

## اخلاق اسلامی حریم خصوصی در شبکه‌های اجتماعی سایبر: (با تأکید بر واتس آپ)

\* کریم خان محمدی

\*\* علی اکبر شاملی

### چکیده

ورود شبکه‌های اجتماعی سایبری، به‌ویژه، شبکه‌های اجتماعی بر پایه موبایل؛ همچون واتس آپ، با آسیب‌هایی همراه بوده که یکی از این آسیب‌ها، تهدید حریم خصوصی کاربران است. در این گونه شبکه‌ها، حریم خصوصی کاربر، از سه جهت، یعنی: در مقابل کاربران دیگر، در مقابل گردانندگان این شبکه‌ها و در برابر دولت‌ها در معرض تهدید قرار می‌گیرد. این مقاله، به روش تحلیلی توصیفی، و با استناد به متون اصیل دینی، ضمن استخراج اصول اخلاقی مرتبط با «حریم خصوصی»، مانند: استیذان، ستاریت، رازداری، عدم تجسس، اصل انعکاس و همچنین پرهیز از ظلم، پرهیز از سرقت، پرهیز از آزار دیگران، این اصول را نسبت به اطلاعات مکنون در فضای مجازی جاری دانسته، و نتیجه می‌گیرد: دولت‌ها در مواجهه با دو اصل اخلاقی، یعنی؛ حفظ امنیت کاربران و حفظ حریم خصوصی آنان - تا جایی که امکان دارد - باید با ترویج اصول اخلاقی و تاسیس شبکه‌های ملی، زمینه‌های حفظ حریم خصوصی شهروندان را تامین نموده و از بهره‌گیری از اطلاعات کاربران بر علیه خودشان، پرهیز کنند.

### کلیدواژه‌ها

اخلاق، حریم خصوصی، شبکه‌های اجتماعی، فضای سایبر، واتس آپ.

### مقدمه

با گسترش فناوری اطلاعات، ارتباطات اجتماعی به سهولت انجام می‌پذیرد. از پیامدهای گسترش فناوری، شکل‌گیری شبکه‌های اجتماعی است. شبکه اجتماعی، ساختاری اجتماعی است که از گروه‌هایی، که فردی یا سازمانی هستند، تشکیل شده است. این گروه‌ها توسط یک یا چند نوع خاص از وابستگی به هم متصل‌اند. از این وابستگی‌ها، می‌توان به روابط دوستانه، همشهری بودن، هم‌وطن بودن، روابط تجاری و روابط خانوادگی اشاره کرد.

یک نمونه از این شبکه‌های اجتماعی، پایگاه‌های شبکه‌های اجتماعی است. این پایگاه‌ها، با پیداشدن و فراگیر شدن فناوری ارتباطات، شکل گرفتند. علت نام‌گذاری آن‌ها به شبکه‌های اجتماعی، به خاطر شباهت بسیار زیاد این پایگاه‌ها به شبکه اجتماعی انسانی بود. چراکه در این پایگاه‌ها، همانند شبکه‌های اجتماعی انسانی، افراد در تعاملات چندسویه به وسیله خطوطی به هم متصل می‌شوند و می‌توانند از این طریق، ارتباطات و اطلاعات خود را به اشتراک بگذارند (علم الهدی، ۱۳۹۲: ۱۰۶).

بررسی‌های جدید نشان داده است که یک‌پنجم ساکنان جهان، عضو شبکه‌های اجتماعی هستند و دست‌کم ماهی یک‌بار سراغ صفحات شخصی خود در شبکه‌های اجتماعی می‌روند؛ البته پیش‌بینی می‌شود این رقم طی چند سال آینده به میزان قابل ملاحظه افزایش یابد. به گزارش ایتنا، مرکز تحقیقاتی امارکتر (Emarketer) بر اساس جدیدترین بررسی‌های خود، اعلام کرد که حدود ۱.۶۱ میلیارد نفر از مردم جهان در شبکه‌های اجتماعی عضو هستند (سایت ایتنا، ۱۳۹۳/۱۲/۱۱).

با فراگیر شدن شبکه‌های اجتماعی، تفکر دربارهٔ مرزبندی حریم خصوصی، بیش از پیش اهمیت دارد؛ چون امروزه تجاوز به حریم خصوصی، بیشتر از قبل برای افراد و شرکت‌ها آسان شده است. از آنجا که رایانه‌ها و اینترنت بسیار جدید هستند، بیشتر افراد، تجربهٔ کافی در به‌کارگیری این رسانه ندارند و درک نمی‌کنند که این کانال ارتباطاتی تا چه اندازه برای سوءاستفاده، باز و در دسترس است (پاتر، ۱۳۹۱: ۲۲۳).

حریم خصوصی در شبکه‌های اجتماعی، حقی است برای افراد نسبت به حفاظت از اطلاعات شخصی و ارتباطات آن‌ها با دیگران، در برابر افراد و شرکت‌های دیگر.

حریم خصوصی هر کاربر در شبکه‌های اجتماعی از سه جهت، یعنی؛ از جهت کاربران دیگر، گردانندگان شبکه‌ها و دولت‌ها در خطر است. هر کدام از این سه جهت، مصادیقی آشکار دارد. مثلاً هک کردن و نفوذ به سیستم کاربر یکی از مصادیق عدم امنیت و هتک حریم خصوصی در برابر کاربران دیگر است.

یکی از آموزه‌های اخلاق اسلامی در روابط میان انسان‌ها، احترام گذاشتن به حریم خصوصی آن‌ها است. اسلام، برای حفظ حریم خصوصی دیگران اصول اخلاقی دارد که این اصول به افراد می‌آموزد به حریم خصوصی دیگران باید احترام گذاشت و در زندگی خصوصی دیگران نباید دخالت کرد.

در این مقاله، با شناساندن اصول اخلاقی حریم خصوصی، به هر یک از سه جهت هتک حریم خصوصی کاربر از لحاظ اخلاقی، پرداخته خواهد شد. لذا مسئله اصلی این تحقیق، بررسی اخلاقی حریم خصوصی کاربران شبکه‌های اجتماعی با تأکید بر شبکه اجتماعی واتس‌آپ است.

## مفاهیم

### ۱. شبکه‌های اجتماعی سایبری

اگرچه مفهوم شبکه‌های اجتماعی به زمان‌های بسیار دور برمی‌گردد، چنان‌که خانواده، کوچک‌ترین شبکه اجتماعی است اما جعل این واژه در سال ۱۹۴۵ توسط جی‌ای بارنز صورت پذیرفت. او از این واژه برای ارتباط میان روستاییان نروژ استفاده کرد و در آخر به این نتیجه رسید که زندگی هر فرد مانند نقطه‌ای است و این نقاط در زندگی اجتماعی به وسیله خطوطی به یکدیگر متصل‌اند. از طریق این خطوط، یک شبکه به دست می‌آید که نشان‌دهنده ارتباط میان افراد در شبکه اجتماعی است (Cross, 2006: 12). اصطلاح شبکه‌های اجتماعی به روابط اجتماعی به دست آمده در میان افراد، مانند روابط افراد درون خانواده، روابط روستاها، جوامع و مناطق مختلف، اشاره دارد. روابط خویشاوندی، معمول‌ترین مثال برای این ارتباطات و تشکیل شبکه‌های اجتماعی محسوب می‌گردد (Lazer, 2008: 2).

برای شبکه‌های اجتماعی سایبری، تعاریف زیادی ذکر شده است. هر کدام از این تعاریف، به نوعی به دنبال توصیف این پدیده نوظهور می‌باشند. بر اساس استدلال راین گلد

«شبکه اجتماعی سایبری، معمولاً به معنای شبکه الکترونیکی ارتباطات متقابل است که محدودده‌اش را خود تعریف می‌کند و پیرامون علاقه یا هدف مشترکی تشکیل شده است؛ گرچه در برخی مواقع، ایجاد ارتباط فی‌نفسه به هدف تبدیل می‌شود» (کاستلز، ۱۳۸۰: ۳۸۶) وی، معتقد است یک اجتماع مجازی دارای اجزایی می‌باشد که عبارت‌اند از:

روابط فردی که شبکه اجتماعی را می‌سازد؛ دسترسی آسان و آزاد برای دسترسی به اجتماع؛ ملاقات‌های شخصی؛ دیالوگ، بازخورد و تقسیم جزئیات؛ یک تاریخ مشترک (Gattiker et al, 2001: 167).

شبکه‌های اجتماعی مجازی، انسان‌ها را قادر می‌سازند تا با تعداد زیادی از دوستان که به لحاظ جغرافیایی پراکنده هستند، ارتباط برقرار کنند و احتمالاً بخش بزرگی از کاربران آن، جوانان هستند. والتر و رامیرز، ادعا می‌کنند که «فیس‌بوک، بزرگ‌ترین ابزار سیستم‌های شبکه اجتماعی است که تاکنون مورد بررسی قرار گرفته است. این سیستم‌ها، راه‌های جدید چشمگیری را برای نگهداری روابط فراهم می‌کنند» (Walther & Ramirez, 2009: 302).

یکی از این شبکه‌های اجتماعی که امروزه بیشترین استفاده را دارد، «واتس‌آپ» است. به زعم برخی نویسندگان، واتس‌آپ، یک برنامه برای گوشی‌های هوشمند بوده که جایگزین خوبی برای پیام‌رسانی موبایل است. همچنین علاوه بر پیام‌های متنی، قابلیت ارسال تصاویر و فیلم را هم دارا است (Buchenscheit et al, 2014: 1). این نرم‌افزار به علت قابل حمل بودن و دسترسی آسان، محبوبیت زیادی به دست آورده است. واتس‌آپ به وسیله جان کوم<sup>۱</sup> و بریان اکتون<sup>۲</sup> - که از کارمندان قبلی شرکت یاهو بودند - ساخته شد. این نرم‌افزار در سال اول نصب، کاملاً رایگان است اما برای هر سال بعد، مبلغ ۹۹ سنت از کاربران خود دریافت می‌کند؛ البته در ایران، در سال‌های بعد نیز به صورت کاملاً رایگان در دسترس است. این موضوع، سؤالات و گمانه‌زنی‌های متعددی را برای کاربران ایرانی مطرح کرده است.

در سال ۲۰۱۳ واتس‌آپ، رکورد کاربران خود را شکست و تعداد آن‌ها را به ۴۵۰

1. Jan Koum

2. Brian Acton

میلیون نفر رساند. این افراد، حداقل ماهی یکبار به این نرم‌افزار سر می‌زنند. در سال ۲۰۱۴ شرکت فیس‌بوک، این نرم‌افزار را به مبلغ ۱۹ میلیارد دلار خرید. این قیمت زیاد برای نرم‌افزار واتس‌آپ، اظهار نظرهای متفاوتی به دنبال داشت؛ مثلاً گفته می‌شد: فیس‌بوک به دنبال جاسوسی کردن به وسیله این نرم‌افزار است. بعد از فروش واتس‌آپ، تعداد کاربران او در سال ۲۰۱۵ به بیش از ۸۰۰ میلیون نفر رسید که حکایت از گسترش و محبوبیت این نرم‌افزار دارد. تحقیقات نشان می‌دهد، در سال ۲۰۱۴ روزانه بیش از ۲۰ میلیارد پیام به وسیله واتس‌آپ میان کاربران منتقل شده است (Hong, 2014: 4).

از قابلیت‌های واتس‌آپ می‌توان به پشتیبانی از سیستم‌عامل‌های مختلف، ارسال پیام و تماس اینترنتی، مصرف دیتای اینترنت فوق‌العاده کم، بازبودن برنامه در پس‌زمینه گوشی - به طوری که با وصل به اینترنت پیام‌های آن به دست کاربر می‌رسد و نیاز به باز کردن دستی ندارد - قابلیت فرستادن عکس، فیلم و صوت، امکان ساختن گروه و فرستادن چت گروهی، امکان مسدود کردن افرادی که کاربر نمی‌خواهد با آن‌ها در ارتباط باشد و مانند آن، نام برد.

## ۲. حریم خصوصی

تاکنون تعریف جامعی از حریم خصوصی که مورد اتفاق همه متفکران باشد، نشده است. به علاوه، مبانی فلسفی، انسان‌شناختی و جامعه‌شناختی این مفهوم، آن‌چنان متنوع است که رسیدن به یک مفهوم واحد را غیرممکن ساخته است. لذا بسیاری از اندیشمندان به جای تبیین مفهوم حریم خصوصی به دنبال معرفی مصادیق می‌باشند. از مصادیق حریم خصوصی می‌توان به حریم مکانی، جسمی، حیثیتی، خانوادگی، لوازم شخصی، اطلاعات شخصی و ارتباط شخصی اشاره کرد (سروش، ۱۳۹۳: ۱۱-۲۳).

برخی، حریم خصوصی را حقی برای افراد می‌دانند که به وسیله این حق، آن‌ها باید در برابر مداخله بی‌اجازه دیگران در زندگی شخصی مورد حمایت قرار بگیرند (Landwehr & Heitmeyer, 2011: 43). همچنین برخی حریم خصوصی را حقی برای افراد در برخورداری از حمایت شدن در برابر مداخله دیگران در زندگی شخصی و خانوادگی چه با ابزار مستقیم و چه غیرمستقیم می‌دانند (Shostack & Syverson, 2004: 31). برخی دیگر نیز،

ارکانی برای این حریم خصوصی مشخص کرده‌اند، مثلاً خانم روت گیسون، سه رکن اساسی یعنی؛ محرمانگی (رازداری)، گمنامی (ناشناسی) و خلوت (انزوا و تنها بودن) [را] برای حریم خصوصی در نظر گرفته است (ایران پور، ۱۳۹۱: ۳۲).

می‌توان چنین نتیجه گرفت که مفهوم و ماهیت حریم خصوصی از مقولات نسبی است و بر اساس زمان، مکان و باورهای اجتماعی متفاوت است و تعریف مورد وفاقی از آن وجود ندارد. به همین دلیل، برای شناخت و تعریف آن باید از معیارهای شخصی و نوعی استفاده کرد.

### ۳. حریم خصوصی فضای سایبر

حریم خصوصی باید بر اساس هر نوع فضا، به اقتضای همان موقعیت تعریف شود. حریم خصوصی، جایی است که فرد در آن احساس امنیت کند و این احساس امنیت است که باعث می‌شود اطلاعات و وسایل گران‌بهای خود را در آنجا قرار دهد تا از دسترس دیگران دور باشد. فضای سایبر نیز چنین القایی را به کاربر می‌دهد که این فضا کاملاً امن بوده و کاربر از تجاوز دیگران در امان است.

چیزی که در فضای سایبر برای افراد مهم است و از موارد شخصی انسان شناخته می‌شود، اطلاعات و ارتباطات فرد است. اطلاعات، مفهوم گسترده‌ای از هویت کاربر، شماره تماس‌ها، عکس و فیلم‌های ذخیره‌شده کاربر در دستگاه شخصی و غیره می‌باشد و منظور از ارتباطات، هر نوع رابطه با هر کسی و به هر شکلی (پیام یا تماس) را شامل می‌شود. این احترام به ارتباطات افراد، نمود بیشتری در شبکه‌های اجتماعی دارد؛ چرا که شبکه‌های اجتماعی پا به عرصه وجود گذاشتند تا ارتباطات انسانی را گسترده‌تر نمایند.

بنابراین می‌توان حریم خصوصی در شبکه‌های اجتماعی را به حفظ اطلاعات و ارتباطات شخصی از دید عموم و عدم هرگونه سوءاستفاده از این اطلاعات و ارتباطات برعلیه کاربر تعریف کرد؛ به این معنا که هر کاربر در شبکه‌های اجتماعی دارای اطلاعات و ارتباطات شخصی می‌باشد که نباید برای همگان مشخص شود و یا از آن سوءاستفاده کنند.

### اصول اخلاقی حریم خصوصی

همان‌طور که ذکر شد، ورود شبکه‌های اجتماعی به ایران موجب بروز خطراتی در حریم خصوصی کاربران شده است. یکی از آموزه‌های اخلاقی در اسلام، احترام گذاشتن به حریم خصوصی افراد است. لذا لازم است نقض حریم خصوصی کاربران در شبکه‌های اجتماعی با تمسک به آموزه‌های اخلاقی اسلام مورد بررسی قرار گیرد و وظایف اخلاقی کاربران و اجتماع پیرامون آنها مشخص شود.

احترام به حریم خصوصی افراد، در بسیاری از منابع اسلامی به صورت اصول اخلاقی حریم خصوصی موجود است. در ادامه برخی از اصول اخلاقی حریم خصوصی، مستفاد از آیات و روایات، اشاره می‌شود؛ البته اصول اخلاقی حریم خصوصی گسترده‌تر از موارد زیر است و برای رعایت اختصار به مهم‌ترین آنها پرداخته می‌شود:

#### ۱- استیذان

در آیات و روایات متعدد، بر اجازه گرفتن برای ورود به منزل دیگران، تأکید شده است. از آن جمله است آیه ۲۴ سوره نور که خداوند می‌فرماید: «يَا أَيُّهَا الَّذِينَ آمَنُوا لَا تَدْخُلُوا بُيُوتًا غَيْرَ بُيُوتِكُمْ حَتَّى تَسْتَأْذِنُوا...»؛ شما که ایمان دارید به خانه هیچ کس غیر از خانه‌های خود داخل نشوید تا آنکه اجازه ورود بگیرید». این اجازه ورود، به این خاطر است که خداوند، منزل افراد را حریم خصوصی آنان دانسته؛ چراکه افراد در آن باید احساس امنیت کنند نه آن که هر کسی هر وقت دلش خواست، وارد منزل آن‌ها شود. همچنین، خداوند حفظ این حریم خصوصی را برای همه واجب کرده است. این حکم استیذان، یک حکم اخلاقی است که از اصول حفظ حریم خصوصی دیگران است.

حفظ حریم خصوصی دیگران، فقط به ورود بدون اجازه به منزل چهاردیواری افراد متوقف نیست. امروزه می‌توان به خیلی از مکان‌ها، منزل گفت: مثلاً کسی که در پارکی چادری زده، آن چادر منزل اوست؛ یعنی مکانی است که او برای خود اختیار کرده و خود را در آن ایمن می‌داند، در صورتی که زمین آن مکان به ملکیت او نرسیده ولی همه انسان‌ها آنجا را منزلی برای او می‌دانند، لذا هیچ کس بدون اجازه وارد آن نمی‌شود.

در عصر حاضر، که عصر پیشرفت تکنولوژی است، کامپیوتر و موبایل شخصی به‌مثابه

منازل انساهاست که تمام اطلاعات و ارتباطات شخصی و خانوادگی خود را در آن می‌ریزند. کاربران این دو دستگاه را مانند منزل خود، فضایی امن تلقی کرده‌اند که اطلاعات و ارتباطات مهم خود را در آن ذخیره می‌کنند. همین حس امنیت است که وجه اشتراک منزل افراد با کامپیوتر و موبایل افراد بوده و حریم خصوصی را به وجود می‌آورد؛ بنابراین ورود به این دو دستگاه از هر طریق، مصداق ورود بدون اجازه به حریم خصوصی دیگران بوده و امری غیراخلاقی است.

## ۲- ستاریت خداوند

ستاریت یا پرده‌پوشی صفتی از صفات الهی است. «اهل معرفت نیز، در سلوک عملی خود، به اصل «تخلق به اخلاق الهی» تمسک کرده و برای شناخت زیبایی‌ها به «جمیل مطلق» چشم می‌دوزند و سپس تلاش می‌کنند تا اسماء الهی را در نفس خویش تحقق بخشند. برای مثال، ستاریت خداوند را الگوی خود قرار داده و در میان خلق، به اقتضای آن رفتار می‌کنند» (سروش، ۱۳۹۳: ۵۹).

این ستاریت، در حدی است که خداوند برای اثبات بدترین فواحش یعنی زنا، مسیری سخت، قرار داده که با این مسیر بسیار سخت زنا به راحتی اثبات نمی‌شود. این ستاریت، فقط مختص به دنیا نمی‌شود؛ چراکه «در روایت وارد شده که هرگاه خداوند عیب بنده را در دنیا پوشاند، همانا او کریم‌تر از آن است که در آخرت فاشش سازد و اگر در دنیا آن را آشکار کند، کریم‌تر از آن است که دیگر بار در آخرت ظاهرش سازد» (نراقی، ۱۳۸۸، ج ۲: ۱۲۲). از آن جمله است فرازی از مناجات شعبانیه که آمده است: «إلهی قد سترت علی ذنوبی فی الدنیا و أنا أحوج إلی سترها علی منک فی الآخری / الهی گناهانی را در دنیا بر من پرده‌پوشی فرمودی که من به پرده‌پوشی آن‌ها در آخرت محتاج‌ترم» (ابن طاووس، ۱۳۷۶، ج ۳: ۲۹۷).

پس زمانی که خداوند، با اینکه عالم به گناه افراد بوده و قدرت در افشای آن را نیز دارد، ولی به خاطر عنایت خویش، عیوب گناهکاران را می‌پوشاند، چه توجیهی برای انسان‌هاست که به دنبال عیوب دیگران باشند و از آن‌ها سوءاستفاده نمایند. اخلاق در اینجا حکم می‌کند که انسان‌ها به تمسک از پروردگار خود، عیب‌هایی را که از دیگران می‌داند،



آشکار نکند و به دنبال عیوب و رازهای دیگران به هر نحوی - چه در عالم واقعی و چه در فضای مجازی و شبکه‌های اجتماعی - نباشد.

### ۳- رازداری

تفاوت رازداری با ستاریت در آن است که ستار، کسی است که از عیب دیگران آگاه می‌شود و آن را برای دیگران مکشوف نمی‌کند ولی رازداری، به دو صورت متصور است: اول، به این صورت که انسان، اسرار خودش را حفظ کند؛ چه رازهای خوب خویش که سبب حسادت دیگران شده و چه رازهای بد خویش که سبب خوشحالی دشمنان می‌گردد و دوم، به این صورت که رازی که دیگری به او گفته را حفظ کند؛ بنابراین ستار، کسی است که علم به واقع افراد دارد و آن کسی جز خداوند نمی‌تواند باشد ولی اگر انسان به عیبی از دیگران آگاه شد، باید مانند خداوند ستر باشد و آن را حفظ کند؛ اما رازدار، کسی است که به او رازی گفته شده و از او خواسته می‌شود که آن را حفظ کند.

هرکسی در زندگی خود رازهایی دارد که دوست ندارد افشا شود. اسلام، رازداری را صفت پسندیده‌ای می‌داند. خداوند نیز در آیات قرآن به خوبی رازداری و زشتی افشای اسرار اشاره کرده و در آیه ۱۶ سوره توبه می‌فرماید: «أَمْ حَسِبْتُمْ أَنْ تُتْرَكُوا وَلَمَّا يَعْلَمِ اللَّهُ الَّذِينَ جَاهَدُوا مِنْكُمْ وَلَمْ يَتَّخِذُوا مِنْ دُونِ اللَّهِ وَلَا رَسُولِهِ وَلَا الْمُؤْمِنِينَ وَلِيجَةً وَاللَّهُ خَبِيرٌ بِمَا تَعْمَلُونَ»؛ آیا گمان کردید که (به حال خود) رها می‌شوید، در حالی که هنوز آن‌ها که از شما جهاد کردند و غیر از خدا و رسولش را محرم اسرار خویش انتخاب ننمودند (از دیگران)، مشخص نشده‌اند (باید آزمون شوید و صفوف از هم جدا شود) و خداوند به آنچه عمل می‌کنید، آگاه است». این آیه، اگرچه به صورت صریح مطابقی و یا تضمینی دلالت بر خوبی حفظ اسرار و بدی افشای سر اشاره نمی‌کند ولی با دلالت التزامی به این امر اشاره دارد. لذا به مسلمانان می‌فرماید که اسرار خودشان را به کسانی بگویند که اطمینان به آن‌ها دارند و اسرارشان را حفظ می‌کنند. بنابراین، مفهوم این آیه این است که حفظ اسرار فضیلت و افشای آن رذیلت است، چرا که خداوند به فضیلت امر و از رذیلت نهی می‌کند (مکارم شیرازی، ۱۳۷۷، ج ۳: ۳۶۰).

نقطه مقابل افشای سر، کتمان آن است. در روایات زیادی تأکید بر کتمان راز دیگران

شده است. پیامبر اکرم ﷺ در این باره فرمودند: «طُوبَى لِعَبْدٍ نُومَةٍ عَرَفَهُ اللهُ وَ لَمْ يَعْرِفْهُ النَّاسُ أُولَئِكَ مَصَابِيحُ الْهُدَى وَ يَنَابِيعُ الْعِلْمِ يَنْجَلِي عَنْهُمْ كُلُّ فِتْنَةٍ مُظْلِمَةٍ لَيْسُوا بِالْمَدَائِيحِ الْبُذْرِ وَ لَا بِالْجَفَاةِ الْمُرَائِيْنَ» (کلینی، ۱۳۶۵، ج ۲: ۲۲۵)؛ خوشا به حال بنده گمنام، او را خداوند می‌شناسد و مردمان نمی‌شناسند؛ آن‌ها چراغ‌های هدایت و چشمه‌های دانش هستند، هر فتنه‌ای از آنان دفع می‌شود، نه فاش‌کننده سرها و نه ستمگران ریاکار هستند افشای راز، در جایی است که انسان از دیگران رازی بداند و آن را افشاء کند؛ بنابراین به دنبال راز دیگران گشتن و بعد افشا کردن آن، تجسس است که کاری ناپسندتر خواهد بود.

#### ۴- عدم تجسس

در اسلام کاوش و جست‌وجو کردن عیب دیگران از صفات ناپسند شمرده شده است. خداوند در سوره حجرات آیه دوازدهم به مسلمانان می‌فرماید: «وَلَا تَجَسَّسُوا»؛ و کنجکاو (از احوال مردم) مکنید و حتی این تجسس کردن را زمینه غیبت کردن افراد می‌داند و در ادامه همان آیه می‌فرماید: «لَا يَغْتَابُ بَعْضُكُمْ بَعْضًا»؛ بنابراین گاهی تجسس کردن به احوال مردم سبب غیبت و ریختن آبروی افراد نیز می‌شود. حتی می‌توان این دو را لازم و ملزوم همدیگر دانست؛ پس فردی که به دنبال پیدا کردن رازهای مردم و تجسس کردن در زندگی آن‌هاست، اگر به رازی دست پیدا کند، آن را در سینه اسرار خود حفظ نخواهد کرد و بی‌شک آن راز را افشاء می‌کند. لذا در این آیه، غیبت کردن بعد از تجسس آمده و از هر دو نهی شده است.

تجسس کردن می‌تواند به اشکال مختلفی انجام شود. شاید روزی پشت‌در ایستادن و گوش دادن صحبت‌های چند فرد و یا باز کردن نامه‌های شخصی افراد مصداق تجسس کردن بود، ولی امروزه تجسس کردن مصادیق جدیدی پیدا کرده است. مثلاً سرک کشیدن به کامپیوتر دیگران و سوءاستفاده از فایل‌های شخصی آن‌ها، هک کردن کاربران، زیر نظر داشتن ارتباطات کاربر و ... به‌نوعی تجسس در احوال دیگران بوده و از رذیلت‌های اخلاقی به‌شمار می‌رود.

بنابراین، دوری جستن از تجسس، از اصول حفظ حریم خصوصی دیگران است. دنبال کردن ارتباط و اطلاعات کاربران دیگر در شبکه‌های اجتماعی مصداق بارز

تجسس کردن است. این تجسس کردن زمینه افشای اسرار دیگران بوده و هر دو از کارهای ناپسند و غیراخلاقی است.

##### ۵- اصل انعکاس

اصل انعکاس، اصلی است که به افراد گوشزد می‌کند، اگر به دنبال اسرار دیگران برآمدی، خداوند اسرار خودت را افشاء می‌کند. رسول خدا ﷺ در این باره فرمودند: «لَا تَطْلُبُوا عَثْرَاتِ الْمُؤْمِنِينَ فَإِنَّ مَنْ تَبَعَ عَثْرَاتِ أَخِيهِ تَبَعَ اللَّهُ عَثْرَاتِهِ وَمَنْ تَبَعَ اللَّهُ عَثْرَاتِهِ يَفْضَحْهُ وَلَوْ فِي جَوْفِ بَيْتِهِ» (کلینی، ۱۳۶۵، ج ۴: ۵۸)؛ لغزش‌های مؤمنان را جست‌وجو نکنید؛ زیرا هر که لغزش‌های برادرش را جست‌وجو کند، خداوند لغزش‌هایش را دنبال می‌کند و هر که خداوند لغزش‌هایش را دنبال کند، رسوایش سازد، گرچه درون خانه‌اش باشد. امیر مؤمنان ۷ با عبارت صریح‌تر فرمودند: «مَنْ بَحَثَ عَنْ أَسْرَارِ غَيْرِهِ أَظْهَرَ اللَّهُ أَسْرَارَهُ»؛ (خوانساری، ۱۳۶۶، ج ۵: ۳۷۱). کسی که اسرار دیگران را جست‌وجو کند، خداوند رازهایش را برملا می‌سازد. نکته جالبی که از این احادیث برمی‌آید این است که، نه افشای اسرار، که اصل جست‌وجوی اسرار، نهی شده است. این به این معناست که خود این جست‌وجو، عمل غیراخلاقی و زشتی است که خداوند از آن هم انتقام می‌گیرد حتی اگر آن فرد افشاء سرّ نکرده باشد.

بنابراین، کاربران باید به این نکته توجه کنند که اگر به دنبال اسرار مردم باشند و بخواهند آن‌ها را برای دیگران بازگو کنند، خداوند رازهای خود آنان را افشاء خواهد کرد. پس کاربر، ملزم به حفظ احترام حریم خصوصی دیگران است. کاربران نباید عکس‌هایی که افراد دیگر از زندگی خصوصی مردم نشر داده‌اند، بازنشر کنند حتی اگر این عکس‌ها، فراوان نشر پیدا کرده باشند؛ چرا که شاید با این کار، او عده‌ای بی‌خبر را از راز آن افراد، باخبر کند. این صفت اخلاقی، پسندیده‌ای است که همگان باید آن را منش خود قرار دهند.

##### ۶- پرهیز از ظلم

تجاوز به حریم خصوصی کاربران، مصداق واضح ظلم در حق کاربر است. در اسلام

عدالت، حسن و ظلم، قبیح است. برای مثال، فقها غیبت کردن را مصداق ظلم به غیبت‌شونده می‌دانند؛ چراکه این کار موجب هتک حرمت آن فرد می‌گردد و این باعث حرمت غیبت می‌شود و این حکم حرمت را مستنبط از حکم عقل می‌دانند که می‌گوید هتک حرمت دیگران ظلم، است و ظلم قبیح و حرام است «و قد حکم العقل بحرمتها ایضا لکونه ظلماً للمغتتاب و هتکاً له» (توحیدی، ۱۴۱۲، ج ۲: ۵).

حال سؤال اینجاست که وقتی بازگو کردن صفات واقعی فردی، هتک حرمت و مصداق ظلم است، آیا هتک حریم خصوصی و نفوذ به سیستم دیگران و برداشتن اطلاعات آن‌ها و همچنین سوءاستفاده کردن از آن، مصداق هتک حرمت و ظلم نیست؟ در جواب باید گفت که، هرگونه هتک حریم خصوصی - چه در مواجهه حقیقی باشد و چه در مواجهه مجازی - مصداق هتک حرمت دیگران و ظلم است و ظلم نیز از لحاظ اخلاقی کاملاً قبیح است.

البته عده‌ای ظلم را در برابر «تضییع حق» می‌دانند؛ یعنی می‌گویند اول باید برای کاربر حقی ثابت باشد و در صورت تضییع آن حق، ظلم ایجاد می‌شود. اگر که ظلم را تضییع حق بدانیم نیز، در این مسئله ظلم متحقق است؛ چراکه اطلاعات و ارتباطات افراد، حقی است که فرد برای خودش دارد و دوست ندارد این اطلاعات و ارتباطات در اختیار دیگران قرار بگیرد. همچنین این حق را اهل عرف نیز تأیید می‌کنند؛ بنابراین نفوذ هر بیگانه و سوءاستفاده کردن از این حق، مصداق ظلم خواهد بود.

#### ۷- سرقت

با روی کار آمدن فضای مجازی، سرقت فقط مختص به بالارفتن از دیوار مردم نمی‌شود. امروزه؛ ورود به حریم خصوصی کاربران و استفاده کردن از اطلاعات و ارتباطات او، مصداق بارز سرقت است؛ زیرا، علاوه بر اینکه اطلاعات، ارزش مالی دارند و یا می‌توانند به سرمایه مالی تبدیل شوند، به‌ذاته دارای ارزش بوده و فراتر از سرمایه مالی ارزش دارند. امام رضا ۷ می‌فرماید: «... وَ حَرَّمَ السَّرْقَةَ لِمَا فِيهِ مِنْ فُسَادِ الْأَمْوَالِ وَ قَتْلِ الْأَنْفُسِ لَوْ كَانَتْ مُبَاحَةً» (شیخ حرعاملی، ۱۴۰۹، ج ۲۸: ۲۴۱)؛ و خداوند، دزدی را نیز به این خاطر حرام کرد که اگر جایز بود، سبب تباهی ثروت‌ها و کشتن نفوس می‌شد.

سرقت اطلاعات و ارتباطات افراد، بدتر از سرقت مال بوده و مفسده سرقت اطلاعات فراتر از سرقت اموال است؛ چراکه اولاً، سرقت مال، باعث سوءاستفاده‌های بعدی نمی‌شود اما سرقت اطلاعات باعث می‌شود که یک فرد بارها به این وسیله اخاذی گردد. ثانیاً، اینکه مال اگر از دست برود، باز با کوشش دست‌یافتنی است اما آبروی انسان به راحتی قابل بازیافت نیست؛ بنابراین، این نوع سرقت از بدترین شکل آن است که حس امنیت را در یک جامعه کاملاً نابود می‌کند. این حس امنیت، باعث آرامش افراد و حس اعتماد میان همگان است. ولی با از بین رفتن این حس، آرامش نیز از بین رفته و کسی به دیگری اعتماد نخواهد کرد.

#### ۸- آزار و اذیت

تجاوز به حریم خصوصی دیگران، مصداق اذیت و آزار رساندن به کاربران است. در اسلام، اذیت و آزار رساندن به مسلمان‌ها از گناهان بزرگ است به طوری که خداوند در قرآن، آیه ۴۸ سوره احزاب، این آزار و اذیت را گناه آشکار می‌نامد: «وَالَّذِينَ يُؤْذُونَ الْمُؤْمِنِينَ وَالْمُؤْمِنَاتِ بَغَيْرِ مَا كَتَبْنَا فَتَقَدِرُوا حَتْمًا مَبِينًا»؛ و کسانی که مؤمنین و زنان مؤمن را بدون جرم اذیت می‌کنند، مرتکب بهتان و گناهی بزرگ می‌شوند».

البته بر اساس این آیه، هرگونه آزار و اذیت کردن، ظلم نیست. مثلاً برای کسانی که به سبب گناهی، مستوجب قصاص و حدود شده‌اند، ایذاء کردن آن‌ها ظلم نیست (طباطبایی، ۱۳۷۴، ج ۱۶: ۵۰۹). بلکه آزار و اذیت کسانی که استحقاق آن را ندارند، ظلم بوده که نقض حریم خصوصی کاربران، یکی از مصادیق این ظلم بدون استحقاق است.

به طور کلی، آزار و اذیت به معنای ایجاد ناراحتی برای دیگران است؛ یعنی هر چیزی که موجب ناراحتی دیگران شود، مصداق آزار و اذیت است؛ بنابراین هتک حریم خصوصی کاربران نیز ایجاد آزار و اذیت برای او است؛ چراکه این از بین بردن حریم خصوصی و کندوکاو فعالیت کاربر برای هیچ کس خوشایند نیست. لذا بر این مبنا، هتک حریم خصوصی موجب آزار و اذیت شده و به لحاظ اخلاقی کار قبیحی است.

### عوامل ناقضین حریم خصوصی

حریم خصوصی کاربران از سه جهت، یعنی؛ از سوی سایر کاربران، گردانندگان شبکه‌های اجتماعی و دولت‌ها، به مخاطره افتاده است. در این بخش با تمرکز بر اخلاق اسلامی، هر کدام از این سه جهت به‌طور مجزا بررسی می‌گردد.

#### ۱- کاربران شبکه‌های اجتماعی

تجاوز به حریم خصوصی در شبکه‌های اجتماعی توسط کاربران دیگر، مصادیقی مانند هک کردن، انتشار عکس و فیلم‌های خصوصی افراد، سوءاستفاده از نام و هویت افراد مشهور، نشر اکاذیب در مورد دیگران و مانند آن دارد.

در سال ۲۰۱۱، شکاف امنیتی در نرم‌افزار پیام‌رسان فوری واتس‌آپ گزارش شد که بر اساس آن، حساب کاربری افراد برای استراق‌نشت و پوشگر بسته‌ها، باز بود؛ در حمله‌ی استراق‌نشت، اطلاعات کاربر (اطلاعاتی که برای ورود به سایت، نرم‌افزار یا شبکه ذخیره شده تا مجبور نباشد این اطلاعات را دوباره وارد کند) توسط هکرها دزدیده می‌شود و آن‌ها می‌توانند با داشتن نام کاربری و رمز عبور، به همه‌ی اطلاعات کاربر دسترسی پیدا کنند. همچنین، پوشگر بسته‌ها نیز برنامه‌ای است که می‌تواند به رهگیری و ثبت جریان اطلاعات در شبکه بپردازد. پوشگر، جریان بسته‌هایی را که در سطح شبکه در حال تبادل هستند، زیر نظر می‌گیرد و می‌تواند اطلاعات خام بسته‌ها را کدگشایی کند و اطلاعات بخش‌های مختلف بسته را نمایان سازد (سایت برهان، ۱۳۹۴/۰۵/۲۲).

در ساده‌ترین حالت، کاربران با رجوع به پروفایل کاربر دیگر، می‌توانند آخرین وضعیت حضور فرد را درک کنند و بفهمند آن فرد، الآن آنلاین است یا نه یا آخرین لحظه حضور او کی بوده است؛ البته واتس‌آپ، گزینه‌ای برای قطع این دسترسی قرار داده که بسیاری از کاربران واتس‌آپ اطلاع نسبت به این گزینه نداشته و وضعیت خود را ناخواسته در دسترس بقیه کاربران قرار می‌دهند (Buchenscheit et al, 2014: 8).

این دسترسی به وضعیت فرد، به‌ویژه درباره افراد مشخص، نقض حریم خصوصی کاربران است. شاید کاربری علاقه نداشته باشد وضعیت او برای دیگران مشخص شود و از روش قطع کردن آن نیز مطلع نباشد. عدم حفظ حریم خصوصی کاربر توسط کاربران دیگر

به معنای اخلاقی نفوذ در حریم خصوصی فرد است. هتک حریم خصوصی از طرف اسلام نهی شده است. در این باره، هیچ شبهه اخلاقی وجود ندارد، بلکه همه، ورود در حریم خصوصی دیگران را امری ناپسند می‌دانند.

## ۲- گردانندگان شبکه‌های اجتماعی

دومین نوع هتک حریم خصوصی کاربر مربوط به گردانندگان شبکه‌های اجتماعی است. در این سال‌ها، خبرهایی مبنی بر جاسوسی برخی از شبکه‌های اجتماعی از کاربران خود منتشر شده است. برای مثال، کاربران شبکه اجتماعی فیس‌بوک، از اینکه این شبکه اسامی و تصاویری که به اشتراک گذاشته بودند به همراه اطلاعات اساسی آن‌ها را در دسترس عموم قرار داده بود، اعتراض داشتند. حتی فیس‌بوک پا را از سایت خود فراتر گذاشته و حرکات کاربران را در تمام سایت‌های اینترنتی نیز تحت نظر می‌گرفت (بادینر، ۱۳۸۹: ۲۱). این شبکه‌های اجتماعی منبعی از اطلاعات و ارتباطات کاربران دارند که شاید به جرئت بتوان گفت، هیچ دولتی چنین منبعی از افراد خود در دست ندارد.

واتس‌آپ نیز از این هتک حریم خصوصی مبرا نیست. میلیون‌ها کاربر از فروش اسرار خود از قبیل آدرس، امضاء الکترونیکی و غیره توسط واتس‌آپ ترس دارند (Buttarelli, 2015: 5) در یک نظرسنجی که چورچ و الیویرا را از بین ۱۳۱ کاربر واتس‌آپ انجام دادند، اکثر آن‌ها در مورد حفظ حریم خصوصی خود در واتس‌آپ نگران بودند (Church & Oliveira, 2013: 13).

هر کاربر، بدون اطلاع، با نصب برنامه واتس‌آپ، به این نرم‌افزار چند مجوز دسترسی می‌دهد. این مجوزها از این قبیل هستند:

الف) مجوزهای واتس‌آپ در مورد حساب کاربر؛ واتس‌آپ می‌تواند از حساب‌های کاربر مانند ایمیل یا جیمیل و مانند آن استفاده کند و از این طریق، هویت فرد را کاملاً مشخص نماید. همچنین، اجازه دارد حسابی را دوباره اضافه کند و یا رمز عبور آن را حذف کند؛

ب) مجوزهای واتس‌آپ در مورد موقعیت کاربر؛ واتس‌آپ مجوز به دست آوردن

مکان تقریبی (به وسیله شبکه اینترنت) و محل دقیق (به وسیله شبکه اینترنت و جی‌پی‌اس<sup>۱</sup>) کاربر را دارد. این به دست آوردن موقعیت مکانی، موجب مصرف بیشتر باتری گوشی کاربر نیز می‌شود؛

ج) مجوزهای واتس‌آپ در مورد پیام‌های کاربر؛ واتس‌آپ اجازه دارد پیام‌های متنی کاربران را دریافت و پردازش کند؛ البته منظور از پیام‌ها، صرفاً پیام‌های متنی واتس‌آپ نیست بلکه واتس‌آپ می‌تواند پیامک‌های فرد را نیز دریافت و پردازش کرده و بدون اطلاع کاربر، پیام‌های ارسال شده را حذف کند. همچنین مجوز دارد از طرف کاربر و بدون اطلاع او، پیامک به دیگران بفرستد و این کار هم موجب تحمیل هزینه زیادی به کاربر شده و هم می‌تواند از این طریق اتهامات غیرمنتظره به فرد وارد کند؛

د) دسترسی کامل به شبکه اینترنت کاربر؛ واتس‌آپ اجازه دارد به صورت کامل شبکه اینترنتی فرد از قبیل مرورگرها، جست‌وجوگرها و غیره را در اختیار داشته و کنترل کند؛  
 ر) مجوز واتس‌آپ در مورد اطلاعات شخصی کاربر؛ واتس‌آپ می‌تواند اطلاعات شخصی کاربر از قبیل نام، عکس، شماره تماس، لیست مخاطبین فرد و غیره را در اختیار بگیرد؛

ز) مجوز واتس‌آپ در مورد تماس‌های تلفنی کاربر؛ واتس‌آپ اجازه دارد تماس‌های کاربر را شناسایی و کنترل کند و همچنین اجازه دارد بدون مداخله کاربر، تماس بگیرد که این کار موجب ایجاد هزینه‌های اضافی می‌گردد؛

س) مجوزهای واتس‌آپ در مورد ذخیره‌سازی؛ واتس‌آپ اجازه دارد اطلاعات گوشی فرد از قبیل عکس و فیلم و غیره را در آرشیو خود ذخیره نماید؛

ش) اطلاع نسبت به برنامه‌های کاربردی کاربر؛ واتس‌آپ می‌تواند با بازیابی اطلاعات از برنامه‌هایی که کاربر استفاده می‌کند اطلاع یابد؛

دسترسی به میکروفن گوشی؛ واتس‌آپ می‌تواند از طریق میکروفن گوشی، مکالمات کاربر را ضبط کند؛

و) در دسترس داشتن اطلاعات اجتماعی کاربر؛ واتس‌آپ اجازه دارد پیام‌های افرادی



که به وسیله واتس آپ یا ایمیل با کاربر در ارتباط هستند را تحت نظر بگیرد. همچنین می تواند برای اینکه کاربر از تماس های گرفته شده به وسیله واتس آپ اطلاع پیدا نکند، داده های گوشی فرد را تغییر دهد و مخاطبین آن را اصلاح کند (Terpstra, 2013: 6.9).

این نقض حریم خصوصی در حالی است که این شبکه اجتماعی وعده های فراوانی برای حفظ اطلاعات کاربران داده بود. در سال ۲۰۱۴ که فیس بوک سهام واتس آپ را خریداری کرد، کمیسیون تجارت فدرال آمریکا به هر دو شرکت هشدار داد که وعده های خودشان را در حفظ داده های مشتریان اجرا کنند (Nili, 2014: 1).

این نقض حریم خصوصی کاربران کاری کاملاً غیراخلاقی بوده که همه مکاتب اخلاقی از جمله مکتب اخلاقی اسلام به آن اذعان دارد.

مسئله اصلی این مقاله در این بخش آن است که آیا به لحاظ اخلاقی، کاربران می توانند خود را به خطر انداخته و با آنکه می دانند چنین شبکه هایی از اطلاعات و ارتباطات آنها سوءاستفاده می کند، اطلاعات خود را فاش سازند؟ به بیان دیگر، آیا به لحاظ اخلاق اسلامی، کاربر حق دارد، خودافشاگری نماید؟ جواب کوتاه و روشن به این سؤال داد این است که از منظر اخلاق، خود را در بوته خطر انداختن از مصادیق اضرار به خود است و ضرر رساندن به خود امری ناپسند و غیراخلاقی است.

همچنان که قبلاً نیز گفته شد، بر طبق روایات در مورد حفظ اسرار دو جنبه وجود دارد؛ یک جنبه آن، نسبت به حفظ اسرار دیگران است و جنبه دیگر، در مورد حفظ اسرار خود است؛ به این معنا که افراد نسبت به اسرار خود باید بخیل باشند و آن را در معرض دیگران قرار ندهند. امام صادق ۷ می فرماید: «سِرُّكَ مِنْ دَمِّكَ فَلَا يَجْرِيَنَّ مِنْ غَيْرِ أَوْدَاجِكَ» (مجلسی، ۱۴۰۳، ج ۷۵: ۷۱)؛ راز تو، بخشی از خون توست، پس نباید در غیر رگ های جاری شود. از این حدیث شریف استفاده می شود، همان طور که جریان طبیعی خون در بدن باعث ادامه حیات است و چنانچه به جای جریان یافتن در رگ ها، به بیرون ریخته شود، منجر به مرگ می شود، اسرار انسان نیز این گونه است، اگر از دل خارج شود و در مجرای غیر طبیعی قرار گیرد، زندگی عادی انسان را متزلزل کرده، آبروی او را در معرض خطر جدی قرار می دهد (الهامی نیا، ۱۳۸۶: ۳۵).

بنابراین، کاربر نباید خود را در معرض از بین رفتن اسرارش قرار دهد و تا جایی که

می‌تواند از برنامه‌های امنیتی برای حفظ اطلاعات خود در مقابل گردانندگان شبکه‌ها استفاده کند و یا از برنامه‌های جایگزین دیگری استفاده کند. برای مثال، در ایران چندین شبکه اجتماعی مشغول فعالیت هستند لذا کاربر در صورت لزوم استفاده، باید از این نوع شبکه‌ها که امنیت‌شان بیشتر است، استفاده نماید.

علاوه بر کاربر، خانواده‌ها نیز باید کاربران را یاری کنند و با آموزش‌های خود و آگاه‌سازی کاربران، آنان را به مخاطرات این گونه شبکه‌ها آشنا کنند. همچنین دولت باید در این زمینه به کاربران کمک کند. دولت به دو شکل می‌تواند به کاربران کمک کند: اول، به صورت سلبی؛ که این مورد با فیلترینگ هوشمند مضامین غیراخلاقی، قابل دسترسی است و دوم، به صورت ایجابی؛ یکی از کارهایی که دولت به صورت ایجابی موظف به انجام آن است، راه‌اندازی اینترنت ملی است که راه نفوذ هکرها و بدافزارها و همچنین شرکت‌ها را سد می‌کند. همچنین از کارهای دیگر دولت در این زمینه، بالابردن سواد رسانه‌ای کاربران است که این وظیفه را می‌تواند از طریق آموزش و پرورش و دانشگاه‌ها دنبال کند.

### ۳- دولت‌های حاکم بر شبکه‌های اجتماعی

علاوه بر گردانندگان شبکه‌های اجتماعی، که عمدتاً پایگاه برون‌مرزی دارند، دولت‌ها نیز اشراف دارند. در ایران، نیروی انتظامی دو وظیفه عمده برای برخورد با مجرمین دارد؛ اولین وظیفه او، کشف جرم و دومین آن، جلوگیری از وقوع جرم است؛ در مورد کشف جرم، این وظیفه طبق بند هـ شق ۸ ماده ۴ قانون نیروی انتظامی جمهوری اسلامی علاوه بر دادرها، به عهده نیروی انتظامی نیز قرار داده شده است (آشوری، ۱۳۷۹: ۲۵۰) و جلوگیری از وقوع جرم نیز بر اساس بند د از شق ۸ همان ماده ۴، به عهده پلیس قرار داده شده است. مفهوم جلوگیری از وقوع جرم، عبارت است از: «مجموعه وسایل و ابزارهایی که دولت برای مهار بهتر بزهکاری از دو طریق حذف یا معدوم کردن عوامل جرم‌زا و اعمال مدیریت مناسب نسبت به عوامل محیطی و فیزیکی و اجتماعی که به نوبه خود فرصت‌هایی را برای ارتکاب جرم ایجاد می‌کنند، مورد استفاده قرار می‌دهند» (نجفی، ۱۳۸۱: ۷۴۸).

در شهریور سال ۱۳۹۳ رئیس پلیس فتا اعلام کرد: پیام‌های خصوصی در واتس‌آپ

قابل پیگیری است. این پیگیری، به خاطر توهین‌هایی که به مقدسات اسلامی، توسط افرادی در این شبکه شده بود، انجام گرفت. همچنین به علت کلاه‌برداری‌هایی که افراد سودجو از کاربران انجام داده بودند، پرونده آن‌ها در پلیس فتا پیگیری شد و تعدادی از این افراد با نفوذ پلیس به این شبکه دستگیر شده بودند. سؤال این است که آیا اخلاقاً پلیس می‌تواند به پروفایل کاربران نفوذ کند و اطلاعات و ارتباطات شخصی او را کنترل نماید یا خیر؟

بنابراین دو وظیفه‌ای که مأموران امنیتی دارند، باید برای کشف جرم و پیشگیری از وقوع جرم در شبکه‌های اجتماعی، به حریم خصوصی کاربران، تعرض کنند. این کار از یک طرف، برای صیانت از حقوق اجتماع و از دید امنیت اجتماعی و امنیت عمومی در مورد پیگیری و ردیابی مجرمین رایانه‌ای و تروریست‌ها، مانیتور کردن و رصد شبکه و داخل شدن در حریم خصوصی افراد اهمیت دارد و از طرف دیگر، این نظارت‌ها با مصالح زندگی شخصی و احترام به شخصیت و حریم خصوصی افراد و آزادی آن‌ها در تضاد است. ایجاد رابطه منطقی بین این دو هدف و رسیدن به مصالح اجتماعی و مصالح شخصی، بسیار اهمیت دارد. در اینجا، قوانین اخلاقی می‌تواند بسیار راهگشا باشد (شهریاری و خسروی، ۱۳۹۰: ۱۲۶). لذا این تراحم اخلاقی میان حفظ حریم خصوصی و حفظ امنیت کاربران بررسی می‌گردد.

در اینجا با دو مسئله اخلاقی روبه‌رو هستیم؛ از طرفی احترام به حریم خصوصی کاربر، امری اخلاقی است؛ هیچ کس حق ندارد به هیچ شکلی در حریم خصوصی او ورود کرده و اطلاعاتی از آن بیرون آورد ولی از طرفی دیگر، حفظ امنیت کاربران وظیفه اخلاقی نهادهای اطلاعاتی، امنیتی می‌باشد که این حفظ امنیت، جز با رصد کاربر و نقض حریم خصوصی تأمین نمی‌شود.

گاهی عملی از منظر اخلاقی به خوب و خوب‌تر یا بد و بدتر منتهی می‌شود؛ مانند همین مسئله که میان خوب (احترام به حریم خصوصی) و خوب‌تر (حفظ امنیت همه کاربران) ایجاد شده است. حل چنین مسائلی، نیاز به معرفتی خاص دارد. این معرفت از طریق نیروی عقل از درون فرد و نیروی نقل بر گرفته از وحی، عهده‌دار داوری در چنین مسائلی خواهد بود (جوادی آملی، ۱۳۹۱: ۳۳۹).

در سیره معصومین هم انتخاب خوب‌تر نسبت به خوب دیده می‌شود. برای مثال،

زکریای آدم می‌گوید: «بر امام رضا 7 وارد شدم و از آغاز شب پیوسته با من گفت و گو می‌کرد تا صبح شد و برخاست و نماز صبح به جای آورد. این داستان نشان می‌دهد با آنکه فضیلت نماز شب نزد امام 7 زیاد است ولی گفت و گوی دینی با مهمان خود را خوب‌تر دید، بدین جهت آن را ترجیح داد؛ البته امام معصوم، بهتر می‌داند کدام عبادت نزد خداوند محبوب‌تر است» (همان، ۳۴۱).

بنابراین، در تراحم اخلاقی میان احترام به حریم خصوصی و امنیت تمام کاربران، باید اهم نسبت به مهم برگزیده شود. در این مسئله، حفظ امنیت کاربران، اصل اخلاقی اهم است؛ به این خاطر که تمام افراد را مدنظر قرار می‌دهد و حتی برای همان فردی هم که حریم خصوصی‌اش شکسته، امنیت به بار خواهد آورد. لذا این اصل اولویت دارد. البته در اینجا دو نکته حائز اهمیت است که اولین نکته این است که نهادها تا جایی که امکان دارد باید به حریم خصوصی کاربران حرمت نهند و در جایی که هیچ راهی به جز ورود در حریم خصوصی ندارند، چنین مجوزی داده می‌شود. پس باید در ابتدا، راه‌های دیگر، امتحان شود و در صورت لزوم، به حریم خصوصی کاربران ورود کنند. و دوم آنکه، مجوز ورود به حریم خصوصی دیگران به این معنا نیست که اطلاعات افراد سرقت رود و در جایی بر علیه آن‌ها استفاده شود. مثلاً نمی‌شود اطلاعات به دست آورده را برای استخدام افراد در دولت لحاظ کرد بلکه این مجوز، بر اساس حفظ امنیت کاربران داده شده در صورتی که این موارد ذکر شده برخلاف حفظ امنیت کاربران است. لذا این مجوز اخلاقی، اطلاق ندارد و مقید به حفظ امنیت کاربر است.

### نتیجه‌گیری

شبکه‌های اجتماعی مانند واتس‌آپ، برنامه‌هایی هستند که کارکردهای مثبتی دارند که از آن جمله می‌توان: به دسترسی راحت، آسانی ارتباط، قابل حمل و کم‌هزینه بودن آن‌ها، اشاره کرد. ولی این شبکه‌ها، علاوه بر کارکردهای مثبت، آسیب‌هایی نیز به دنبال داشته‌اند، که تجاوز به حریم خصوصی کاربران، یکی از این آسیب‌هاست. واتس‌آپ به حریم خصوصی کاربران خود تجاوز کرده و با حفرة‌های موجود در خود، باعث شده کاربران دیگر نیز به راحتی بتوانند به حریم خصوصی کاربران نفوذ کنند. کاربران

باید بدانند اطلاعات و ارتباطات آنها به وسیله این شبکه اجتماعی به مخاطره افتاده است. در این مقاله با تمرکز بر اخلاق اسلامی، برخی از اصول اخلاقی حریم خصوصی، مانند: استیذان، ستاریت، رازداری، عدم تجسس، اصل انعکاس و همچنین پرهیز از ظلم، پرهیز از سرقت، پرهیز از آزار دیگران، مورد بحث قرار گرفته و این نتیجه به دست آمد که اخلاق اسلامی، علاوه بر اینکه تجاوز به حریم خصوصی کاربران شبکه‌های اجتماعی را توسط دیگران (کاربران دیگر، شرکت‌ها و دولت‌ها)، مصداق ظلم، آزار و اذیت، سرقت، ورود بدون اجازه و ... دانسته، حفظ اسرار و به خطر نینداختن خود را نیز، برای کاربر فضیلت می‌داند. لذا کاربران به لحاظ اخلاقی موظف‌اند تمام جوانب احتیاط را برای حفظ اطلاعات و ارتباطات خود انجام دهند. با توجه به اخلاق اسلامی، کاربران شبکه‌های اجتماعی برای صیانت از حریم خصوصی، وظایفی به عهده دارند، که به برخی، اشاره می‌گردد:

افراد نباید به سیستم دیگران نفوذ کنند؛ چرا که این کار مصداق ظلم، سرقت، آزار و اذیت، ورود بدون اجازه و غیره می‌باشد که هر یک از این مصادیق ردیلتی اخلاقی است؛ نباید عکس، فیلم و اطلاعات خصوصی افراد را بازنشر نمایند؛ باید اطلاعات و ارتباطات خود را مخفی نگه داشته و خود افشاگری ننمایند؛ در شبکه‌های اجتماعی به هر کسی اعتماد نکرده و ارتباط برقرار نکند؛ به اندازه نیاز خود از شبکه‌های اجتماعی استفاده کرده و از استفاده افراطی پرهیزند؛ باید تا می‌توانند از شبکه‌های اجتماعی جایگزین داخلی، به جای شبکه‌های اجتماعی مانند واتس‌آپ، استفاده کنند؛ خانواده‌ها با آگاهی بخشی به کاربران آنها را با خطرهای این شبکه‌ها آشنا کنند.

دولت نیز با فیلترینگ هوشمند مانع دسترسی به حریم خصوصی در شبکه‌های اجتماعی شود؛ با راه‌اندازی اینترنت ملی امنیت کاربران را حفظ کند؛ با آموزش سواد رسانه‌ای در مدارس و دانشگاه‌ها، راه مقابله بانفوذ شبکه‌های اجتماعی را آموزش دهند و در مواجهه با دو اصل اخلاقی، یعنی؛ حفظ امنیت کاربران و حفظ حریم خصوصی آنان، تا جایی که امکان دارد باید از تجاوز به حریم خصوصی کاربران دوری کنند. همچنین نباید از اطلاعات کاربران بر علیه آنها سوءاستفاده کنند.

## کتابنامه

### ✽ قرآن کریم

۱. آشوری، محمد (۱۳۷۹)، «گزارش کل همایش بین‌المللی مواد مخدر»، مجله: دانشکده حقوق و علوم سیاسی، دوره ۵۰.
۲. ابن طاووس، علی بن موسی (۱۳۷۶)، الاقبال بالاعمال الحسنه، تحقیق: جواد قیومی اصفهانی، قم: دفتر تبلیغات اسلامی.
۳. الهامی‌نیا، علی اصغر (۱۳۸۶)، اخلاق اطلاعاتی، ج ۱، قم: زمزم هدایت.
۴. ایران‌پور، پرستو (۱۳۹۱)، میزان سواد رسانه‌ای و نقش آن در استفاده از رسانه‌های تعاملی، پایان‌نامه کارشناسی‌ارشد، تهران: دانشکده علوم اجتماعی دانشگاه علامه طباطبائی.
۵. بادینر، آلن (۱۳۸۹)، «چگونه فیس‌بوک حریم خصوصی را از بین برده است»، مجله: سیاحت غرب، ش ۸۵.
۶. پاتر، جیمز (۱۳۹۱)، بازشناسی رسانه‌های جمعی با رویکرد سواد رسانه‌ای، ترجمه: امیر یزدیان، منادعلی و پیام آزادی، ج ۱، قم: مرکز پژوهش‌های صداوسیما.
۷. توحیدی، میرزا محمدعلی (۱۴۱۲ق)، مصباح‌الفقاهه (تقریرات آیت‌الله خویی)، ج ۲، بیروت: دارالهادی.
۸. جوادی آملی، عبدالله (۱۳۹۱)، مفاتیح‌الحیاه، ج ۱، قم: اسراء.
۹. حرعاملی، محمد بن حسن (۱۴۰۹ق)، وسائل‌الشیعه، ج ۳۰، قم: مؤسسه آل‌البیت ۷.
۱۰. خوانساری، محمد بن حسین (۱۳۶۶)، شرح غررالحکم و ذرر الکلم، ج ۷، تهران: دانشگاه تهران.
۱۱. سروش، محمد (۱۳۹۳)، اصول حریم خصوصی (بر اساس منابع اسلامی)، ج ۱، قم: پژوهشگاه حوزه و دانشگاه.
۱۲. شهریاری، حمید و آرش خسروی (۱۳۹۰)، «مزایا و چالش‌های هویت مجازی در فضای سایبر»، فصلنامه: ره‌آوردنور، ش ۵۲.

۱۳. طباطبایی، سیدمحمدحسین (۱۳۷۴)، المیزان فی تفسیرالقرآن، ج ۲۰، قم: دفتر انتشارات اسلامی.
۱۴. علم‌الهدی، عبدالرسول (۱۳۹۲)، مصادیق ارتباط عقیفانه در شبکه‌های اجتماعی سایبری، ج ۱، تهران: پژوهشگاه فرهنگ، هنر و ارتباطات.
۱۵. کاستلز، مانوئل (۱۳۸۰)، عصر اطلاعات: اقتصاد، جامعه و فرهنگ، ترجمه: احد علیقلیان، افشین خاک‌باز و علی پایا، ج ۱، تهران: طرح نو.
۱۶. کلینی، محمد بن یعقوب (۱۳۶۵)، الکافی، چاپ چهارم، ج ۸، تهران: دارالکتب‌الاسلامیه.
۱۷. مجلسی، محمدباقر (۱۴۰۳ق)، بحارالانوار، چاپ دوم، ج ۱۱۱، بیروت: دارالاضواء.
۱۸. مکارم شیرازی، ناصر (۱۳۷۷)، اخلاق در قرآن، ج ۳، قم: مدرسه الامام علی بن ابی طالب ۷.
۱۹. نجفی، علی حسین (۱۳۸۰)، تقریرات درس جرم‌شناسی: جرائم سازمان‌یافته، کارشناسی ارشد، تهران: دانشگاه شهید بهشتی.
۲۰. نراقی، محمد مهدی (۱۳۸۸)، جامع‌السعادات، ترجمه: کریم فیضی، ج ۲، قم: انتشارات قائم آل محمد.
21. Boyd, d.m, & Ellison, n.b (2007), "social network sites: Definition, history, and scholarship" Journal of computer\_ mediated communication, <http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html>.
22. Buchenscheit, Andreas & Könings, Bastian & Neubert, Andreas & Schaub, Florian & Schneider, Matthias & Kargl, Frank (2014), "Privacy Implications of Presence Sharing in Mobile Messaging Applications", [http://www.uniulm.de/fileadmin/website\\_uni\\_ulm/iui.inst.100/institut/Papers/Prof\\_Weber/2014.MUM\\_whatsapp-privacy.pdf](http://www.uniulm.de/fileadmin/website_uni_ulm/iui.inst.100/institut/Papers/Prof_Weber/2014.MUM_whatsapp-privacy.pdf).
23. Buttarelli, Giovanni (2015), "Privacy and Competition in the Digital Economy, [https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2015/15\\_01\\_21\\_speech\\_GB\\_EN.pdf](https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2015/15_01_21_speech_GB_EN.pdf).
24. Cross, Richard (2006), "Social Network Analysis: an introduction", Social Networking [http://www.bioteams.com/2006/03/28/social\\_network\\_analysis.html](http://www.bioteams.com/2006/03/28/social_network_analysis.html).
25. Church. Karen and Oliveira. Rodrigo (2013), "What's up with whatsapp?: Comparing mobile instant messaging behaviors with traditional SMS", In Proc. MobileHCI '13. ACM.

26. Lazer, David (2008), *Introduction To Social Network Analysis*, Director Program on Networked Governance Kennedy School of Government Harvard University.
27. Gattiker. E. & Perlusz. Stefano & Bohmann. Kristoffer & Morck Sorensen. Christian, (2001), *The virtual community: Building on social structure*, Relation and trust to achieve value, in in, *Community informatic reader*, edited by Keeble.L and Loader.B, London and New York, Routledg.
28. Hong. K (2014), “Whatsapp hits new record after handling 64 billion messages in one day, The Next Web, apr” <http://thenextweb.com/apps/2014/04/02/whatsapp-hits-new-record-handling-64-billion-messages-one-day>.
29. Landwehr.C.E and Heitmeyer.C.L and McLean.J.D (2011), *A security model for military message systems: Retrospective*, Naval Research Laboratory, Washington DC.
30. Nili, Yaron (2014), “Key Privacy Issues in M&A Transactions”, <http://corpgov.law.harvard.edu/2014/10/21/key-privacy-issues-in-ma-transactions>.
31. Shostack.A and Syverson.P (2004), *What price privacy, J. in Economics of Information Security*, The Netherland, Kluwer.
32. Terpstra, Martijn (2013), “WhatsApp & privacy”, [http://www.cs.ru.nl/bachelorscripties/2013/Martijn\\_Terpstra\\_0814962/WhatsApp\\_and\\_privacy.pdf](http://www.cs.ru.nl/bachelorscripties/2013/Martijn_Terpstra_0814962/WhatsApp_and_privacy.pdf).
33. Walther, J. B. & Ramirez, Jr. A (2009), “New technologies and new direction in online relating”. In S. Smith, & S. Wilson (Eds.), *New directions in interpersonal communication* (pp. 264-284). Thousand Oaks, CA: Sage.
34. <http://www.itna.ir/vdcccpi.2bq4181aa2.html> ۱۳۹۳/۱۲/۱۱ آخرین بازدید
35. <http://www.borhan.ir/NSite/FullStory/News/?Id=7470>، ۱۳۹۳/۰۵/۲۲ آخرین بازدید