فصلنامه پژوهش‌های فقه و حقوق اسلامی/ سال هفدهم/ شماره شصت و شش/ زمستان ۱۴۰۰/ صفحات ۲۵۱ - ۲۲۶

علمی- پژوهشی

تحلیل فقهی هک کردن سامانه‌های اطلاعاتی[1]

سعید نظری توکلی *
زینب گیلانی **
شکیبا امیرخانی** *

چکیده

از مباحث مهم در حوزه فناوری اطلاعات، هک کردن سامانه‌های اطلاعاتی، یعنی یافتن نقاط ضعف امنیتی یک سیستم به‌منظور نفوذ و دسترسی به اطلاعات آن است که با انگیزه‌های مختلفی، همچون دفاع از امنیت، کنجکاوی و سود شخصی انجام می‌شود. با ملاحظه همین جهت است که هکرها به گونه‌های مختلفی، همچون کلاه‌سفید، کلاه خاکستری و کلاه‌سیاه طبقه‌بندی می‌شوند. هدف از انجام این پژوهش که به روش تحلیلی توصیفی و به استناد منابع کتابخانه‌ای انجام شده، بررسی مشروعیت هک ازنظر فقه اسلامی است. یافته‌های پژوهش حاضر نشان می‌دهد که هک کردن با توجه به نیت و عملکرد هکرها حکم فقهی یکسانی ندارد. عملکرد هکرهای کلاه‌سفید مشروع، عملکرد هکرهای کلاه‌سیاه امری نامشروع و عملکرد هکرهای کلاه خاکستری نیز بسته به مورد می‌تواند مشروع یا نامشروع باشد. مهم‌ترین مؤلفه در تحلیل مشروعیت هک، «مصلحت اهم» و مهم‌ترین مؤلفه در عدم مشروعیت آن، «عدم جواز تعدی به حقوق دیگران» است. ازاین‌رو، گرچه هک کردن از نظر حکم اولی حرام است؛ اما اگر برای رسیدن به مصلحت مهم‌تر، راهی جز هک کردن سامانه‌های اطلاعاتی وجود نداشته باشد، این عمل از نظر حکم ثانوی جایز است.

کلید واژه‌ها: هک، هکر، اطلاعات، سامانه‌های اطلاعاتی

۱- تاریخ وصول: ۱۳۹۸/۱۱/۰۹ تاریخ پذیرش: ۱۳۹۹/۰۴/۰۳

*استاد، دانشکده الهیات و معارف اسلامی، دانشگاه تهران، تهران، ایران sntavakkoli@ut.ac.ir
** دانش‌آموخته دکتری فقه و مبانی حقوق اسلامی، گروه فقه و حقوق، دانشگاه مذاهب اسلامی، تهران، ایران. zeinabgilani@gmail.com (نویسنده مسؤول)
*** استادیار، گروه فقه و حقوق، دانشگاه مذاهب اسلامی، تهران، ایران. Sh_amirkhani@ut.ac.ir

۱- مقدمه

یکی از ظرفیت‌های فضای مجازی، امکان هک شدن سامانه‌های اطلاعاتی است. این امر با ایجاد چالش در «حریم خصوصی» و «مالکیت»، جامعه را با مشکلات مختلف اقتصادی، امنیتی، فرهنگی و غیره روبرو کرده است. بنا به مطالعه شرکت HP در سال ۲۰۱۵ میلادی، خسارت‌های اقتصادی ناشی از هک شدن سیستم‌های اطلاعاتی در کشورهای مختلفی همچون آمریکا، انگلستان، آلمان، استرالیا، ژاپن، روسیه و برزیل به‌واسطه افزایش تعداد و شدت حملات نفوذگری، رو به افزایش بوده است. این حملات عبارت‌اند از: سرقت حق مالکیت معنوی شرکت‌ها و سازمان‌ها، مصادره حساب‌های بانکی برخط، ایجاد و پخش ویروس در رایانه‌های دیگر، انتشار اطلاعات تجاری محرمانه در اینترنت و اختلال در زیرساخت‌های حیاتی و ملی کشور هدف (آل‌بویه، ۱۳۹۴، ۱۰۷). همچنانکه بنا به گزارش شرکت امنیت سایبری McAfee و مرکز مطالعات راهبردی و بین المللی CSIS در سال ۲۰۱۸، مشاغل جهانی سالیانه نزدیک به یک درصد از تولید ناخالص داخلی جهانی (ناخالص داخلی) خود را که حدود ۶۰۰ میلیون دلار برآورد می‌شود در برابر جرایم سایبری از دست می‌دهند که تأثیر منفی زیادی بر اشتغالزایی، نوآوری و رشد اقتصادی دارد (پالمر، ۲۰۱۸؛ لوئیز، ۲۰۱۸، ۴). نظیر این مطلب در مورد تأثیر جرایم رایانه‌ای همچون هک بر فعالیت های اقتصادی ایالات متحده آمریکا در سال ۲۰۱۸ نیز قابل مشاهده است (دفتر ریاست جمهوری آمریکا، ۲۰۱۸، ۱).

با توجه به گسترش هک و تنوع حوزه کارکردی هکرها، ضروری به نظر می‌رسد تا این مسئله ازنظر فقهی بررسی شود؛ چراکه هکرها در کشورهای مختلف فعالیت می‌کنند و مخاطب آن‌ها نیز می‌تواند مسلمانان مذاهب مختلف اسلامی باشد.

۲- مفهوم شناسی

۲-۱- هک

واژه «هک» فارسی نبوده، فرهنگستان زبان و ادب فارسی آن را معادل «رخنه» و «نفوذ» قرار داده است (فرهنگ واژه‌های مصوب فرهنگستان، ۱۳۷۶-۱۳۸۵، بخش لاتین، ۱۰۴). واژه انگلیسی «Hack» در فرهنگ آکسفورد به «دستیابی غیرمجاز به سیستم رایانه‌ای یا داده‌های الکترونیکی» معنا شده است (برد بری، ۲۰۱۱، ۲۰۹). منظور از عمل «هک کردن» در متون تخصصی IT عبارت است از: «پیدا کردن نقاط ضعف امنیتی یک سیستم برای نفوذ به آن؛ بدون اینکه اجازه دسترسی به آن سیستم وجود داشته باشد» (داونینگ و دیگران، ۲۰۰۹، ۲۲۳).

۲-۲- هکر

برای این واژه دو معنا مطرح شده است. در آغاز، هکر عبارت بود از «برنامه‌نویس کنجکاوی که به دست‌کاری و ارتقای نرم‌افزارها و سیستم‌های الکترونیکی علاقه‌مند بوده از کشف و یادگیری کار سیستم‌های رایانه‌ای لذت می‌برد» (کوین، ۱۳۹۷، ۲۳)؛ «کسی است که از سرک کشیدن به جزئیات سیستم‌های قابل‌برنامه‌ریزی و نفوذ و رسوخ در آن لذت می‌برد و مصمم به شکست دادن توانایی‌های محاسباتی ماشین در مقابل هوش و ذکاوت بشری خویش است. فردی که با سماجت و به‌گونه‌ای لجوجانه، شیفته برنامه‌نویسی است. نفوذگر، بدخواه نیست و صدمه نمی‌زند» (ملکیان، ۱۳۸۵، ۱۷). بر این اساس، هکر فردی است که استعداد زیادی در گسترش کار و عملکرد رایانه‌ها و نیز طراحی اصلی آن‌ها دارد و به‌عنوان فردی کنجکاو و شرافتمند عمل می‌کند (اسکودیس، ۱۳۸۸، ۲۳)؛ اما در سال‌های اخیر، واژه هکر در معنای جدیدی به کار گرفته و منظور از آن، «فردی است که با انگیزه نادرست، اقدام به هک سامانه‌های اطلاعاتی و اهداف بداندیشانه خود را با نفوذ به سیستم‌های رایانه‌ای عملی می‌کند» (کوین، ۱۳۹۷، ۲۳). هکر در این تعریف، همسان با واژه «کِرَکِر»[۱] به کار می‌رود.

۲-۳- اطلاعات

منظور از اطلاعات[۲]، داده‌هایی است که به شکل قابل‌فهم و قابل‌استفاده برای انسان‌ها درآمده باشند. در مقابل، داده‌ها[۳] جریانی از وقایع داخل و خارج سازمان را تصویر می‌کنند که هنوز سازماندهی و مرتب نشده‌اند.

۲-۴- سامانه اطلاعاتی

سامانه اطلاعاتی مجموعه‌ای از عناصر به هم وابسته[۱] است که وظیفه جمع‌آوری[۲]، پردازش[۳]، ذخیره[۴] و توزیع اطلاعات[۵] به‌منظور پشتیبانی و تصمیم سازی از کنترل در یک سازمان را بر عهده

۱. Cracker
۲. information
۳. data

دارد. افزون بر پشتیبانی از تصمیم‌سازی، هماهنگی و کنترل بخش‌های مختلف سازمان، یک سیستم اطلاعاتی می‌تواند به مدیران و کارکنان در تحلیل مشکلات، تجسم بهتر موضوعات پیچیده، همچنین تولید محصولات جدید کمک کند (شقیری، ۲۰۱۴، ۱۸).

سیستم‌های اطلاعاتی قابلیت ذخیره کردن اطلاعات مربوط به افراد، مکان‌ها و هر جزء قابل‌تصوری از داخل و خارج سازمان را دارند. یک سیستم اطلاعاتی از سه بخش تشکیل شده است که با همکاری هم اطلاعات لازم را برای سازمان تولید می‌کنند: ورودی[۶]، پردازش[۷] و خروجی[۸]. بخش ورودی، داده‌های خام را از محیط داخل و خارج گرفته و جمع‌آوری می‌کند. بخش پردازش، این داده‌های خام را از ورودی گرفته و به شکل معناداری به تولید اطلاعات می‌پردازد. بخش خروجی، اطلاعات پردازش‌شده را به افرادی که به آن نیاز دارند یا فعالیت‌هایی که قرار است از آن اطلاعات استفاده کنند، منتقل می‌کند. چنانچه سیستم اطلاعاتی نیازمند به بخش دیگری به نام بازخورد[۹] است که اطلاعاتی را جهت ارزیابی و اصلاح بخش ورودی سیستم تولید می‌کند (شقیری، ۲۰۱۴، ۱۸).

۳- گونه‌های هک

هک به اعتبارات مختلف، دارای تقسیم‌بندی‌های متفاوتی است. یکی از این اعتبارات که مرتبط با تحلیل فقهی آن است بر مبنای روش هک است که می‌توان آن را در موارد زیر خلاصه کرد:

۱. interrelated
۲. collect, retrieve
۳. process
۴. store
۵. distribute
۶. input
۷. processing
۸. output
۹. feedback

۳-۱- انواع حملات مختل‌کننده سیستم‌های رایانه‌ای[۱]؛

هدف در این نوع حملات، ایجاد اختلال در سیستم‌های رایانه‌ای و از کار انداختن آن‌هاست که از راه‌های مختلفی صورت می‌پذیرد و با استفاده از این تکنیک، مهاجم از دسترسی کاربران مجاز به یک سیستم یا امکان سرویس گیری کاربران راه دور از یک شبکه جلوگیری می‌کند (ماندنی خالدی، ۱۳۸۶، ۲۴۷).

۳-۲- جعل[۲]

این روش که فریبکاری اینترنتی نیز نامیده می‌شود، به این معناست که مهاجم با جعل عنوان یا تغییر هویت، قصد کلاه‌برداری، فریبکاری یا حتی تمسخر کاربر را داشته باشد (السان، ۱۳۹۶، ۲۰۲-۲۰۳).

۳-۳- استراق سمع[۳]

این روش، ابزاری برای شنود ترافیک عبوری شبکه و اطلاعات هنگام تبادل آن‌ها صورت می‌گیرد که هم کاربرد مدیریتی و هم خرابکارانه می‌تواند داشته باشد (ملکیان، ۱۳۸۵، ۳۳۱).

۳-۴- مهندسی اجتماعی[۴]

این روش، تکنیکی است که الزاماً نیاز به رایانه ندارد و بدون آن نیز صورت می‌پذیرد. این روش نوعی ورود غیر تکنیکی به سیستم است که با استفاده از اطلاعات جمع‌آوری‌شده در سازمان صورت می‌گیرد و به مهارت‌های رفتاری، زیرکی و ذکاوت هکر بستگی دارد و به صورت‌های مختلفی انجام می‌شود با این نکته مشترک که هکر از هک شونده درخواست می‌کند که اطلاعات خود را در جایی دیگر وارد کند؛ سپس هکر از آن اطلاعات به نفع خواسته خود بهره می‌گیرد (کوین، ۱۳۹۷، ۸۹؛

---

۱. Denial of Service (DOS) & Distributed DOS

۲. Spoofing

۳. Sniffing

۴. Social Engineering

قهرمانی، کاهانی، ۱۳۸۸، ۲۳۹).

۵-۳- کلاه‌برداری

هکر در این روش ابتدا به جلب اعتماد کاربر پرداخته و سپس به تهاجم علیه او می‌پردازد و با ارسال نامه‌های الکترونیکی وسوسه‌انگیز به جمع‌آوری اطلاعات موردنظر خود از کاربر اقدام می‌کند (گودرزی اصفهانی، ۱۳۹۲، ۲۲).

۶-۳- استفاده از نرم‌افزارهای آلوده (بدافزارها[۱])

در این روش، هکر با استفاده از نرم‌افزارهای آلوده‌کننده به‌صورت زیرکانه و با ارسال کدهای اجرایی خطرناک با کمترین زحمت به عمل هک می‌پردازد (ماندنی خالدی، ۱۳۸۶، ۲۶۳).

۴- گونه پذیری هکرها

هکرها به اعتبارهای مختلف، گونه‌های متفاوتی دارند. یکی از پرکاربردترین این گونه‌بندی‌ها، تقسیم هکرها بر اساس رنگ کلاه است؛ چراکه برای آن‌ها بسته به هدف و پیامد فعالیتشان کلاه‌های سفید، سیاه، خاکستری، آبی، قرمز، زرد، صورتی، سبز و بنفش در نظر گرفته می‌شود که رایج‌ترین آن‌ها در ادبیات جهانی هک، هکرهای کلاه‌سفید، کلاه‌سیاه و کلاه‌خاکستری هستند.

۱-۴- هکرهای کلاه‌سفید[۲] (نفوذگران خوب):

این گروه افراد نخبه‌ای هستند که فعالیتشان زیان‌بار نبوده، موجب سازندگی و پویایی سیستم‌های اطلاعاتی می‌شوند. نفوذگرهای خوب بدون داشتن انگیزه بد، می‌کوشند با شکستن حریم امنیتی سیستم‌ها، معایب آن‌ها را در رویارویی با نفوذگران بیمار یا مغرض نمایان کنند (تست نفوذ). هکرهای کلاه‌سفید پایبند به رعایت اصول «هک اخلاقی» هستند و به‌طورمعمول از سطح علمی بالا و تجربه زیادی برخوردارند. «نفوذگران اصول‌گرا»، عنوانی است که به‌واسطه داشتن مرام‌نامه

---

۱. Malware

۲. White Hat Hacker Group

اخلاقی، به آن‌ها داده می‌شود. آسیب نرسانی به سیستم، عدم نفوذ به شبکه‌های دولتی یا امنیتی که مشغول انجام وظیفه ملی هستند، عدم دستبرد به فایل‌های سیستم و انتقال آن‌ها، عدم گذاشتن ردپا و اثر در سیستم مورد نفوذ، ندادن اطلاعات و آگاهی به افراد دیگر نسبت به دانش و مهارت‌های نفوذگری خود (جز به افراد متخصص و مورداطمینان برای بالا بردن مهارت‌های تخصصی و تبادل افکار)، عدم مبادله اطلاعات بر روی شبکه اینترنت در مورد جزئیات نفوذگری خود، عدم نفوذ به یک سیستم برای بار دوم؛ داشتن خلاقیت و ارائه روشی نو (دست‌کم برای یک‌بار)، از اصول اخلاقی این مرامنامه است (سانچیت، ۲۰۱۹، ج ۱۰، مقاله ۵).

۲-۴- هکرهای کلاه‌سیاه[۱] (نفوذگران بداندیش و مخرب):

این افراد در برابر هکرهای کلاه‌سفید، تنها برای سود شخصی یا نیت‌های غیراخلاقی به سیستم‌های اطلاعاتی نفوذ می‌کنند؛ هرچند در بسیاری از موارد، اشتباه‌های کاربران موجب نفوذ این هکرها می‌شود. برای مثال، انتخاب سال تولد یا شماره تلفن به‌عنوان رمز ورود (پسورد)، عاملی برای نفوذ هکرهای کلاه‌سیاه به سیستم افراد است. این هکرها با استفاده از روش یا ساخت و ارسال یک بدافزار (ویروس) درصدد خراب کردن سیستم‌های رایانه‌ای و کشف اطلاعات کاربران آن‌ها هستند. دوران طلایی هکرهای کلاه‌سیاه، دهه هشتاد میلادی بود که سیستم‌های کامپیوتری تازه گسترش پیدا کرده بودند؛ اما امروزه کسی نمی‌تواند از این راه درآمد قابل قبولی به دست آورد و به دلیل پیشرفت سیستم‌های امنیتی، این افراد دستگیر و دچار مشکلات جدی اجتماعی می‌شوند (کوین، ۱۳۹۷، ۲۳- ۲۴). کاربران بداندیش گونه‌های مختلفی دارند؛ برخی به کار خود بسیار مسلط و چیره‌دست هستند؛ برخی نیز بدون تسلط و مهارت نسبت به حوزه فن‌آوری اطلاعات یک سازمان، اقدام به نفوذ می‌کنند (ملکیان، ۱۳۸۵، ۱۸).

۳-۴-هکرهای کلاه خاکستری[۲] (نفوذگران کمی خوب و کمی بد):

با توجه به ترکیب خاکستری از دو رنگ سیاه و سفید، هکر کلاه خاکستری هکری است که

۱. Black Hat Hacker Group

۲. Gray Hat Hacker Group

برخی ویژگی‌های دو هکر کلاه‌سفید و کلاه‌سیاه را در دارد. برخی هکرها با بررسی وضعیت امنیتی سایت‌ها و سرورها و با انگیزه یادگیری یا کنجکاوی، اقدام به هک کردن سامانه‌های اطلاعاتی می‌کنند از این هکرها با نام «واکر»[۱] یاد شده، بدون آسیب‌رسانی به سیستم‌های مقصد، اطلاعات آن‌ها را سرقت می‌کنند. هکرهای کلاه خاکستری از سطح پایین‌تری از دانش و اطلاعات نسبت به هکرهای کلاه‌سفید برخوردارند و بدون اجازه وارد سیستم دیگران می‌شوند؛ همچنان که آسیب‌رسانی کمتری نسبت به هکرهای کلاه‌سیاه‌ها به سیستم وارد می‌کنند (کوین، ۱۳۹۷، ۴۵؛ گراوز، ۲۰۱۰، ۴).

۵- وضعیت فقهی هکر

به‌منظور تحلیل وضعیت فقهی هک کردن سامانه‌های اطلاعاتی، ضروری است ادله مشروعیت و عدم مشروعیت آن ازنظر امامیه و اهل سنت بررسی شود؛ اما ازآنجاکه نتیجه این بررسی بسته به نوع هکرها متفاوت خواهد بود، تحلیل فقهی خود را در دو سطح عملکرد هکرها کلاه‌سفید و هکرهای کلاه‌سیاه تبیین می‌کنیم. هکرهای کلاه خاکستری به‌واسطه برخورداری از وضعیت دوگانه، هم می‌توانند مشمول ادله مشروعیت عملکرد هکرهای کلاه‌سفید شوند و هم مشمول ادله عدم مشروعیت عملکرد هکرهای کلاه‌سیاه؛ ازاین‌رو آن‌ها را به‌صورت مستقل بررسی نمی‌کنیم.

۵-۱-مشروعیت عملکرد هکرهای کلاه‌سفید

یکی از مهم‌ترین دلایل اثبات کننده مشروعیت عملکرد هکرهای کلاه سفید، استناد به مقاصد شریعت است. مقاصد شریعت عنوانی است که ازنظر غزالی شامل پنج عنوان: دین، نفس، عقل، نسل و مال می‌شود (غزالی، ۱۴۱۳، ج ۱، ۲۸۶). به نظر ابن عاشور، این مقاصد هم شامل مقاصد کلی شریعت و هم شامل مقاصد خاصی که قانون‌گذار برای حفظ مصلحت افراد در نظر گرفته، می‌شود (ابن عاشور، ۱۳۶۶، ۵۰). به‌عبارت‌دیگر، مقاصد عمومی شریعت، معانی یا حکمت‌هایی هستند که شارع مقدس در همه یا بیشتر قانون‌گذاری‌های خود آن‌ها را موردنظر قرار داده و به نوع خاصی از احکام وابسته نیستند (ابن عاشور، ۱۳۶۶، ۵۱؛ حسنی، ۱۴۱۶، ۱۱۳– ۱۱۴). در امامیه هم تعریف‌هایی از مقاصد شریعت ارائه شده، ازجمله: «علم مقاصد شریعت، علمی است که در پیوند با تشریع قرار

[۱]. whacker

دارد و از اهداف کلی یا اهداف موردتوجه آن در عموم یا انواع بسیاری از این احکام سخن می‌گوید» (تسخیری، ۱۳۸۸، ۱۱). بر این اساس، چون مقاصد شریعت برای حفظ مصلحت عموم مردم وضع شده‌اند، حفظ مصلحت از مقاصد کلی شریعت به‌حساب آمده، احکام اسلامی تابع مصالح و مفاسد هستند (شوشتری و دیگران، ۱۳۹۵، ۹۱– ۹۳). بدون شک، هرگاه هک کردن سامانه‌های اطلاعاتی تنها راه پیشگیری از آسیب جامعه و روش عقلایی برای خنثی کردن توطئه دشمنان یا جلوگیری از گسترش یک امر غیراخلاقی (منکر) باشد، این عمل ازنظر فقهی مشروع خواهد بود (مجمع فتاوای دوحه، فتوای شماره ۱۶۰۹۷۱، مورخ ۲۰۱۱/۰۷/۱۸ م و فتوای شماره ۱۱۴۰۹۷، مورخ ۲۰۰۸/۱۰/۳۰ م؛ فتوای هفت تن از علمای شیعه در مورد فضای مجازی، کد ۱۱۹۲۹۱، مورخ ۱۳۹۵/۰۳/۰۹).

افزون بر این، به برخی از قواعد فقهی نیز می‌توان برای اثبات مشروعیت عملکرد هکرهای کلاه سفید استناد کرد؛ قواعدی که تعدادی از آن‌ها قابلیت استناد در همه مذاهب اسلامی را دارند، تعدادی نیز تنها اختصاص به برخی از مذاهب دارند.

۱-۵-۱-قاعده «الوسائل لها حکم المقاصد»

بر اساس این قاعده، اگر مقصد، حرام باشد، وسیله‌ای که برای رسیدن به آن هدف استفاده می‌شود نیز حرام خواهد بود و بالعکس، اگر هدف نیکو باشد، وسیله رسیدن به آن مشروع است؛ درنتیجه، نمی‌توان برای رسیدن به هدف مشروع از وسیله حرام استفاده کرد (تویجری، ۱۴۳۰، ج ۲، ۲۸۹). روشن است که وسیله می‌تواند قول، فعل یا ترک فعل باشد؛ همچنان که می‌تواند محسوس یا نامحسوس (معنوی) باشد. مقصد هم می‌تواند عبادت یا معامله باشد. ازاین‌رو، برخی از فقها این قاعده را فرع قاعده «الأمور بمقاصدها» و برخی آن را فرع قاعده «إنما الأعمال بالنیات» می‌دانند (الزحیلی، ۱۴۲۷، ج ۱، ۶۳– ۶۴). بر این اساس، هرگاه هک برای مقاصد صحیح و واجبی همچون دفاع سایبری، ممانعت از عمل سایت‌های پورنو، یافتن اشکالات سیستم‌ها و ... به کار گرفته شود، نه‌تنها مشروع، بلکه در برخی از موارد چون مقدمه برای عمل واجب است، واجب خواهد بود (سند، ۲۰۱۰، ۱۰– ۱۲).

۱-۵-۲-قاعده وجوب حفظ نظام

حفظ نظام از اموری است که از دیرباز موردتوجه فقها بوده (وحدتی شبیری، ۱۳۸۰، ۳۳– ۳۵)، برخی از فقها آن را از مصادیق مستقلات عقلیه به شمار آورده‌اند (موسوی گلپایگانی، ۱۴۱۲، ج ۲، ۱۵۴). این قاعده ناظر به حفظ نظام نوع مردم و حیات اجتماعی است و خرده نظام‌هایی همچون مدرسه، شرکت‌های کوچک و خصوصی که اختلال در آن‌ها موجب اخلال در نظام اجتماعی نمی‌شود را در بر نمی‌گیرد (سیفی مازندرانی، ۱۴۲۵، ج ۱، ۲۱). ازاین‌رو، درصورتی‌که تزاحمی میان مصلحت عمومی جامعه و احکام فرعی واقع شود، مصلحت جامعه با توجه به میزان اهمیت آن مقدم خواهد شد؛ مانند جواز شنود (استراق سمع) از طریق هک کردن سامانه اطلاعاتی اشخاص برای رسیدن به مصلحت مهم‌تر با وجود حرمت ذاتی آن (مصباح، ۱۳۶۹، ۷۹؛ ابن فرحون، ۱۴۰۶، ج ۲، ۱۸۷).

۱-۵-۳-قاعده لاضرر

یکی از مهم‌ترین قواعد فقهی، قاعده «لاضرر» است که بنا به نظر مشهور، مفاد آن نفی حکم ضرری (تکلیفی و وضعی) است (مشکینی، ۱۳۷۱، ج ۱، ۲۰۳). ازنظر شیخ انصاری و محقق خراسانی قاعده لاضرر بر ادله همه احکام ضرری حاکم بوده، هیچ حکم ضرری در اسلام وجود ندارد (انصاری، ۱۴۱۹، ج ۲، ۴۶۰؛ خراسانی، ج ۱، ۳۸۱)؛ اما امام خمینی بر این باور است که این قاعده تنها بر قاعده تسلیط حکومت دارد (خمینی، ۱۴۱۰، ج ۱، ۶۰). به نظر برخی از فقها اگر تصرف مالک از روی احتیاج یا به‌منظور انتفاع نبوده، بلکه تصرفاتی عبث و بیهوده باشد، قاعده لا ضرر بر قاعده تسلیط حکومت دارد، چه مالک در تصرفات خود، قصد اضرار به دیگری داشته باشد یا نداشته باشد؛ در غیر این صورت، قاعده تسلیط بر قاعده لاضرر حکومت خواهد داشت (علامه حلی، ۱۴۲۰، ج ۱۰، ۳۸۶؛ شهید اول، بی‌تا، ج ۳، ۳۳۹– ۳۴۰).

بر این اساس، از آن‌جا که داده‌های رایانه‌ای قابل تقویم بوده و در نظر عرف «مال» به‌حساب می‌آید (عبدی پور فرد و وصالی ناصح، ۱۳۹۶؛ بهمن پوری و دیگران، ۱۳۹۳، ۲۴۲)، اصل بر لزوم احترام به مالکیت صاحبان داده‌های رایانه‌ای و حرمت تصرف در آن‌ها بدون اجازه ایشان است. نتیجه چنین رویکردی، حرمت هک کردن سامانه‌های اطلاعاتی است، مگر بپذیریم حکم به جواز تصرف مالکان داده‌های رایانه‌ای، موجب آسیب رساندن به افراد یا منافع عمومی شود که در این صورت،

هک کردن سامانه‌های اطلاعاتی به‌واسطه تقدم قاعده لاضرر بر قاعده تسلیط، امری مشروع خواهد بود (ابن قدامهٔ، ج ۵، ۵۲؛ اصفهانی، ۱۴۱۹، ج ۱، ۴۴۱- ۴۴۲)؛ به‌ویژه اگر ضرر فاحشی را به دنبال داشته باشد (محقق سبزواری، ۱۳۸۱، ج ۲، ۵۵۶). البته مشروعیت هک کردن، منافاتی با مسئولیت مدنی هکرها نسبت به ضرر و زیان وارد بر صاحبان داده‌های رایانه‌ای ندارد؛ زیرا برای محترم بودن یک سامانه اطلاعاتی، وجود دو عنصر ضروری است: داشتن منفعت حلال و محترم بودن مالک آن. ازاین‌رو، اگر یک سامانه اطلاعاتی دارای منافع حرام باشد، مانند سایت‌های پورنو، قمار و مانند آن، داده‌های آن مالیت شرعی چون فاقد منفعت حلال هستند (ابن نجیم، ۱۴۱۸، ج ۵، ۲۷۷؛ ابن عابدین، ۱۴۱۲، ج ۴، ۵۰۱؛ سرخسی، ۱۴۱۴، ج ۱۱، ۷۹). همچنین اگر مالک سامانه اطلاعاتی محترم (مسلمان، اهل کتاب، معاهد، مستأمن) نباشد (شبل، ۱۴۳۳، ۸۸)، تصرف در آن حرام نبوده، اتلافش جایز (لجنهٔ الفتوی فی الأزهر، کد ۶۷۶۴، ۱۴۲۲/۰۲/۰۶) و گاه واجب خواهد بود (اللبان و حمال الدین، ۲۰۱۰، ۴۷). درنتیجه، هکر مسئولیتی نسبت به از بین بردن اطلاعات آن‌ها نخواهد داشت (شبل، ۱۴۳۳، ۳۵۵- ۳۵۶).

۱-۵-۴-قاعده وجوب دفع ضرر محتمل

دو خوانش متفاوت برای قاعده وجوب دفع ضرر محتمل وجود دارد: الف) این قاعده بیانگر حکم عقل به لزوم پیشگیری از ضرری است که احتمال تحقق آن وجود دارد (المروج الجزائری، ۱۴۱۵، ج ۸، ۴۰۰)، چه این ضرر اندک باشد یا زیاد (نراقی، ۱۴۰۸، ج ۱، ۱۴۷)؛ چراکه انجام فعل همراه با احتمال ضرر، قبیح و از مصادیق ظلم است (خمینی، ۱۳۸۵، ۱۴۴). ب) قاعده‌ای عقلایی است که بر اساس آن، نسبت میان ضررها سنجیده شده، ممکن است به خاطر یک مصلحت بزرگ‌تر، فرد خود را در موقعیت ضرر قرار دهد؛ ضرری که عرف آن را تحمل نمی‌کند (خمینی، ۱۳۸۵، ۱۴۳)؛ چه این ضرر دنیوی یا اخروی باشد (بجنوردی، ۱۳۷۷، ج ۷، ۳۳۴).

قاعده وجوب دفع ضرر محتمل در اصول فقه اهل سنت نیز موردتوجه قرار گرفته است (فخر رازی، ۱۴۲۰، ج ۱، ۱۷۱؛ طوفی، ۱۴۰۷، ج ۲، ۱۱۳) و قواعد مشابهی همچون «درء المفاسد أولی من جلب المفاسد» (زحیلی، ۱۴۲۷، ج ۱، ۲۳۸)، «الدفع، أقوی من الرفع»، «الدفع أسهل من الرفع» و

«الدافع أقوی من الرافع» (جزائری، ۱۴۲۱، ۴۶۶) نیز ناظر به همین مطلب هستند.

بر این اساس، اگر برای جلوگیری از فعالیت سامانه‌های اطلاعاتی غیراخلاقی یا مخل به امنیت کشور راهی به‌جز هک کردن آن‌ها وجود نداشته باشد، این عمل به‌حکم وجوب دفع ضرر محتمل، جایز و چه‌بسا واجب خواهد بود (مجمع فتاوای دوحه، فتوای شماره ۱۱۴۰۹۷، مورخ ۲۰۰۸/۱۰/۳۰ م)؛ زیرا در تزاحم میان حقوق مالکان سامانه‌های اطلاعاتی موردنظر و حفظ امنیت اخلاقی، روانی، اقتصادی و فرهنگی جامعه، اصل بر تقدیم اهم نسبت به مهم است. از این رو در این موارد، قاعده وجوب دفع ضرر محتمل بر قاعده لاضرر نسبت به تصرف در داده های رایانه ای فردی که اقدام به انتشار مطالب غیر اخلاقی نموده است، مقدم می شود (زحیلی، ۱۴۲۷، ج ۱، ۲۲۶).

۱-۵-۵-وجوب نهی از منکر

برخی از فقها با استناد به اطلاق آیه ۱۰۴ آل‌عمران و برخی از روایات ناظر به آن (حر عاملی، ۱۳۷۶، ج ۱۱، ۴۰۷)، نهی از منکر را با استفاده از هر روشی جایز می‌دانند (فاضل مقداد، ۱۴۰۴، ج۱، ۵۹۴-۵۹۵). از آنجا که راه‌اندازی عالمانه و عامدانه سامانه‌های غیراخلاقی (مروج فساد) و به‌روز رسانی اطلاعات آن‌ها یکی از مصادیق ترویج منکر (فحشاء) به‌حساب آمده و یکی از راه‌های مؤثر برای جلوگیری از فعالیت آن‌ها، هک کردن و از دسترس خارج کردن اطلاعات این سامانه‌ها است؛ برخی از فقهای اهل سنت (همچون ابوزید مقرئ إدریسی و عبد الباری الزمزمی) نه‌تنها هک کردن سایت‌های مروج فساد را از باب نهی از منکر واجب می‌دانند؛ بلکه از بین بردن سایت‌های مروج فساد و شبه را از مصادیق جهاد در راه خدا دانسته‌اند (شبل، ۱۴۳۴، ۳۵۵). همچنانکه برخی از فقهای امامیه (همچون آیت الله مکارم شیرازی) نیز در مواردی که فضای مجازی، منشأ فساد در جامعه باشد و مسئولین از باب نهی از منکر، هک کردن آن را به مصلحت جامعه بدانند، هک کردن سامانه‌های اطلاعاتی مورد نظر را جایز شمرده‌اند (فتوای هفت تن از علمای شیعه در مورد فضای مجازی، کد ۱۲۴۵۶۱، مورخ ۱۳۹۵/۰۵/۳۱).

۲-۵-عدم مشروعیت عملکرد هکرهای کلاه‌سیاه

برخی از مهم‌ترین دلایل حرمت هک کردن سامانه‌های اطلاعاتی توسط هکرهای کلاه‌سیاه

عبارت‌اند از:

۲-۵-۱-حرمت تصرف در اموال دیگران

منظور از «تصرف» در اصطلاح فقهی عبارت است از: «اقدامی ارادی منتسب به شخص، در مالی (عین و غیر عین) که دارای اثر شرعی است؛ خواه این اثر به سود تصرّف‌کننده باشد یا به زیان او» (عبدالمنعم، ۱۴۱۹، ج ۱، ۴۵۶؛ زحیلی، ۱۴۰۹، ج ۴، ۲۹۲۱ و ج ۶، ۴۴۶۸). صرف‌نظر از اینکه مستند این قاعده، آیه «لاَ تَأْكُلُواْ أَمْوَالَكُمْ بَيْنَكُمْ بِالْبَاطِلِ إِلاَّ أَن تَكُونَ تِجَارَةً عَن تَرَاضٍ» (نساء، ۴/ ۲۹) باشد یا روایات ناظر به احترام اموال دیگران (کلینی، ۱۳۶۵، ج ۲، ۳۶۰)؛ مادام که تصرف در اموال دیگران جبران نشود، متصرف همچنان در حال ارتکاب است و به همین خاطر، تصرف در مال دیگری از گونه جرائم مستمر به‌حساب می‌آید که افزون بر حکم تکلیفی، متضمن حکم وضعی (ضمان) نیز خواهد بود (محقق داماد، ۱۴۰۶، ۲۱۵؛ اصفهانی، ۱۴۱۹، ج ۱، ۳۱۹).

بر این اساس، چون داده‌های اطلاعاتی در نظر عرف مال به‌حساب می‌آیند، هرگاه هک کردن سامانه اطلاعاتی افراد منجر به استفاده از اطلاعات اشخاص بدون اجازه و رضایت آن‌ها باشد، مشمول حکم تصرف در مال غیر خواهد شد. به همین دلیل، اگر سامانه‌های اطلاعاتی دارای منافع مباحی همچون منافع آموزشی، دینی، پزشکی و ... باشند، ازنظر شارع مالیت داشته و تعدی بر آن‌ها حرام است (شبل، ۱۴۳۴، ۳۵۱).

۲-۵-۲-حرمت نقض حریم خصوصی دیگران

احترام به حریم خصوصی از حقوق بنیادین بشر است که قرآن ما را از تعدی به آن نهی کرده است (نور،۲۴/ ۲۷- ۲۸ و ۳۰- ۳۱)؛ حقی که برآمده از اصل کرامت ذاتی انسان است (إسراء،۷۰/۱۷). ازنظر برخی فقها، هرگاه ناقض حریم خصوصی دیگران از عمل خود دست برندارد، تنبیه و حتی کشتن او نیز جایز خواهد بود (خمینی، ۱۳۹۰، ج ۱، ۴۹۱). بدون شک، یکی از مصادیق نقض حریم خصوصی، نقض حریم خصوصی اطلاعات است (نقیبی، ۱۳۸۹، ۳؛ اصلانی، ۱۳۸۴، ۴۴). منظور از

«حریم خصوصی اطلاعاتی»،[۱] «حق اولیه افراد در محرمانه ماندن و جلوگیری از تحصیل پردازش و انتشار داده‌های شخصی مربوط به ایشان، مگر در موارد قانونی» است (منصور نژاد، ۱۳۸۶، ۱۴۰). بدین ترتیب، دسترسی به اطلاعات و داده‌های شخصی افراد از راه هک کردن سامانه‌های اطلاعاتی، مصداق نقض حریم خصوصی آن‌هاست و چون هکرهای کلاه‌سیاه این عمل را با انگیزه‌های شرورانه انجام می‌دهند، عملی حرام است (فتاوای هفت تن از علمای شیعه در مورد فضای مجازی، کد ۱۲۴۵۶۱، مورخ ۱۳۹۵/۰۵/۳۱؛ الشیخ المنجد، فتوای شماره ۱۱۸۵۰۱، مورخ ۲۰۰۹/۱۱/۲۴).

۲-۵-۳-حرمت تجسس

یکی از دلایل حرمت تجسس، آیه «ولا تجسَّسوا» (حجرات،۱۲/۴۹) است. مفسران در تعریف تجسس نوشته‌اند: «کاوش در امور پنهانی دیگران و چیزی که دیگران مایل به آشکارسازی آن نیستند» (طبرسی، ۱۴۱۵، ج ۹، ۲۲۸؛ آلوسی، ۱۴۱۶، ج ۱۳، ۳۰۸). نبود قید و شرط در این آیه، نشان از عمومیت و حرمت تجسس در همه امور داشته، جواز آن وابسته به وجود دلیل خاص است (مکارم شیرازی، ۱۴۲۶، ج ۲۲، ۱۸۸-۱۸۷؛ ابن فرحون، ۱۴۰۶، ج ۲، ۱۸۷). هرچند قرائن موجود در آیه، همچون شأن نزول آن، نشان از اختصاص حریم خصوصی به جنبه‌های شخصی زندگی افراد دارد، ولی در زندگی اجتماعی نیز این حکم صادق است (مکارم شیرازی، ۱۴۲۶، ج ۲۲، ۱۸۷). همچنین دلالت برخی از روایات به حرمت تجسس در امور مسلمانان (کلینی، ۱۳۶۵، ج ۸، ۱۵۰ و ج ۱، ۳۲۴)؛ اثبات‌کننده جواز تجسس در امور غیرمسلمانان نبوده، وصف یا لقب «مسلمان» و مانند آن، فاقد مفهوم است (بای و پورقهرمانی، ۱۳۸۸، ۲۰۷).

بر این اساس، ازآنجاکه هک کردن سامانه‌های اطلاعاتی افراد و دسترسی به محتوای آن‌ها، تجسس در امور آن افراد به‌حساب آمده و تجسس نیز صرف‌نظر از اینکه نسبت به چه چیزی و در مورد چه فردی است، حرام است؛ عمل هکرهای کلاه‌سیاه حرام خواهد بود (شبل، ۱۴۳۳، ۴۰۱؛ روحانی، ۱۳۸۷، ۱۸۸). این حرمت، وابسته به محتوای سامانه‌های اطلاعاتی و تعلق آن به افراد یا گروه‌های خاصی نیست؛ مگر این‌که مجوزی شرعی برای انجام چنین عملی وجود داشته باشد که در

[۱]. Information Privacy

این صورت، از حوزه عملکردی هکرهای کلاه‌سیاه خارج و در زمره عمل هکرهای کلاه‌سفید قرار خواهد گرفت (دغمی، ۱۴۰۶، ۳۱؛ شبل، ۱۴۳۳، ۴۰۴-۴۰۷).

۲-۵-۴-حرمت هتک حیثیت

منظور از «هتکِ حیثیث»، از بین بردن آبرو و اعتبار افراد است (ابن منظور، ۱۴۱۴، ج ۱۰، ۵۰۲). حرمت هتک حیثیت، افزون بر آنکه مستند به آموزه‌های قرآنی (نساء، ۴/ ۱۴۸؛ توبه، ۹/ ۷۹؛ نور، ۲۴/ ۴) و حدیثی است (طوسی، ۱۳۶۴، ج ۱، ۳۷۵)، ازنظر مذاهب اسلامی امری ضروری بوده (قرافی، ۱۴۱۶، ج ۷، ۳۲۶۱)، حفظ آبرو و شرافت انسان‌ها یکی از مقاصد شریعت به‌حساب می‌آید (زحیلی، ۱۴۲۷، ج ۱، ۱۹۳). قانون‌گذار نیز در ماده ۱۷ قانون جرائم رایانه‌ای (ماده ۷۴۵ قانون مجازات اسلامی) دراین‌باره مقرر کرده است: «هر کس به‌وسیله سامانه‌های رایانه‌ای یا مخابراتی صوت یا تصویر یا فیلم خصوصی یا خانوادگی یا اسرار دیگری را بدون رضایت او جز در موارد قانونی منتشر کند یا در دسترس دیگران قرار دهد، به‌نحوی‌که منجر به ضرر یا عرفاً موجب هتک حیثیت او شود، به حبس از نودویک روز تا دو سال یا جزای نقدی از پنج میلیون (۵,۰۰۰,۰۰۰) ریال تا چهل میلیون (۴۰,۰۰۰,۰۰۰) ریال یا هر دو مجازات محکوم خواهد شد».

بدون تردید، هک کردن سامانه‌های اطلاعاتی توسط هکرهای کلاه‌سیاه و سرقت فیلم یا عکس‌های خصوصی افراد و در وضعیت‌های ناخواسته، می‌تواند تهدیدی برای آبروی کاربران به‌حساب آید. این عمل در برخی موارد، منجر به اشاعه فساد می‌شود که فقهای مسلمان بر حرمت آن تأکید دارند (ر.ک: خوئی، ۱۳۷۴، ج ۱، ۴۵۷؛ نجفی، ۱۳۶۲، ج ۳۱، ۳۷۴). همچنانکه رمزگشایی سامانه‌ها و ورود غیر مجاز به فضای آن‌ها نیز می‌تواند منجر به فساد و کشف اسرار سیاسی و امنیتی کشور شده، پیامدهای نامطلوب زیادی به دنبال داشته باشد (ایزدی فرد، حسین نژاد، ۱۳۹۵، ۴۳).

۲-۵-۵-حرمت آزار و اذیت دیگران

قرآن کریم آزردن افراد بی‌گناه را گناهی بزرگ دانسته (احزاب/ ۳۳: ۵۸)، در متون روایی نیز بر حرمت آن تأکید شده است (شیخ مفید، ۱۴۱۴، ج ۱، ۲۲۷). فقهای مسلمان در تعریف آزار، نظرهای

مختلفی بیان کرده‌اند. دو واژه «ایذاء» و «أذی» در متون فقهی به «شر اندک» معنا شده است و در تفاوت میان آزار و ضرر آمده است: زیان اندک، ایذاء و زیان بزرگ، ضرر است (مقدس اردبیلی، ۱۴۰۳، ج ۱۲، ۳۳۹؛ نجفی، ۱۳۶۲، ج ۲۲، ۷۴)؛ ضرر موجب ضمان بوده؛ ولی ایذاء ضمان‌آور نیست (مؤسسهٔ دائرهٔ المعارف الفقه الإسلامی، ۱۴۲۳، ج ۱۹، ۲۸۴). ایذاء حرمت مطلق نداشته، اگر کسی بدون داشتن قصد، زمینه آزار و اذیت دیگری را فراهم کند، کار او حرام نخواهد بود (خوئی، ۱۳۷۷، ج ۱، ۳۴۲؛ طباطبائی قمی، ۱۴۱۳، ج ۴، ۱۱۲)؛ همچنان که وجوب امربه‌معروف و نهی از منکر اطلاق دارد، هرچند دستکم منجر به آزار روانی طرف مقابل شود (اراکی، ۱۴۱۳، ۲۴۵).

به‌هرحال، اگر بپذیریم افراد از آشکار شدن اطلاعات خود ناخرسند بوده و این امر سبب رنجش روانی آن‌ها می‌شود، می‌توان ادعا کرد که عمل هکرهای کلاه‌سیاه، حرام است؛ زیرا عملکرد هکرهای کلاه‌سیاه وابسته به سوءنیت آن‌هاست (کوین، ۱۳۹۷، ۲۳– ۲۴) و آن‌ها از روی قصد، داده‌ها و اطلاعات دیگران ا تخریب می‌کنند (بای و پورقهرمانی، ۱۳۸۸، ۱۴۱– ۱۴۲).

۲-۵-۶-حرمت تجاوز به حقوق دیگران

ظلم در لغت به معنای تجاوز از حد و قرار دادن شیء در غیر محل خود است (عبد المنعم، ۱۴۱۹، ج ۲، ۴۵۰؛ قلعجی و قنیبی، ۱۴۰۸، ج ۱، ۲۹۶). قبح ظلم از اموری است که عقل در درک آن استقلال داشته (مظفر، ۱۳۹۰، ۲۳۲)، آیات قرآنی (آل‌عمران ۳/ ۵۷؛ نساء ۴/ ۱۰؛ انعام، ۶/ ۲۰؛ اعراف ۷/ ۴۴) و احادیث معصومین (حر عاملی، ۱۳۷۶، ج ۸، ۵۴۸) بر حرمت آن تأکید دارد (موسوی قزوینی، ۱۴۲۴، ج ۵، ۴۲۳؛ تویجری، ۱۴۳۱، ج ۱، ۷۷۲).

ازآنجاکه از بین بردن داده‌ها، تخریب سیستم‌ها و مختل کردن عملکرد عادی آن‌ها توسط هکرهای کلاه‌سیاه با انگیزه سرگرمی، خودنمایی، باج‌گیری و مانند آن، همگی از مصادیق تجاوز به حقوق دیگران است و تجاوز به حقوق دیگران نیز حرام است، هک کردن سامانه‌های اطلاعاتی عملی حرامی خواهد بود (طارمی، ۱۳۸۷، ج ۲۳۳، ۵).

۲-۵-۷-حرمت أکل مال به باطل

هک کردن سامانه‌های اطلاعاتی و دسترسی به حساب‌های بانکی کاربران و برداشت و انتقال وجه از آن‌ها، فروش اطلاعات و داده‌های دیگران و هرگونه کسب درآمد از این راه، افزون بر اینکه در صورت وجود شرایط، عنوان سرقت بر آن بار می‌شود، مصداق کسب درآمد از راه نامشروع به شمار می‌رود (اکل مال به باطل) (بقره ۲/ ۱۸۸) ازنظر فقها عنوان «اکل مال به باطل» مفهومی گسترده داشته، شامل تصرفات مالی و غیرمالی حرام می‌شود (خمینی، ۱۴۱۰، ج ۱، ۶۴) و مرجع تشخیص آن نیز عرف است (انصاری، ۱۴۱۵، ج ۵، ۲۰).

افزون بر این، چنانچه در جواز هک سامانه‌های اطلاعاتی توسط هکرهای کلاه‌سیاه تردید داشته باشیم، اصل عملی احتیاط دلالت بر پرهیز از انجام چنین کاری داشته، نوبت به استناد به اصل برائت نمی‌رسد؛ زیرا به استناد نظریه حق الطاعه، در شک بین تکلیف الزامی (همچون حرمت هک کردن به دلیل تعدی به حقوق دیگران) و تکلیف غیر الزامی (جواز هک کردن با هدف سرگرمی و تفریح)، عقل حکم به احتیاط می‌کند (صدر، ۱۴۰۶، ج ۳، ۲۸)؛ همچنان که وجوب دفع ضرر محتمل (خوئی، ۱۳۶۸، ج ۲، ۱۸۶) نیز می‌تواند دلالت بر لزوم پرهیز از انجام هک توسط هکرهای کلاه‌سیاه کند. ازاین‌رو، هک کردن سامانه های اطلاعاتی توسط هکرهای کلاه سیاه و کلاه سفید، مستلزم تصرف در مال غیر و تعدی به حقوق افراد بوده، حکم اولی آن حرمت (عدم مشروعیت) است؛ ولی عملکرد هکرهای کلاه سفید به‌واسطه نیت خیرخواهانه و وجود مصلحت مهم‌تر، به عنوان حکم ثانوی جایز به‌حساب می‌آید؛ به ویژه هنگامی که هیچ راهی برای رسیدن به مصلحت مهم‌تر، به جز هک کردن سامانه‌های اطلاعاتی دیگران وجود نداشته باشد و به همین دلیل این ادله مشروعیت، بایستی تفسیر مضیق شوند به حالتی که مصلحت اهم وجود دارد.

عملکرد هکرهای کلاه خاکستری با توجه به نیت و انگیزه و نیز نوع عملکرد می تواند زیر مجموعه هکرهای کلاه سفید یا کلاه سیاه قرار گیرد و نمی توان حکم فقهی یکسانی برای این گروه از هکرها در نظر گرفت. چراکه این افراد به صورت دایمی قصد خرابکاری ندارند و تفاوت اصلی آنها با هکرهای کلاه سفید و کلاه سیاه، در روش کشف آسیب پذیری است. بنابراین هر دو حکم را می توان در مورد آنها داشت. از جهتی اگر مصلحت اهمی وجود داشته باشد، عملکرد آنها مشمول حکم جواز است و هرچند ورود بدون اذن به سیستم ها دارند، ولی به دلیل اشتغال به اهم، نمی توان

فعل آنها را مستحق مذمت یا عقاب دانست. از طرف دیگر در مواقعی که چنین مصلحتی وجود نداشته باشد، با توجه به حکم اولیه حرمت تصرف در مال غیر بدون اذن آنها، عمل آنها مشروع نیست. بنابراین ادله مشروعیت و عدم مشروعیت در مورد این هکرها نیز قابل صدق است و لزومی به ذکر دوباره آنها نیست.

۶- نتایج

پژوهش حاضر نشان می‌دهد:

۱-۶- هک کردن سامانه‌های اطلاعاتی ازجمله افعالی است که وضعیت حکم تکلیفی آن، وابسته به نیت هکر بوده، در شرایط مختلف، احکام متفاوتی دارد.

۲-۶-لزوم حفظ مقاصد شریعت، الوسائل لها حکم المقاصد، وجوب حفظ نظام، لاضرر، وجوب دفع ضرر محتمل و وجوب نهی از منکر می‌توانند ازجمله دلایلی باشند که مشروعیت عمل هکرهای کلاه‌سفید را اثبات می‌کنند.

۳-۶-عملکرد هکرهای کلاه‌سیاه، به دلیل تصرف در اموال دیگران، نقض حریم خصوصی افراد، تجسس، هتک حیثیت، ایذاء، تجاوز به حقوق افراد و اکل مال به باطل، مشمول حکم حرمت است.

۴-۶-فارغ از ادله اجتهادی، اصل حاکم به هنگام شک در جواز هک کردن سامانه‌های اطلاعاتی، احتیاط است.

۵-۶-درصورتی‌که رسیدن به مصلحت مهم‌تر وابسته به انجام هک نباشد، هک کردن سامانه‌های اطلاعاتی و دسترسی به اطلاعات دیگران بدون رضایت آن‌ها، عملی حرام است.

فهرست منابع

*قرآن کریم

۱. ابن عابدین، محمد أمین (۱۴۱۲). رد المحتار علی الدر المختار (چاپ دوم). بیروت: دار الفکر.

۲. ابن عاشور، محمد طاهر (۱۹۷۸). مقاصد الشریعه الاسلامیه. تونس: مصنع الکتاب.

۳. ابن فرحون الیعمری المالکی، إبراهیم شمس الدین محمد (۱۴۰۶). تبصرة الحکام فی أصول الأقضیة ومناهج الأحکام. قاهره: مکتبة الکلیات الأزهریة.

۴. ابن قدامة مقدسی، موفق الدین أبو محمد (۱۴۲۱). المقنع فی فقه الإمام أحمد. تحقیق محمود الأرناؤوط و یاسین محمود الخطیب. جدة: مکتبة السوادی.

۵. ابن منظور، محمد بن مکرم (۱۴۱۴). لسان العرب (چاپ سوم). بیروت: دار الفکر للطباعة والنشر والتوزیع.

۶. ابن نجیم مصری، زین‌الدین بن إبراهیم (۱۴۱۸). البحر الرائق شرح کنز الدقائق، وبالحاشیة منحة الخالق لابن عابدین. بیروت: دار الکتاب الإسلامی.

۷. اراکی، محمد علی (۱۴۱۳). المکاسب المحرمة. قم: مؤسسه در راه حق.

۸. اسکودیس اد (۱۳۸۸). آموزش گام به گام هک و ضد هک (چاپ ششم). ترجمه ابوالفضل طاریان ریزی و داوود تاتی بختیاری. تهران: سها دانش، تهران.

۹. اصفهانی، محمدحسین (۱۴۱۸ ـ ۱۴۱۹). حاشیه کتاب المکاسب. قم: چاپ عباس محمد آل سباع قطیفی.

۱۰. اصلانی، حمیدرضا (۱۳۸۴). حقوق فناوری اطلاعات. تهران: نشر میزان.

۱۱. السان، مصطفی (۱۳۹۶). حقوق فضای مجازی(چاپ هشتم). تهران: مؤسسه مطالعات و پژوهش های حقوقی.

۱۲. انصاری، مرتضی (۱۴۱۵). کتاب المکاسب. قم: مجمع الفکر الأسلامی.

۱۳. انصاری، مرتضی (۱۴۱۹). فرائد الأصول. تحقیق لجنة تحقیق تراث الشیخ الأعظم. قم: مجمع الفکر الإسلامی.

۱۴. آل‌بویه، علیرضا؛ آل‌بویه، زینب (۱۳۹۴). هک کردن و نفوذ به سیستم‌های رایانه‌ای از منظر اخلاقی. نقد و نظر، فصلنامه علمی- پژوهشی فلسفه و الاهیات، سال بیستم، شماره دوم.

۱۵. آلوسی، محمود (۱۴۱۶). روح المعانی و تفسیر القرآن العظیم والسبع المثانی. بیروت: دارالکتب العلمیة.

۱۶. ایزدی فرد، علی اکبر؛ حسین نژاد، مجتبی (۱۳۹۵). بررسی فقهی افساد فی الارض اینترنتی. فصلنامه پژوهش های فقه و حقوق اسلامی، سال دوازدهم، شماره چهل و چهار.

۱۷. بای، حسینعلی و پورقهرمانی، بابک (۱۳۸۸). بررسی فقهی حقوقی جرایم رایانه‌ای. قم: پژوهشگاه علوم و فرهنگ اسلامی معاونت پژوهشی دفتر تبلیغات اسلامی حوزه علمیه قم.

۱۸. برد بری، جنیفر (۲۰۱۱). Oxford basic American dictionary for learners English (چاپ اول). تهران: گویش نصف جهان.

۱۹. بهمن پوری، عبداله؛ شادمان‌فر، محمدرضا؛ پورغلامی فراشبندی، مجتبی (۱۳۹۳). بررسی فقهی حقوقی مال بودن داده‌های رایانه‌ای، فقه و مبانی حقوق اسلامی، سال چهل و هفتم، شماره دوم.

۲۰. تسخیری، محمدعلی (۱۳۸۸). فقه مقاصدی و حجیت آن، تهران: اندیشه تقریب، شماره ۱۸.

۲۱. تویجری، محمد بن إبراهیم (۱۴۳۱). مختصر فی الفقه الإسلامی فی ضوء القرآن و السنة (چاپ یازدهم). المملکة العربیة السعودیة: دار أصداء المجتمع.

۲۲. تویجری، محمد بن إبراهیم (۱۴۳۰). موسوعة الفقه الإسلامی. السعودیة و الأردن: بیت الأفکار الدولیة.

۲۳. جزائری، عبدالمجید جمعة (۱۴۲۱). القواعد الفقهیة المستخرجة من کتاب إعلام الموقعین ابن قیم الجوزیة. السعودیة و المصر: دار ابن قیم، دار ابن عفان.

۲۴. حر عاملی، محمد بن حسن (۱۳۷۶). وسائل الشیعة إلی تحصیل مسائل الشریعة. بیروت: دار إحیاء التراث العربی.

۲۵. حسنی، اسماعیل (۱۴۱۶). نظریة المقاصد عند الامام محمد الطاهر العاشور. قاهره: المعهد العالمی للفکر الاسلامی.

۲۶. حلی، حسن بن مطهر (۱۴۲۰). تذکرة الفقهاء. قم: مؤسسة آل البیت علیهم‌السلام لإحیاء التراث.

۲۷. خراسانی، محمدکاظم (۱۴۰۹). کفایة الأصول. قم: مؤسسة آل البیت علیهم‌السلام لإحیاء التراث.

۲۸. خمینی، سید روح‌الله (۱۳۹۰). تحریر الوسیلة (چاپ دوم). قم: دار الکتب العلمیة، مؤسسة مطبوعاتی

إسماعیلیان.

۲۹. خمینی، سید روح‌الله (۱۴۱۰). الرسائل. قم: اسماعیلیان.

۳۰. خمینی، سید روح‌الله (۱۴۱۰). کتاب البیع (چاپ چهارم). قم: مؤسسه مطبوعاتی اسماعیلیان.

۳۱. خمینی، سید مصطفی (۱۳۸۵). التحقیق فی قاعدهٔ لزوم دفع الضرر المحتمل.تهران: مؤسسه تنظیم و نشر آثار امام خمینی.

۳۲. خوئی، سید ابوالقاسم (۱۳۶۸). أجود التقریرات (چاپ دوم).قم: مؤسسه صاحب الأمر.

۳۳. خوئی، سید ابوالقاسم (۱۳۷۷). مصباح الفقاهۀ، بقلم محمد علی التوحیدی التبریزی. قم: داوری.

۳۴. خوئی، سید ابوالقاسم (۱۳۷۴). مستند عروۀ الوثقی، کتاب الإجارۀ. قم: مؤسّسه احیاء آثار الامام الخوئی.

۳۵. دغمی، محمد راکان (۱۴۰۶). التجسس و أحکامه فی الشریعۀ الإسلامیۀ (چاپ دوم). قاهره: دارالسلام.

۳۶. طارمی، محمدحسین (۱۳۸۷). طبقه‌بندی و آسیب‌شناسی جرایم رایانه‌ای، دفتر تبلیغات اسلامی حوزه علمیه قم، دوهفته‌نامه پگاه حوزه، قم: دفتر تبلیغات اسلامی حوزه علمیه قم.

۳۷. رازی، فخر الدین (۱۴۲۰). مفاتیح الغیب (التفسیر الکبیر) (چاپ سوم). بیروت: دار إحیاء التراث العربی.

۳۸. روحانی، سید محمدصادق (۱۳۸۷). استفتائات قضائیه و مؤسسه حقوقی وکلای بین‌الملل. تهران: نشر سپهر.

۳۹. زحیلی، محمد مصطفی (۱۴۲۷). القواعد الفقهیۀ وتطبیقاتها فی المذاهب الأربعۀ. دمشق: دار الفکر.

۴۰. زحیلی، وهْبَۀ بن مصطفی (۱۴۰۹). الفقه الاسلامی و ادلّته (چاپ چهارم). دمشق: دار الفکر.

۴۱. سرخسی، محمد بن أحمد (۱۴۱۴). المبسوط. بیروت: دار المعرفۀ.

۴۲. سند، عبدالرحمن (۲۰۱۰). وسائل الإرهاب الإلکترونی حکمها فی الإسلام وطرق مکافحتها. السعودیۀ: الکتاب منشور علی موقع وزارۀ الأوقاف السعودیۀ.

۴۳. سیفی مازندرانی، علی‌اکبر (۱۴۲۵). مبانی الفقه الفعال فی القواعد الفقهیۀ الأساسیۀ. قم: مؤسسۀ النشر الاسلامی التابعۀ بجامعۀ المدرسین.

۴۴. شبل، عبدالعزیز بن إبراهیم (۱۴۳۳). الاعتداء الإلکترونی – دراسۀ فقهیَّۀ. الریاض: دار کنوز إشبیلیا.

۴۵. شوشتری، مهدی؛ ناصری مقدم، حسین؛ صابری، حسین (۱۳۹۵). سازوکارهای حفظ مقاصد شریعت،

مجله پژوهش‌های فقهی، دوره ۱۲، شماره ۱.

۴۶. شهید اول، محمد مکی (بی‌تا). الدروس الشرعیهٔ فی الفقه الإمامیهٔ. قم: مؤسسهٔ النشر الاسلامی التابعهٔ لجماعهٔ المدرسین.

۴۷. الشیخ المنجد، محمد صالح. الإسلام سؤال و جواب. http://www.islam-qa.com/ar/ref/118501

۴۸. طوسی، محمد بن حسن (۱۳۶۴). تهذیب الأحکام فی شرح المقنعهٔ للشیخ المفید رضوان الله علیه (چاپ چهارم). تحقیق حسن خرسان. تهران: دار الکتب الإسلامیهٔ.

۴۹. مفید، محمدبن محمد (۱۴۱۴). الاختصاص. بیروت: دار المفید للطباعهٔ والنشر والتوزیع.

۵۰. صدر، محمد باقر (۱۴۰۶). دروس فی علم الأصول (چاپ دوم). بیروت: دار الکتاب اللبنانی.

۵۱. طباطبائی قمی، تقی (۱۴۱۳). عمده المطالب فی التعلیق علی المکاسب. قم: محلاتی.

۵۲. طبرسی، فضل بن حسن (۱۴۱۵). تفسیر مجمع‌البیان. بیروت: مؤسسهٔ الأعلمی للمطبوعات.

۵۳. طوفی صرصری، نجم الدین (۱۴۰۷). شرح مختصر الروضهٔ. تحقیق عبدالله بن عبدالمحسن ترکی. بیروت: مؤسسهٔ الرسالهٔ.

۵۴. عبد المنعم، محمود عبدالرحمان (۱۴۱۹). معجم المصطلحات و الألفاظ الفقهیهٔ. قاهره: دار الفضیلهٔ.

۵۵. عبدی پور فرد، ابراهیم؛ وصالی ناصح، مرتضی (۱۳۹۶). توسعه مفهوم و مصادیق مال در فضای مجازی (مطالعه تطبیقی مالیت داده‌های رایانه‌ای در حقوق اسلام، ایران و کامن لا)، فصلنامه پژوهش‌های تطبیقی حقوق اسلام و غرب، دوره ۴، شماره ۱.

۵۶. غزالی، محمد بن محمد (۱۴۱۳). المستصفی فی علم الأصول. بیروت: دارالکتب العلمیهٔ.

۵۷. فاضل مقداد، جمال الدین (۱۴۰۴). التنقیح الرائع لمختصر الشرائع. قم: مکتبهٔ آیت الله المرعشی النجفی.

۵۸. فتاوای هفت تن از علمای شیعه در مورد فضای مجازی

https://www.shia-news.com/fa/news/۱۱۹۲۹۱

۵۹. قرافی، أحمد بن إدریس (۱۴۱۶). نفائس الأصول فی شرح المحصول. مصر: مکتبهٔ نزار مصطفی الباز.

۶۰. قلعجی، محمد رواس و قنیبی، حامد صادق (۱۴۰۸). معجم لغهٔ الفقهاء (چاپ دوم). بیروت: دار النفائس.

۶۱. قهرمانی، معصومه؛ کاهانی، محسن (۱۳۸۸). مهندسی اجتماعی و امنیت اطلاعات: مطالعه موردی، مجموعه مقالات اولین کنفرانس حوادث و آسیب‌پذیری‌های امنیت فضای تبادل اطلاعات، مرکز تحقیقات مخابرات ایران.

۶۲. کلینی، محمد بن یعقوب (۱۳۶۵). الکافی (چاپ چهارم). تهران: دار الکتب الإسلامیة.

۶۳. کوین، بیور (۱۳۹۷). مرجع کامل هک و ضد هک اخلاقی (چاپ سوم). ترجمه محمد محمدی. تهران: نبض دانش.

۶۴. گودرزی اصفهانی، وحید (۱۳۹۲). نبرد با سارقان اطلاعات و راهکارهای مقابله با آن. تهران: انتشارات ناقوس.

۶۵. لبان، شریف درویش؛ می محمد، حمال الدین (۲۰۱۰). خطاب المعادی للإسلام علی شبکة الإنترنت آلیات الهجوم و استراتیجیات الردع دراسة تحلیلة لعینة من المواقع الأجنبیة، المجلة الاتجاهات الحدیثة فی المکتبات والمعلومات، العدد ۳۴.

۶۶. لجنة الفتوی فی الأزهر. الجهاد الإلکترونی. ۱۴۲۲/۰۲/۰۶.

http://www.maktabatalfeker.com/book.php?id=٦٧٦٤

۶۷. ماندنی خالدی، فاطمه؛ سلیمی، عابد (۱۳۸۶). امنیت در اینترنت و اصول زیربنایی آن (چاپ دوم). تهران: انتشارات واژگان و آصال.

۶۸. مجمع فتاوای دوحه قطر، www.islamweb.net.

۶۹. محقق داماد، سید مصطفی (۱۴۰۶). قواعد فقه جلد اول (چاپ دوازدهم). تهران: مرکز نشر علوم اسلامی.

۷۰. محقق سبزواری، محمدباقر بن محمد (۱۳۸۱). کفایه الفقه (الاحکام) (چاپ اول). قم: مؤسسة النشر الإسلامی.

۷۱. مروج جزائری، محمد جعفر (۱۴۱۵). القواعد الفقهیة والاجتهاد والتقلید (منتهی الدرایة فی توضیح الکفایة) (چاپ سوم). قم: مؤسسه دار الکتاب.

۷۲. مشکینی، علی (۱۳۷۱). اصطلاحات الأصول و معظم أبحاثها (چاپ پنجم). قم: نشر الهادی.

۷۳. مصباح، محمدتقی (۱۳۶۹). حکومت اسلامی و ولایت‌فقیه. تهران: سازمان تبلیغات.

۷۴. مظفر، محمدرضا (۱۳۹۰). أصول الفقه (چاپ هشتم). قم: مؤسسهٔ بوستان کتاب.

۷۵. اردبیلی، احمد بن محمّد (۱۴۰۳). مجمع الفائدة والبرهان فی شرح إرشاد الأذهان. قم: مؤسسهٔ النشر الإسلامی.

۷۶. مکارم شیرازی، ناصر (۱۴۲۶). انوار الفقاهة (کتاب التجارة). قم: مدرسه الامام علی بن ابی طالب.

۷۷. ملکیان، احسان (۱۳۸۵). نفوذگری در شبکه و روش‌های مقابله (چاپ چهارم). تهران: مؤسسه علمی- فرهنگی نص.

۷۸. منصور نژاد، محمد (۱۳۸۶). نظام اسلامی و حریم خصوصی شهروندان، نشریه حکومت اسلامی، سال دوازدهم، شماره دوم.

۷۹. موسوی گلپایگانی، سید محمدرضا (۱۴۱۲). الدر المنضود فی أحکام الحدود. قم: دارالقرآن الکریم.

۸۰. موسوی بجنوردی، سیدحسن (۱۳۷۷). القواعد الفقهیة. قم: نشر الهادی.

۸۱. موسوی قزوینی، سیدعلی (۱۴۲۴). ینابیع الأحکام فی معرفة الحلال والحرام. قم: مؤسسهٔ النشر الإسلامی.

۸۲. مؤسسهٔ دائرة معارف الفقه الإسلامی (۱۴۲۳). موسوعة الفقه الاسلامی طبقاً لمذهب أهل البیت علیهم‌السلام. قم: مؤسسهٔ دائرة معارف الفقه الإسلامی.

۸۳. نجفی، محمد حسن (۱۳۶۲). جواهر الکلام فی شرح شرائع الإسلام (چاپ هفتم). بیروت: دار إحیاء التراث العربی.

۸۴. نراقی، مولی أحمد (۱۴۰۸). عوائد الأیام (چاپ سوم). قم: مکتبهٔ بصیرتی.

۸۵. نقیبی، سید ابوالقاسم (۱۳۸۹). حریم خصوصی در مناسبات و روابط اعضای خانواده، فصلنامه فقه و حقوق خانواده (ندای صادق)، شماره ۵۲.

۸۶. وحدتی شبیری، سید حسن (۱۳۸۰). وضعیت حقوقی- فقهی رایانه در ایران، نشریه اطلاع‌رسانی و کتابداری کتاب‌های اسلامی، شماره ۷.

۸۷. Downing, A., & others. (۲۰۰۹). *Dictionary of computer and internet terms*.

۸۸. Executive Office of President of United States. (۲۰۱۸). *The council of economic advisers, The cost of malicious cyber activity to the U.S.*

economy. United States.
۸۹. Graves, K. (۲۰۱۰). *CEH: Certified ethical hacker study guide*. Indiana: Wiley Publishing, Inc.
۹۰. Lewis, J (۲۰۱۸). *Economic impact of cybercrime—No slowing down*. Report CSIS. United States.
۹۱. Palmer, D. (۲۰۱۸). *Cybercrime drains $۶۰۰ billion a year from the global economy, says report*. (۲۰۱۸). https://www.zdnet.com/article/cybercrime-drains-٦٠٠-billion-a-year-from-the-global-economy-says-report/
۹۲. Sanchit, N. (۲۰۱۹). World of white hat hackers, Thapar Institute of Engineering and Technology, Patiala, Punjab – ١٤٧٠٠٣, India. *International journal of scientific & engineering research*, ١٠(٥).
۹۳. Shaqiri, A. (۲۰۱۴). Management information system and decision making. *Academic journal of interdisciplinary studies*, Rom, ۳ (۲), ۱۸.