Submit Date: 13 October 2023
Revise Date: 22 January 2024
Accept Date: 30 January 2024
Publish Date: 13 March 2024

The Encyclopedia of Comparative Jurisprudence and Law

Hacktivism: Opportunities and Human Rights Challenges from the Perspective of Islamic Jurisprudence

Nasrin Emami[1], Homa Davoudi Garmaroudi*[2], Batoul Pakzad[3]

1. Department of Criminal Law and Criminology, Ard.C., Islamic Azad University, Ardabil, Iran.
2. Department of Criminal Law and Criminology, Ka.C., Islamic Azad University, Karaj, Iran.
3. Department of Criminal Law and Criminology, NT.C., Islamic Azad University, Tehran, Iran.

* Corresponding Author's Email: homa.davoodi@kiau.ac.ir

ABSTRACT

This article examines the opportunities and human rights challenges arising from the phenomenon of hacktivism from the perspective of Islamic jurisprudence. The objective is to present a jurisprudential framework for assessing this type of activity and its implications for human rights. The present study employs a descriptive-analytical method and relies on library sources, including jurisprudential texts, legal documents, and scholarly articles related to hacktivism. Hacktivism may be regarded as a tool for exposing injustices and defending violated rights, which aligns with the general principles of enjoining good and forbidding wrong in Islamic jurisprudence. However, the methods employed in hacktivism, such as violations of privacy and disruption of systems, create serious ethical and legal challenges that require precise jurisprudential scrutiny. Hacktivist actions, with their dual nature, create challenges for the international criminal justice system, as they often blur the boundaries between lawful conduct and criminal activity. This duality raises fundamental questions regarding legitimacy, moral and legal responsibility, and the manner of addressing this phenomenon from the perspectives of human rights and Islamic jurisprudence.

Keywords: *Hacktivism, Human Rights, Islamic Jurisprudence, Cyberspace.*

How to cite: Emami, N., Davoudi Garmaroudi, H., & Pakzad, B. (2023). Hacktivism: Opportunities and Human Rights Challenges from the Perspective of Islamic Jurisprudence. *The Encyclopedia of Comparative Jurisprudence and Law, 1*(2), 1-16.

تاریخ ارسال: ۲۱ مهر ۱۴۰۲
تاریخ بازنگری: ۲ بهمن ۱۴۰۲
تاریخ پذیرش: ۱۰ بهمن ۱۴۰۲
تاریخ چاپ: ۲۳ اسفند ۱۴۰۲

دانشنامه فقه و حقوق تطبیقی

هکتیویسم: فرصت‌ها و چالش‌های حقوق بشری از منظر فقه اسلامی

نسرین امامی[۱]، هما داوودی گرمارودی[۲*]، بتول پاکزاد[۳]

۱. گروه حقوق جزا و جرم‌شناسی، واحد اردبیل، دانشگاه آزاد اسلامی، اردبیل، ایران.
۲. گروه حقوق جزا و جرم‌شناسی، واحد کرج، دانشگاه آزاد اسلامی، کرج، ایران.
۳. گروه حقوق جزا و جرم‌شناسی، واحد تهران شمال، دانشگاه آزاد اسلامی، تهران، ایران.
* پست الکترونیک نویسنده مسئول: homa.davoodi@kiau.ac.ir

چکیده

این مقاله به بررسی فرصت‌ها و چالش‌های حقوق بشری ناشی از پدیده هکتیویسم از منظر فقه اسلامی می‌پردازد. هدف، ارائه چارچوبی فقهی برای ارزیابی این نوع فعالیت‌ها و تأثیرات آن بر حقوق بشر است. تحقیق حاضر با روش توصیفی-تحلیلی و با استفاده از منابع کتابخانه‌ای، شامل متون فقهی، حقوقی، و مقالات مرتبط با هکتیویسم انجام شده است. هکتیویسم می‌تواند به عنوان ابزاری برای افشای مظالم و دفاع از حقوق پایمال شده در نظر گرفته شود که با اصول کلی امر به معروف و نهی از منکر در فقه اسلامی همخوانی دارد. با این حال، روش‌های مورد استفاده در هکتیویسم، مانند نقض حریم خصوصی و ایجاد اختلال در سیستم‌ها، چالش‌های جدی اخلاقی و حقوقی ایجاد می‌کند که نیازمند بررسی دقیق فقهی است. اقدامات هکتیویستی، با ماهیت دوگانه خود، چالش‌هایی را برای نظام حقوق کیفری بین‌المللی ایجاد می‌کند، زیرا غالباً مرزهای بین قانون و جرم را کمرنگ می‌کند. این دوگانگی، پرسش‌های اساسی در مورد مشروعیت، مسئولیت اخلاقی و قانونی، و نحوه برخورد با این پدیده از منظر حقوق بشر و فقه اسلامی را مطرح می‌سازد.

کلیدواژگان: *هکتیویسم، حقوق بشر، فقه اسلامی، فضای سایبر.*

نحوه استناددهی: امامی، نسرین. داوودی گرمارودی، هما. و پاکزاد، بتول. (۱۴۰۲). هکتیویسم: فرصت‌ها و چالش‌های حقوق بشری از منظر فقه اسلامی. *دانشنامه فقه و حقوق تطبیقی*، *۱*(۲)، ۱۶-۱.

مقدمه

هکتیویسم، به عنوان پدیده‌ای نوظهور در فضای سایبر، فرصت‌ها و چالش‌های حقوق بشری قابل توجهی را از منظر فقه اسلامی مطرح می‌کند. این کنشگری نوین، با بهره‌گیری از ابزارهای سایبری، اهدافی چون افشای فساد، حمایت از آزادی بیان و دفاع از حقوق گروه‌های تحت ستم را دنبال می‌کند. گروه‌هایی مانند "آنانیموس" در این راستا فعالیت دارند. از سوی دیگر، اقدامات هکتیویستی اغلب با نقض قوانین و ارزش‌های اخلاقی همراه است که این امر، چالش‌های حقوقی و فقهی را به همراه دارد. سوال اصلی این است که چگونه می‌توان از فرصت‌های هکتیویسم در راستای ارتقای حقوق بشر بهره برد و در عین حال، چالش‌های ناشی از آن را در چارچوب فقه اسلامی مدیریت کرد؟ این پژوهش در تلاش است تا با تبیین این فرصت‌ها و چالش‌ها، راهکارهایی برای مواجهه مسئولانه و موثر با این پدیده ارائه دهد.

مواد و روش‌ها

پژوهش حاضر یک مطالعه توصیفی - تحلیلی است. از روش کتابخانه‌ای به منظور جمع‌آوری داده‌ها و مطالب در این تحقیق استفاده شده است.

بحث

در این قسمت ابتدا به تبیین مفهوم هکتیویسم پرداخته خواهد شد.

۱. مفهوم‌شناسی هکتیویسم

حوزه "هکتیویسم" حوزه‌ای نامشخص است و بحث بر سر مفهوم، تفسیر و محتوای این واژه با پیچیدگی‌های بسیاری همراه است. مفهوم "هکتیویسم" به طور گسترده و در زمینه‌های مختلفی مورد استفاده قرار گرفته است (Karagianopoulos, 2018). هکتیویسم را می‌توان تلاشی برای تسری نظریه‌های مربوط به کنش‌های جمعی به اینترنت و توضیح چگونگی ترکیب تفکر انتقادی با مهارت‌های برنامه‌نویسی برای دستیابی به تحول اجتماعی-سیاسی و نوعی اعتراض مشروع در دنیای آنلاین دانست. از سوی دیگر، برخی آن را "هک غیرقانونی" و تقریباً معادل اعمال مجرمانه‌ای می‌دانند که امنیت اینترنت را به خطر می‌اندازد. ردای هکتیویسم همچنین توسط افرادی پوشیده می‌شود که تلاش می‌کنند سوءاستفاده‌های خود را تحت یک توجیه سیاسی مشروع جلوه دهند. از آنجا که این اعمال ممکن است رنگ و بوی سیاسی داشته باشند، بیشترین بحث و پیچیدگی را از نظر مقررات دارند؛ زیرا عناصر قابل مجازات نقض‌کننده قوانین کیفری را با عناصر سیاسی قابل حمایت مانند آزادی بیان ترکیب می‌کنند.

«پیتر کراپ» (۲۰۰۵)، در مقاله «ترور و بازی: هکتیویسم چه بود؟» می‌نویسد: «هدف هکتیویسم جلب توجه است؛ این هدف، برای حداکثر تأثیر رسانه‌ای در نظر گرفته شده است؛ تلاش برای افزایش آگاهی شهروندان در مورد برخی حقوق و آزادی ها: آزادی بیان، حریم خصوصی، آزادی دسترسی.... اساساً، هکتیویسم چیزی را در قلمرو دیجیتالی تعریف می‌کند که سیاست طغیانگر یا بیانگر، قرن هاست که از آن استفاده می‌کند: تظاهرات، تحصن و اعتصابات‌کارگری.» (Li, 2013).

به گفته « دیوید ام »: «تکنولوژی، در تار و پود زندگی ما بافته شده است؛ بنابراین تعجبی ندارد که دنیای واقعی را در دنیای سایبری منعکس کنیم. این بازتاب می‌تواند شامل تلاش برای کسب درآمد، سرقت داده ها، مختل کردن خدمات، تخریب منابع و یا صرفاً طرح مسائل اجتماعی و سیاسی باشد....از این نظر، تشخیص اینکه آیا یک حمله را می‌توان به عنوان «هکتیویسم» (یعنی اعتراض اجتماعی و سیاسی)، تعریف کرد یا اینکه بخشی از یک کمپین گسترده تر است، دشوار است.» (Davis, 2022)

۲. تعریف هکتیویسم

هکتیویسم یک پدیده پیچیده است که جنبه‌های فرهنگی، روانی، اجتماعی، اخلاقی، حقوقی و سیاسی را در بر می‌گیرد.

از نظر «جردن»: هکتیویسم، به زبان ساده، مخفف « هک با انگیزه سیاسی » است (Musiani, 2015).

«دنینگ»، هکتیویسم را پدیده‌ای می‌داند که در آن هک با فعالیت سیاسی همگرا می‌شود (Denning, 2001).

«هالت»، هکتیویسم را به چالش کشیدن قوانین جرایم سایبری، با هدف بیان نمادین مخالفت یا تسهیل بیان سیاسی، در فضای مجازی عنوان نموده است (Karagianopoulos, 2018).

از نظر فنی، «هکتیویسم، به اقدام جمعی در فضای مجازی اشاره دارد که زیرساخت‌های شبکه را هدف قرار می‌دهد یا از ویژگی‌های فنی و هستی شناختی زیرساخت‌ها برای تغییرات سیاسی یا اجتماعی استفاده می‌کند.» (Jordan, 2004)

به اعتقاد نگارنده، «هکتیویسم، هنر استفاده از مهارت‌های هک برای تغییر جهان و پیشبرد اهداف سیاسی است. این جنبش، یک شکل از کنشگری سایبری محسوب می‌شود که از تکنیک‌های سایبری به عنوان ابزاری برای اعتراض و پیشبرد اهداف سیاسی بهره می‌گیرد. هکتیویسم، تلاقی خلاقانه فناوری و کنشگری اجتماعی را در فضای سایبری نشان می‌دهد.»

۵. انواع اقدامات هکتیویستی

اینترنت با تغییرات چشمگیر در زندگی واقعی و مجازی، جامعه و سیاست مدرن را دگرگون کرده است. این تحولات فناورانه، زمینه‌ساز ظهور «هکتیویسم» شده است.

بر اساس دیدگاه همپسون (۲۰۱۲)، ایدئولوژی و اهداف، شکل هکتیویسم را تعیین می‌کنند (Fletcher, 2014).

هکتیویسم، که زیرمجموعه کنشگری دیجیتال است، شامل فعالیت‌هایی از ارسال ایمیل به سیاستمداران تا حملات انکار سرویس (DoS) می‌شود. ادغام فناوری در اقدامات، یکی از مفاهیم کلیدی هکتیویسم است که انتخاب روش‌ها را بر اساس نیاز جنبش‌های اجتماعی شکل می‌دهد. هکتیویست‌ها غالباً روش‌هایی را انتخاب می‌کنند که غافلگیرکننده، نوآورانه و مستقیم باشند.

برخی هکتیویست‌ها بدون حضور فیزیکی و آسیب پایدار عمل می‌کنند. حملات رایج شامل حملات ممانعت از سرویس(DoS/DDoS)، تحصن‌های مجازی، بمباران ایمیلی، انتشار ویروس‌ها، تخریب وب‌سایت (Defacement) و نفوذ به سیستم‌ها است (Broussard, 2018).

حملات منع سرویس (DoS): این حملات تلاشی برای مسدود کردن دسترسی کاربران به وب‌سایت‌ها است. در این حملات، سرور میزبان با حجم عظیمی از درخواست‌های اطلاعاتی اشباع می‌شود که منجر به کندی یا از دسترس خارج شدن کامل سایت می‌گردد (Samuel, 2004, p. 10).

حملات منع سرویس توزیع شده (DDoS): نوع رایج‌تر حملات **DoS**، حملات DDoS است که با استفاده از شبکه‌ای از چندین کامپیوتر مهاجم (بات‌نت) انجام می‌شود. این حملات با هدایت سیل ترافیک به سمت سرور هدف، منابع آن را مصرف کرده و دسترسی کاربران قانونی را مختل می‌کنند. یک حمله DDoS قوی می‌تواند روزها ادامه یابد (Fletcher, 2014).

اولین "اعتصاب شبکه‌ای" یا نوعی حمله DDoS در سال ۱۹۹۵، زمانی رخ داد که فعالان اینترنتی با بارگذاری مداوم صفحات وب‌سایت‌های دولتی فرانسه، دسترسی به آن‌ها را برای مدتی مسدود کردند (Miller, 2020). گروه غیرمتمرکز "آنانیموس" نیز کمپین‌هایی برای اختلال در وب با هدف آزادی بیان آنلاین اجرا کرده و در حملات DDoS علیه وب‌سایت‌های دولتی و تجاری شرکت کرده‌اند (Miller, 2020).

تحصن مجازی، شکلی از اعتراض در فضای اینترنت است که با الهام از تحصن‌های فیزیکی عمل می‌کند. هدف اصلی آن جلب توجه عمومی به یک موضوع خاص از طریق ایجاد اختلال در دسترسی به یک وب‌سایت است. این کار با هدایت هزاران کاربر به صورت همزمان به سمت یک سایت، باعث افزایش ترافیک و کندی یا از دسترس خارج شدن آن می‌شود.این روش شباهت

زیادی به حملات DDoS دارد؛ هر دو با غرق کردن سرور هدف در حجم عظیمی از درخواست‌ها، عملکرد عادی آن را مختل می‌کنند. با این حال، تفاوت کلیدی در نحوه اجراست: تحصن مجازی معمولاً توسط معترضان منفردی انجام می‌شود که به صورت دستی یا با استفاده از نرم‌افزارهای خودکار، صفحات وب را مکرراً بارگذاری می‌کنند، در حالی که DDoS اغلب با استفاده از شبکه‌ای از دستگاه‌های آلوده (بات‌نت) صورت می‌گیرد. (Carty, 2007, p. 520; Castells, 2012; Chen, 2018).

گروهی به نام "شبکه استرانو" در سال ۱۹۹۵ یکی از اولین نمونه‌های تحصن مجازی را با اعتراض به سیاست‌های هسته‌ای و اجتماعی دولت فرانسه اجرا کرد (Denning, 2001).

تخریب وب‌سایت: در این نوع حمله، ظاهر یا محتوای یک وب‌سایت تغییر داده می‌شود تا پیامی سیاسی یا اعتراضی به نمایش گذاشته شود. این روش معمولاً کم‌خطرترین شکل هکتیویسم محسوب می‌شود و می‌تواند محدود به یک وب‌سایت یا در مقیاس وسیع‌تر، شامل صدها یا هزاران سایت باشد. اگرچه هکتیویست‌ها با این کار کنترل وب‌سایت را به دست می‌گیرند، اما تخریب وب‌سایت لزوماً به زیرساخت آن آسیب نمی‌رساند.این نوع حملات اغلب به منظور نمایش مهارت‌های فنی هکرها و نیز انتقال یک پیام خاص انجام می‌شوند (Jordan, 2004).

سرقت اطلاعات: در این رویکرد، هکتیویست‌ها اقدام به سرقت اطلاعات هویتی یا مالی افراد کرده و از آن برای افشای بی‌عدالتی یا ارسال پیام‌های اعتراضی استفاده می‌کنند. با وجود غیرقانونی بودن این عمل، سرقت اطلاعات در بین هکتیویست‌ها رواج دارد (Hajjarian, 2019).

هدف از این حملات معمولاً رسوا کردن یک شرکت یا برجسته کردن ضعف‌های امنیتی آن است (Jamali, 2024).

برای مثال، گروه انانیموس با هک کردن شرکت امنیتی HBGary، اطلاعات شخصی و ایمیل‌های کارکنان آن را پس از تهدید به افشای هویت اعضای گروه، منتشر کرد (Solomon, 2017). همچنین، این گروه اطلاعات ۶۴۰۰۰ کارگر و کاربر یک شرکت مخابراتی در تانزانیا را به سرقت برده و به صورت آنلاین منتشر کرد (Solomon, 2017).

در رویدادی دیگر، هکرها با نفوذ به سیستم کامپیوتری مجمع جهانی اقتصاد در داووس سوئیس، اطلاعات شخصی شرکت‌کنندگان در کنفرانس را به سرقت برده و برای یک روزنامه سوئیسی ارسال کردند (Brown, 2019).

بمب‌های ایمیل: بمب ایمیل روشی برای ارسال انبوه هزاران پیام به یک صندوق پستی است که آن را غیرقابل استفاده می‌کند. این عمل، نوعی "محاصره مجازی" است و اغلب با هدف انتقام یا آزار به کار می‌رود، اما گاهی نیز به عنوان ابزار اعتراض سیاسی استفاده می‌شود (Denning, 2001).

یکی از اولین موارد، حمله به سفارتخانه‌های سریلانکا توسط چریک‌های تامیل بود که با ارسال هزاران ایمیل با عنوان "ببرهای سیاه اینترنتی" ارتباطات را مختل کردند (Denning, 2001).

سازمان‌هایی مانند عفو بین‌الملل و گرین‌پیس نیز اعضای خود را تشویق می‌کنند تا با ارسال پیام‌های اعتراضی (گاهی با کمک نرم‌افزارهای خودکار) از این روش استفاده کنند (Krotofil, 2018).

بدافزار (نرم‌افزار مخرب) به برنامه‌هایی اطلاق می‌شود که بدون اطلاع کاربر، با هدف نفوذ، آسیب رساندن به داده‌ها، حریم خصوصی، یا اختلال در عملکرد سیستم‌ها طراحی می‌شوند (Owen, 2017).

بدافزارها که معمولاً از طریق ایمیل یا لینک‌های آلوده منتشر می‌شوند، انواع مختلفی دارند از جمله ویروس‌ها، کرم‌ها،

تروجان‌ها، جاسوس‌افزارها، ابزارهای تبلیغاتی مزاحم و باج‌افزارها (Krotofil, 2018).

هکتیویست‌ها از بدافزارها به عنوان ابزاری برای بیان اعتراض و آسیب رساندن به سیستم‌های هدف استفاده می‌کنند. اگرچه کاربران عادی اغلب همه انواع بدافزار را "ویروس" می‌نامند، اما تفاوت‌های فنی وجود دارد. ویروس‌ها به برنامه‌های دیگر متصل شده و با تکثیر خود، موجب خرابی داده‌ها یا اختلال در عملکرد سیستم می‌شوند (Denning, 2001; Pahlevani, 2012).

کرم‌ها نیز مخرب هستند اما برخلاف ویروس‌ها، مستقل عمل کرده و به تنهایی منتشر می‌شوند (Pahlevani, 2012).

۴. هکتیویسم از منظر فقهی

فقه اسلامی، به عنوان یک نظام حقوقی و اخلاقی مبتنی بر وحی الهی، چارچوبی جامع برای ارزیابی رفتارهای انسانی ارائه می‌دهد. با توجه به نقش مهم فقه اسلامی در شکل گیری قوانین کیفری، بررسی اشکال مختلف هکتیویسم و تطبیق رفتارهای ارتکابی در هر یک از این اشکال با قواعد فقهی، می‌تواند در تعیین دایره جرم انگاری رفتارهای هکتیویستی مؤثر باشد.

تعریف هکتیویسم از منظر فقهی نیازمند تطبیق آن با مفاهیم و اصول موجود در فقه اسلامی است، چرا که "هکتیویسم" به عنوان اصطلاحی مدرن، در منابع کلاسیک فقه نیامده است. اما می‌توان آن را با استفاده از مفاهیمی مانند امر به معروف، نهی از منکر، تجسس، افساد، تعاون بر برّ یا اثم، و نیت اعمال تحلیل و تعریف کرد.

مشروع یا نامشروع بودن هکتیویسم در فقه، مطلق نیست، بلکه بستگی به شرایط و نیت و شیوه اجرا دارد، درست مانند(بسیاری از افعال که در فقه با قاعده نظری به نیت و نتیجه سنجیده می‌شوند) (Makarim Shirazi, 1999).

در مواجهه با پدیده‌ی نوظهور هکتیویسم، فقه اسلامی رویکردی چندوجهی را ایجاب می‌کند که در آن، اصول و قواعد بنیادین شریعت ملاک سنجش قرار می‌گیرند. هیچ نص صریحی در منابع اولیه اسلامی (قرآن و سنت) در خصوص "هکتیویسم" وجود ندارد، اما با استنباط و تطبیق از قواعد کلی، می‌توان به دیدگاه‌های فقهی دست یافت:

۱. قصد و نیت:

نیت ـ از ریشه نوی، ینوی ـ اشتقاق یافته و به معنی قصد و عزم بر انجام کاری است و ناظر بر جهت دهی نفس به انجام رفتار است. نیت، همچنین به معنی روح عمل آمده است. به اعتبار صحت نیت، رفتار صحیح و با فساد آن، فاسد است. به این دلیل پیامبر اکرم (ص) فرموده است:«همانا صحت اعمال به نیات است و هر کس به اعتبار آنچه قصد نموده، نتیجه می‌گیرد (Majlisi, 2003).

در فرهنگ اسلامی، نیت فاعل، نقشی بنیادین در تعیین حکم شرعی عمل دارد. این اصل که "الأعمال بالنیات" (اعمال تابع نیت‌ها هستند)، مبنای سنجش در فقه است. اسلام نیت را سرچشمه اعمال می‌داند و در مورد پاک نمودن و پاک نگهداشتن آن سفارش بسیار نموده است، و به طور کلی ساختار وجود انسان را در رابطه تنگاتنگ با نیت می‌داند، خداوند در قرآن کریم میفرماید: قُلْ كُلٌّ يَعْمَلُ عَلَى شَاكِلَتِهِ فَرَبُّكُمْ اعْلَمُ بِمَنْ هُوَ اهْدَى سَبِيلا: بگو هر کس طبق روش (و خلق وخوی) خود عمل میکند. منظور از شاکله، همان نیت است (Hajjarian, 2019).

اهداف مشروع: اگر هدف از فعالیت هکتیویستی، دفاع از مظلوم، افشای فساد گسترده و آشکار، جلوگیری از ظلم فاحش، مبارزه با تبعیض، یا احقاق حق مستضعفان باشد، و این اهداف از طریق ابزارهای مشروع قابل تحصیل نباشند، ممکن است از منظر شرعی، تحت شرایط خاصی، قابل توجیه باشد. این توجیه در صورتی ممکن است که عمل در راستای مصالح عامه و دفع مفاسد بزرگتر صورت گیرد. که در ادامه به آن خواهیم پرداخت.

اهداف نامشروع: در مقابل، اگر هدف از هکتیویسم، ایجاد فتنه، ترویج باطل، آسیب رساندن به افراد بی‌گناه، کسب منافع شخصی از راه حرام، ایجاد اختلال در نظم عمومی، یا تضعیف پایه‌های دین و جامعه باشد، چنین عملی به طور قطع جایز نیست. مقام معظم رهبری حضرت آیت‌الله‌العظمی خامنه‌ای (حفظه‌الله تعالی): در پاسخ به استفتاء شماره ۷۲۰۳۵۵ فرموده اند: هر کاری که به نحوی موجب تضعیف نظام اسلامی شود، جایز نیست[1].

۲. مصلحت و ضرر:

یکی از قواعد مهم فقهی، قاعده "جلب مصلحت و دفع مفسده" است. هر عملی که مصلحت بیشتری داشته باشد و ضرر و فساد کمتری به همراه داشته باشد، از نظر شرعی ارجح است. این قاعده ناظر به جنس و طبیعت مصلحت و مفسده است و در ذیل قاعد تقدیم اهم مطرح میشود به این شکل که در تعارض مصلحت و مفسده آنچه اهم باشد مقدم میشود و درصورت تساوی میان مصلحت و مفسده، دفع مفسده مقدم است (Hosseini, 2021).

- سنجش فواید و مضرات: فعالیت‌های هکتیویستی باید با سنجش دقیق فواید و مضرات احتمالی آن‌ها مورد ارزیابی قرار گیرند. اگر یک عمل هکتیویستی، هرچند با نیت خیر، منجر به ایجاد فتنه، هرج و مرج، آسیب رساندن به حقوق شهروندان، یا تضعیف امنیت عمومی شود، در حکم ضرر محسوب شده و از منظر شرعی مذموم یا ممنوع خواهد بود.
- قاعده "لا ضرر و لا ضرار": بر اساس این قاعده، عقل به لزوم پیشگیری از ضرری که احتمال تحقق آن وجود دارد حکم می‌کند. بر مبنای این قاعده لازم است که با بررسی ضررها و نسبت میان آنها، ضرر بزرگتر دفع شود و بر این مبنا گاهی واردکردن ضرر برای دفع یک ضرر بزرگتر، به مصلحت است. با این توجیه به عنوان مثال اگر برای جلوگیری از فعالیت سامانه‌های اطلاعاتی غیراخلاقی یا مخل به امنیت کشور راهی به جز هک کردن آن‌ها وجود نداشته باشد، این عمل به حکم وجوب دفع ضرر محتمل، جایز و چه بسا واجب خواهد بود؛ زیرا در تزاحم میان حقوق مالکان سامانه‌های اطلاعاتی مورد نظر و حفظ امنیت اخلاقی، روانی، اقتصادی و فرهنگی جامعه، اصل بر تقدم اهم نسبت به مهم است. از این رو در این موارد، قاعده وجوب دفع ضرر محتمل بر قاعده لاضرر نسبت به تصرف در داده‌های رایانه‌ای فردی که اقدام به انتشار مطالب غیر اخلاقی نموده است، مقدم می‌شود (Nazari Tavakkoli, 2021).
- فقه اسلامی به شدت بر حفظ کرامت انسانی، حریم خصوصی افراد، و محرمانه بودن اطلاعات تأکید دارد. حرمت هتک حیثیت و از بردن آبرو و اعتبار افراد، مستند به آموزه‌های قرآنی[2] بوده، یکی از مقاصد شریعت به شمار می‌آید (Nazari Tavakkoli, 2021).
- حرمت هتک حرمت و تعرض به اموال: نفوذ به سیستم‌های کامپیوتری، سرقت اطلاعات، و دسترسی غیرمجاز به داده‌ها، در حکم تعرض به حریم خصوصی و اموال (اعتبار، اطلاعات) افراد است. این اعمال، بدون مجوز شرعی، حرام هستند. هک کردن سامانه‌های اطلاعاتی توسط هکرهای کلاه سیاه و سرقت فیلم یا عکسهای خصوصی افراد و در وضعیت‌های ناخواسته، می‌تواند تهدیدی برای آبروی کاربران به حساب آید. این عمل در برخی موارد، منجر به اشاعه فساد می‌شود که فقهای مسلمان بر حرمت آن تأکید دارند (Nazari Tavakkoli, 2021). رمزگشایی سامانه‌ها و ورود غیر

[1] https://118ahkam.ir

[2]–سوره نساء، آیات ۹ و ۷۹؛ سوره توبه آیات۴ و ۱۴۸؛ سوره نور آیات ۴ و ۲۴

مجاز به فضای آن‌ها نیز می‌تواند منجر به فساد و کشف اسرار سیاسی و امنیتی کشور شده، پیامدهای نامطلوب زیادی به دنبال داشته باشد (Nazari Tavakkoli, 2021).

- مطابق فقه اسلامی، تجسس در امور دیگران نیـز حرام است. در هکتیویسم با دسترسی غیرمجاز به داده ها، می‌توان نشانه‌های تجسس در امور دیگران را دید. عقل بر قبیح بودن دسترسی غیرمجاز به داده‌هایی که حاوی اطلاعات اشخاص می‌باشند حکم می‌کند. زمانی که هـکرهای کلاه سیاه و کلاه خاکستری عملیات هـک را انجام می‌دهند و به صورت غیرمجاز به داده‌ها و سامانه‌های دیگران که می‌تواند حاوی اطلاعات خصوصی و زندگی خانوادگی اشخاص باشد، در واقع در امور دیگران به تجسس پرداخته اند.

قرآن کریم آن گاه که از آسیب‌های اخلاقی و شخصیتی انسان‌ها سخن می‌راند، تجسس در امور و زندگی شخصی دیگران را یاد می‌کند و ایمان آورندگان را از استمرار این رفتار ناپسند اخلاقی بر حذر می‌دارد :«يَا أَيُّهَا الَّذِينَ آمَنُوا اجْتَنِبُوا كَثِيراً مِنَ الظَّنِّ إِنَّ بَعْضَ الظَّنِّ إِثْمٌ وَلا تَجَسَّسُوا[1] »

در بخشی از سخنان امام خمینی آمده است: « کسانی که با انگیزه‌های سیاسی یا غیر سیاسی حریم خصوصی دیگران را محترم نمی‌شمارند و اقدام‌های خود را به لحاظ عرفی یا شرعی توجیه می‌کنند، از مسأله حرمت اظهار و افشای گناهان و لغزش‌های مردم و طبعاً اشاعه زشتی در جامعه، چه تلقی دارند؟ چون به هر حال این گونه دخالت‌های ناروا پیامدهایی غیر منتظره به همراه خواهد داشت. پندار باطلی است اگر تصور شود که زیان این گونه حرکت‌ها گریبانگیر یک فرد یا گروه می‌شود؛ چرا که امنیت اجتماعی یک جامعه و نظام را زیر سؤال می‌برد. وقتی کسی یا کسانی در محل مسکونی یا اشتغال خود احساس نا امنی داشته باشند، چگونه می‌توان از اخلاق اجتماعی اسلام سخن به میان آورد یا مدعی کرامت انسان و عدالت اجتماعی شد؟ » از این رو رهبر فقید انقلاب اسلامی در فرمان هشت ماده‌ای خود ـ که بر پیشانی نظام و انقلاب می‌درخشد ـ آشکارا از مسئولان خواستند که حرمت مردم را نگاه دارند و حریم خصوصی کسی را جولانگاه پندار و شیوه غیر انسانی ـ اسلامی خود قرار ندهند (Hedayati Fakhr Davoud, 2009).

به اعتقاد نگارنده در تطبیق قواعد فقهی با پدیده هکتیویسم، می‌توان گفت که هکتیویسم نوعی اقدام سایبری است که با نیت مقابله با ظلم، افشای فساد یا دفاع از حقوق مردم صورت می‌گیرد، اما ماهیت آن از نظر شرعی تابع میزان مطابقت با اصولی چون حرمت تجسس، قاعده لاضرر، مشروعیت وسیله، و رعایت مصالح عمومی است. بنابراین، هکتیویسم در فقه اسلامی می‌تواند در مواردی که از مرزهای شرعی تجاوز نکند و به قصد نهی از منکر یا دفع ظلم باشد، مشمول مشروعیت مشروط قرار گیرد، و در غیر این صورت، می‌تواند در زمره‌ی افساد، تجسس حرام یا تعدی به حقوق دیگران تلقی شود.با توجه به آنچه بیان شد می‌توان نتیجه گرفت: از منظر فقه اسلامی، هکتیویسم به خودی خود نه مطلوب است و نه مذموم، بلکه حکم آن وابسته به نیات، اهداف، روش‌ها، و پیامدهای عمل است. فعالیت‌هایی که با اهداف تخریبی، فسادآلود، یا ایجاد فتنه صورت می‌گیرند، جایز نیستند. اما اگر فرد هکتیویست، با داشتن نیت خالصانه برای دفع فساد بزرگ، احقاق حق مظلوم، یا افشای حقیقت، و با رعایت اصول شرعی (مانند عدم ضرر به بی‌گناهان، حفظ حریم خصوصی در حد امکان، و در نظر گرفتن مفسده و مصلحت) دست به عمل زند، ممکن است عمل او مورد بررسی دقیق‌تری قرار گیرد و در شرایط خاص، حتی واجد حکم جواز یا وجوب باشد، البته در چارچوب ضوابط شرعی

[1] سوره حجرات، آیه ۴۹

و تنها در صورت فقدان راه‌های مشروع دیگر. با این حال، به نظر می‌رسد در عصر حاضر، به دلیل پیچیدگی‌های فنی و پیامدهای گسترده‌ی هکتیویسم، رویکرد احتیاطی و پرهیز از اقدامات غیرقانونی در اولویت باشد.

۵. چالش‌های حقوق بشری در اقدامات هکتیویستی

هکتیویسم، به عنوان شکلی از کنشگری سیاسی در فضای سایبر، اغلب با هدف برجسته کردن و پیشبرد مسائل مربوط به حقوق بشر ظهور می‌کند. این پدیده، که با استفاده از ابزارها و تکنیک‌های هک برای دستیابی به اهداف اعتراضی یا سیاسی شناخته می‌شود، می‌تواند ابزاری قدرتمند برای افشای بی‌عدالتی‌ها و نقض حقوق بشر باشد (Brown, 2019). با این حال، مرز باریک بین هکتیویسم به عنوان یک ابزار مشروع برای بیان و هک به عنوان یک عمل مجرمانه، همواره موضوع بحث و چالش بوده است (Solomon, 2017).

هکتیویست‌ها، با بهره‌گیری از ناشناس بودن نسبی در فضای آنلاین، گاهی نقش مهمی در افشای اطلاعات و آگاهی‌بخشی عمومی ایفا می‌کنند. این گروه‌ها می‌توانند به عنوان "نگهبانان پاسخگویی" عمل کنند، به ویژه زمانی که نهادهای سنتی در اجرای عدالت یا حفظ حقوق افراد ناکام می‌مانند (Chen, 2018). اما این فعالیت‌ها، غالباً با نگرانی‌های امنیتی و قانونی همراه است، زیرا ماهیت ناشناس و اقدامات فنی مورد استفاده، تشخیص هویت و انگیزه واقعی هکتیویست‌ها را دشوار می‌سازد (Brown, 2019). از سوی دیگر، بحث در مورد "حقوق اولیه" و اقدامات هکتیویستی به عنوان شکلی از اعتراض، نشان می‌دهد که رویکردهای قانونی و اخلاقی نسبت به هکتیویسم باید با دقت بیشتری مورد بررسی قرار گیرد. ممنوعیت کلی تمامی اشکال هکتیویسم ممکن است فعالیت‌های اعتراضی سازنده‌ای را نیز که با هدف ارتقای دموکراسی و حقوق شهروندی صورت می‌گیرد، در بر گیرد (Wang, 2022). این موضوع، لزوم تعریف دقیق‌تر و تفکیک قائل شدن بین انواع مختلف فعالیت‌های سایبری را برجسته می‌سازد، به طوری که بتوان از سوءاستفاده‌ها جلوگیری کرد و در عین حال، امکان ابراز عقیده و اعتراض مشروع را نیز حفظ نمود (Davis, 2022; Lee, 2021).

۶. چالش‌های حقوق کیفری در خصوص هکتیویسم در عرصه بین‌المللی

ماهیت فراسرزمینی فضای سایبر و همچنین ماهیت دوگانه اقدامات هکتیویستی، چالش‌های قابل توجهی را برای نظام حقوق کیفری در سطح بین‌المللی ایجاد کرده است.

مشکل تعیین صلاحیت: هکتیویسم، گاهی با نقض قوانین سایبری، از جمله دسترسی غیرمجاز به سیستم‌ها، افشای اطلاعات و تخریب داده ها، همراه است که چالش‌های جدی در زمینه تعیین صلاحیت قضایی ایجاد می‌کند.

بند ۵ ماده ۲۲ کنوانسیون بوداپست مقرر می‌دارد: « چنانچه بیش از یک عضو کنوانسیون نسبت به یک جرم سایبری که در کنوانسیون پیش بینی شده ادعای صلاحیت داشته باشد، اعضاء باید در صورت لزوم با یکدیگر مشورت کرده، مناسبترین راه حل ممکن را برای اعمال صلاحیت و تعقیب مرتکب مشخص کنند. » چنین ماده‌ای فاقد ضمانت اجرای لازم است و به خصوص بر مبنای میزان خسارات وارد شده، ممکن است کشورها مصمم به اعمال صلاحیت خود باشند. قانون جرایم رایانه‌ای ایران نیز در این خصوص راه حلی ارائه ننموده است.

امروزه بسیاری از فعالیت‌های هکتیویستی بدون توجه به جنبه‌های افتراق آن‌ها با این پدیده، با عناوینی نظیر جنگ سایبری، جاسوسی سایبری و تروریسم سایبری (به خصوص پس از حملات ۱۱ سپتامبر) به عمد یا به سهو، یکی انگاشته می‌شوند و زمینه صلاحیت جهانی را برای مقابله با آن فراهم می‌کنند.

با وجود همه این فرض‌ها و قانونگذاری ها، اطلاعات در فضای سایبر با سرعت و سهولت بی‌سابقه‌ای منتقل می‌شوند. این امر نه

تنها تعیین صلاحیت قضایی را پیچیده می‌کند، بلکه به چالش کشیدن مفاهیم سنتی حاکمیت ملی را نیز در پی دارد. با توجه به ماهیت فرامرزی و پیچیده این پدیده، مواجهه با چالش‌های حقوقی و عملیاتی ناشی از هکتیویسم و پاسخ دهی مناسب در صورت لزوم، نیازمند رویکردها و توافقات بین المللی است.

مشکل استرداد مجرمین: حتی اگر یک کشور بتواند هکتیویست را شناسایی و متهم کند، استرداد وی از کشوری دیگر که قوانین متفاوتی دارد یا همکاری قضایی مورد نیاز را فراهم نمی‌کند، می‌تواند بسیار دشوار باشد. تفاوت در تعاریف جرایم سایبری و وجود پناهگاه‌های سایبری، این مشکل را تشدید می‌کند.

جامعه بین المللی همواره تلاش کرده است تا به واسطه انعقاد معاهدات دو یا چند جانبه، زمینه همکاری در رسیدگی به جرایم سایبری را فراهم نماید. بنابراین می‌توان گفت که نظام کنونی حاکم بر جرایم سایبری تا حدود زیادی متکی بر همکاری بین المللی است (Eslami, 2014).

فقدان یک نظام قضایی بین‌المللی یکپارچه: برخلاف برخی حوزه‌های حقوق بین‌الملل، یک دادگاه کیفری بین‌المللی دائمی و جامع برای جرایم سایبری وجود ندارد. رسیدگی به این جرایم اغلب نیازمند همکاری‌های دوجانبه یا چندجانبه میان کشورهاست که پیچیدگی‌های خاص خود را دارد.

سازمان ملل متحد با ایجاد دفتر مبارزه با جرم[1](UNODC) در بطن خود، به دنبال ایجاد معیارهای سازنده در سطوح مختلف همکاری‌های بین المللی تابعین خود در مواجهه و مقابله با پدیده مجرمانه است. این دفتر در ابتدا در جهت مبارزه با پدیده جرایم مواد مخدر به وجود آمد و در حال حاضر با توجه به ماهیت بین المللی جرایم سایبری در این حوزه نیز متمرکز شده است به طوری که در سال ۲۰۱۳ با انتشار پیش نویس سندی با عنوان « مطالعه جامع بر جرایم سایبری » نگرانی‌های خود را در این مورد ابراز کرد (Pourghahramani, 2021).

۷. چارچوب‌های حقوقی موجود

برخی از چارچوب‌های حقوقی موجود برای مواجهه با چالش‌های مطرح شده در خصوص هکتیویسم، عبارتند از:

قوانین ملی: اکثر کشورها قوانین کیفری خاصی برای مقابله با جرایم سایبری دارند که دسترسی غیرمجاز به سیستم‌ها، انتشار بدافزار، و حملات DDoS را جرم‌انگاری می‌کنند. با این حال، همانطور که گفته شد، این قوانین از نظر پوشش و شدت مجازات متفاوت هستند.

در حال حاضر بریتانیا، هکتیویسم را به موجب قانون سوء استفاده از رایانه سال ۱۹۹۰ به عنوان جرم سایبری، جرم انگاری نموده است.

هر چند قوانین قابل اجرا در کشور بریتانیا، به طور کلی هکتیویسم را ممنوع می‌کند، با این حال، این کشور از حق اعتراض، به عنوان عنصر اساسی آزادی بیان حمایت می‌کند. (Wall, 2007; Weber, 2014).

در ایالات متحده نیز، مشابه بریتانیا، نظام حقوقی بر پایه اصول و آموزه‌هایی استوار است که از دیرباز مدافع آزادی بیان بوده‌اند. این آموزه‌ها می‌توانند در حوزه هکتیویسم، نقش محافظتی ایفا کرده و از یک بخش محدود از فعالیت‌های هکتیویستی در برابر ممنوعیت مطلق هک، پشتیبانی کنند. به عبارت دیگر، نظام حقوقی آمریکا، با تکیه بر اصول آزادی بیان، امکان حمایت از برخی اشکال هکتیویسم را فراهم می‌آورد (Li, 2013).

قوانین متعددی در سطح فدرال و ایالتی در ایالات متحده آمریکا، جرایم مرتبط با رایانه را پوشش می‌دهند. «قانون کلاهبرداری و سوءاستفاده رایانه‌ای[2]»، یکی از مهمترین قوانین فدرال در این زمینه است که فعالیت‌هایی مانند دسترسی غیرمجاز به رایانه‌های دولتی

[1]-United Nations Office on Drugs & Crime

[2]-Computer Fraud and Abuse Act (CFAA)

یا اطلاعات طبقه بندی‌شده، کسب اطلاعات از طریق دسترسی غیرمجاز، ارتکاب کلاهبرداری با استفاده از دسترسی غیرمجاز، تهدید به انجام جرایم سایبری برای اخاذی و ایجاد آسیب به رایانه‌های محافظت شده را ممنوع می‌کند (Li, 2013).

کنوانسیون‌ها و توافق‌نامه‌های بین‌المللی:

کنوانسیون شورای اروپا در مورد جرایم سایبری

«کنوانسیون شورای اروپا در مورد جرایم سایبری» (۲۰۰۱) یا همان «کنوانسیون بوداپست»، در راستای هماهنگ نمودن تلاش‌های بین المللی ضد هک، چهارچوبی را برای رژیم‌های حقوقی داخلی ایجاد کرده است. راهکارهای تجویز شده در این کنوانسیون از نظر دامنه،کلی هستند و می‌توان آن را در مورد اشکالی از هکتیویسم که شبیه اشکال سنتی اعتراض است به کار برد.

به موجب کنوانسیون بوداپست،کشورهای امضاکننده کنوانسیون مکلفند اعمالی را که کنوانسیون، آن‌ها را به عنوان جرایم عمدی سایبری شناخته است، در قوانین جزایی داخلی شان هم به عنوان رفتارهای مجرمانه در نظر بگیرند. رفتارها شامل دسترسی غیرقانونی به اطلاعات رایانه‌ای و شبکه‌های رایانه‌ای از طریق نفوذ در داده و دستکاری در آنها، تخریب تعامل میان داده‌های سامانه‌ای از طریق حمله به شبکه‌های بزرگ، دسترسی غیرقانونی به کدهای برنامه‌های حساس، نادیده گرفتن قوانین کپی رایت و نقض حقوق تألیف نظری اینترنت و تکثیر غیرقانونی موسیقی و فیلم روی اینترنت و تخریب اطلاعات هستند (Svensson, 2017).

با توجه به محتوای کنوانسیون، مشخص می‌شود که کنوانسیون بوداپست، به صراحت به مفهوم هکتیویسم نمی‌پردازد؛ بلکه صرفاً قوانینی را پیشنهاد می‌کند که در شرایطی که از تکنیک‌های هکتیویستی استفاده شود، چنین فعالیت‌هایی را غیرقانونی می‌سازد.

کشور ایران به کنوانسیون بوداپست نپیوسته و آن را امضا نکرده است، ولی در قانون جرایم رایانه‌ای رد پای این کنوانسیون دیده می‌شود.

«منشور آفریقایی حقوق بشر و مردم»

ماده ۳ « منشور آفریقایی حقوق بشر و مردم »(۱۹۸۱) مقرر می‌دارد:« مردم حق دارند نظرات خود را در چارچوب قانون بیان و منتشر کنند.» این ماده، اَشکال اعتراض را به مواردی که توسط قانون مشخص شده محدود می‌کند؛ بنابراین کاربرد محدودی برای هکتیویسم دارد. با این حال کمیسیون آفریقایی حقوق بشر و مردم، در بیانیه اصول آزادی بیان در آفریقا، با بیان اینکه این حق می‌تواند از طریق رسانه‌های سنتی و همچنین هر شکل دیگرارتباطی اعمال شود، کاربرد گسترده تری به ماده ۳ داده است. اعلامیه همچنین تأکید می‌کند که: « حق آزادی بیان نباید به بهانه نظم عمومی یا امنیت ملی محدود شود؛ مگر اینکه خطر واقعی صدمه به منافع مشروع وجود داشته باشد و بین خطر آسیب و بیان رابطه علّی نزدیک وجود داشته باشد. » بنابراین، باید برای آسیب‌های ناشی از هکتیویسم نیز این محدودیت‌ها برقرار شود (Solomon, 2017).

- **میثاق بین المللی حقوق مدنی و سیاسی**

هکتیویسم، با انگیزه بیان اعتراضات سیاسی ظهور می‌کند. ماده ۱۳ « میثاق بین المللی حقوق مدنی و سیاسی »(۱۹۶۶) از آزادی عقیده و بیان به هر وسیله‌ای که ابراز شود، حمایت می‌کند. در ماده ۲۱ این میثاق، به طور خاص از اعتراضات خیابانی حمایت شده است وفقط محدودیت‌هایی که در یک جامعه دموکراتیک به نفع امنیت ملی و منافع عمومی و بر مبنای ضرورت و مطابق با قانون اعمال شود مجاز می‌باشد.

کنوانسیون جامع بین المللی مقابله با استفاده از فناوری‌های اطلاعات و ارتباطات برای مقاصد مجرمانه(کنوانسیون مبارزه با جرایم سایبری)

سازمان ملل متحد در دسامبر سال ۲۰۱۹، قطعنامه‌ای را تصویب کرد که به موجب آن یک «کمیته اختصاصی موقت نامحدود[1]» ایجاد شد. ماموریت و هدف کمیته مزبور، تدوین یک کنوانسیون بین‌المللی جامع در باب مقابله با استفاده از فناوری اطلاعات و ارتباطات برای مقاصد مجرمانه بود. مذاکرات از اوایل سال ۲۰۲۲ آغاز شد. در ۷ آگوست ۲۰۲۴، پس از سه سال مذاکره، کمیته ویژه سازمان ملل متحد، به اتفاق آرا، کنوانسیون مبارزه با جرایم سایبری را تصویب کرد. ماده ۷ پیش نویس این کنوانسیون، دسترسی غیرقانونی، ماده ۹ مداخله در داده‌های الکترونیکی، ماده ۱۰ مداخله در سیستم فناوری اطلاعات و ارتباطات، ماده ۱۱ سوءاستفاده از دستگاه‌ها را مورد توجه قرار داده است.

این کنوانسیون اشاره مستقیمی به هکتیویسم و اشکال شناخته شده آن ندارد؛ اما چنانچه جرایم مذکور در مواد فوق با انگیزه سیاسی صورت گرفته باشد، در قالب اقدامات هکتیویستی قرار می‌گیرد که نیاز به مقابله با آن در کنوانسیون مورد توجه قرار گرفته است.

نتیجه‌گیری

با توجه به بررسی ابعاد هکتیویسم و ارتباط آن با حقوق بشر در پرتو فقه اسلامی، می‌توان نتیجه گرفت که این پدیده نوظهور، چالش‌های قابل توجهی را در برابر هنجارهای حقوق بشری و اصول بنیادین فقهی ایجاد می‌کند. از یک سو، امکان استفاده از ابزارهای سایبری برای بیان اعتراضات و پیگیری اهداف اجتماعی و سیاسی، می‌تواند به عنوان ابزاری برای احقاق حقوق مشروع در نظر گرفته شود؛ اما از سوی دیگر، ماهیت فراگیر و گاه غیرقابل ردیابی این اقدامات، نگرانی‌هایی جدی را در خصوص نقض حریم خصوصی، امنیت داده‌ها و نظم عمومی برمی‌انگیزد. فقه اسلامی با تأکید بر مصالح عمومی، حفظ نظم اجتماعی و پرهیز از ضرر، رویکردی چندوجهی را نسبت به این پدیده ایجاب می‌کند که در آن، ضمن شناسایی امکان مشروعیت برخی از این اقدامات در چارچوب احکام اولی یا ثانوی، بر لزوم پرهیز از هرگونه ضرر، تجاوز به حقوق دیگران و برهم زدن نظم عمومی تأکید می‌شود. بنابراین، ارزیابی هکتیویسم از منظر حقوق بشر و فقه اسلامی، نیازمند درک عمیق ماهیت هر عمل، انگیزه‌های پشت آن و پیامدهای مترتب بر آن است تا بتوان قضاوت دقیقی در خصوص انطباق یا عدم انطباق آن با اصول و موازین اسلامی و حقوق بشری صورت پذیرد.

برای مقابله مؤثر با چالش‌های حقوق کیفری مرتبط با هکتیویسم، رویکردهای زیر پیشنهاد می‌شوند:

تدوین چارچوب‌های حقوقی و فقهی به‌روز: با توجه به نوظهور بودن پدیده هکتیویسم، لازم است نهادهای قانون‌گذاری و مراجع فقهی به تدوین و به‌روزرسانی چارچوب‌های حقوقی و فقهی متناسب با این تحولات اقدام کنند تا امکان انطباق و پاسخگویی به چالش‌های جدید فراهم شود .

تقویت همکاری‌های بین‌المللی: با توجه به ماهیت فرامرزی جرایم سایبری و هکتیویسم، تقویت همکاری‌های بین‌المللی در زمینه تبادل اطلاعات، شناسایی مجرمان و استرداد آن‌ها امری ضروری است تا بتوان با این پدیده به صورت مؤثر مقابله کرد .

آموزش و افزایش سواد رسانه‌ای و سایبری: ارتقای سطح آگاهی عمومی نسبت به حقوق و تکالیف در فضای مجازی، آشنایی با مخاطرات احتمالی و آموزش اصول امنیت سایبری، می‌تواند به پیشگیری از وقوع جرایم سایبری و سوءاستفاده از فناوری کمک شایانی نماید .

تأکید بر مسئولیت‌پذیری در فضای مجازی: لازم است با تبیین ابعاد شرعی و حقوقی مسئولیت‌پذیری در فضای مجازی، افراد را نسبت به پیامدهای اقدامات خود در این فضا آگاه ساخت و بر لزوم رعایت حقوق دیگران و پرهیز از هرگونه ضرر و زیان تأکید کرد .

[1]-Open-ended ad hoc committee(AHC)

تفکیک میان کنش‌های مشروع و نامشروع: با توجه به تنوع انگیزه‌ها و شیوه‌های هکتیویسم، ضرورت دارد تا با رویکردی فقهی و حقوقی، میان کنش‌هایی که در چارچوب بیان اعتراضات مشروع و احقاق حقوق صورت می‌گیرد و اقداماتی که منجر به نقض حقوق دیگران، برهم زدن نظم عمومی یا ارتکاب جرایم سایبری می‌شود، تمایز قائل شد .

بررسی تطبیقی رویکردهای فقهی و حقوقی: انجام مطالعات تطبیقی میان رویکردهای فقهی مذاهب مختلف اسلامی و همچنین نظام‌های حقوقی سایر کشورها در مواجهه با هکتیویسم، می‌تواند به غنای دانش در این حوزه و دستیابی به راهکارهای جامع‌تر کمک کند .

حمایت از آزادی بیان در چارچوب ضوابط: با در نظر گرفتن اهمیت آزادی بیان به عنوان یکی از حقوق بشری، باید تلاش شود تا فضایی امن برای بیان دیدگاه‌ها و پیگیری مطالبات مشروع در چارچوب ضوابط شرعی و قانونی فراهم شود، به گونه‌ای که این آزادی به ابزاری برای سوءاستفاده و نقض حقوق دیگران تبدیل نگردد .

توسعه پژوهش‌های میان‌رشته‌ای: با توجه به ماهیت میان‌رشته‌ای موضوع هکتیویسم که ابعاد فنی، حقوقی، اجتماعی، سیاسی و فقهی را در بر می‌گیرد، تشویق و حمایت از پژوهش‌های میان‌رشته‌ای در این حوزه می‌تواند به درک عمیق‌تر و ارائه راهکارهای عملی‌تر منجر شود.

مشارکت نویسندگان

در نگارش این مقاله تمامی نویسندگان نقش یکسانی ایفا کردند.

تعارض منافع

در انجام مطالعه حاضر، هیچ‌گونه تضاد منافعی وجود ندارد.

EXTENDED ABSTRACT

Hacktivism, as a hybrid phenomenon combining hacking skills with political and social activism, presents both opportunities and profound challenges when examined through the lenses of human rights and Islamic jurisprudence. Its conceptual ambiguity has sparked considerable debate in scholarly discourse. Some define hacktivism as a legitimate extension of collective action theories into cyberspace, a means of combining critical thought with technical expertise to achieve social or political transformation, while others equate it with illegal hacking practices that compromise internet security (Karagianopoulos, 2018). Scholars like Peter Krapp have emphasized its performative dimension, framing hacktivism as a form of protest designed to attract public attention and increase awareness of rights such as freedom of expression and privacy (Li, 2013). Yet, its manifestations range from political symbolism to outright cybercrime, blurring the line between lawful protest and unlawful intrusion. As Davis notes, the growing integration of technology into everyday life complicates the task of distinguishing acts of hacktivism from broader cyber campaigns, since the same methods may underpin criminal endeavors or social resistance (Davis, 2022). This definitional tension has profound implications, especially when assessing the legitimacy of hacktivist activities in legal, ethical, and religious frameworks, where the act, intent, and outcome are equally important.

Typologies of hacktivist activities reveal the diversity of tactics and their varying implications for human rights. Scholars emphasize that ideology and goals often determine the forms hacktivism takes (Fletcher, 2014). Actions range from relatively benign email campaigns to disruptive denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks (Broussard, 2018). The first “net strike” of 1995 in France marked the beginning of coordinated online protests, which later evolved into sophisticated DDoS campaigns by groups like Anonymous (Miller, 2020). Other methods include virtual sit-ins

(Castells, 2012; Chen, 2018), website defacement (Jordan, 2004), and data theft (Hajjarian, 2019; Jamali, 2024). These actions are often justified as exposing institutional weaknesses or highlighting injustices, yet they can simultaneously undermine privacy and security. For example, Anonymous famously breached HBGary and released personal data of its employees (Solomon, 2017), as well as sensitive information from a Tanzanian telecommunications firm (Solomon, 2017), while other hackers targeted the World Economic Forum in Davos, stealing personal data of attendees (Brown, 2019). Additional tools such as email bombs (Denning, 2001), malware (Krotofil, 2018; Owen, 2017; Pahlevani, 2012), and spyware highlight how hacktivism straddles protest and criminality. While some tactics mirror peaceful protest in digital form, others pose direct threats to fundamental human rights such as privacy, security, and property, necessitating nuanced interpretation in both secular and Islamic jurisprudence.

From the perspective of Islamic jurisprudence, the challenge is to reconcile a modern cyber phenomenon with long-established ethical and legal principles. Hacktivism does not appear in classical sources, but it can be examined through analogies to principles such as *amr bi-l-maʿrūf* (enjoining good), *nahy ʿan al-munkar* (forbidding wrong), and prohibitions against espionage (*tajassus*) or corruption (*ifsād*). The jurisprudential assessment depends heavily on intention (*niyyah*), which in Islamic legal thought is central to determining the legitimacy of an act (Hajjarian, 2019; Majlisi, 2003). Acts carried out with sincere intentions to defend the oppressed, expose widespread corruption, or prevent grave injustice might under certain conditions be justified as serving the public interest (*maslaha*) (Hosseini, 2021; Makarim Shirazi, 1999). Conversely, actions motivated by personal gain, sedition, or harm to innocents are categorically impermissible. Jurists emphasize the principle of balancing benefits and harms, applying the rule of "avoiding greater harm by tolerating lesser harm" in specific cases (Nazari Tavakkoli, 2021). Yet Islamic law also strictly prohibits violations of privacy, damage to reputations, and unlawful intrusion into others' property, whether physical or digital (Hedayati Fakhr Davoud, 2009). Therefore, while hacktivism aimed at preventing greater harm could, under exceptional conditions, be conditionally legitimate, the prevailing jurisprudential stance favors caution and prioritizes social order, privacy, and respect for rights over potentially destabilizing acts of cyber resistance.

The human rights dimension of hacktivism reveals its ambivalence as both a tool of empowerment and a source of vulnerability. On one hand, hacktivists may act as guardians of accountability, uncovering state or corporate misconduct when traditional mechanisms fail (Brown, 2019; Chen, 2018). Their anonymity can protect them from repression and enable whistleblowing that serves democratic values. On the other hand, the indistinguishability between politically motivated hacktivism and ordinary cybercrime creates risks of over-criminalization and the suppression of legitimate dissent (Solomon, 2017). Legal scholars caution that blanket prohibitions against hacktivism might inadvertently criminalize constructive forms of protest that advance human rights (Davis, 2022; Lee, 2021; Wang, 2022). This dilemma underscores the necessity of carefully distinguishing between destructive acts that infringe upon privacy, property, or security, and expressive acts aimed at raising awareness or resisting oppression. International law and human rights instruments increasingly grapple with this ambiguity, reflecting the tension between safeguarding security and protecting freedoms

of expression and association. The lack of universally accepted definitions or frameworks complicates enforcement and heightens the risk of abuse by states seeking to suppress dissent under the guise of combating cybercrime.

At the international level, hacktivism challenges conventional criminal law frameworks due to its transnational nature and dual identity as both activism and crime. Determining jurisdiction in cyber disputes is notoriously complex, as highlighted by the Budapest Convention's call for states to consult in cases of overlapping claims, though without strong enforcement mechanisms (Eslami, 2014; Pourghahramani, 2021). Problems of extradition persist when offenders operate across borders with divergent legal standards or seek refuge in "cyber havens." Meanwhile, international bodies like the UN Office on Drugs and Crime attempt to foster cooperation, yet no unified international criminal court for cyber offenses exists. Some states, like the UK, have criminalized hacktivism under the Computer Misuse Act 1990 (Wall, 2007; Weber, 2014), while still upholding freedom of expression, and the US adopts a similar balance through its Computer Fraud and Abuse Act (Li, 2013). The Budapest Convention (2001) provides the most comprehensive framework but does not explicitly address hacktivism (Svensson, 2017), while regional charters such as the African Charter on Human and Peoples' Rights emphasize freedom of expression within lawful limits (Solomon, 2017). These fragmented frameworks expose inconsistencies between national and international approaches, amplifying the need for harmonized legal standards that can distinguish legitimate protest from harmful cyber aggression without undermining fundamental rights.

In conclusion, hacktivism embodies a paradox at the intersection of technological innovation, political resistance, human rights, and religious jurisprudence. Its tactics can empower marginalized voices and hold powerful actors accountable, but they also risk violating privacy, destabilizing systems, and eroding trust in digital infrastructures. From an Islamic jurisprudential standpoint, the morality and legality of hacktivism depend upon intent, proportionality, and alignment with overarching principles of justice and social welfare. From a human rights perspective, its legitimacy hinges on balancing the right to protest with the obligation to protect security and privacy. Addressing hacktivism requires updated jurisprudential reasoning, adaptive legal frameworks, and nuanced ethical debate. Only by integrating perspectives from technology, law, ethics, and religion can societies develop balanced responses that recognize the dual potential of hacktivism—either as a vehicle for justice or as a source of harm—while preserving both human rights and societal order.

References

Broussard, M. (2018). *Dark matters: On the ontology of cybernetic objects*. MIT Press.

Brown, A. (2019). *Digital property rights and cybercrime*. Tech Publications.

Castells, M. (2012). *Networks of outrage and hope: Social movements in the Internet age*. Polity Press.

Chen, L. (2018). *Sovereignty in the digital age: Cyber interference and international law*. Global Press.

Davis, R. (2022). *The ethics of hacking and data manipulation*. Cyber Ethics Publishing.

Denning, D. E. (2001). Activism, hacktivism, and cyberterrorism: the internet as a tool for influencing foreign policy. In J. Arquilla & D. Ronfeldt (Eds.), *Networks and Netwars: The Future of Terror, Crime, and Militancy* (pp. 239-288).

Eslami, A. (2014). The Method of Courts' Jurisdiction in Adjudicating Cybercrimes. *Journal of Justice Legal Affairs*, *78*(88), 37-64.

Fletcher, R. (2014). Cyber activism: The politics of the internet. In C. de Vreese, C. R. Berger, & S. J. Ball (Eds.), *The international encyclopedia of political communication* (pp. 1-11). John Wiley & Sons, Inc.

Hajjarian, P. R. (2019). An Examination of Mens Rea in Different Types of Crimes in Islamic Jurisprudence and Iranian Law. *Quarterly Journal of Iranian and International Comparative Law*, *12*(44), 93-119.

Hedayati Fakhr Davoud, A. (2009). *Usul-e Akhlaq-e Ejtemaei-ye Eslam az Manzar-e Imam Khomeini (r.a.)*. Institute for Compilation and Publication of Imam Khomeini's Works.

Hosseini, A. A. (2021). A Critique on the Validity of the Rule "Preventing Corruption Takes Precedence Over Attracting Benefit". *Fiqhi and Usuli Researches*, *7*(23), 7-40. https://doi.org/10.53315.2020.jrj/22034.10

Jamali, R. (2024). A Comparative Study of Cyber Laws in China, the United States, and Russia: Necessities and Requirements for the Cyber Security of the Islamic Republic of Iran. *Quarterly Journal of Defense Logistics and Technology*, *7*(3), 77-108.

Jordan, T. (2004). *Hacktivism and Cyberwars*. Routledge. https://doi.org/10.4324/9780203490037

Karagianopoulos, V. (2018). Living with hacktivism: From conflict to symbiosis. In T. J. Holt & M. H. M. M (Eds.), *Digital activism* (pp. 97-114). Springer. https://doi.org/10.1007/978-3-319-71758-6

Krotofil, A. (2018). The politics of hacktivism. In *Digital activism* (pp. 97-114). Palgrave Macmillan, Cham.

Lee, S. (2021). *Misinformation and disinformation in the digital landscape*. Media Studies Publishing.

Li, X. (2013). Hacktivism and the first amendment: drawing the line between cyber protests and crime. *Harvard Journal of Law & Technology*, *27*.

Majlisi, M. B. (2003). *Bihar al-Anwar* (Vol. 67). Dar Ihya' al-Turath al-Arabi.

Makarim Shirazi, N. (1999). *Al-Madkhal fi Ilm al-Usul*. Madrasat al-Imam Ali ibn Abi Talib Publications.

Miller, D. (2020). *Understanding DDoS attacks: Impact on freedom and access*. Network Security Books.

Musiani, F. (2015). Hacktivism: A new frontier in political activism. In *The handbook of digital politics* (pp. 275-287). Oxford University Press.

Nazari Tavakkoli, V. (2021). A Jurisprudential Analysis of Hacking Information Systems. *Researches in Islamic Jurisprudence and Law*, *17*(66), 226-251.

Owen, T. (2017). Hacktivism: The digital age of protest. In *The Routledge handbook of protest movements* (pp. 375-388). Routledge.

Pahlevani, M. T. (2012). Challenges and Opportunities in Cyber Criminology. *Semanan Law Enforcement Science Quarterly*, *2*(6).

Pourghahramani, B. (2021). A Conceptual Model of Criminal Policy for Cybercrimes in Iran. *NAJA Strategic Studies Quarterly*, *6*(20), 129-154.

Solomon, R. (2017). Electronic protests: Hacktivism as a form of protest in Uganda. *Computer Law & Security Review*, *33*, 718-728. https://doi.org/10.1016/j.clsr.2017.03.024

Svensson, J. (2017). Hacktivism and its political implications. *Global Jurist*, *17*(1), 1-21.

Wall, D. (2007). Cybercrime: The interrogation of the digital offender. In *The Blackwell companion to Criminology* (pp. 349-363).

Wang, F. (2022). *Freedom of speech in the internet age: Responsibilities and misuses*. Communication Studies Press.

Weber, R. (2014). Legal aspects of computer crime. In *The Cambridge handbook of the hacker ethic and the Internet* (pp. 209-228). Cambridge University Press.