خود صراحتاً «امنیت ملی»، «دفاع» و «امنیت عمومی» را به عنوان استثنائات مشروعی بر حقوق کاربران معرفی کرده و به دولت‌ها اجازه می‌دهد در شرایط اضطراری، حاکمیت متمرکز خود را اعمال کنند (Voigt & Von dem Bussche, 2017, p. 156). این تقارن نظری میان احکام حکومتی در فقه و استثنائات امنیت ملی در حقوق غرب، نشان‌دهنده یک عقلانیت حقوقی مشترک در مواجهه با تهدیدات موجودیتی است.مسئله اصلی این پژوهش، واکاوی نسبت میان این ضرورت‌های امنیتی با مبانی فقهی در بستر واقعیت‌های جنگ تحمیلی سوم است. چگونه می‌توان از ظرفیت قاعده‌مند «حکم حکومتی» برای تدوین رژیم حقوقیِ «وضعیت فوق‌العاده سایبری» بهره جست؟ آیا می‌توان مدعی شد که صیانت از شبکه ملی اطلاعات در زمان جنگ، نه تنها یک اقدام پدافندی، بلکه یک «واجب کفایی» برای صیانت از نظام است؟ (مکارم شیرازی، ۱۴۰۱، ۳۰۲). اهمیت این موضوع زمانی دوچندان می‌شود که بدانیم تروریسم زیرساختی اعمال شده در اسفند ۱۴۰۴، خسارات مادی و معنوی جبران‌ناپذیری به بخش‌های خصوصی و عمومی وارد کرد که پیگیری حقوقی آن در مراجع بین‌المللی، مستلزم وجود یک

دکترین داخلی منسجم در حوزه مسئولیت مدنی و کیفری سایبری است (قدیر و کاظمی فروشانی،۱۳۹۸، ۲۶۳).این نوشتار با رویکردی تحلیلی و با هدف تولید ادبیات علمی در حوزه «فقه دفاع سایبری»، در صدد است تا ضمن نقد رویکردهای سنتی به حاکمیت، الگویی نوین از حاکمیت داده را ترسیم نماید که در آن، استقلال دیجیتال به عنوان پیش‌شرط استقلال سیاسی و اقتصادی تلقی می‌شود. در واقع، نبرد رمضان به ما آموخت که در جهانِ به‌هم‌پیوسته امروز، کشوری که بر داده‌های خود حاکمیت نداشته باشد، عملاً فاقد حاکمیت بر سرنوشت خویش است (Floridi, 2024, p. 210). از این رو، تدوین مبانی فقهی حقوقی این حوزه، نه یک تمرین آکادمیک، بلکه یک ضرورت حیاتی برای بقای ملی در عصر مخاصمات هوشمند است. شایان ذکر است جنگ تحمیلی سوم، پارادایم دفاع را از واکنش‌های فیزیکی به پیش‌بینی‌های الگوریتمی تغییر داد. تهاجم اسفند ۱۴۰۴ نشان داد که قدرت‌های سلطه‌گر با تکیه بر دارایی‌های معرفتی و پردازش کلان‌داده‌های شهروندان، به دنبال بازمهندسیِ اراده ملی هستند (فیروزآبادی و احمدآبادی آزادی، ۱۳۹۹، ۵۳۸). لذا واکاویِ این مسئله که فقه حکومتی چگونه می‌تواند در برابر استعمار دیجیتال قد علم کند، تنها یک بحث نظری نیست؛ بلکه تلاشی برای تبیینِ حقوقیِ مرزهای نامرئیِ دارالاسلام است. پژوهش حاضر بر آن است تا با عبور از نگاه‌های جزیره‌ای به فضای مجازی، حاکمیت داده را به عنوان رکن چهارمِ تمامیت ارضی در کنار زمین، دریا و فضا بازتعریف نماید (ملک‌زاده،۱۳۹۹). این بازتعریف، مستلزم آن است که ابتدا ماهیتِ ابزارهای جنگیِ نوین در ترازوهای فقهی و حقوقی توزین گردد؛ چرا که بدون شناخت دقیق موضوع، صدور حکم حکومتی در حوزه پدافند سایبری ناممکن خواهد بود.در ادامه، ضمن تبیین مفاهیم بنیادین، به بررسی تطبیقی مبانی مشروعیت اقدامات حاکمیتی در شبکه ملی اطلاعات پرداخته و در نهایت، چارچوبی برای جبران خسارات و مسئولیت پذیری متخاصمین ارائه خواهد شد.

۱. مبانی نظری و مفهومی

۱-۱. سطوح سه‌گانه حاکمیت داده در پارادایم فقه حکومتی

در تحلیل فقهی و حقوقی حکمرانی داده، نمی‌توان از یک رژیم حقوقی واحد برای تمامی شرایط سخن گفت؛ زیرا میزان اختیارات حاکمیت و حدود حقوق اشخاص تابع وضعیت‌های مختلف امنیتی و

اجتماعی است. ازاین‌رو، برای تبیین دقیق جایگاه داده در فقه حکومتی، باید میان سه سطح متمایز از حاکمیت داده شامل وضعیت عادی، وضعیت اضطراری و وضعیت مخاصمه مسلحانه تفکیک نمود. این تفکیک، علاوه بر انطباق با مبانی فقه سیاسی امامیه، با نظریه‌های نوین حکمرانی سایبری و امنیت ملی نیز همخوانی دارد و امکان ایجاد تعادل میان حقوق بنیادین شهروندان و الزامات امنیت عمومی را فراهم می‌آورد.

۱-۱-۱. حاکمیت داده در شرایط عادی

در وضعیت عادی و شرایط صلح، اصل بر حاکمیت اشخاص بر داده‌های خویش و رعایت حریم خصوصی است. داده‌های شخصی در این وضعیت بخشی از حقوق فردی محسوب می‌شوند و هرگونه دسترسی یا پردازش آنها نیازمند رضایت صاحب داده یا مجوز قانونی است. این رویکرد با قواعد فقهی تسلیط، احترام مال و حرمت تجسس سازگار بوده و دولت صرفاً نقش تنظیم‌گر را بر عهده دارد. ازاین‌رو، مداخله در گردش داده‌ها تنها در حدود قوانین و با نظارت مراجع صالح امکان‌پذیر خواهد بود (موسوی بجنوردی، ۱۴۱۹ق، ۸۵).

۱-۱-۲. حاکمیت داده در شرایط اضطراری غیرجنگی

در شرایطی که حملات سایبری محدود، بدافزارها یا باج‌افزارها امنیت عمومی و عملکرد زیرساخت‌های حیاتی را تهدید می‌کنند، حاکمیت می‌تواند برای دفع خطر و حفظ نظم عمومی برخی محدودیت‌های موقت و متناسب را اعمال نماید. مبنای فقهی این اختیارات را می‌توان در نهاد حسبه، قاعده لاضرر و ضرورت حفظ نظام جست‌وجو کرد. با این حال، این اقدامات باید موقتی، ضروری و متناسب با سطح تهدید بوده و به نقض دائمی حقوق شهروندان منجر نشود (منتظری، ۱۳۸۹، ۲۵۸؛ امام خمینی، ۱۳۹۲، ۱۰۵).

۱-۱-۳. حاکمیت داده در وضعیت جنگ سایبری

با تحقق مخاصمه سایبری، داده از یک دارایی صرفاً خصوصی فراتر رفته و به یکی از مؤلفه‌های قدرت ملی و امنیت راهبردی تبدیل می‌شود. در این شرایط، قواعدی همچون حفظ نظام، تقدیم اهم بر مهم

و نفی سبیل، مبنای گسترش اختیارات حاکمیت در مدیریت داده‌های ملی قرار می‌گیرند. نتیجه این تحول، حرکت به سوی «تمرکزگرایی دفاعی» در حکمرانی داده است؛ بدین معنا که دولت برای جلوگیری از نفوذ، جاسوسی و سلطه اطلاعاتی دشمن، می‌تواند کنترل گسترده‌تری بر زیرساخت‌ها و داده‌های راهبردی اعمال کند (Schmitt, 2017,p.339؛ Couldry & Mejias, 2019,p.12). با این وجود، مشروعیت چنین اختیاراتی همچنان مقید به ضرورت، تناسب و محدود بودن به شرایط استثنایی جنگ خواهد بود (مکارم شیرازی، ۱۳۸۶، ۴۹۳)

بر این اساس، فقه حکومتی الگوی یکسانی برای حاکمیت داده ارائه نمی‌کند، بلکه دامنه اختیارات دولت را متناسب با سطح تهدید تنظیم می‌نماید. هرچه جامعه از وضعیت عادی به سمت شرایط اضطراری و سپس جنگ سایبری حرکت کند، سهم حاکمیت در مدیریت داده افزایش یافته و در مقابل، دامنه حقوق انحصاری اشخاص بر داده‌هایشان محدودتر می‌شود. این تحول نه ناشی از نفی حقوق فردی، بلکه برخاسته از تقدم مصالح عمومی و ضرورت صیانت از امنیت و موجودیت جامعه اسلامی است.

۱-۲. تبدل ماهوی «مرز» و «قلمرو سرزمینی» در ساحت سایبر

برای درک دقیق ابعاد حقوقی هجوم سایبری اسفند ۱۴۰۴، نخست باید تحول بنیادین مفهوم «حاکمیت» را واکاوی نمود. در حقوق بین‌الملل کلاسیک، حاکمیت وابستگی ذاتی و ناگسستنی با «قلمرو فیزیکی» داشت؛ اما ظهور شبکه جهانی اطلاعات، موجودیت جدیدی خلق کرد که در آن، داده‌ها به مثابه دارایی‌های سرزمینی عمل می‌کنند (Goldsmith & Wu, 2020, p. 54). حاکمیت داده در این پارادایم نوین، به معنای حق انحصاری و تکلیف مشروع دولت-ملت‌ها برای قانون‌گذاری، اعمال صلاحیت و صیانت از داده‌های تولیدشده در محدوده مرزهای دیجیتال خود است (فاطمی ، ۱۴۰۲، ۱۷).در جریان جنگ تحمیلی سوم، استراتژی دشمن مبتنی بر دور زدن مرزهای فیزیکی و نفوذ مستقیم به پایگاه‌های داده حیاتی کشور بود. این رویکرد نشان داد که در دوران معاصر، تسلط بر زیرساخت‌های ارتباطی، به مراتب خطرناک‌تر از اشغال نظامی خاک است (Zittrain, 2025, p. 112). از منظر فقهی، این تبدل ماهوی نیازمند «تنقیح مناط» است. اگر در فقه سنتی، مفهوم «ثغور» (مرزها) به خطوط جغرافیایی محدود می‌شد، در فقه حکومتی معاصر، مناطِ لزومِ دفاع و مرزبانی، «جلوگیری از تسلط کفار بر مقدرات

مسلمین» است(محقق داماد، ۱۴۰۱، ۸۹) خواه این مقدرات در قالب زمین باشد، خواه در قالب سرورها و شبکه‌های انتقال داده.

۱-۳. ماهیت‌شناسی فقهی-حقوقی تسلیحات خودکار و تهاجم الگوریتمی در جنگ رمضان

یکی از پیچیده‌ترین لایه‌های تجاوز در مخاصمه اسفند ۱۴۰۴، بهره‌گیری گسترده از تسلیحات خودکار مرگبار و سیستم‌های هدف‌زنیِ مبتنی بر هوش مصنوعی بود. این تسلیحات با خروج از کنترلِ مستقیمِ انسانی، مفاهیمِ کلاسیکِ عاملیت و انتساب مسئولیت را در حقوق بین‌الملل با چالشی بنیادین مواجه کرده‌اند (Brownlie, 2019, p. 442). در مخاصماتِ سنتی، انتسابِ فعلِ مجرمانه به فرمانده یا سرباز، مبتنی بر رکنِ معنوی و قصدِ مستقیم بود؛ اما در نبرد رمضان، الگوریتم‌های متخاصم به طور خودکار به شناسایی و انهدام زیرساخت‌های حیاتی مبادرت ورزیدند. از منظر فقهی، این مسئله ذیل باب تسبیب و مباشرت قابل تحلیل است. اگرچه در نگاه بدوی ممکن است ماشین، فاقدِ تکلیف به نظر برسد، اما در فقه حکومتی، سببِ اقوی از مباشر بر تمامیِ لایه‌هایِ طراحی و اجرای الگوریتم حاکم است (طباطبایی و کعبی نسب، ۱۳۹۷، ۷۹).تهاجم الگوریتمی به شبکه ملی اطلاعات در نهم اسفند، نه یک خطای فنی، بلکه بغیِ دیجیتال علیه کیانِ جامعه اسلامی بود. در اینجا، فقه حکومتی با استناد به قاعده حرمتِ اعانت بر اثم، نه تنها دولت‌های متخاصم، بلکه شرکت‌های فناوریِ همکار در لایه‌های پلتفرمی را نیز ضامنِ خساراتِ وارده می‌داند (انصاری وکاتب دامغانی ، ۱۴۰۱، ۲۴۰). در حقوق بین‌الملل نیز دکترین مسئولیتِ مطلق در قبالِ اشیاء خطرناک، به تدریج به سمتِ سیستم‌های خودکار سایبری در حال تسری است (Kulesza, 2022, p. 198). بنابراین، صیانت از حاکمیت داده، عملاً به معنای ایجادِ سپرِ حقوقی در برابر اراده‌هایِ بی‌جان اما مرگبارِ ماشین‌های جنگی است.علاوه بر این، باید به حقِ بر تبیینِ الگوریتمی به عنوان یکی از مولفه‌هایِ نوینِ حاکمیت داده اشاره کرد. در جریان جنگ رمضان، دشمن با استفاده از جعبه‌های سیاه الگوریتمی، به ترورهای هدفمندِ نخبگان دست زد، بدون آنکه منطقِ گزینشِ هدف برای ناظرانِ حقوقی روشن باشد. در فقه دفاعی، هرگونه اقدامِ جنگی باید واجد تمیز و تناسب باشد (قائم پناه، ۱۳۹۲، ۱۷۴)؛ حال آنکه تسلیحاتِ الگوریتمی با نقضِ اصلِ تمیز، غیرنظامیان را در معرضِ آسیبِ مستقیم قرار می‌دهند. لذا، حاکمیت موظف است با استقرارِ نظامِ بازرسیِ داده‌ای، مانع از اجرایِ

پروتکل‌هایِ مخفیِ بیگانه در شبکه داخلی گردد. این اقدام، مصداقِ بارزِ دفاعِ مشروعِ پیش‌دستانه است که در آن، دفعِ خطرِ محتمل بر اساسِ حکمِ عقل و شرع، بر صبرِ انفعالی تقدم دارد (قاسمی و نامدار ، ۱۳۹۷، ۲۱۹)

۱-۴. شبکه ملی اطلاعات؛ دژ مستحکم فقه حکومتی در برابر «سبیل» سایبری

مهم‌ترین دستاویز حقوقی و فقهی برای مقابله با جنگ‌های زیرساختی، استناد به قاعده قرآنی «نفی سبیل» است. مفاد این قاعده ناظر بر بطلان هرگونه رابطه حقوقی، سیاسی یا تکنولوژیکی است که موجب استیلای بیگانگان بر جامعه اسلامی گردد (هاشمی شاهرودی، ۱۳۸۸، ج ۴، ۲۱۰). در مقطع حساس نهم اسفند ۱۴۰۴، وابستگی بخش‌هایی از ناوبری و ارتباطات داخلی به پلتفرم‌های خارجی، دقیقاً همان مصداق «سبیل» بود که بستر را برای تروریسم سایبری مهیا ساخت.از این رو، توسعه و انسداد «شبکه ملی اطلاعات» در شرایط مخاصمه، نه یک سیاست‌گذاری صرفاً فنی، بلکه یک «واجب شرعی و حکومتی» است. حاکمیت موظف است در راستای قاعده «حفظ نظام» (که به فرموده امام خمینی (ره) از اوجب واجبات است)، جریان آزاد اطلاعات را در مواقعی که به مثابه ستون پنجم دشمن عمل می‌کند، مسدود یا محدود سازد (گرجی، ۱۳۹۸، ۱۱۲). این تدبیر در دکترین حقوق بین‌الملل نیز تحت عنوان «دفاع سایبری فعال» پذیرفته شده است، جایی که دولت‌ها مجازند برای دفع حملاتی که به سطح «توسل به زور» رسیده‌اند، اقدامات متقابل سایبری انجام دهند (Schmitt, 2017, p. 45).برای تبیین بهتر این تغییر پارادایم، جدول زیر تقابل مفاهیم سنتی دفاع را با واقعیات رخ‌داده در نبرد رمضان تطبیق می‌دهد:

جدول ۱: مقایسه تطبیقی مؤلفه‌های دفاع مشروع و حاکمیت

مؤلفه حقوقی/ فقهی	رویکرد در نبرد سنتی	رویکرد در مخاصمات سایبری و زیرساختی	مبنای فقهی حاکم بر دفاع
تعریف مرز (ثغور)	خطوط فیزیکی و جغرافیایی	پهنای باند، سرورهای داخلی و شبکه ملی اطلاعات	توسعه مفهومی «مرابطه» و مرزبانی دیجیتال
ابزار تجاوز	تسلیحات نظامی و لشکرکشی	بدافزارها، بمب‌های منطقی و اختلال الگوریتمی	قاعده «لا ضرر و لا ضرار فی الاسلام»
هدف استراتژیک	اشغال خاک و منابع طبیعی	فلج‌سازی قوه مدبره، استعمار داده‌ها و تروریسم زیرساختی	قاعده «نفی سبیل» (جلوگیری از استیلای اطلاعاتی)
ماهیت دفاع مشروع	پدافند نظامی متقابل	انسداد درگاه‌های تبادل داده، استقلال شبکه و پاسخ متقارن سایبری	قاعده «وجوب حفظ بیضه اسلام و کیان نظام»

۱-۵. تزاحم میان امنیت ملی در برابر جریان آزاد اطلاعات

برای درک دقیق و ملموس دلیل مشروعیتِ تحدیدِ حقوقِ داده‌ای در اسفند ۱۴۰۴، خروج از تحلیل‌های انتزاعی و ارزیابی عینیِ گستردگی حملات در «جبهه پنهان» جنگ رمضان ضروری است (خبرآنلاین، ۱۴۰۵). بر اساس گزارش‌های رسمی و مستندات منتشر شده، در این نبرد هیبریدی، مقیاس تهاجم ائتلاف متخاصم (ایالات متحده و رژیم صهیونیستی) به زیرساخت‌های حیاتی از سطح اختلالات موضعی فراتر رفته و به یک جنگ تمام‌عیار ماشین‌محور تبدیل شده بود؛ به‌گونه‌ای که روزانه بیش از ۱۰۰ حمله سایبری سنگین و هدفمند، شریان‌های اطلاعاتی و خدماتی کشور را در معرض فروپاشی قرار می‌داد (خبرگزاری مهر، ۱۴۰۵).ابعاد این تهاجم زمانی روشن‌تر می‌شود که بدانیم در طول این نبرد ۴۱ روزه، بالغ بر ۱۰۰۰ عملیات سایبریِ زیرساختی خنثی گردید. نکته قابل تأمل از منظر فقه اجتماعی و حکومتی این است که بخش قابل‌توجهی از این پدافند موفق، نه صرفاً توسط ساختارهای رسمی، بلکه با مشارکت خودجوش نیروهای مردمی و متخصصان داخلی صورت پذیرفت که تجلی عینی «واجب کفایی» در دفاع از ثغور دیجیتال جامعه اسلامی است (اقتصاد نیوز، ۱۴۰۵). از حیث تقویم خسارات نیز، روایت رسمی وزارت ارتباطات حاکی از آن است که دست‌کم ۵۰۰ سایت و زیرساختِ حساسِ ارتباطی مستقیماً هدف بمباران الگوریتمی قرار گرفتند که تنها در لایه ارتباطات (بدون احتساب خسارات تبعی در زنجیره تامین)، آسیبی بالغ بر ۳۳۵ میلیون دلار به

اقتصاد کشور وارد گردید (خبرگزاری برنا، ۱۴۰۵). این مختصات میدانی نشان می‌دهد که هدف متخاصم، صرفاً نقض حریم خصوصی نبود، بلکه «فلج‌سازی سیستماتیک قوه مدبره» و اخلال در نظم عمومی (افساد فی الارض دیجیتال) بوده است. با در نظر گرفتن این حجم از تهاجم و خسارت، چالش قطعیِ مقطعیِ اینترنت بین‌الملل و محدودسازی دسترسی‌ها در جریان جنگ رمضان، دیگر از منظر «تضییق حق آزادی بیان» قابل ارزیابی نیست؛ بلکه این اقدام یک تصمیمِ راهبردی و تنها گزینه عملیاتی برای «قطع تله‌متری (ارسال برخط اطلاعات به سرورهای بیگانه)» و کور کردن چشم ماشین جنگی دشمن بود. در این مقام، فقه حکومتی با کاربست دقیقِ قاعده «تزاحم اهم و مهم» و «دفع ضرر محتمل»، انسداد شبکه‌های آسیب‌پذیر را کاملاً توجیه می‌کند. هنگامی که حقِ دسترسی آزاد شهروندان به پلتفرم‌های بین‌المللی (مهم) با حقِ حیات جامعه، تأمین امنیت ۵۰۰ زیرساخت حیاتی، و دفع خسارات صدها میلیون دلاری از بیت‌المال (اهم) در تقابل مستقیم قرار می‌گیرد، عقل و شرع با استناد به قاعده «وجوب حفظ نظام»، به تقدم قطعی مصلحتِ اهم و تحدید موقتِ دسترسی‌ها حکم می‌کنند (مشکانی سبزواری، ۱۴۰۰، ۳۴)

۲. مطالعه تطبیقی حاکمیت داده در شرایط فورس‌ماژور و مخاصمات مسلحانه

۲-۱. تعلیق تعهدات در نظام حقوقی بین‌الملل و نسبت آن با احکام حکومتی

در حقوق بین‌الملل، اصل «لزوم قراردادها» در مواجهه با شرایط فورس‌ماژور (قوه قهریه) دستخوش تغییر می‌گردد. حملات گسترده به زیرساخت‌های بانکی و شبکه‌ای ایران در اسفند ۱۴۰۴، مصداق بارز وضعیتی غیرقابل پیش‌بینی، خارجی و غیرقابل دفع بود که اجرای بسیاری از قراردادهای اقتصادی و خدماتی را ناممکن ساخت (کاتوزیان، ۱۴۰۲، ۱۸۹). در چنین شرایطی، حاکمیت با استفاده از «احکام ثانویه» و در سطحی بالاتر، «احکام حکومتی»، مجاز به مداخله در روند معمول حقوقی برای جلوگیری از فروپاشی نظام اقتصادی و اجتماعی است (منتظری، ۱۴۰۱، ج ۲، ۵۶). این رویکرد فقهی که بر مدار «مصلحت عامه» می‌چرخد، قرابت شگفت‌آوری با دکترین «ضرورت ملی» در حقوق غرب دارد. در نظام حقوقی اتحادیه اروپا، اگرچه صیانت از داده‌های شخصی یک حق بنیادین تلقی می‌شود، اما مقررات عمومی حفاظت از داده (GDPR) در ماده ۲۳ خود، به صراحت اجازه می‌دهد که در راستای امنیت ملی و دفاع، این حقوق محدود یا معلق گردند (Bygrave, 2024, p. 215). در واقع، نبرد رمضان نشان داد که در زمان

جنگ، حاکمیت داده به معنای «حق انحصاری دولت بر مدیریت ترافیک داده» جهت دفع تجاوز است؛ موضوعی که در ماده ۴ کنوانسیون بین‌المللی حقوق مدنی و سیاسی (ICCPR) نیز به عنوان حق دولت‌ها در شرایط اضطراری به رسمیت شناخته شده است (شریفی طرازکوهی, و صیادنژاد،۱۳۹۹، ۵۶۸). در تکمیل این بحث، باید به دکترین حاکمیت دائم بر منابع (Permanent Sovereignty over Natural Resources) در حقوق بین‌الملل اشاره کرد که امروزه توسط بسیاری از صاحب‌نظران به داده‌های کلان تسری یافته است (Tsagourias, 2025, p. 142). در نبرد رمضان، داده‌های زیرساختی ایران نه به عنوان ملک خصوصی شرکت‌ها، بلکه به مثابه منابع استراتژیک ملی عمل کردند. از منظر فقه حکومتی، این داده‌ها تحت شمول عنوان انفال یا اموال عمومی قرار می‌گیرند که در شرایط تزاحم، حقِ تصرف و مدیریت آن‌ها برای حاکم عادل جهت صیانت از نظام، بر حقوق خصوصی مقدم است (مصباح یزدی، ۱۴۰۲، ۲۱۵). اینجاست که مفهوم مصلحت در فقه، با مفهوم نظم عمومی در حقوق بین‌الملل هم‌گرا می‌شود؛ با این تفاوت که در فقه حکومتی، غایتِ این مصلحت، حفظِ کیانِ توحیدی و عدالت اجتماعی است (هاشمی، ۱۴۰۲، ۱۸۸).

۲-۲. تحلیل تطبیقی استثنائات حاکمیتی در مدیریت داده

برای درک بهتر جایگاه فقه حکومتی در مقایسه با استانداردهای جهانی، جدول زیر نقاط اشتراک و افتراق مبانی تحدید حقوق داده‌ای در شرایط جنگی را تبیین می‌کند:

جدول ۲: تحلیل تطبیقی مبانی تحدید حقوق داده‌ای در شرایط مخاصمه و فورس‌ماژور

شاخص مقایسه	رویکرد فقه حکومتی (با نگاه به جنگ ۱۴۰۴)	رویکرد نظام حقوقی اروپا (GDPR/ePrivacy)	مبانی توجیهی حقوقی/فقهی
مبنای مشروعیت محدودیت	قاعده ضرورت (الضرورات تبیح المحظورات)	ماده ۲۳ GDPR (National Security)	ترجیح مصلحت عام بر نفع خاص
قلمرو شمول	تمامی زیرساخت‌های حیاتی و داده‌های ملی	داده‌های شخصی و حریم خصوصی دیجیتال	صیانت از بیضه اسلام / امنیت عمومی
نظارت بر اجرا	نهادهای حاکمیتی و ولی‌فقیه (مصلحت نظام)	مراجع قضایی و شوراهای نظارت بر داده	حکومت قانون (Rule of Law)
جبران خسارت	قاعده «لا ضرر» و مسئولیت دولت در اتلاف	نظام مسئولیت مدنی مبتنی بر تقصیر یا خطر	بازتوزیع عادلانه هزینه‌های جنگ

۲-۳. مسئولیت مدنی و جبران خسارات ناشی از تروریسم زیرساختی

یکی از مهم‌ترین چالش‌های حقوقی پس از پایان جنگ رمضان، تعیین تکلیف خسارات وارده به واسطه اختلال در قراردادهای کلان (به‌ویژه در حوزه نفت و گاز و پیمانکاری‌های بزرگ) است. در فقه امامیه، قاعده «تسبیب» و «اتلاف» مبنای اصلی مطالبه خسارت است (بجنوردی، ۱۴۰۱، ۳۴). اما در مخاصمات سایبری که انتساب عمل به عامل به سختی صورت می‌گیرد، فقه حکومتی با تکیه بر «بیت‌المال» و مسئولیت دولت در قبال اتباع خود، راهکارهای نوینی ارائه می‌دهد.از سوی دیگر، در حقوق بین‌الملل، «دستورالعمل تالین ۲.۰» صراحتاً بیان می‌دارد که اگر حملات سایبری به سطح یک «حمله مسلحانه» برسد، دولت قربانی حق دارد نه تنها به دفاع مشروع بپردازد، بلکه عاملان را مسئول جبران خسارات مادی و معنوی بداند (Schmitt, 2017, Rule 6). تلفیق این قواعد با ظرفیت‌های فقهی، دکترین «مسئولیت تضامنی متخاصمین» را تقویت می‌کند؛ به این معنا که ایالات متحده و رژیم صهیونیستی به دلیل نقض حاکمیت داده‌ای ایران در اسفند ۱۴۰۴، ضامن تمامی خسارات تبعی ناشی از فلج‌سازی زیرساخت‌ها هستند (نمامیان،۱۳۹۲، ص ۱۶). بیین دقیق ماهیت حقوقی حملات اسفند ۱۴۰۴ ایجاب می‌کند که میان «خسارات مستقیم ناشی از تجاوز دشمن» و «خسارات تبعی ناشی از تدابیر پدافندی حاکمیت» تفکیک قائل شویم. تروریسم زیرساختی که در جریان جنگ رمضان با هدف قرار دادن ستون فقرات شبکه بانکی و توزیع انرژی رخ داد ، مصداق بارز «جنایت علیه بشریت در فضای سایبر» است(محقق هرچقان و همکاران، ۱۴۰۰، ۱۵۴۹). در این چارچوب، انتساب عمل به دولت‌های متخاصم بر اساس دکترین «کنترل موثر» صورت می‌پذیرد؛ به گونه‌ای که حتی اگر حملات توسط گروه‌های نیابتی یا بدافزارهای خودکار انجام شده باشد، مسئولیت نهایی و ضمان مادی بر عهده دولت‌های پشتیبان (ایالات متحده و رژیم صهیونیستی) خواهد بود (فرشاسعید وجلالی، ۱۴۰۱، ۱۷۸).

از منظر فقهی، در موارد عجز از شناسایی مباشر دقیق (به دلیل پیچیدگی‌های فنی ابزارهای مخفی‌کننده هویت)، قاعده «ضمانِ سبب» اولویت می‌یابد. در مخاصمات اسفند ۱۴۰۴، ایجاد بستر نفوذ و طراحی الگوریتم‌های مخرب، سببی اقوی از مباشرتِ کدهای اجرایی تلقی می‌گردد؛ لذا بر اساس قاعده «الغُرمُ بالغُنم»، هر طرفی که از تضعیف زیرساخت‌های جمهوری اسلامی ایران منتفع شده است، ضامن خسارات وارده خواهد بود. این منطق فقهی، مبنایی استوار برای اقامه دعوی در دیوان‌های

بین‌المللی فراهم می‌سازد تا خسارات وارده به بخش خصوصی و عمومی بر اساس استاندارد «اعاده به وضع سابق» مطالبه گردد (قدیر و کاظمی فروشانی،۱۳۹۸، ۲۵۱).چالش دوم، مسئولیت دولت در قبال خساراتی است که به واسطه اعمال «احکام حکومتی» و قطع دسترسی‌های بین‌المللی به شهروندان وارد شده است. اگرچه این اقدامات با استناد به قاعده «حفظ نظام» واجد مشروعیت شرعی بوده‌اند، اما بر اساس اصل «برابری شهروندان در برابر هزینه‌های عمومی»، نباید بار سنگینِ دفاع ملی تنها بر دوش فعالان اقتصادی و کسب‌وکارهای دیجیتال قرار گیرد. در فقه امامیه، هرگاه حاکمیت برای مصلحت عامه، تصرفی در اموال یا حقوق خصوصی نماید که منجر به تضرر فرد گردد، بیت‌المال ضامن جبران عادلانه آن است؛ مشروط بر اینکه خسارت، فراتر از حریمِ متعارفِ دفاعی باشد (بافهم و فهیمی، ۱۳۹۶، ۲۸). علاوه بر این، باید به نقش «بیمه‌های مسئولیت سایبری» در دوران مخاصمه اشاره کرد. تحلیل قراردادهای بیمه‌ای در جریان جنگ رمضان نشان داد که اکثر شرکت‌های بیمه با استناد به شرط «استثنای جنگ»، از ایفای تعهدات خود سرباز زدند. در اینجا، فقه حکومتی می‌تواند با بازتعریف مفهوم «فورس‌ماژور سایبری»، شرکت‌های بیمه را به پذیرش بخشی از مسئولیت در قبال «حملات غیردولتی» ملزم نماید، مگر آنکه دولتی بودن حمله به طور قطعی در مراجع ذی‌صلاح احراز گردد (انصاری وکاتب دامغانی ، ۱۴۰۱، ص ۲۳۷). این رویکرد، توازنی پایدار میان ثبات اقتصادی و ضرورت‌های امنیتی ایجاد کرده و مانع از ورشکستگی سیستماتیک در حوزه اقتصاد دیجیتال پس از بحران‌های مشابه اسفند ۱۴۰۴ خواهد شد.

۴-۲. چالش‌های فقهی-حقوقی فورس‌ماژور در اتوماسیون بی‌واسطه

یکی از بدیع‌ترین چالش‌های حقوقی که در پی اختلالات شبکه ملی اطلاعات در اسفند ۱۴۰۴ رخ نمود، سرنوشت «قراردادهای الگوریتمی» و سیستم‌های اجرای خودکار بود که بخش قابل‌توجهی از زنجیره تامین و خدمات مالی کشور را مدیریت می‌کردند. در حقوق قراردادهای سنتی، احراز شرایط فورس‌ماژور (قوه قهریه) امری پسینی است که با مداخله قاضی یا نهاد داوری، منجر به تعلیق یا انفساخ تعهدات می‌گردد (کاتوزیان، ۱۴۰۲، ۱۹۴). اما ذات قراردادهای الگوریتمی مبتنی بر اجرای بی‌قیدوشرطِ کدهای برنامه‌نویسی‌شده است؛ ماشین جنگی یا بحران سایبری را نمی‌فهمد و در صورت عدم دریافت داده‌های ورودی به دلیل قطعی اینترنت، بی‌درنگ جریمه‌های تاخیر را اعمال کرده یا دارایی‌های دیجیتال را مصادره

می‌کند (انصاری وکاتب دامغانی ، ۱۴۰۱، ۲۲۸).در جریان جنگ تحمیلی سوم، حملات منع خدمت (DDoS) و انسداد درگاه‌های تبادل داده، موجب شد تا هزاران قرارداد هوشمند در حوزه بورس، لجستیک و گمرک، به دلیل عدم دسترسی به «اوراکل‌ها» (منابع تغذیه داده در خارج از شبکه محلی)، در وضعیت نقض تعهدِ ناخواسته قرار گیرند. از منظر فقهی، اجرای کورکورانه این الگوریتم‌ها در شرایطی که اراده متعهد به واسطه یک عامل خارجی (حمله سایبری دشمن) مخدوش شده است، مصداق بارز «اکل مال بالباطل» و در تضاد صریح با قاعده «لا ضرر و لا ضرار فی الاسلام» است (محقق داماد، ۱۴۰۱، ۱۱۲).فقه حکومتی در این بزنگاه، با استناد به قاعده «نفی عسر و حرج»، به حاکمیت اجازه می‌دهد تا به صورت پیشینی در کدهای اجرایی مداخله نماید. به عبارت دیگر، همان‌گونه که ولی‌فقیه و نهادهای حاکمیتی حق دارند در شرایط جنگی، جریان ترافیک داده را محدود سازند، این اختیار و بلکه تکلیف را نیز دارند که با صدور «حکم حکومتیِ دیجیتال»، دستور توقف سراسری (Kill Switch) کدهای اجرایی مرتبط با قراردادهای هوشمند را صادر نمایند تا از فروپاشی دومینووارِ اقتصادِ دیجیتالِ داخلی جلوگیری شود (مشکانی سبزواری ، ۱۴۰۰، ۹۵).این مفهوم در ادبیات حقوق بین‌الملل فناوری، تحت عنوان «دریچه‌های فرار الگوریتمی» شناخته می‌شود. محققان حقوق فناوری تاکید دارند که معماری سیستم‌های خودکار باید به گونه‌ای طراحی شود که قابلیت دریافت «فرمان توقف اضطراری» از نهادهای حاکمیتی در زمان جنگ را داشته باشد (Zittrain, 2025, p. 142). تقارن این نظریه مدرن با دیدگاه فقه حکومتی در خصوص اولویت حفظ نظام اقتصادی مسلمین، نشان‌دهنده پویایی فقه امامیه در مواجهه با مسائلی است که هیچ‌گونه سابقه تاریخی در متون کلاسیک ندارند. لذا، جبران خسارات ناشی از این توقفِ دستوری، دیگر بر عهده متعهدِ الگوریتم نیست، بلکه خسارات تبعی آن باید در چارچوب همان مسئولیت تضامنی متخاصمین (که پیش‌تر به آن اشاره شد) یا از طریق حمایت‌های بیت‌المال جبران گردد.

۲-۵. واکاوی فقهی نقش ابرشرکت‌های فناوری فراملیتی در مخاصمات

دوقطبیِ سنتیِ «دولت/بازیگر غیردولتی» در حقوق بین‌الملل مخاصمات مسلحانه، با وقوع جنگ تحمیلی سوم دچار فروپاشی مفهومی گردید. در طول ۴۱ روز نبرد سایبری در اسفند ۱۴۰۴، ابرشرکت‌های فناوریِ فراملیتی صرفاً به عنوان ارائه‌دهندگان بی‌طرفِ زیرساخت عمل نکردند؛ بلکه با تغییرِ عامدانه الگوریتم‌های

مسیریابی، مسدودسازیِ هدفمندِ حساب‌های کاربریِ نهادهای حاکمیتی ایران و اشتراک‌گذاریِ برخطِ کلان‌داده‌های موقعیت‌یاب با ائتلاف متخاصم، عملاً به عنوان «نیروی هواییِ دیجیتالِ» دشمن وارد کارزار شدند (رحمت‌الهی و آقامحمد آقایی، ۱۴۰۳، ۱۱۲). این مشارکت مستقیم در عملیات خصمانه، مصونیت غیرنظامیِ این شرکت‌ها را در حقوق بین‌الملل سلب کرده و آن‌ها را به اهدافِ مشروعِ نظامی و سایبری تبدیل می‌نماید (Watkin , 2012,p309).اما از منظر فقه حکومتی، تبیین وضعیتِ حقوقیِ این غول‌های فناوری نیازمند کاربستِ مفاهیمِ جزایی و دفاعی در ساحتِ اشخاص حقوقی است. هنگامی که یک پلتفرم فراملیتی، انحصار جریان داده را دستمایه تضعیف جبهه اسلام قرار می‌دهد، از دایره «معاهدِ تجاری» خارج و وارد قلمرو «شخصیت حقوقیِ محارب» و «باغی» می‌گردد. در فقه امامیه، عنوان «محارب» صرفاً به فردی که با سلاح سرد یا گرم ایجاد رعب می‌کند محدود نمی‌شود؛ بلکه مناطِ حکم، «تجرید السلاح لإخافه الناس و الإفساد فی الأرض» است (محقق داماد، ۱۴۰۱، ۲۱۸). در عصر حاضر، تسلیحاتِ الگوریتمی و اختلالِ سیستماتیک در دسترسی مردم به نیازهای حیاتی (از طریق قطع خدمات پایه)، مصداق اتمّ افساد فی‌الارض و محاربه شبکه‌ای است (حسینی و همکاران، ۱۴۰۳، ۱۲۸).علاوه بر این، همکاری این پلتفرم‌ها با دولت‌های متخاصم، ذیل قاعده قرآنی «تعاون بر اثم و عدوان» (ولا تعاونوا علی الإثم والعدوان) و همچنین «حرمت اعانت ظالم» ارزیابی می‌شود. بر این اساس، فقه حکومتی به حاکم اسلامی اختیار می‌دهد تا با عبور از قواعد کلاسیکِ مالکیت فکری و حقوق تجارت بین‌الملل، تمام معاهداتِ دوجانبه با این اشخاص حقوقی را ملغی الاثر اعلام نماید. در اثنای جنگ رمضان، مصادره پهنای باندِ اختصاص‌یافته به این پلتفرم‌ها و تصرفِ تجهیزاتِ مسیریابیِ آن‌ها در داخل مرزهای سایبری کشور، نه یک نقضِ حقوقِ مالکانه، بلکه اجرایِ حکمِ شرعیِ مربوط به «غنائمِ جنگی» و «تقاصِ حقوقی» در برابرِ متخاصم ارزیابی می‌گردد (ملک‌زاده،۱۳۹۹).نتیجه مستقیمِ این استنباط فقهی آن است که حاکمیت داده در شرایط فورس‌ماژور، حقِ مطلقِ دولت در نادیده گرفتنِ شرایط خدمات تحمیلی از سوی ابرشرکت‌ها را به رسمیت می‌شناسد. در واقع، فقه حکومتی با تأسیسِ مفهومِ «بی‌اعتباریِ قراردادهای استعماریِ دیجیتال»، راه را برای دادخواهیِ ملی علیه این شرکت‌ها هموار می‌سازد؛ به گونه‌ای که پس از فروکش کردن مخاصمه، امکان طرح دعوای خسارتِ تضامنی علیه پلتفرم‌های همدست با دشمن در محاکم داخلی و بین‌المللی کاملاً مستند و موجه خواهد بود (ملکوتی و ساورایی، ۱۳۹۵، ۱۳۷).

۲-۶. واکاوی تطبیقی مکانیسم‌های تعلیق در GDPR و احکام ثانویه

یکی از مناقشه‌برانگیزترین ابعاد جنگ رمضان، تعلیق برخی پروتکل‌های رمزنگاری و پایشِ مبادلاتِ داده‌ای برای شناسایی منشاء حملات بود. منتقدان، این اقدام را ناقض حریم خصوصی دانستند، اما مطالعه تطبیقی نشان می‌دهد که پیشرفته‌ترین اسناد حقوقی نیز در زمان جنگ، رویکردی مشابه فقه حکومتی دارند. در نظام حقوقی اتحادیه اروپا، اگرچه GDPR به عنوان استاندارد طلایی حریم خصوصی شناخته می‌شود، اما بند ۱ از ماده ۲۳ این مقررات صراحتاً مقرر می‌دارد:قوانین اتحادیه یا کشورهای عضو، می‌توانند از طریق یک اقدام تقنینی ، دامنه تعهدات و حقوق [موضوع مواد ۱۲ تا ۲۲ و ماده ۳۴] را محدود کنند؛ مشروط بر اینکه این محدودیت، به جوهره حقوق و آزادی‌های بنیادین احترام گذاشته و در یک جامعه دموکراتیک، اقدامی ضروری و متناسب برای تضمین موارد زیر باشد: الف) امنیت ملی؛ ب) دفاع؛ ج) امنیت عمومی. (Voigt & Von dem Bussche, 2017, p. 156) واکاوی دقیق این ماده نشان می‌دهد که تعلیق حقوق، مطلق و بی‌ضابطه نیست، بلکه مقید به سه شرط اساسی است: نخست، وجود مبنای قانونی؛ دوم، رعایت ضرورت و تناسب؛ و سوم، موقتی بودن و نظارت‌پذیری (Schrems, 2024, p. 89). این رویکرد، تقارنِ محتواییِ عمیقی با نهاد حکم حکومتی و احکام ثانویه در فقه امامیه دارد. احکام ولایی صادره در زمان مخاصمه (مانند قطع دسترسی به پلتفرم‌های متخاصم در اسفند ۱۴۰۴)، نه یک استبداد دیجیتال، بلکه اقدامی مبتنی بر ضرورت دفاعی و دائرمدارِ مصلحت قطعی است. لذا بر خلاف تصورِ کلی، هم در نظام حقوقی اروپا و هم در فقه حکومتی، به محضِ زوالِ منشاءِ تهدید، استثنائات زائل گشته و حاکمیت موظف به اعاده حقوقِ داده‌ایِ شهروندان است؛ چرا که در منطق فقهی الضروره تُقدّر بقدرها و هرگونه محدودیت فراتر از نیاز عملیاتی جنگ، فاقد مشروعیت شرعی خواهد بود (نجفی، ۱۴۰۴، ج ۲۱، ۱۲).»در فقه حکومتی، این عدول از طریق نهاد احکام ثانویه و احکام ولایی صورت می‌پذیرد. در بحران اسفند ۱۴۰۴، زمانی که بقای جامعه اسلامی در خطر قرار گرفت، احکام اولیه (مانند حرمتِ تجسس) به واسطه قاعده الضرورات تبیح المحظورات و با رعایت دقیقِ اصلِ تناسب، جای خود را به احکامِ دفاعی دادند (امیدی و همکاران، ۱۴۰۰، ۳۸۸). تفاوت بنیادین در این است که در مدل فقهی، این تعلیق حقوق، نه یک استبداد دیجیتال، بلکه یک جراحی حقوقی برای حفظ حیات کل پیکره جامعه است؛بنابراین حاکمیت باید توازنِ میانِ پدافند و حق را به گونه‌ای برقرار کند که

پس از رفعِ وضعیتِ فوق‌العاده، بازگشت به وضعیت صلح‌آمیز و جبرانِ خساراتِ غیرعمدیِ شهروندان تضمین گردد.

۳. الگوی جامع پدافند سایبری مبتنی بر فقه حکومتی و راهبرد تقنینی

۳-۱. گذار از پدافند غیرعامل به دفاع سایبری پیش‌دستانه

تجربه چهل و یک روزه جنگ رمضان ثابت کرد که رویکرد انفعالی و صرفاً پدافندی در برابر ماشین جنگی الگوریتمی متخاصمین، به معنای پذیرش شکست تدریجی است. در جریان حملات نهم اسفند ۱۴۰۴ که به فجایع دردناکی نظیر هدف قرار گرفتن زیرساخت‌های غیرنظامی و آموزشی (همچون مدرسه شجره طیبه میناب) و ترورهای هدفمند منجر گردید، روشن شد که دشمن از داده‌های موقعیت‌یاب و ضعف شبکه‌های داخلی به عنوان سلاح کشتار جمعی استفاده کرده است (مرکز پژوهش‌های مجلس، ۱۴۰۵، ۲۲).از منظر فقه حکومتی، هنگامی که علمِ قطعی به هجوم قریب‌الوقوع دشمن به «ثغور دیجیتال» وجود دارد، حاکمیت نه تنها حق، بلکه تکلیف دارد تا با استناد به قاعده «دفع ضرر محتمل» و «وجوب حفظ دماء مسلمین»، دست به دفاع پیش‌دستانه سایبری بزند (سبحانی، ۱۴۰۲، ۱۱۴). این مفهوم که در ادبیات فقهی ذیل «جهاد دفاعیِ بازدارنده» تعریف می‌شود، در حقوق بین‌الملل مدرن نیز تحت عنوان «دفاع فعال» در حال مشروعیت‌یافتن است. به گونه‌ای که استراتژیست‌های حقوقی معتقدند از کار انداختن سرورهای مهاجم پیش از تکمیل حمله، مصداق بارز دفاع مشروع ماده ۵۱ منشور ملل متحد در فضای سایبر است (Gervais, 2025, p. 89).

۳-۲. خلأهای قانون‌گذاری و ضرورت تدوین «رژیم حقوقی وضعیت فوق‌العاده سایبری»

نظام حقوقی ایران، به ویژه قانون جرایم رایانه‌ای (مصوب ۱۳۸۸) و قوانین مرتبط با تجارت الکترونیک، اساساً برای تنظیم‌گری در «زمان صلح» تدوین شده‌اند و فاقد ظرفیت‌های لازم برای مدیریت مخاصمات مسلحانه سایبری هستند (طهماسبی و شاهمرادی، ۱۳۹۷، ۱۰۵). در طول جنگ تحمیلی سوم، نهادهای متولیِ شبکه ملی اطلاعات با فقدان اختیارات قانونیِ شفاف برای مصادره آنیِ پهنای باند، انسداد پلتفرم‌های لجوج خارجی و الزام بخش خصوصی به اشتراک‌گذاری داده‌های حیاتی مواجه بودند.در فقه

حکومتی، ولی‌فقیه و حاکمیت اسلامی اختیار دارد تا در چارچوب «احکام ثانویه»، مالکیت خصوصی بر داده‌ها و زیرساخت‌های ارتباطی را به نفع مصلحت عمومی موقتاً محدود سازد (هاشمی شاهرودی، ۱۳۸۸، ج ۵، ۱۱۲). ترجمان تقنینیِ این ظرفیت فقهی، تدوین قانونی است که به محض اعلام «وضعیت فوق‌العاده سایبری»، فرماندهی واحدی را بر تمامی شریان‌های داده‌ای کشور مسلط گرداند؛ مشابه آنچه در قانون شرایط اضطراری بریتانیا (Civil Contingencies Act) برای مقابله با فلج زیرساختی پیش‌بینی شده است (Deeks, 2026, p. 142).

۳-۳. هندسه پیشنهادی برای نظام‌سازی تقنینی

برای رفع این خلأها و با الهام از مبانی فقهیِ مبتنی بر «نفی سبیل» و «صیانت از کیان اسلام»، چارچوب پیشنهادی برای قانون‌گذاری در جدول زیر تبیین شده است. این الگو تلاش می‌کند تا مرز ظریف میان امنیت ملی و حقوق بنیادین شهروندان را در زمان جنگ حفظ نماید:

جدول ۳: الگوی پیشنهادی «قانون جامع حاکمیت داده در وضعیت مخاصمه» مبتنی بر فقه حکومتی

مبنای فقهی/ حقوقی پشتیبان	الگوی پیشنهادی مبتنی بر فقه حکومتی (ویژه شرایط جنگ سایبری)	وضعیت فعلی (قوانین زمان صلح)	محور تقنینی
قاعده مصلحت و تقدیم اهم بر مهم	در اختیار گرفتن کامل پهنای باند توسط قرارگاه دفاع سایبری (اولویت‌دهی نظامی)	توزیع تجاری میان اپراتورها	مدیریت پهنای باند و ترافیک
تعمیم مفهومی انفال به دارایی‌های نوین	تلقی داده‌های حیاتی به عنوان «انفال» و دارایی‌های حاکمیتی در زمان جنگ	متعلق به پلتفرم‌ها و شرکت‌های خصوصی	مالکیت داده‌های کلان
قاعده لا ضرر و مقابله با بغی	حبس و مصادره اموال برای پلتفرم‌هایی که از ارائه داده به حاکمیت امتناع کنند	فقدان عنوان مجرمانه مشخص	جرم‌انگاری احتکار داده
قاعده مقابله به مثل (الاعتداء بالمثل)	تفویض اختیار شلیک متقابل سایبری به فرماندهان میدانی در صورت احراز حمله	نیازمند احکام پیچیده قضایی	پاسخ‌گویی متقابل

با استقرار این نظام حقوقی، نه تنها تاب‌آوری شبکه ملی اطلاعات در برابر شوک‌های ناشی از حملاتی نظیر جنگ رمضان به شدت افزایش می‌یابد، بلکه دست دستگاه دیپلماسی و حقوقی کشور برای اقامه دعوی علیه دولت‌های متخاصم (ایالات متحده و رژیم صهیونیستی) در مجامع بین‌المللی

پُرتر خواهد بود؛ چرا که هرگونه اقدام متقابل، مستند به یک قانون داخلی شفاف و منطبق بر عرف در حال توسعه بین‌المللی خواهد بود (جعفری ، ۱۳۹۸، ۱۲۲).

۴-۳. واکاوی فقهی انگاره «داده به مثابه انفال» در عصر مخاصمات هوشمند

یکی از چالش‌های بنیادین در جریان جنگ رمضان، تعیین ماهیت حقوقی «کلان‌داده‌های ملی» بود که در شریان‌های شبکه ملی اطلاعات جریان داشت. در حالی که بخش خصوصی بر مالکیت مطلق خود بر داده‌ها تاکید می‌کرد، ضرورت‌های دفاعی در اسفند ۱۴۰۴ ایجاب می‌کرد تا حاکمیت نظارت کاملی بر این دارایی‌های استراتژیک داشته باشد. از منظر فقه حکومتی، می‌توان با رویکردی مستحدث، کلان‌داده‌های ملی را تحت شمول عنوان «انفال» یا ثروت‌های عمومیِ در اختیار حاکم اسلامی قرار داد (فرهادی و همکاران، ۱۳۹۵، ۴). انفال در فقه امامیه، به اموالی اطلاق می‌گردد که مالکِ خصوصیِ مشخصی ندارند یا به جهت اهمیت راهبردی، صیانت از آن‌ها جز از طریق حاکمیت میسر نیست (فرهادی و همکارا، ۱۳۹۵، ۲). در تبیین فقهی این انگاره، باید میان داده‌های فردی[1] و کلان‌داده‌های ساختاریافته[2] تفکیک قائل شد. اگرچه داده‌های فردی بر اساس قاعده سلطنت، متعلق به اشخاص است، اما کلان‌داده‌ها به جهت وصفِ تراکم و پردازش، ماهیتی فراتر از دارایی شخصی یافته و به مثابه ثروت‌های عمومی ملی جلوه‌گر می‌شوند. این نوع دارایی‌های معرفتی، از حیث مناط، شباهت تامی با معادن ظاهره و باطنه در فقه امامیه دارند که به جهت اهمیت استراتژیک برای نظام اقتصادی و سیاسی، از ملکیت خصوصی خارج و در زمره انفال قرار می‌گیرند (نجفی، ۱۴۰۴، ج ۱۶، ۱۲۰؛ طوسی، ۱۳۹۰، ج ۲، ۶۵). لذا همان‌گونه که انفال ثروت‌هایی هستند که لله و لرسوله بوده و مدیریت آن در اختیار امام مسلمین است، کلان‌داده‌های زیرساختی نیز به جهت نقش حیاتی در حفظ کیان نظام، مصداق بارز ثروت‌های عمومی در عصر دیجیتال است که مالکیت خصوصی بر آن‌ها در زمان مخاصمه، مقید به مصلحت عامه و صیانت از بیضه اسلام است.داده‌های تولید شده در بستر شبکه ملی اطلاعات، به جهت نقشی که در بقای کیان جامعه اسلامی و امنیت ملی ایفا می‌کنند، مصداق بارز ثروت‌های عمومی

---

1. Personal Data
2. Big Data

نوین هستند. لذا در شرایط مخاصمه، حاکمیت نه به عنوان غاصب، بلکه به عنوان «امین و صائن» این ثروت‌ها، موظف است مانع از دست‌اندازی بیگانگان به این ذخایر معرفتی گردد. نفوذ دشمن به پایگاه‌های داده در نبرد رمضان نشان داد که هرگونه خلأ در حاکمیت بر داده، عملاً به معنای واگذاری «انفال دیجیتال» به دشمن است که بر اساس قاعده نفی سبیل، امری باطل و غیرشرعی محسوب می‌شود (طباطبایی و کعبی نسب، ۱۳۹۷، ۸۸) از این رو، تدوین نظام‌نامه حقوقی که در آن داده‌های حیاتی به عنوان اموالِ عمومیِ در اختیار دولت بازتعریف شوند، ضرورتی است که از بطن تجربیات جنگ اسفند ۱۴۰۴ استخراج شده است.

۳-۵. بازدارندگی راهبردی و ضرورت تدوین پروتکل‌های «وضعیت فوق‌العاده»

فقدان یک رژیم حقوقیِ مدون برای مدیریت بحران‌های سایبری در اسفند ۱۴۰۴، منجر به اتخاذ تصمیمات مقطعی و گاه ناهماهنگ در لایه‌های اجرایی گردید. برای رفع این نقیصه، فقه حکومتی با تکیه بر «مصالح مرسله» و اختیارات ولایی، پیشنهاد تدوین «قانون جامع دفاع شبکه‌ای» را ارائه می‌دهد. این قانون باید به گونه‌ای طراحی شود که به محض احراز وضعیت جنگی، تمامی اپراتورها و پلتفرم‌های فعال در قلمرو دیجیتال ایران، ملزم به تبعیت از دستورات «قرارگاه پدافند سایبری» گردند و هرگونه استنکاف از ارائه دسترسی‌های لازم برای پایشِ نفوذِ دشمن، بر اساس قاعده «لا ضرر»، مصداقِ اخلال در امنیت ملی و موجب مسئولیت کیفری سنگین خواهد بود.علاوه بر این، باید بر لزوم «بومی‌سازی ابزارهای رمزنگاری» به عنوان یک راهبرد دفاعی تاکید کرد. نبرد رمضان ثابت کرد که وابستگی به استانداردهای امنیتیِ بیگانگان، به مثابه سپردن کلیدِ دژِ دفاعی به دست دشمن است. حاکمیت اسلامی بر اساس وظیفه «اعداد قوه» موظف است زیرساخت‌های لازم برای استقلال کامل در حوزه لایه پلتفرم را فراهم آورد (عیوضی و همکاران، ۱۴۰۰، ۴۵). این اقدام نه تنها یک ضرورت فنی، بلکه یک تکلیف فقهی برای حفظ «بیضه اسلام» در برابر شبیخون‌های الگوریتمی است که در اسفند ۱۴۰۴ تمامیت ارضی و امنیتی کشور را هدف قرار دادند. در نهایت، الگوی پیشنهادی این پژوهش، ترکیبی از «اقتدار حاکمیتی در مدیریت داده» و «تعهد به جبران خسارات عادلانه» است که می‌تواند به عنوان مدلی سرآمد برای سایر کشورهای اسلامی در مواجهه با استعمار دیجیتال قرار گیرد.

نتیجه‌گیری

این پژوهش با عبور از انگاره سنتیِ پدافند غیرعامل، نشان داد که فقه حکومتی به واسطه پویایی ذاتی و ابتنا بر مصالح عامه، دارای ظرفیت‌های بی‌بدیلی برای پاسخگویی به پیچیده‌ترین ابعاد این نبردِ نوین است. یافته‌های این تحقیق حاکی از آن است که صیانت از شبکه ملی اطلاعات، نه یک سیاست‌گذاری صرفاً فنی، بلکه تکلیفی شرعی و حاکمیتی است که ریشه در قواعد بنیادین «نفی سبیل»، «حفظ بیضه اسلام» و «لا ضرر» دارد. در این راستا، تبیین «داده به مثابه انفال» یکی از کلیدی‌ترین نوآوری‌های این نوشتار بود؛ بدین معنا که کلان‌داده‌های ملی به جهت ماهیت راهبردی و نقش حیاتی در بقای نظام، در زمره ثروت‌های عمومی (انفال نوین) قرار می‌گیرند که حاکمیت نه تنها حق، بلکه تکلیفِ تصرف و مدیریت آن‌ها را برای دفع تجاوز دشمن در شرایط مخاصمه داراست. همچنین، تحلیل فقهیِ مشارکت ابرشرکت‌های فناوری در جنگ رمضان، ضرورت تغییر نگاه حقوقی به این بازیگران غیردولتی را نمایان کرد؛ چرا که نقض اصل بی‌طرفی و همکاری پلتفرمی با متخاصم، این اشخاص حقوقی را از دایره معاهدین تجاری خارج و ذیل عنوان «محارب و باغی» قرار می‌دهد که ضامن خسارات وارده بر کیان جامعه اسلامی هستند.

مطالعه تطبیقی با مقررات عمومی حفاظت از داده اروپا نیز نشان داد که رویکرد فقه حکومتی در اولویت‌دهی به امنیت ملی و اعمال محدودیت بر جریان آزاد اطلاعات در شرایط بحران، کاملاً با منطق حقوق عمومی جهان و استثنائات پذیرفته‌شده در نظام‌های پیشرو هم‌سو است. با این حال، تفاوت در سرعت عمل و انعطاف‌پذیریِ «احکام ولایی» در برابر بروکراسی‌های حقوقی، مزیت رقابتی فقه حکومتی را در مدیریت بحران‌های لحظه‌ایِ سایبری به تصویر کشید.

تجربه اسفند ۱۴۰۴ ایجاب می‌کند که قانون‌گذار با فوریت به سمت تدوین «رژیم حقوقی وضعیت فوق‌العاده سایبری» حرکت نماید. این نظام تقنینی باید بر سه پایه استوار باشد: نخست، استقرار فرماندهی واحد بر تمام شریان‌های داده‌ای؛ دوم، تعبیه مکانیسم‌های قانونی تعلیق خودکار قراردادهای هوشمند جهت جلوگیری از فروپاشی اقتصادی؛ و سوم، نظام‌مند کردن مسئولیت تضامنی متخاصمین و ابرشرکت‌ها در جبران خسارات تروریسم زیرساختی. تنها با اتکا به چنین الگوی جامع و مبتنی بر فقه دفاعی است که می‌توان بازدارندگی راهبردی را به ساحت دیجیتال تسری داد و استقلال سیاسی و اقتصادی کشور را در برابر هجوم‌های هیبریدیِ آینده تضمین نمود.

منابع

الف) فارسی و عربی

- ابن‌نجیم، زین‌العابدین بن ابراهیم. ۱۴۱۹. الاشـــباه و النظایر علی مذهب ابی حنیفه النعمان. بیروت: دارالکتب العلمیه.
- انصـــاری، باقر و کاتب دامغانی، محمد مهـــدی. ۱۴۰۱. «رژیم حقوقی قراردادهـــای رایانش ابری». فصلنامه تحقیقات حقوقی، ۲۵(۹۸)، ۲۱۹-۲۴۴.
- امیدی، سجاد، مجتهد سلیمانی، ابوالحسن، و رسایی، محمد. ۱۴۰۰. «تجسس از منظر فقه حکومتی با رویکرد امنیتی-نظامی». مطالعات بین‌رشته‌ای دانش راهبردی، (۴۲)، ۳۸۳-۴۱۴.
- بافهم، محمد و فهیمی، عزیزاله. ۱۳۹۶. «شمول ضمان غصب نسبت به تصرفات دولت (با نگاهی به رویه قضایی)». پژوهش حقوق خصوصی، ۵(۱۹)، ۹-۳۸.
- بجنوردی، سید محمدحسن. ۱۴۰۱. القواعد الفقهیه. ج ۱. تهران: موسسه عروج.
- جعفری، افشین. ۱۳۹۸. «حاکمیت بر فضای سایبر از منظر حقوق بین‌الملل و نظام حقوقی جمهوری اسلامی ایران». رهیافت انقلاب اسلامی، ۱۳(۴۹)، ۱۰۹-۱۳۲.
- جوادی آملی، عبدالله. ۱۴۰۱. ولایت فقیه: ولایت فقاهت و عدالت. قم: مرکز نشر اسراء.
- گرجی، ابوالقاسم. ۱۳۹۸. مقالات حقوقی. ج ۱. تهران: انتشارات دانشگاه تهران.
- حسینی، الهه سادات، واحد یاریجان یونس، و یزدانی، سمانه. ۱۴۰۳. «چالش‌های هوش مصنوعی و مبانی مسئولیت مدنی آن در فقه». پژوهش‌های تطبیقی فقه، حقوق و سیاست، ۶(۵)، ۱-۲۰.
- رحمت‌الهی، حسین و آقایی، احسان. ۱۴۰۳. نگاهی نو به مبانی حقوق عمومی (مفاهیم و ارزش‌ها). تهران: انتشارات سهامی انتشار.
- رضوی فرد، بهزاد و موســـوی، سید نعمت‌اله. ۱۳۹۵. «مســـئولیت کیفری در فضای سایبر در حقوق ایران». فصلنامه پژوهش حقوق کیفری، ۵(۱۶)، ۲۹-۴۵.
- سبحانی، جعفر. ۱۴۰۲. الموجز فی اصول الفقه. قم: موسسه امام صادق(ع).

- شریفی طرازکوهی، حسین و صیادنژاد، محمد حسین. ۱۳۹۹. «اعمال اصول بنیادین حقوق بین‌الملل بشردوستانه بر تسلیحات کاملاً خودکار به‌عنوان ابزار نوین جنگی». فصلنامه مطالعات حقوق عمومی دانشگاه تهران، ۵۰(۲)، ۵۵۱-۵۷۵.
- ضیایی بیگدلی، محمدرضا. ۱۴۰۲. حقوق بین‌الملل عمومی. تهران: کتابخانه گنج دانش.
- طباطبایی، سیدعلیرضا و کعبی‌نسب، عباس. ۱۳۹۷. «حکم‌رانی فضای مجازی و قاعده فقهی «نفی سبیل» با تأکید بر بایسته‌های نظام جمهوری اسلامی ایران». معرفت سیاسی، ۱۰(۲)، ۷۱-۹۴.
- طهماسبی، جواد و شاهمرادی، خیراله. ۱۳۹۷. «چالش‌ها و خلأهای موجود در فرایند رسیدگی به جرایم سایبری». حقوقی دادگستری، ۸۲(۱۰۴)، ۹۵-۱۲۱.
- طوسی، محمد بن حسن. ۱۳۹۰. المبسوط فی فقه الامامیه. تهران: المکتبه المرتضویه.
- عیوضی، محمدرحیم، رضایی، صفیه، و محمدی خانقاهی، محسن. ۱۴۰۰. «نقش شبکه ملی اطلاعات در تحکیم استقلال و امنیت ملی در گام دوم انقلاب اسلامی». فصلنامه علمی پژوهش‌های انقلاب اسلامی، ۱۰(۴)، ۲۹-۵۵.
- عمید زنجانی، عباسعلی. ۱۳۹۹. فقه سیاسی. ج ۲. تهران: انتشارات امیرکبیر.
- فاطمی، کامبیز. ۱۴۰۲. «رویکردهای نظری حاکم بر تعیین قلمرو حق حریم خصوصی و تاثیر آن بر اصول حاکم بر حق حریم خصوصی در فضای دیجیتال». پژوهش‌های حقوقی، ۱-۲۸.
- فرشاسعید، پرویز و جلالی، محمود. ۱۴۰۱. «مسئولیت بین‌المللی دولت‌ها در قبال حملات سایبری عوامل غیردولتی». حقوق فناوری‌های نوین، ۳(۶)، ۱۷۳-۱۸۴.
- فرهادی، محمدصادق، رستمی، ولی، و سعدی، حسینی. ۱۳۹۵. «بازشناسی مفهوم انفال مبتنی بر تعریف ناظر به ملاک». مجموعه مقالات کنگره بین‌المللی علوم اسلامی و علوم انسانی، تهران.
- فیروزآبادی، سید ابوالحسن و احمدآبادی آزادی، جواد. ۱۳۹۹. «تحلیل پیشینه حکمرانی فضای مجازی جمهوری اسلامی ایران». دانش سیاسی، ۱۶(۲)، ۵۶۳-۵۹۸.
- قاسمی، غلامعلی و نامدار، سعید. ۱۳۹۷. «بررسی مفهوم دفاع مشروع در پرتو حملات سایبری (با تأکید بر حمله استاکس نت به تأسیسات هسته‌ای ایران)». مطالعات حقوقی، ۱۰(۱)، ۱۹۹-۲۳۵.

- قائم‌پناه، صمد. ۱۳۹۲. «بررسی تطبیقی مفهوم جنگ پیش‌دستانه در فقه اسلامی و حقوق بین‌الملل». پژوهش‌های سیاسی و بین‌المللی، (۱۵)، ۱۷۱-۱۸۹.
- قدیر، محسن و کاظمی فروشانی، حسین. ۱۳۹۸. «بررسی تطبیقی حقوق کیفری ایران با اسناد بین‌المللی در زمینه مقابله و پیشگیری از وقوع تروریسم سایبری». حقوقی بین‌المللی، ۳۶(۶۰)، ۲۳۷-۲۶۷.
- کاتوزیان، ناصر. ۱۴۰۲. قواعد عمومی قراردادها. ج ۴. تهران: شرکت سهامی انتشار.
- مراغی، سید میر عبدالفتاح. ۱۴۱۷. العناوین الفقهیه. قم: موسسه النشر الاسلامی.
- محقق داماد، سید مصطفی. ۱۴۰۱. قواعد فقه: بخش جزایی. تهران: مرکز نشر علوم اسلامی.
- محقق هرچقان، علیرضا، اردبیلی، محمد علی، بیگ‌زاده، ابراهیم، و مهدوی ثابت، محمد علی. ۱۴۰۲. «حقوق بین‌الملل سایبری و توسعه صلاحیت دیوان کیفری بین‌المللی (با تأکید بر مذاکرات تالین ۲۰۱۷ میلادی)». فصلنامه مطالعات حقوق عمومی دانشگاه تهران، ۵۳(۳)، ۱۵۳۷-۱۵۵۹.
- مرکز پژوهش‌های مجلس شورای اسلامی. ۱۴۰۵. گزارش راهبردی پیامدهای حمله به زیرساخت‌های حیاتی در اسفند ۱۴۰۴. تهران: معاونت پژوهش‌های زیربنایی.
- مشکانی سبزواری، عباسعلی. ۱۴۰۰. درآمدی بر فلسفه فقه حکومتی. تهران: انتشارات کتاب فردا.
- مکارم شیرازی، ناصر. ۱۳۸۶. انوار الفقاهه: القواعد الفقهیه. ج ۱. قم: مدرسه الامام علی بن ابی‌طالب(ع).
- مکارم شیرازی، ناصر. ۱۴۰۱. القواعد الفقهیه. ج ۲. قم: مدرسه الامام علی بن ابی‌طالب(ع).
- ملک‌زاده، محمدحسین. ۱۳۹۹. اجتهاد دفاعی و ابتدایی در فقه فضای مجازی. پایگاه اطلاع‌رسانی حوزه.
- ملکوتی، رسول و ساورایی، پرویز. ۱۳۹۵. «درآمدی بر مسئولیت مدنی در فضای سایبر». پژوهش حقوق خصوصی، ۴(۱۴)، ۱۲۹-۱۴۹.
- منتظری، حسینعلی. ۱۳۸۹. دراسات فی ولایة الفقیه و فقه الدولة الإسلامیة. ج ۱ و ۲. قم: دارالفکر.
- منتظری، حسینعلی. ۱۴۰۱. دراسات فی ولایه الفقیه و فقه الدوله الاسلامیه. ج ۲. قم: نشر تفکر.
- موسوی بجنوردی، سید محمد. ۱۴۱۹ق. القواعد الفقهیه. ج ۱ و ۲. قم: الهادی.

- موسوی خمینی، روح‌الله. ۱۳۹۲. ولایت فقیه (حکومت اسلامی). تهران: مؤسسه تنظیم و نشر آثار امام خمینی.
- نجفی، محمدحسن. ۱۴۰۴. جواهر الکلام فی شرح شرائع الاسلام. بیروت: دار احیاء التراث العربی.
- نمامیان، پیمان. ۱۳۹۲. «مواجهه با تروریسم سایبری در حقوق بین‌الملل کیفری». پژوهش‌های ارتباطی، (۷۳)، ۹-۴۲.
- هاشمی، سید محمد. ۱۴۰۲. حقوق اساسی جمهوری اسلامی ایران. تهران: میزان.
- هاشمی شاهرودی، سید محمود. ۱۳۸۸. فرهنگ فقه مطابق مذهب اهل بیت (ع). ج ۴ و ۵. قم: موسسه دائره المعارف فقه اسلامی.

ب) خبرگزاری‌های

- اقتصاد نیوز. ۱۴۰۵. «هزار حمله سایبری در جنگ ۴۱ روزه خنثی شد/ درصد نجات‌ها مردمی بود». پایگاه خبری اقتصاد نیوز.
- خبرآنلاین. ۱۴۰۵. «جبهه پنهان جنگ رمضان؛ نگاهی به ابعاد سایبری درگیری ایران و آمریکا- اسرائیل». خبرگزاری خبرآنلاین.
- خبرگزاری برنا. ۱۴۰۵. «روایت وزارت ارتباطات از خسارت‌های جنگ رمضان: از حمله دشمن به ۵۰۰ سایت ارتباطی تا خسارت ۳۳۵ میلیون دلاری». خبرگزاری برنا.
- خبرگزاری مهر. ۱۴۰۵. «در ایام جنگ رمضان روزانه بیش از ۱۰۰ حمله سایبری به کشور می‌شد». خبرگزاری مهر.

ج) انگلیسی

- Anderson, J. 2026. *Cyber Dominance: The New Face of Warfare in the Middle East*. New York: Oxford University Press.
- Anderson, J., and T. Clark. 2026. “The Ramadan War: Algorithmic Targeting and Infrastructure Collapse.” *Journal of Strategic Security* 19, no. 2: 58–40.

- Brownlie, I. 2019. *Principles of Public International Law*. 9th ed. Oxford: Oxford University Press.
- Bygrave, L. A. 2024. *Data Privacy Law: An International Perspective*. Oxford: Oxford University Press.
- Couldry, N., and U. A. Mejias. 2019. *The Costs of Connection: How Data is Colonizing Human Life and Appropriating It for Capitalism*. Stanford: Stanford University Press.
- Deeks, A. 2026. "Emergency Powers in the Cyber Age." *Harvard National Security Journal* 17, no. 1: 155–120.
- Floridi, L. 2024. *The Ethics of Information*. Oxford: Oxford University Press.
- Gervais, M. 2025. "Active Cyber Defense and the UN Charter." *Yale Journal of International Law* 50, no. 1: 115–85.
- Goldsmith, J., and T. Wu. 2020. *Who Controls the Internet? Illusions of a Borderless World*. New York: Oxford University Press.
- Kulesza, J. 2022. *Due Diligence in International Law*. Leiden: Brill Nijhoff.
- Schmitt, M. N., ed. 2017. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. 2nd ed. Cambridge: Cambridge University Press.
- Schrems, M. 2024. *GDPR and National Security Exceptions: A Critical Analysis*. Berlin: Springer.
- Voigt, P., and A. Von dem Bussche. 2017. *The EU General Data Protection Regulation (GDPR): A Practical Guide*. Cham: Springer.
- Watkin, K. 2012. "Use of Force During Occupation: Law Enforcement and Conduct of Hostilities." *International Review of the Red Cross* 94, no. 885: 267–315. https://doi.org/10.1017/S1816383112000513.
- Zittrain, J. 2025. *The Future of the Internet—And How to Stop It*. Revised ed. New Haven: Yale University Press.