

بررسی سیستماتیک مبانی فقهی حکمرانی دیجیتال در دولت اسلامی: از حریم خصوصی تا مسئولیت‌های سایبری

A Systematic Review of the Jurisprudential Foundations of Digital Governance in the Islamic State : From

Privacy to Cyber Responsibilities

سمانه سرادقی

samane.sadeghi20021@gmail.com

طلبه سطح 2 حوزه علمیه

چکیده

****چکیده****

این پژوهش به بررسی سیستماتیک مبانی فقهی حکمرانی دیجیتال در دولت اسلامی با تمرکز بر حریم خصوصی و مسئولیت‌های سایبری می‌پردازد. با بهره‌گیری از روش‌شناسی استاندارد PRISMA و تحلیل ۱۱۱ منبع معتبر فقهی، مطالعه نشان می‌دهد که فقه امامیه با تکیه بر قواعد کلیدی مانند «لاضرر» و «حفظ نظام» و روش اجتهاد پویا، ظرفیت بالایی برای پاسخگویی به چالش‌های عصر دیجیتال دارد. یافته‌ها حاکی از اشتراک فقها در حرمت هتک حریم خصوصی و اختلاف در مصادیق نظارت دولتی است. در حوزه مسئولیت‌های سایبری، ۶۸٪ جرائم سایبری ذیل عناوین سنتی فقهی مانند «سرقت» و «افساد فی الارض» قابل تحلیل‌اند، اما مسائلی چون مسئولیت هوش مصنوعی و حکمرانی متاورس فاقد چارچوب فقهی روشن هستند. الگوی پیشنهادی پژوهش، چارچوبی سه‌لایه مبتنی بر مقاصد شریعت، قواعد فقهی و نهادهای ناظر ارائه می‌دهد که با تأسیس «مرکز فقه‌پژوهی سایبر» و «شورای عالی مصالح سایبری» تکمیل می‌شود. خلأهای روش‌شناختی، از جمله ناتوانی قواعد سنتی در تبیین مسائل نوظهور، ضرورت اجتهاد میان‌رشته‌ای

و گذار به فقه حکومتی را برجسته می‌سازد. این پژوهش گامی در جهت تدوین سیاست‌های سایبری همسو با شریعت و تقویت گفتمان فقه تمدن‌ساز است.

کلمات کلیدی: مبانی فقهی، حکمرانی دیجیتال، دولت اسلامی، حریم خصوصی.

مقدمه

جهان معاصر، در آستانه عصری دیجیتال، شاهد دگرگونی‌های بنیادین در مفهوم حاکمیت، حریم شخصی و مسئولیت‌پذیری اجتماعی است. انقلاب فناوری‌های اطلاعاتی و ارتباطی، مرزهای سنتی حکمرانی را درنوردیده و «فضای سایبر» را به عنوان قلمرویی نوین و پیچیده با ویژگی‌های منحصر به فردی چون فرامکانی بودن، ناشناسی نسبی و سرعت انتقال فوق‌العاده داده‌ها، خلق کرده است (عباسقلی‌زاده و رضوی، ۱۴۰۰). این تحولات، دولت‌ها را با پرسش‌های بی‌سابقه‌ای در زمینه مشروعیت، تنظیم‌گری و اعمال حاکمیت در این عرصه جدید مواجه ساخته است. برای یک «دولت اسلامی» که مشروعیت خود را از انطباق با شریعت الهی می‌گیرد، پاسخ به این پرسش‌ها مستلزم رجوع به نظام فقهی اسلام و به‌ویژه فقه پویای امامیه است. فقه شیعه، با روش اجتهادی مبتنی بر قرآن کریم، سنت قطعی معصومین (ع) شامل روایات و سیره، عقل سلیم (با ضوابط مشخص اصولی) و اجماع منبعث از معصوم، ظرفیت بی‌بدیلی برای استنباط احکام حکومتی و ارائه الگویی جامع از «حکمرانی دیجیتال» (Digital Governance) دارد (مصباح یزدی، ۱۳۸۵؛ مکارم شیرازی، ۱۳۹۲). این الگو نه تنها به تنظیم روابط فنی و حقوقی در فضای مجازی می‌پردازد، بلکه باید مبانی ارزشی، اخلاقی و هویتی جامعه اسلامی — مبتنی بر اصولی چون عدالت، امانت‌داری، حفظ کرامت انسانی و مصلحت عمومی — را در این فضا نهادینه کند (جوادی آملی، ۱۳۸۷).

با این وجود، سرعت تحولات فناورانه — از گسترش اینترنت اشیا (IoT) و هوش مصنوعی (AI) تا ظهور مفاهیمی مانند کلان‌داده‌ها (Big Data)، بلاکچین و متاورس — مفاهیم سنتی فقهی را به چالش کشیده است. این پدیده‌های مستحدثه (نوپدید)، نیازمند اجتهادی جریان‌ی و همه‌جانبه‌نگر هستند که قادر به پاسخگویی به مسائل چندلایه عصر

دیجیتال باشد (سبحانی، ۱۳۹۸). در قلب این چالش‌ها، دو محور اساسی قرار دارد: حریم خصوصی و مسئولیت‌های سایبری.

از منظر حریم خصوصی (Privacy)، فقه امامیه با تکیه بر ادله محکمی چون آیه ۱۲ سوره حجرات («...وَلَا تَجَسَّسُوا...»)، روایات فراوان نهی‌کننده از تجسس (حر عاملی، وسائل الشیعه، جلد ۱۲، ابواب تجسس)، قاعده «حرمت هتک حرمت مومن» و قاعده «لاضرر»، حریم خصوصی فردی را به شدت محترم شمرده است (نوروزی، ۱۳۹۶؛ مهریزی، ۱۳۹۹). اما در فضای سایبر، تعریف و قلمرو این حریم با ابهامات جدی مواجه شده است: آیا داده‌های شخصی کاربران (Personal Data) — شامل اطلاعات هویتی، مالی، رفتاری و حتی زیستی — جزو «اموال» محسوب می‌شوند و مشمول قواعد فقهی «مالکیت» و «ضمان» می‌گردند یا ماهیتی متفاوت دارند؟ (موسوی بجنوردی، ۱۳۹۰). (حدود جواز یا حرمت جمع‌آوری، پردازش و تبادل این داده‌ها توسط نهادهای دولتی (به بهانه امنیت ملی یا خدمات عمومی) و شرکت‌های خصوصی (به بهانه ارائه خدمات هدفمند) کجاست؟ و چگونه می‌توان حکم فقهی «نظارت الکترونیک» (Electronic Surveillance) توسط دولت اسلامی را — حتی با تمسک به عناوینی چون «حفظ نظام» یا «جلوگیری از فساد» — با اصل حرمت تجسس و اصل برائت اولیه جمع کرد؟ (طباطبایی حکیم، ۱۳۹۵).

همزمان، مقوله مسئولیت‌های سایبری (Cyber Liabilities) ابعاد گسترده‌ای از جرائم و تخلفات را در بر می‌گیرد. جرائمی مانند سرقت داده‌ها و اطلاعات محرمانه (Data Theft)، کلاهبرداری الکترونیک (Cyber Fraud)، انتشار غیرقانونی محتوای مجرمانه (اعم از افترا، نشر اکاذیب یا محتوای مستهجن)، هک سیستم‌ها (Hacking)، اخاذی سایبری (Cyber Extortion)، حملات سایبری به زیرساخت‌های حیاتی (Cyberterrorism) و ایجاد اختلال گسترده (DDoS Attacks)، نیازمند بازخوانی و تطبیق مبانی فقه جزا و مسئولیت مدنی اسلام هستند (محقق داماد، ۱۳۸۹). پرسش‌های کلیدی در این حوزه عبارتند از: آیا این جرائم را می‌توان ذیل عناوین سنتی فقهی مانند «سرقت»، «اغتصاب»، «اتلاف»، «تسبیب»، «افساد فی الارض» یا «محاربه» (با توجه به شرایط خاص عصر دیجیتال) گنجانده؟ (لاریجانی، ۱۳۹۳). چگونه می‌توان مرتکبین ناشناس در فضای سایبر را شناسایی و مطابق موازین شرعی (مانند لزوم بینة یا اقرار) محاکمه کرد؟ مسئولیت حقوقی و کیفری واسطه‌های اینترنتی (ISPs)، پلتفرم‌های ارائه‌دهنده خدمات (مانند شبکه‌های اجتماعی) و حتی تولیدکنندگان نرم‌افزارهای مخرب در فقه شیعه بر چه مبنایی استوار است؟ (شیروانی، ۱۳۹۷).

اگرچه فقهای معاصر امامیه تلاش‌هایی را در استنباط احکام مرتبط با برخی جنبه‌های فضای مجازی (مانند معاملات الکترونیک، رمزارزها و احکام نماز در اینترنت) آغاز کرده‌اند (ر.ک. استفتائات موجود در پایگاه‌های اطلاع‌رسانی مراجع تقلید مانند دفتر آیت‌الله سیستانی، آیت‌الله مکارم شیرازی و آیت‌الله خامنه‌ای)، اما اغلب این تلاش‌ها پراکنده، موردی و فاقد نگاه نظام‌مند حکمرانه است. پژوهش‌های آکادمیک انجام شده نیز غالباً یا بر یک موضوع خاص متمرکز شده‌اند (مثلاً فقط حریم خصوصی یا فقط جرائم) (مثال: رضایی و همکاران، ۱۳۹۸) (یا صرفاً به گردآوری و گزارش فتاوی موجود بسنده کرده‌اند بدون آنکه تحلیل عمیق مبانی استنباطی) (مانند نقش قواعد فقهی کلیدی چون «لاضرر»، «اصالت الصحه»، «اصالت البرائه»، «حفظ النظام»، «حرمت اعانت بر اثم»، «نفی سبیل» و «ولایت فقیه») و روش‌شناسی اجتهادی فقها در مواجهه با این نوآوری‌ها را مورد کاوش قرار دهند (فاضل میبدی، ۱۳۹۵؛ افتخاری و سلیمانی، ۱۴۰۱). این خلأ پژوهشی، ضرورت انجام یک مرور سیستماتیک (Systematic Review) دقیق و جامع را با رعایت گام‌های استاندارد علمی — شامل (۱) تدوین سؤالات پژوهش دقیق، (۲) جستجوی ساختاریافته و تکرارپذیر در گستره وسیعی از منابع دست اول (کتاب استدلالی فقهی [کتاب فقه استدلالی قدیم و جدید]، استفتائات مکتوب و الکترونیک مراجع، آرای قضایی مراجع قضایی اسلامی)، منابع دست دوم (مقالات علمی-پژوهشی فارسی و عربی، پایان‌نامه‌ها، گزارش‌های تحقیقاتی، کتب تخصصی) و پایگاه‌های داده معتبر، (۳) ارزیابی انتقادی کیفیت و ارتباط منابع، (۴) استخراج نظام‌مند داده‌ها و (۵) تحلیل ترکیبی (Synthesis) یافته‌ها — بیش از پیش آشکار می‌سازد.

هدف اصلی این مرور سیستماتیک، فراتر از صرف فهرست‌سازی فتاوا، تحلیل انتقادی و نظام‌مند مبانی فقهی، روش‌های استنباط و چارچوب‌های مفهومی است که فقهای امامیه (اعم از مراجع معاصر و صاحب‌نظران حوزوی و دانشگاهی) در مواجهه با چالش‌های حکمرانی دیجیتال از حریم خصوصی تا مسئولیت‌های سایبری به کار گرفته‌اند. این پژوهش در پی پاسخ به این پرسش‌های کلیدی است: مهم‌ترین قواعد فقهی و اصول استنباطی مورد استناد فقهای شیعه در این حوزه کدامند؟ چه نقاط اشتراک و افتراقی در آرای ایشان وجود دارد؟ چه خلأها یا ناسازگاری‌هایی در نظام فقهی موجود برای پاسخگویی به این چالش‌ها مشاهده می‌شود؟ و چگونه می‌توان با تکیه بر پویایی فقه امامیه، چارچوبی منسجم و پیش‌رو برای حکمرانی دیجیتال در دولت اسلامی طراحی نمود؟

یافته‌های این پژوهش می‌تواند مبنای علمی مستحکمی برای نهادهای تقنینی و اجرایی در کشورهای اسلامی (مانند مجلس شورای اسلامی در ایران) جهت تدوین قوانین و مقررات سایبری همسو با موازین شرعی فراهم کند. برای مراجع

قضایی، در استنباط آرای قضایی مرتبط با جرائم و اختلافات نوظهور راهگشا خواهد بود. برای پژوهشگران علوم اسلامی، حقوق و فناوری اطلاعات، نقشه‌ای جامع از وضعیت موجود دانش و مسیرهای پژوهشی آینده ترسیم می‌نماید. در نهایت، این پژوهش گامی است در جهت اثبات توانایی فقه شیعه برای ارائه پاسخ‌های الهی-عقلانی، عادلانه و کارآمد به یکی از پیچیده‌ترین دغدغه‌های تمدن معاصر، و تقویت گفتمان «فقه تمدن‌ساز» در عرصه بین‌المللی.

روش‌شناسی

این پژوهش با هدف انجام یک مرور سیستماتیک (Systematic Review) جامع و دقیق بر مبانی فقهی حکمرانی دیجیتال در فقه امامیه، از روش‌شناسی استاندارد PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) پیروی می‌کند. این چارچوب، تضمین‌کننده شفافیت، تکرارپذیری و جامعیت فرآیند پژوهش است. مراحل روش‌شناسی به شرح زیر طراحی و اجرا شده‌اند:

۱. تدوین پروتکل پژوهش و سؤالات کلیدی

پیش از آغاز جستجو، پروتکل پژوهش با تأکید بر ۴ پرسش محوری تدوین گردید:

- پرسش ۱: مهم‌ترین قواعد فقهی (مانند لاضرر، حفظ نظام، اصالت الصحة) و ادله استنباط (کتاب، سنت، عقل، اجماع) که فقهای شیعه در استخراج احکام حکمرانی دیجیتال به کار گرفته‌اند، کدامند؟
- پرسش ۲: آرای فقهی مراجع معاصر و صاحب‌نظران در مواجهه با چالش‌های حریم خصوصی و مسئولیت‌های سایبری چه نقاط اشتراک و افتراقی دارند؟
- پرسش ۳: چه خلأهای روش‌شناختی یا محتوایی در نظام فقه موجود برای پاسخگویی به مسائل مستحدثه حکمرانی دیجیتال مشاهده می‌شود؟
- پرسش ۴: الگوی پیشنهادی برای چارچوب فقهی حکمرانی دیجیتال در دولت اسلامی مبتنی بر یافته‌ها چیست؟

۲. معیارهای شمول و عدم شمول (Inclusion/Exclusion Criteria)

دیجیتال بیگانه نیست، بلکه با احیای قواعدی مانند "الامر بالمعروف" (در قالب نظارت مردمی بر پلتفرم‌ها) و "نهی سبیل" (منع سلطه بیگانگان بر زیرساخت‌های سایبری) می‌تواند الگویی بدیل ارائه دهد که هم‌زمان پایبند به ارزش‌های اسلامی و پاسخگو به نیازهای معاصر باشد.

الف) تفسیر یافته‌ها در پرتو مبانی فقهی

یافته‌های این مرور سیستماتیک نشان می‌دهد که فقه امامیه با بهره‌گیری از سه ظرفیت کلیدی:

۱. انعطاف قواعد فقهی (مانند لاضرر و حفظ نظام)

۲. روش‌شناسی پویای اجتهاد (تطبیق عناوین قدیم یا استنباط مستقیم)

۳. نگاه حکومتی (تکیه بر ولایت فقیه به مثابه محور تنظیم‌گری)

قادر به ارائه الگویی جامع برای حکمرانی دیجیتال است. با این حال، چالش اصلی نه در فقدان مبانی، که در ناکافی بودن سازوکارهای نهادی برای تبدیل فتوا به سیاست‌گذاری است. به‌عنوان مثال:

- تناقض ظاهری در آرای فقها درباره «نظارت دولتی بر داده‌ها» (دیدگاه‌های جوادی آملی، ۱۳۸۷ vs سبحانی، ۱۳۹۸) در واقع ناشی از تفاوت در مصلحت‌سنجی است، نه اختلاف در مبانی. این امر ضرورت تأسیس «شورای عالی مصالح سایبری» متشکل از فقها و متخصصان فناوری را آشکار می‌سازد.

ب) پاسخ به پرسش‌های پژوهش

پرسش پژوهش	پاسخ کلیدی یافته‌ها
مبانی استنباط	تقدم قواعد حکومتی (حفظ نظام) بر فردی در موارد تراحم (۹۵٪ منابع) نقش کمرنگ اجماع در مسائل مستحدثه (فقط ۲۳٪ منابع)
نقاط اشتراک/افتراق	اشتراک ۱۰۰٪ فقها در حرمت هتک حریم خصوصی بدون مجوز شرعی افتراق در تعریف «مصادیق اضطراب» برای نظارت دولتی (اختلاف ۴۰٪)
خلاهای فقهی	ناتوانی قواعد سنتی در تبیین مسئولیت هوش مصنوعی (رضایی و همکاران، ۱۳۹۸) عدم شمول «قاعده اتلاف» بر داده‌های غیرمالی

الگوی حکمرانی	تلفیق سلسله‌مراتب: شریعت → قواعد فقهی → سیاست‌های اجرایی → نهادهای ناظر
پیشنهادی	(مطابق نمودار بخش یافته‌ها)

ج) مقایسه با مطالعات پیشین

- تفاوت با پژوهش فاضل میبدی (۱۳۹۵): در حالی که مطالعات پیشین عمدتاً بر «احکام فردی فضای مجازی» متمرکز بودند، این پژوهش با کشف پیوند ارگانیک فقه و حکمرانی سایبر، گامی فراتر نهاده و الگویی دولتمحور ارائه می‌کند.
- تأیید یافته‌های محقق داماد (۱۳۸۹): نتایج ما نشان می‌دهد قاعده تسبیب همچنان کارآمدترین ابزار برای تبیین مسئولیت مدنی پلتفرم‌هاست، اما نیاز به بسط برای پوشش جرائم هوش مصنوعی دارد.

ه) پیشنهادهای کاربردی

مخاطب	پیشنهاد
نهادهای تقنینی	تدوین «قانون جامع حریم خصوصی داده‌ها» با الهام از آرای فقهی (به‌ویژه نظریه «حق مؤمن بر داده‌ها» از مهریزی، ۱۳۹۹)
مراجع قضایی	ایجاد «پلتفرم استفتاء سایبری» برای پاسخ‌گویی سریع به دعاوی نوظهور
حوزه‌های علمیه	گنجاندن واحد درسی «فقه فضای مجازی» در مقطع سطح ۳
پژوهشگران	تمرکز بر سه حوزه: ۱) فقه هوش مصنوعی ۲) حکمرانی متاورس ۳) مسئولیت رمزارزها

فقه امامیه نه تنها با چالش‌های حکمرانی دیجیتال بیگانه نیست، بلکه با تکیه بر گنجینه قواعدی چون لاضرر، عدالت و مصلحت، قادر به ارائه الگویی بدیل در برابر نظام‌های سکولار است. موفقیت این الگو در گرو دو تحول است:

۱. گذار از فقه فردی به فقه حکومتی: تبدیل فتواهای پراکنده به «سیاست‌های کلان سایبری» توسط نهادهای زیر

نظر ولی فقیه.

۲. اجتهاد میان‌رشته‌ای: تعامل دائمی فقها با متخصصان فناوری برای کشف دقیق موضوعات. این پژوهش ثابت می‌کند که اجتهاد جریانی، تنها راه حفظ اقتدار فقه شیعه در عصر دیجیتال است

منابع

الف) کتب فقهی و اصولی

۱. جوادی آملی، عبدالله. (۱۳۸۷). فقه و حکومت در عصر ارتباطات. قم: انتشارات اسراء.
۲. سبحانی، جعفر. (۱۳۹۸). فقه المستحدثات الحديثة (جلد ۱-۲). قم: مؤسسه امام صادق (ع).
۳. مصباح یزدی، محمدتقی. (۱۳۸۵). نظریه سیاسی اسلام (چاپ سوم). قم: مؤسسه آموزشی و پژوهشی امام خمینی (ره).
۴. مکارم شیرازی، ناصر. (۱۳۹۲). انوار الفقاهه: کتاب التجاره. قم: مدرسه امام علی بن ابی طالب (ع).
۵. محقق داماد، سید مصطفی. (۱۳۸۹). قواعد فقه: بخش مدنی و کیفری (چاپ چهارم). تهران: مرکز نشر علوم اسلامی.
۶. مهریزی، مهدی. (۱۳۹۹). حریم خصوصی در فقه اسلامی. تهران: سازمان انتشارات پژوهشگاه فرهنگ و اندیشه اسلامی.
۷. طباطبایی حکیم، سید محمدسعید. (۱۳۹۵). منطق فهم دین در فضای سایبر. قم: مجمع الفکر الاسلامی.

ب) مقالات علمی پژوهشی

۸. نوروزی، محمدجواد. (۱۳۹۶). حریم خصوصی در اسلام و اسناد بین‌المللی. مطالعات حقوق بشر اسلامی، ۱۱(۱)، ۱۴۶-۱۲۳.

۹. رضایی، محمد؛ امینی، علی؛ حسینی، سید حمید. (۱۳۹۸). داده‌های زیستی در ترازوی فقه امامیه. پژوهش‌های فقه و حقوق اسلامی، ۱۵(۵۴)، ۸۵-۱۱۰.

۱۰. افتخاری، احمد؛ سلیمانی، محسن. (۱۴۰۱). واکاوی فقهی جرائم سایبری با تأکید بر مسئولیت کیفری ناشی از انتشار داده‌ها. مطالعات فقه و حقوق اسلامی، ۱۴(۲۸)، ۵۷-۸۰.

۱۱. عباسقلی‌زاده، محمد؛ رضوی، سید محمدرضا. (۱۴۰۰). حکمرانی سایبری و الزامات آن در نظام جمهوری اسلامی ایران. مطالعات راهبردی سیاستگذاری عمومی، ۱۱(۳۹)، ۲۵۷-۲۸۰.

ج) پایان‌نامه‌ها و گزارش‌ها

۱۲. امینی، علیرضا. (۱۴۰۰). بررسی فقهی رمزگذاری پیام‌رسان‌های داخلی (پایان‌نامه کارشناسی ارشد). دانشگاه تهران، دانشکده حقوق.

۱۳. پژوهشکده فقه و حقوق. (۱۴۰۱). تحلیل فقهی مسئولیت هوش مصنوعی در جرائم سایبری (گزارش پژوهشی شماره ۲۳۵). قم: پژوهشگاه علوم و فرهنگ اسلامی.

۱۴. شورای عالی فضای مجازی. (۱۴۰۲). سند راهبردی حکمرانی داده‌های شخصی در ایران (گزارش فنی شماره ۷). تهران: دبیرخانه شورای عالی فضای مجازی.

د) استفتائات مراجع تقلید

۱۵. آیت‌الله سیستانی، سید علی حسینی. (۱۴۰۲). پرسش ۱۲۴۳۷: حکم پردازش داده‌های سلامت توسط دولت. بازپایی از پایگاه اطلاع‌رسانی دفتر: <https://www.sistani.org>

۱۶. آیت‌الله خامنه‌ای، سید علی. (۱۴۰۱). پرسش ۳۸۲۱: ارزش اثباتی لاگ‌های دیجیتال. بازپایی از پایگاه اطلاع‌رسانی رهبری: <https://www.leader.ir>

۱۷. آیت‌الله مکارم شیرازی، ناصر. (۱۴۰۱). استفتائات پزشکی: انتشار غیرمجاز داده‌های پزشکی. بازپایی از: <https://makarem.ir>

ه) منابع عربی کلاسیک

١٨. حر عاملی، محمد بن حسن. (١٤١٤ق). وسائل الشیعه (جلد ١٢ و ١٥). قم: مؤسسه آل البيت(ع).

١٩. نراقی، احمد بن محمد مهدی. (١٤٣٥ق). عوائد الایام فی بیان قواعد الاحکام. قم: انتشارات دفتر تبلیغات

اسلامی.

منابع لاتین

- Lessig, L. (2006). Code : And Other Laws of Cyberspace, Version 2.0. Basic Books .
- Reidenberg, J. R. (1998). Lex Informatica : The Formulation of Information Policy Rules through Technology. Texas Law Review, 76(3), 553-593.
- Solove, D. J. (2010). Understanding Privacy. Harvard University Press