Jurisprudence and legal studies of media Journal
VOL. 5 / Autumn 2023 and Winter 2024 / NO. 2 (Serial 10)

Abuse of personal Data by social networks And solutions to resolve it

Ali Saatchi (Ph.D.)[1] 0000-0000-0000-0000
Seyed Alireza Rezaee (Ph.D.)[2] 0000-0000-0000-0000
Ali Javadi[3] 0000-0000-0000-0000

Abstract

Social networks have shaped a major part of our lives today. In addition to benefits for societies, this phenomenon has also brought disadvantages. One of these important problems is breach of users' privacy in social networks. Social networks have access to the data and information of many of their users, who can use that information for different purposes. Therefore, it is necessary to protect the information and privacy of the users more than before. The main question is whether collecting, categorizing and selling users' information in social networks is a breach of their privacy? And what solutions are there to deal with it? In this article, using the analytical descriptive research method, the above issue has been investigated. Finally, this article has reached the conclusion that the use of users' information by social networks is a breach of users' privacy, and it is not possible to accept all conditions when users register in social networks as the user's consent to use their data. Therefore, it is necessary to regulate the use of user information in social networks and prevent further misuse of user information. In this regard, there are three main solutions (regulation, self-regulation and tax collection). It is not effective to use only one method to protect users' data. it is recommended to use a combination of the aforementioned methods, but the most effective method in this regard is to impose a tax on social networks and spend these amounts to develop digital security and protect users' data and compensation for damages. In Iran, due to the existence of a legal gap, in order to protect users' data, a law should be approved to protect users and their information in social networks.

Keywords: Privacy, Internet, Advertising, Self-Regulation.

1- Assistant Professor of Private Law Department, Faculty of Law and Political Sciences, Ferdowsi University of Mashhad, Mashhad, Iran alisaatchi@um.ac.ir
2- PhD of Private Law, Faculty of Law and Political Sciences, Ferdowsi University of Mashhad, Mashhad, Iran alirezarezaee4771@mail.um.ac.ir
3- MS of Public Law, Faculty of Law, Shahid Beheshti University, Tehran, Iran ali.javadi74@gmail.com

[DOI: 10.22034/5.2.119]

دوفصلنامه
مطالعات فقه و حقوق رسانه
دانشکده غیردولتی – غیرانتفاعی رفاه

دوره ۵، شماره ۲ (پیاپی ۱۰)
پاییز و زمستان ۱۴۰۲
صص: ۱۱۹-۱۴۷

سوءاستفاده از داده‌های شخصی توسط شبکه‌های اجتماعی و راهکارهای مقابله با آن

علی ساعتچی[۱]
سیدعلیرضا رضایی[۲]
علی جوادی[۳]

نوع مقاله: پژوهشی
تاریخ دریافت: ۱۴۰۲/۰۹/۱۴
تاریخ پذیرش: ۱۴۰۳/۰۱/۱۸

چکیده

شبکه‌های اجتماعی بخش عمده از زندگی امروز ما را شکل داده‌اند. این پدیده در کنار فواید برای جوامع، معایبی نیز به همراه داشته است. یکی از این معضل‌های مهم، عدم رعایت حریم خصوصی کاربران در شبکه‌های اجتماعی است. شبکه‌های اجتماعی به داده‌ها و اطلاعات بسیاری از کاربران خود دسترسی دارند که می‌توانند از آن اطلاعات در جهت اهداف مختلف استفاده نمایند. ازاین‌رو حفظ اطلاعات و حریم خصوصی مخاطبان بیش از گذشته ضرورت می‌یابد. سؤال اصلی آن است که آیا جمع‌آوری، دسته‌بندی و فروش اطلاعات کاربران در شبکه‌های اجتماعی نقض حریم خصوصی آنان نیست؟ و چه راهکارهایی برای مقابله با آن وجود دارد؟ در این مقاله، با استفاده از روش تحقیقی توصیفی تحلیلی، موضوع فوق بررسی شده است. درنهایت مقاله حاضر به این نتیجه نائل آمده است که استفاده از اطلاعات کاربران توسط شبکه‌های مجازی نقض حریم خصوصی کاربران است و نمی‌توان به صورت مطلق، پذیرفتن تمامی شروط هنگام ثبت‌نام کاربران در شبکه‌های اجتماعی را به معنای رضایت کاربر مبنی بر انتشار داده‌های خود دانست؛ لذا باید به نحوی استفاده از اطلاعات کاربران در شبکه‌های اجتماعی را ضابطه‌مند کرده و از سوءاستفاده‌های بیشتر اطلاعات کاربران جلوگیری نمود. در این خصوص سه راهکار اصلی (وضع قانون، خودتنظیمی و اخذ مالیات) وجود دارد. به کار بستن صرفاً یک روش در خصوص حمایت از داده‌های کاربران مؤثر نیست بلکه استفاده ترکیبی از روش‌های مذکور، پیشنهاد می‌شود؛ اما مؤثرترین روش در این راستا وضع مالیات بر شبکه‌های اجتماعی و صرف این مبالغ در جهت توسعه امنیت دیجیتال، حمایت از داده‌های کاربران و جبران خسارات وارده است. در ایران نیز به‌دلیل وجود خلأ قانونی، جهت حمایت از داده‌های کاربران، قانون متناسب با حمایت از کاربران و اطلاعات ایشان در شبکه‌های اجتماعی تصویب شود.

کلمات کلیدی

حریم خصوصی، اینترنت، تبلیغات، خودتنظیمی، شبکه‌های اجتماعی.

۱ـ استادیار گروه حقوق خصوصی، دانشکده حقوق و علوم سیاسی، دانشگاه فردوسی مشهد، مشهد.
alisaatchi@um.ac.ir
۲ـ دکتری حقوق خصوصی، دانشکده حقوق و علوم سیاسی، دانشگاه فردوسی مشهد، مشهد (نویسنده مسئول).
alirezarezaee4771@mail.um.ac.ir
۳ـ کارشناسی ارشد حقوق عمومی، دانشکده حقوق، دانشگاه شهید بهشتی تهران، تهران. ali.javadi74@gmail.com

[DOI: 10.22034/5.2.119]

مقدمه

امروزه به‌سختی می‌توان شخصی را پیدا کرد که به‌نحوی از اینترنت و شبکه‌های اجتماعی استفاده نکند. اینترنت امروزه با گسترش دسترسی افراد به اطلاعات گام بلندی را در جهت رشد و شکوفایی افراد جامعه و تسهیل برخورداری افراد از برخی حقوق خود نظیر آزادی بیان، حق دسترسی به اطلاعات، آزادی تجارت و حق مشارکت در امور عمومی برداشته‌اند و افراد با دسترسی و استفاده از اینترنت می‌توانند به سهولت از برخی خود خود بهره‌مند شوند *(انصاری و عطار، ۱۴۰۲، ص.۱۹)*. شرکت‌های ارائه‌کننده شبکه‌های اجتماعی یا سایر خدمات مرتبط با اینترنت، عمدتاً خدمات خود را به رایگان در اختیار کاربران قرار می‌دهند. در این شرایط نمی‌توان منکر این واقعیت شد که شرکت‌های عرضه‌کننده خدمات اینترنتی من‌جمله شبکه‌های اجتماعی، شرکت‌های تجاری هستند و شرکت‌های تجاری هدفشان کسب سود است. حال مسئله این است این شرکت‌ها در شرایطی که خدمات رسمی خود را به‌صورت رایگان عرضه می‌کنند، راه‌های مختلفی جهت کسب درآمد برای شبکه‌های اجتماعی وجود دارند و یکی از اصلی‌ترین منابع درآمدی این شبکه‌ها، جمع‌آوری و تجمیع اطلاعات کاربران خود و درنهایت، فروش اطلاعات به شرکت‌های تبلیغاتی است. درواقع آنان با دسته‌بندی کاربران بر اساس جنسیت، مذهب، سن، علایق و ... می‌توانند به شرکت‌های تبلیغاتی اطلاعات مرتبط با نیازهای هر کاربر و تبلیغات مورد نیاز او را بدهند. این داده‌ها برای شرکت‌های تبلیغاتی نیز مفید است؛ زیرا می‌توانند با تبلیغات هدفمند، و هر کالا یا خدمت را صرفاً به دسته خاصی از مخاطبان که به تهیه آن تمایل دارند، عرضه کنند.

رعایت حریم خصوصی و حفظ اطلاعات کاربران امری است که در بسیاری از معاهدات حقوق بشری بین‌المللی بر آن تأکید شده است. طبق این معاهدات مداخله در زندگی خصوصی، خانواده، اقامتگاه و مکاتبات افراد ممنوع است و صرفاً در مورد ضروری و به‌دلایلی نظیر جلوگیری از بی‌نظمی یا ارتکاب جرم یا حفاظت از امنیت ملی، امنیت عمومی یا رفاه اقتصادی کشور، بهداشت و اخلاقیات، حقوق و آزادی‌های دیگران می‌توان با مجوز قانون و در چهارچوب آن به‌صورت محدود و موردی حریم خصوصی

[DOI: 10.22034/5.2.119]

افراد را نقض کرد.[۱]

حال سؤال اینجاست که آیا جمع‌آوری، دسته‌بندی و فروش اطلاعات کاربران در شبکه‌های اجتماعی نقض حریم خصوصی آنان نیست؟ آیا می‌توان پذیرفت که پذیرفتن «تمامی شرایط شرکت‌های ارائه‌کننده خدمات» هنگام عضویت در شبکه‌های اجتماعی به‌معنای رضایت کامل کاربران در انتشار و فروش اطلاعات ایشان است؟ و درنهایت آیا می‌توان راهکاری جهت حمایت از داده‌های کاربران در شبکه‌های اجتماعی پیشنهاد داد؟

در این مقاله تلاش شده است که ابتدا نحوه جمع‌آوری اطلاعات کاربران در شبکه‌های اجتماعی و اشکال مختلف استفاده از آن توضیح داده شود. سپس مقررات حقوق ایران و اتحادیه اروپا در حمایت از اطلاعات کاربران شرح داده شود و درنهایت نیز راهکارهایی جهت حمایت بیشتر از داده‌های کاربران، ارائه گردد.

۱. جمع‌آوری اطلاعات کاربران و نحوه استفاده از آن‌ها توسط شبکه‌های اجتماعی

در عصر گسترش اطلاعات، کاربران اطلاعات خود را در شبکه‌های اجتماعی منتشر می‌کنند؛ اما ممکن است به این نکته توجه نکنند که با به‌اشتراک‌گذاری اطلاعات خود در یک موضوع خاص، نظیر حضور در مهمانی دوستانه شب گذشته، علاوه بر دنبال‌کنندگان، داده‌های خود را به‌صورت غیرمستقیم با شرکت‌های تبلیغاتی نیز به‌اشتراک می‌گذارند. درواقع هر فعالیت کاربر، اطلاعاتی را جهت فروش در اختیار شبکه‌های اجتماعی قرار می‌دهد. ممکن است هر شخص به‌طور روزمره، عکس‌های خود را در شبکه‌های اجتماعی نظیر اینستاگرام یا فیس‌بوک منتشر کند و همراه با آن به مکان محل عکس نیز اشاره کند. بعد از مدتی همان شخص با یک تبلیغ از هتل یا رستوران از محل انتشار عکس در همان شبکه اجتماعی یا در شبکه‌های اجتماعی دیگر روبه‌رو می‌شود. مسئله‌ای که در اینجا وجود دارد این است که شبکه‌های اجتماعی اجتماعی شرکت‌های اقتصادی هستند و

۱. ماده ۱۷ میثاق بین‌المللی مدنی و سیاسی و ماده ۸ کنوانسیون حمایت از حقوق بشر و آزادی‌های اساسی رم مصوب ۱۹۵۰.

[DOI: 10.22034/5.2.119]

اگرچه که از کاربران خود مبلغی را دریافت نمی‌کنند؛ اما با فروش اطلاعاتی که کاربران در اختیار آنان می‌گذارند، کسب درآمد می‌کنند. ازاین‌رو با توجه به اینکه شبکه‌های اجتماعی اطلاعات کاربران خود را جهت استفاده تبلیغاتی در اختیار شرکت‌های تبلیغاتی قرار می‌دهند، جای تعجب نیست که میان تبلیغات انبوه در شبکه‌های اجتماعی، تبلیغ مذکور برای کاربر انتخاب‌شده است؛ زیرا که شرکت‌های تبلیغاتی با استفاده از داده‌های کاربران نیازهای کاربران را می‌دانند و تبلیغ مناسب با هر کاربر را نشان می‌دهند (*Dembrow, 2022, p. 325*).

بعد از ایجاد حساب کاربری در یک شبکه اجتماعی، کاربران با شرایط و ضوابط آن شبکه اجتماعی به‌طور کامل موافقت می‌کنند. همچنین در برخی شبکه‌های اجتماعی نظیر فیس‌بوک، کاربر اختیارات خاصی به شبکه اجتماعی در خصوص رعایت حریم خصوصی خود نظیر امکان جمع‌آوری اطلاعات برای شبکه اجتماعی، تجمیع این اطلاعات با کاربران مشابه و فروش آن اطلاعات به شرکت‌های تبلیغاتی می‌دهد؛ لذا کاربران با عضویت در فیس‌بوک، تأیید شرایط عضویت و نصب نرم‌افزار فیس‌بوک بر تلفن همراه خود، اجازه استفاده از اطلاعات خود را در زمینه‌هایی مثل منطقه زمانی، اپراتور تلفن همراه، زبان و موقعیت مکانی به فیس‌بوک می‌دهند. همچنین در شبکه اجتماعی اینستاگرام، کاربر ضمن ثبت‌نام در این شبکه، به‌طور کامل می‌پذیرد که تمامی تصاویر و ویدئوهای آنان، توسط شرکت‌های تبلیغاتی قابل‌استفاده و دریافت است. کاربران گاهی تصاویر خصوصی خود را در اینستاگرام منتشر می‌کنند، درحالی‌که، نسبت به انتشار عمومی آن رضایت ندارند؛ اما بنا به شرایط عضویت در این شبکه اجتماعی، اینستاگرام از این اطلاعات جهت اهداف تبلیغاتی خود استفاده می‌کند *(Dembrow, 2022, pp.325-326)*.

شبکه‌های اجتماعی معمولاً برای جمع‌آوری و استفاده از اطلاعات کاربران از «الگوریتم‌ها»[1] استفاده می‌کنند. الگوریتم‌ها، ساختارهایی هستند که برای حل مشکلات یا تکمیل برخی کارها استفاده می‌شوند. الگوریتم‌ها با دریافت داده‌های خام، آنان را مرحله‌به‌مرحله بر اساس چهارچوب‌های طراحی‌شده خاص، پردازش کرده و نتیجه را ارائه

1. Algorithm

[DOI: 10.22034/5.2.119]

می‌دهند. هیچ شخص یا سازمانی نمی‌تواند تمامی داده‌های خام کاربران شبکه‌های اجتماعی را استخراج نماید و بعد از آن به حجم انبوهی از سؤال‌ها در خصوص سن، جنسیت، علایق و سایر اطلاعات مربوط به کاربران پاسخ دهد و آنان را بنا به ویژگی‌های مختلف دسته‌بندی نماید. در این شرایط دستگاه‌های رایانه‌ای جهت پردازش داده‌های خود از الگوریتم‌ها کمک می‌گیرند *(Bucher, 2018, pp.20-21)*؛ به‌عبارت‌دیگر می‌توان گفت، الگوریتم یک ابزار فنی است که شبکه‌های اجتماعی برای رتبه‌بندی پیام‌ها بر اساس میزان اهمیتشان از آن بهره‌مند می‌شوند. در فضای اینترنت و شبکه‌های اجتماعی، کاربران با نحوه فعالیت خود نظیر: جستجوی واژه‌های مختلف، تعیین اولویت‌ها و علایق، محتوای محبوب و مناسب خود را مشخص می‌کنند؛ سپس الگوریتم مطالب و اطلاعات مورد پسند کاربر را به وی پیشنهاد می‌دهند. در این شرایط، کاربران محتوی موردعلاقه خود را سریع‌تر و راحت‌تر پیدا می‌کنند و این امر باعث استفاده روزافزون از شبکه‌های اجتماعی می‌شود؛ به‌عنوان‌نمونه، الگوریتم اینستاگرام با کسب اطلاعات از نحوه فعالیت کاربر، پست‌ها و استوری‌های مورد علاقه هر شخص را در ابتدا به او نشان می‌دهد. الگوریتم‌ها همواره در حال یادگیری بوده و با استفاده از اطلاعات جدید، توسعه و بهبود پیدا می‌کنند؛ به‌عبارت‌دیگر، آنان طی فرایند خود ایستا و ثابت نیستند بلکه بر اساس فعالیت‌های کاربران، بهبود پیدا می‌کنند *(Hunt & McKelvey, 2019, pp.309-310)*. علاوه‌براین، مهم‌ترین استفاده از الگوریتم‌ها در مسائل تبلیغاتی است. الگوریتم‌ها با استفاده از ارزیابی رفتارهای کاربران در شبکه اجتماعی، بررسی می‌کنند که آن‌ها کدام موضوعات را می‌پسندد؛ سپس شبکه‌های اجتماعی با کنترل جریان محتوایی، اطلاعات را به‌گونه‌ای طبقه‌بندی می‌کنند که مطابق با اهداف تبلیغاتی آن‌ها باشد. بدین نحو که ابتدا پستی را به کاربر نشان می‌دهند که کالای مشابه آن جهت خرید و استفاده در بازار یا همان شبکه اجتماعی موجود باشد. بدین‌صورت، شبکه‌های اجتماعی با فروش اطلاعات کاربران یا ایجاد دسترسی شرکت‌های تجاری به الگوریتم‌ها درآمدزایی می‌کنند (*Tiwaria, 2023, pp.1043-1044*). شبکه‌های اجتماعی این‌گونه ادعا می‌کنند که کاربران با پذیرفتن شرایط عضویت در شبکه اجتماعی، در واقع نسبت به تمامی داده‌های جمع‌آوری شده و نقض حریم خصوصی خود رضایت دارند. با

[DOI: 10.22034/5.2.119]

این استدلال و با جمع‌آوری و فروش اطلاعات کاربران، شرکت‌های حوزه فناوری اطلاعات ظرف دو دهه به یکی از ثروتمندترین شرکت‌های دنیا تبدیل‌شده‌اند (*Dembrow, 2022, p.326*). شبکه‌های اجتماعی به طرق مختلف از داده‌های حاصل از الگوریتم‌های خود استفاده می‌کنند و می‌توانند آن اطلاعات را در اختیار شرکت‌های تبلیغاتی قرار دهند. با جمع‌آوری داده‌های تعداد زیادی از افراد و دسته‌بندی اطلاعات بر اساس هر گروه خاص، شبکه‌های اجتماعی می‌توانند این اطلاعات را جهت اهداف تجاری بفروشند؛ مثلاً ممکن است کاربری در این طبقه‌بندی اطلاعات به‌عنوان طرفدار تیم فوتبالی خاص یا به‌عنوان طرفدار نوع خاصی از غذا شناخته شود، در این‌صورت تبلیغات مرتبط با آن به وی نمایش داده می‌شود. به‌طور کلی هر شبکه اجتماعی که استفاده از آن رایگان است، فروش و استفاده از اطلاعات و داده‌های افراد را به‌عنوان اصلی‌ترین هدف خود قرار می‌دهد. این استفاده از اطلاعات هم شامل داده‌های عمومی نظیر سرگرمی‌ها یا تفریحات. هم شامل اطلاعات شخصی نظیر اسم، تاریخ تولد، آدرس آی پی، جنسیت و... می‌شود. استفاده رایگان از شبکه‌های اجتماعی، سازندگان آن را به انبوهی از اطلاعات ارزشمند می‌رساند که می‌توانند از آن اطلاعات در راستای مشاوره برای تولید و عرضه کالاها و خدمات جدید استفاده کنند (*Tiwaria, 2023, pp.1044-1045*).

شبکه اجتماعی با داشتن اطلاعات کاملی از هر شخص، می‌تواند تبلیغاتی مخصوص هر کاربر را به او نشان دهد. این تبلیغات می‌تواند بر اساس ترجیحات، سابقه جست‌وجو یا موقعیت مکانی هر فرد شخصی‌سازی شوند. در این شرایط هدف یک تبلیغ، تحت‌تأثیر قرار دادن خود شخص است. شرکت‌های تجاری علاقه بسیاری به یادگیری یا خرید اطلاعات مربوط به مشتریان و رفتارهای آنان در شبکه‌های اجتماعی دارند؛ به‌عنوان‌نمونه، شبکه‌های اجتماعی می‌توانند با رهگیری اینکه یک کاربر چگونه از یک خدمت خاص استفاده می‌کند، برنامه‌ریزی بهتری جهت بازاریابی محصول انجام دهند. یکی از ابزارهای شبکه‌های اجتماعی، جهت کسب اطلاعات از کاربران خود استفاده از نظرسنجی‌های مکرر است. شبکه های اجتماعی با انجام نظرسنجی در زمینه‌های مختلف از کاربران خود، اطلاعات مختلفی در زمینه‌های سلایق، عادت‌ها و... کسب می‌کنند که

[DOI: 10.22034/5.2.119]

درنهایت آن اطلاعات را جهت اهداف بازاریابی و فروش استفاده می‌کنند (*Hunt & McKelvey, 2019, p.322*).

در هنگام تجزیه و تحلیل داده‌های مختلف از فرهنگ‌ها و گروه‌های مختلف، الگوریتم‌ها نیز متفاوت عمل می‌کنند؛ مثلاً می‌توان با ارائه برنامه‌ای خاص به نرم‌افزارها، دسترسی به نوع خاصی از هنر یا دانش را در یک منطقه خاص محدود کرد یا آن را صرفاً در اختیار یک منطقه خاص قرار داد. اعمال الگوریتم‌های مختلف هم می‌تواند دارای اثرهای مثبت باشد و هم اثرهای منفی داشته باشد. بسیاری از مواقع، الگوریتم‌ها به‌منظور افزایش آگاهی نسبت به موضوعی خاص توسعه می‌یابند. درنتیجه برخی کاربران ممکن است متوجه افزایش پست‌ها در آن موضوع خاص، نظیر موضوع‌های سیاسی یا فیلم‌ها یا سایر موارد در شبکه اجتماعی خود شوند. از طرفی‌دیگر یکی از معایب الگوریتم‌ها این است که ممکن است موجب شود که محتوای حساسیت‌برانگیزی بارها و بارها در شبکه‌های اجتماعی تکرار شود یا بخشی از اطلاعات دور از دسترس کاربران قرار بگیرد یا اینکه آنان را در مواجهه با اطلاعات ناقصی قرار دهد. در این شرایط الگوریتم‌ها از اطلاعات فردی کاربران برای فهم اینکه چه محتوایی باید در شبکه اجتماعی نمایش داده شود، استفاده می‌کنند که همه این امور نقض حریم خصوصی کاربر و استفاده از داده‌های او را در پی دارد (*Tiwaria, 2023, pp.1046-1047*). از طرف‌دیگر، شبکه‌های اجتماعی با در دسترس قرار دادن بخش زیادی از اطلاعات مرتبط، عملاً باعث ایجاد محدودیت کاربران نسبت به دسترسی به سایر داده‌ها و کسب اطلاعات ناقص توسط کاربران می‌شوند. الگوریتم‌ها با ایجاد محدودیت در شبکه‌های اجتماعی، محتوای موجود را رتبه‌بندی می‌کنند که معمولاً این رتبه‌بندی بر مبنای اولویت‌های درآمدزایی شبکه‌های اجتماعی است. الگوها و نحوه برنامه‌نویسی الگوریتمی تعیین می‌کند که در هر موضوع خاص چه محتوایی و از چه شخص یا شرکتی باید دیده شود. این موضوع تحت عنوان تبعیض الگوریتمی[1] در شبکه‌های اجتماعی مطرح می‌شود. تبعیض الگوریتمی در یک معنای عام به‌معنای اعمال تبعیض دستگاه‌های مختلف بین اشخاص مختلف در اختصاص

1. Algorithmic discrimination

[DOI: 10.22034/5.2.119]

امکانات به آنان است. این روش در سطوح پایین‌تر بین گزینه‌های مختلف، گزینش و غربال‌گری می‌کند و در سطوح بالاتر ممکن است جایگزین نیروهای انسانی شده و تصمیم‌گیری نیز نماید *(انصاری، ۱۴۰۱، ص.۱۵۲)*؛ اما تبعیض الگوریتمی در شبکه‌های اجتماعی به این معناست که موتورهای جست‌وجو، عمدتاً بر اساس ویژگی‌های کاربر نظیر جنسیت، مذهب، ملیت، زبان و... و نیز اطلاعاتی که از کاربر در طی مدت فعالیتش به دست آورده‌اند، در هنگام جست‌وجوی وی در شبکه های اجتماعی مواردی را پیشنهاد داده و برخی گزینه‌ها را نیز حذف می‌کنند. مطلوبیت این امر از آن جهت است که موتورهای جست‌وجو به کمک کاربران می‌آیند و مواردی که برای آنان مناسب‌تر است را به ایشان پیشنهاد می‌دهند؛ اما از طرف‌دیگر چون این اقدام با حذف دسته‌ای از اطلاعات، موجب عدم امکان جست‌وجوی آزاد کاربران می‌شود، انتخاب‌ها و فرصت‌های کاربران را محدود می‌کند. علاوه‌براین، شبکه های اجتماعی می‌توانند به وسیله تبعیض الگوریتمی، یک جریان خاصی را در سطح جامعه ایجاد کرده و یا مانع از ایجاد آن شوند؛ لذا تبعیض الگوریتمی با حق دسترسی آزاد کاربر بر اطلاعات و منع سانسور در تعارض است (*Hunt & McKelvey, 2019, pp.342-343*).

۲. مقررات قانونی جهت حفاظت از اطلاعات کاربران در شبکه‌های اجتماعی

به‌دلیل استفاده گسترده از شبکه‌های اجتماعی و تجارت‌های برخط، اهمیت حفاظت از داده‌های خصوصی افراد بیش‌ازپیش نمایان شده است. نگرانی‌های زیادی بابت جمع‌آوری، استفاده و به‌اشتراک‌گذاری اطلاعات شخصی کاربران، بدون آگاهی و رضایت آنان وجود دارد. فارغ از مقررات و قواعد عامی که در خصوص حمایت از حریم خصوصی کاربران وجود دارد، برخی کشورها نظیر کشورهای حوزه اتحادیه اروپا و ایران تلاش کردند که حفاظت از داده‌های کاربران را در چهارچوب قواعد مشخصی سازمان‌دهی نمایند.

[DOI: 10.22034/5.2.119]

۲-۱- مقررات قانونی اتحادیه اروپا

اتحادیه اروپا یکی از اولین سازمان‌های بین‌المللی است که به حمایت از داده‌های شخصی افراد توجه ویژه‌ای داشته است. ابتدا با تصویب «کنوانسیون اروپایی حقوق بشر» در سال ۱۹۵۰حق بر حمایت از داده‌های شخصی افراد در ماده ۸ کنوانسیون مذکور حمایت شده است و پس از آن نیز در آرای متعدد دیوان اروپایی حقوق بشر و در «کنوانسیون شورای اروپا در حمایت از داده‌های شخصی» به حفاظت از داده‌های شخصی افراد تاکید شده است *(انصاری و دیگران، ۱٤۰۱، ص.۲۲)*. مقررات عمومی اتحادیه اروپا راجع به حمایت از اشخاص در برابر پردازش داده های شخصی[1] (GDPR) مجموعه‌ای قواعد هستند که نحوه دریافت، جمع‌آوری و تحلیل و بررسی داده‌های کاربران در اتحادیه اروپا و خارج از آن را مدیریت می‌کند. بعد از تصویب قانون در ۲۰۱٦، فرایند اجرای قانون در سطح اتحادیه اروپا شروع شد که درنهایت پس از دو سال، قانون مذکور به طور کامل در سطح اتحادیه اروپا اجرایی شد. این قانون در تلاش است که با پاسخگو کردن شرکت‌های تجاری در مورد نحوه مدیریت و رفتار داده‌های کاربران، از استفاده خودسرانه از اطلاعات کاربران در شبکه‌های اجتماعی جلوگیری کند. هر شبکه اجتماعی‌ای که بازدیدکننده‌ای از اروپا داشته باشد، فارغ از اینکه مقر اصلی شرکت در اروپا است یا خیر، ملزم به رعایت این قانون است، حتی اگر کالا یا سرویس مشخصی را در محدوده اروپا ارائه ندهد. مقررات این قانون فارغ از اینکه مقر اصلی شبکه‌های اجتماعی در کجاست، برای تمامی ۲۷ عضو اتحادیه اروپا و منطقه اقتصادی اروپا جاری خواهد بود. به‌عنوان نتیجه، این مقررات باید توسط هر شبکه اجتماعی‌ای که بازدیدکنندگانی در اروپا دارد رعایت شود حتی اگر هدف، فروش کالاها در شبکه اجتماعی در اروپا نباشد؛ حتی این مقررات برای کاربرانی که تابعیت کشوری در اتحادیه اروپا را ندارند؛ اما در یکی از کشورهای عضو زندگی می‌کنند نیز جاری خواهد بود و همانند سایر شهروندان اروپایی از داده‌های آنان حفاظت خواهد شد (*Hoofnagle & others, 2019, p.10*).

این قانون از برخی حقوق اشخاص در برابر شبکه‌های اجتماعی نظیر حق دریافت

1 General Data Protection Regulation

[DOI: 10.22034/5.2.119]

اطلاعات در خصوص داده‌های شخصی، دسترسی به داده‌های شخصی، تصحیح و حذف داده‌های شخصی، درخواست محدودیت پردازش، حق انتقال داده، اعتراض به پردازش و عدم قرار گرفتن در معرض تصمیمات خودکار به رسمیت شناخته و از آنان حمایت کرده است *(لطیف‌زاده و دیگران، ۱۴۰۲، ص.۹۸۳)*. در این قانون برخی حقوق کاربران برای حفاظت از اطلاعات شخصی‌شان در شبکه‌های اجتماعی به‌رسمیت شناخته‌شده است، اشخاص بر مبنای حق دریافت اطلاعات، باید از هرگونه پردازش اطلاعات شخصی‌شان، علت و هدف آن مطلع شوند و بنا به حق دسترسی به داده‌های شخصی و حق بر اصلاح و حذف داده‌ها، کاربران باید به تمامی اطلاعات خود در شبکه‌های اجتماعی دسترسی داشته باشند؛ همچنین درصورتی‌که بخواهند باید بتوانند اطلاعات خود را اصلاح یا حذف نمایند. علاوه‌براین به علت اینکه گاهی اطلاعات کاربران اطلاعات حساس است یا به هر دلیلی کاربران علاقه‌ای به پردازش اطلاعات خود ندارند، آنان می‌توانند به استناد حق بر محدودیت پردازش اطلاعات، در مورد امکان تغییر اطلاعات، محدودیت ایجاد کنند. درصورتی‌که اطلاعات کاربران در هنگام پردازش مورد سوءاستفاده قرار گیرد، کاربران می‌توانند بر این پردازش اطلاعات اعتراض نمایند و درنهایت، گاهی شبکه‌های اجتماعی برخی درخواست‌های کاربران را به صورت خودکار و با الگوریتم‌های خاص خود پردازش می‌کنند و پاسخ می‌دهند که در این شرایط کاربران به علت ماهیت خاص برخی درخواست‌ها، می‌توانند تقاضا کنند که درخواست آنان توسط انسان‌ها بررسی و پاسخ داده شود *(لطیف‌زاده و دیگران، ۱۴۰۲، ص.۱۰۰۱)*.

۲-۲- مقررات حقوق ایران

در ایران حمایت از اطلاعات کاربران در شبکه‌های اجتماعی در مجموعه‌ای از قوانین پراکنده آمده است. هیچ‌کدام از قوانین موجود در ایران جامع نیستند و نمی‌توانند شامل تمامی مصادیق استفاده از داده‌های کاربران در شبکه‌های اجتماعی شوند. ازاین‌روی در جهت حمایت از داده‌های کاربران و در خصوص لزوم رعایت حریم خصوصی باید ابتدا به مبانی فقهی و اصول کلی حقوقی استناد کرد و سپس در قوانین مختلف به جست‌وجوی موارد مورد حمایت قانون‌گذار از داده‌های کاربران پرداخت.

[DOI: 10.22034/5.2.119]

حریم خصوصی تعریف واحدی در متون فقهی و حقوقی ندارد و برخی حریم خصوصی را تعریف کرده‌اند و برخی دیگر به بیان مصادیق آن اکتفا کرده‌اند. در متون فقهی، تعریف مشخصی از حریم خصوصی بیان نشده است و صرفاً به برخی از مصادیق آن نظیر چاه، چشمه، خانه و... پرداخته شده است و اشخاص غیرمالک از دخالت در آن نهی شده‌اند *(ولی‌پور، ۱۳۹۷، ص.۸٦)*. باوجوداین برخی تلاش کرده‌اند که تعریفی از حریم خصوصی ارائه دهند؛ مثلاً برخی محققان، حریم خصوصی را به‌عنوان قسمتی از زندگی انسان که مصون از تعرض دیگران است تعریف کرده‌اند *(جعفری و رهبرپور، ۱۳۹٦، ص.٤٦)* و بعضی دیگر آن را قلمرویی از اطلاعات و دارایی‌های هر فرد می‌دانند که سایر افراد نوعاً و عرفاً بدون اجازه مالک امکان استفاده و بهره‌برداری از آن را ندارند *(اکبری و فلاحیان، ۱٤۰۰، ص.۳٦٤)*. در راستای حمایت از داده‌های کاربران، در مبانی فقهی باید به حمایت شارع از حریم خصوصی اشاره نمود.

از نظر فقهی بر مبنای حدیثی از پیامبر اکرم(ص) که غیبت را به یادکردن برادر دینی نسبت به آنچه که برای او ناخوشایند است، تعریف کرده‌اند، می‌توان گفت مصادیق حریم خصوصی بیش از آنکه نوعی باشد، شخصی است. این امر به این معناست که هر شخص می‌تواند برخی حیطه‌های زندگی شخصی خود را حریم خصوصی خود اعلام کند و در این صورت سایر اشخاص بدون اجازه فرد مجاز به دخالت در حریم خصوصی او نیستند *(شهباز قهفرخی، ۱۳۹٤، ص.۹۷)*. با توجه به شخصی بودن مصادیق حریم خصوصی در متون فقهی، قاعده مشخصی که بر مبنای آن از حریم خصوصی حمایت شود، وجود ندارد؛ اما حمایت از برخی مصادیق حریم خصوصی را می‌توان از منابع فقهی و فتاوای فقها استخراج کرد. تجسس در لغت به‌معنای جست‌وجوی خبرهای پنهانی است *(واعظی و همتی فارسانی، ۱۳۹۵، ص.۱٦۲)* و در اصطلاح به‌معنای جست‌وجوی عیب‌های پنهانی مردم جهت آگاهی از امور ناپسند و پنهانی آنان است *(واعظی و همتی فارسانی، ۱۳۹۵، ص.۱٦۳)*. از نظر آیات قرآن کریم در برخی آیات مؤمنین از تجسس در مورد دیگران منع شده‌اند.[۱] بر مبنای نظر مفسرین این ممنوعیت، ظهور در حکم حرمت دارد و بر این مبنا هرگونه

۱. آیه ۱۲ سوره حجرات

[DOI: 10.22034/5.2.119]

تجسس در امور زندگی اشخاص حرام و ممنوع است *(واعظی و همتی فارسانی، ۱۳۹۵، ص.۱٦٦)*. بر اساس نظر مفسران از این آیه مسلمانان باید در زندگی روزمره خود، رفتار ظاهری افراد را ملاک و مبنا قرار دهند و در جست‌وجوی عیوب مردم نباشند *(واعظی و همتی فارسانی، ۱۳۹۵، ص.۱٦۷)*. در برخی دیگر از آیات قرآن کریم به موضوع ممنوعیت تجسس به صراحت اشاره نشده است؛[1] اما به زشتی و ممنوعیت اشاره فحشا میان اهل ایمان اشاره دارد. بر اساس نظر برخی از محققین به‌صورت کلی شایع شدن فحشا در سطح جامعه نتیجه جاسوسی و تفتیش است و در با توجه به حرمت مقدمه حرام، می‌توان با توجه به حرمت اشاعه فحشا، تفتیش و جاسوسی را که مقدمه اشاعه فحشاست را حرام و ممنوع دانست *(واعظی و همتی فارسانی، ۱۳۹۵، صص.۱٦۷-۱٦۸)*. در برخی دیگر از آیات برخی مصادیق تجاوز به حریم خصوصی افراد ممنوع شناخته شده است[2]؛ به‌عنوان‌نمونه برخی آیات به ممنوعیت ورود به منزل و نقض حریم خصوصی موضوع اشاره دارند. بر اساس این آیات، داخل شدن در منازل دیگران بدون اذن آنان ممنوع است. بر این مبنا می‌توان نتیجه گرفت هنگامی که ورود به منزل افراد بدون اذن آنان ممنوع است، پس به طریق اولی جاسوسی و تجسس از منازل و عیوب و اعمال دیگران نیز ممنوع خواهد بود *(واعظی و همتی فارسانی، ۱۳۹۵، ص.۱٦۹)*. ممنوعیت عدم تجسس بحث بسیار گسترده‌ای است. منع تجسس شامل منع انتشار هرگونه داده و اطلاعات پنهان از اشخاص می‌شود. در خصوص این ممنوعیت فرقی میان اینکه این تجسس با چه هدفی صورت بگیرد نیست؛ البته بنا به نظر برخی فقها این آیه صرفاً در خصوص منع تجسس در اموری است که باعث خواری مؤمنان و از دست رفتن حیثیت اجتماعی آنان شود *(حدادپور، ۱٤۰۱، ص.٤٦)*. در روایات نیز مصادیقی در خصوص ممنوعیت دخالت در حریم خصوصی افراد وجود دارد؛ به‌عنوان‌مثال در روایتی از پیامبر اکرم(ص)، شکستن حریم خصوصی افراد در منزل منع شده است یا ایشان از گوش دادن به گفتگوهای افراد در شرایطی که فرد راضی به این اقدام نیست منع فرموده‌اند یا حضرت علی(ع) در نامه خود به مالک اشتر بر لزوم

---

۱. آیه ۱۹ سوره نور

۲. آیه ۲۷ و ۲۸ سوره نور

[DOI: 10.22034/5.2.119]

پوشـــاندن عیوب مردم تأکید می‌کنند *(حدادپور، ۱٤۰۱، صـص.٤٦-٤٧)*. عقل انســـان نیز از یک طرف هرج‌ومرج و فساد در جامعه را قبیح می‌داند و از طرف‌دیگر پخش و افشای آنچه را که سـبب خواری مؤمنان اسـت، مذموم می‌داند. آنچه که در این شـرایط واضـح اسـت آن است که یکی از امور زمینه‌ساز فساد در جامعه، تجسس در حریم خصوصی افراد است. پس می‌توان گفت تجســس در امور مردم با توجه به مقدمه امور مفســده‌برانگیز بودن از نظر عقل نیز ممنوع اســـت *(واعظی و همتی فارســـانی، ۱۳۹۵، ص.۱۷٤-۱۷۵)*. علاوه‌براین بنای عقلای عالم نیز عدم دخالت در حریم شـخصـی افراد اسـت. در این زمینه فرقی میان اینکه این دخالت آثار زیان بار داشـته باشـد یا نداشـته باشـد نیسـت *(نعیمی، ۱۳۹٤، ص.۱۱۷)*. به تبعیت از آیات، روایت و حکم عقل، در آرای فقهی نیز ممنوعیت برخی مصـــادیق خاص از نقض حریم خصـوصـی وجود دارد. این ممنوعیت تا حدی اسـت که برخی در خصـوص حرمت دیدن غیر مجاز خانه افراد، لزوم حفظ اسـرار و عیوب مردم ادعای اجماع نموده‌اند *(حدادپور، ۱٤۰۱، ص.٤۷)*.

از نظر قانونی، قانون اســـاســـی جمهوری اســـلامی ایران در هیچ‌یک از اصـــول خود به‌صـراحت حق حفظ حریم خصـوصـی را به رسـمیت نشـناخته است بلکه از برآیند اصـول مختلف قانون اسـاسـی می‌توان به حمایت قانون‌گذار از برخی مصـادیق حریم خصـوصـی پی برد. در برخی اصـول قانون اسـاسـی به مصـادیقی از رعایت حریم خصـوصـی نظیر حریم خلوت و تنهایی، حریم مکانی، حریم اطلاعات، حریم ارتباطـات و حـــریم جســـمانی اشـاره شـده اسـت[۱] *(واعظی و علی‌پور، ۱۳۸۹، صـص.۱۳۸-۱۳۹)*. باوجوداین، حریم خصـوصـی به‌عنوان یک اصل و یکی از حقوق مردمی صراحتاً به‌رسمیت شناخته نشده است. همچنین حفظ حریم خصـوصـی در رسـانه‌ها نیز در قانون اسـاسـی مورد بحث قرار نگرفته اسـت. تنها در اصـل ۲٤ قانون اسـاسـی به آزادی اطلاعات و رسـانه‌ها اشـاره‌شـده اسـت و موارد استثنا را «عـدم اخـلال بـه مبـانی اسـلام »و «عـدم اخـلال در حقـوق» دانسته که به‌نظر می‌رسـد اسـتفاده شـبکه‌های اجتماعی از داده‌های کاربران ذیل هیچ‌یک از اسـتثناهای این

۱. اصول ۱۹، ۲۰، ۲۲، ۲۳، ۲٤، ۲۵، ۲٦، ۲۷، ۲۸، ۳۰، ۳۲، ۳۳، ۳۵، ۳۸، ۳۹، ٤۰ و ٤۲ قانون اساسی جمهوری اسلامی ایران.

[DOI: 10.22034/5.2.119]

اصل قرار نگیرد. تنها در اصل ۲۵ قانون اساسی به حمایت از حریم خصوصی در حوزه ارتباطات پرداخته شده است *(واعظی و علی‌پور، ۱۳۸۹، ص.۱٤۲)*. با توجه به ماهیت خاص استفاده از اطلاعات در شبکه‌های اجتماعی، این امر ذیل ممنوعیت موجود در این اصل قرار نمی‌گیرد. در قوانین عادی ایران نیز به بحث حمایت از داده‌های شخصی افراد توجه شده است در خصوص موضوع داده‌های شخصی افراد، در قانون تجارت الکترونیکی مصوب ۱۳۸۲ داده‌پیام‌های شخصی را به داده‌پیام‌های یک شخص حقیقی مشخص و معین تعریف کرده است که از این نظر این تعریف مشابه تعاریف موجود در اسناد اروپایی از مفهوم داده‌پیام است. علاوه‌براین در بند ب ماده ۱ قانون انتشار و دسترسی آزاد به اطلاعات مصوب ۱۳۸۷ برخی مصادیق نظیر نام و نام خانوادگی، نشانی محل سکونت و محل کار، وضعیت زندگی و خانوادگی، عادت‌های فردی، ناراحتی‌های جسمانی، شماره حساب بانکی و رمز عبور از مصادیق داده‌های شخصی دانسته شده است *(انصاری، ۱٤۰۲، صص.۳٤-۳۵)*.

در این تعاریف صرفاً برخی مصادیق داده‌های شخصی ذکر شده است و در آن معیاری که از آن طریق بتوان داده‌های شخصی را از داده‌های عمومی منفک کرد وجود ندارد. ازاین‌رو در جهت حل این ابهام‌ها کمیسیون انتشار و دسترسی آزاد به اطلاعات، در تصویب‌نامه خود تحت عنوان «شیوه نامه تشخیص و تفکیک اطلاعات مربوط به حریم خصوصی و اطلاعات شخصی از اطلاعات عمومی» داده‌های شخصی را به هفت دسته داده‌های هویتی، داده‌های مکانی، داده‌های اقتصادی، داده‌های سلامت، داده‌های ارتباطی، داده‌های اعتقادی و سیاسی و داده‌های استخدامی تقسیم نموده و برخی از مصادیق اهم آن را نیز ذکر کرده است و از این طریق با تفکیک داده‌های شخصی به عمومی و غیرعمومی، دسترسی به داده‌های شخصی عمومی را برای شهروندان مجاز دانسته است. طبق تصریح شیوه نامه مذکور داده‌هایی که یا توسط خود فرد منتشر شده باشد یا هویت افراد موجود در آن معلوم نباشد، داده‌های خصوصی یا شخصی محسوب نمی‌شوند *(انصاری، ۱٤۰۲، ص.۳۵)*.

داده‌های شخصی در قوانین ایران نیز در قانون تجارت الکترونیک و برخی دیگر از قوانین حمایت شده‌است. قانون تجارت الکترونیک را می‌توان قانونی عام دانست که از آن

[DOI: 10.22034/5.2.119]

طریق قانون از تمامی داده‌های افراد در فضای مجازی اعم از اینکه مرتبط با فضای تجارت الکترونیک یا ابزارهای ارتباطی جدید باشد یا نباشد، حمایت می‌کند و شامل تمامی داده‌هایی که با ابزارهای الکترونیک مختلف توسط تمامی اشخاص حقیقی و حقوقی رد و بدل می‌شود، می‌گردد *(زند، ۱۴۰۱، صص.۲۸-۲۹)*؛ مثلاً ذخیره، پردازش و یا توزیع داده‌پیام‌های شخصی که نشان‌دهنده ریشه‌های قومی و نژادی یا دیدگاه‌های کاربر در زمینه‌های مختلف نظیر دیدگاه‌های سیاسی و عقیدتی یا خصوصیت اخلاقی یا جسمی کاربران باشد، ممنوع است.[۱] علاوه‌براین «ذخیره داده‌پیام‌ها» را صرفاً در صورت مشخص بودن اهداف ذخیره، ضروری بودن ذخیره و تناسب میزان ذخیره با میزان ضرورت، صحیح و روزآمد بودن، دسترسی کاربر به اطلاعات ذخیره‌شده و امکان اصلاح اطلاعات توسط کاربر مجاز دانسته شده است.[۲]

موضوع جرائم اینترنتی و سایبری ذیل مواد ۷۲۹ تا ۷۸۵ قانون تعزیرات و مجازات بازدارنده آمده است. در این قانون موضوعات و جرائم مختلف اینترنتی بحث و بررسی شده است؛ اما موضوع جمع‌آوری داده‌های کاربران و انتشار آنان جز در موضوع‌های محدودی نظیر داده‌های سری و محرمانه بحث نشده است.[۳] تنها موضوعی که می‌توان از آن در جهت حمایت از داده‌های کاربران کمک گرفت، ماده ۷۴۵ قانون مذکور است. طبق این ماده هرکس 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 یا جزای محکوم خواهد شد. در نظریه مشورتی ۷/۱۴۰۱/۷۰ مورخ ۱۴۰۱/۰۴/۲۴ در خصوص تعیین مصادیق تصاویر یا فیلم‌های خصوصی در ماده ۷۴۵ قانون مذکور، تصاویر خصوصی را آن دسته از تصاویری می‌داند که به‌صورت عمومی منتشر نشده باشد و افشای آن تصاویر بدون اعلام رضایت کاربر، موجب ضرر و هتک

---

۱. ماده ۵۸ قانون تجارت الکترونیک مصوب ۱۳۸۲.

۲. ماده ۵۹ قانون تجارت الکترونیک مصوب ۱۳۸۲.

۳. مواد ۷۳۱ تا ۷۳۳ قانون تعزیرات و مجازات‌های بازدارنده مصوب ۱۳۷۵.

[DOI: 10.22034/5.2.119]

حرمت او شود.

قانون مجازات اسلامی در خصوص حمایت از داده‌های کاربران در شبکه‌های اجتماعی دارای مشکلات زیر است: اولاً؛ کما اینکه در نظریه مشورتی بیان شده است: ماده ۷۴۵ قانون مجازات اسلامی (تعزیرات) در خصوص اطلاعات خصوصی و محرمانه کاربران است. این در حالی است که بسیاری از داده‌هایی که شبکه‌های اجتماعی جمع‌آوری می‌کنند، داده‌های عمومی افراد است و آنان خود با اختیار و پذیرش شرایط عضویت در شبکه اجتماعی، آن را منتشر می‌کنند. ثانیاً؛ جریمه اختصاص‌یافته برای انتشار داده‌های خصوصی افراد، در مقایسه با سودی که شبکه‌های اجتماعی از جمع‌آوری، تجمیع و انتشار داده‌های کاربران خود می‌برند، بسیار ناچیز است. ثالثاً؛ بنا به ادعای شبکه‌های اجتماعی، کاربران در ابتدای عضویت خود شرایط و ضوابط عضویت در شبکه‌های اجتماعی را می‌پذیرند، پس نمی‌توان گفت رفتار شبکه‌های اجتماعی در این خصوص، بنا به رضایت کاربرانشان نیست. رابعاً؛ در این ماده ورود ضرر و زیان به شخصی که اطلاعات او افشاشده است، شرط است. حال سؤال اینجاست که آیا جمع‌آوری اطلاعات کاربران در شبکه‌های اجتماعی و استفاده از آنان جهت مصارف تبلیغاتی، ورود ضرر و زیان به کاربر محسوب می‌شود؟ کما اینکه عمدتاً شبکه‌های اجتماعی این ادعا را دارند که با جمع‌آوری اطلاعات کاربران می‌توانند شناخت دقیق‌تری از آنان داشته باشند و درنتیجه محتوای مناسب‌تری را در اختیار کاربران قرار دهند. درنهایت با توجه به موارد مذکور به نظر می‌رسد که قانون فعلی نتواند مانعی بر راه استفاده از داده‌های کاربران در شبکه‌های اجتماعی باشد.

با توجه به موارد فوق به‌نظر می‌رسد که منابع فقهی و قوانین مذکور نمی‌توانند به‌طور کامل مشکل استفاده‌های شبکه‌های اینترنتی از داده‌های کاربران را حل نمایند؛ زیرا در خصوص منابع فقهی، هیچ اشاره صریحی به لزوم احترام به حریم خصوصی و ممنوعیت نقض آن نشده است و همچنین آیات و روایات در قالب احکام تکلیفی و نه احکام وضعی از حریم خصوصی حمایت کرده‌اند. درنتیجه اگرچه مسئولیت نقض‌کننده حریم خصوصی ذیل احکام تکلیفی قرار می‌گیرد؛ اما آن را باید از احکام تکلیفی استخراج کرد. یکی از دلایل

[DOI: 10.22034/5.2.119]

این امر می‌تواند این باشد که آیات و روایات، بیشتر جنبه مذهبی و اخلاقی دارند تا جنبه حقوقی و در نتیجه آن تحمیل مسئولیت بر عهده نقض‌کننده قابل استناد باشد *(انصاری، ۱۳۸۳، صص.۱۲-۱۳)*.

در خصوص قانون تجارت الکترونیک نیز به‌نظر می‌رسد، اولاً علی‌رغم حمایت از داده‌پیام‌های شخصی افراد، در خصوص اطلاعاتی که کاربران در هنگام ثبت‌نام در شبکه‌های اجتماعی در اختیار آنان می‌گذارند، حکمی بیان نشده است. ثانیاً شبکه‌های اجتماعی عمدتاً ادعا می‌کنند که کاربر در ابتدای ثبت‌نام در شبکه اجتماعی شرایط و ضوابط دسترسی شبکه اجتماعی را پذیرفته است و لذا جهت جمع‌آوری و پردازش داده‌های خود رضایت دارد. در قانون تجارت الکترونیک به این موضوع پرداخته نشده است و صرفاً به اعلام رضایت صریح کاربر اکتفا شده است. این در حالی است که در قوانین بسیاری از کشورها در خصوص اطلاعات حساس کاربران، شبکه‌های اجتماعی موظف‌اند که از کاربر مجدداً اخذ اجازه نمایند. ثالثاً در این قانون در خصوص مسئولیت شبکه‌های اجتماعی مبنی بر تقویت سیستم ایمنی داده‌های خود صحبتی نشده است. فرض کنیم درصورتی‌که اطلاعات بخشی از کاربران به علت ضعف سیستم ایمنی شبکه اجتماعی هک شود، باید بتوان علاوه بر هکرها، شبکه اجتماعی را به علت ضعف در سیستم ایمنی خود مسئول دانست *(قناد و علیقلی، ۱۳۹۹، ص.۳۱۷)*.

۳.راهکارهای پیشنهادی جهت حفاظت از اطلاعات کاربران در شبکه‌های اجتماعی

با عنایت به تعریف حریم خصوصی، مقررات اتحادیه اروپا و ایران، با توجه به اینکه کاربران در ابتدای عضویت خود در شبکه‌های اجتماعی، رضایت خود را جهت استفاده از اطلاعات توسط شبکه‌های اجتماعی اعلام می‌کنند. به‌نظر می‌رسد که در یک قاعده کلی استفاده شبکه‌های اجتماعی از داده‌های کاربران در چهارچوب توافق‌نامه اولیه، نقض حریم خصوصی کاربران نیست؛ اما باوجوداین به‌نظر می‌رسد بنا به‌دلایل زیر علی‌رغم این رضایت اولیه، نمی‌توان رضایت کامل کاربران را در انتشار داده‌های خصوصی خود

[DOI: 10.22034/5.2.119]

را احراز نمود و بدین‌وسیله تمامی مصادیق استفاده از اطلاعات کاربران را مجاز دانست. اولاً در خصوص احراز اراده واقعی کاربر در این زمینه ابهام وجود دارد؛ زیرا هیچ قطعیتی وجود ندارد که هویت کاربران هنگام ثبت‌نام و پذیرش شروط ثبت‌نام و رعایت حریم خصوصی، با هویت کاربری که حساب کاربری در اختیار اوست و از آن استفاده می‌کند یکسان باشد. ممکن است در هنگام ثبت‌نام بنا به دلایل مختلف، شخصی دیگری ثبت‌نام کرده است و حساب کاربری خود را در اختیار کاربر فعلی قرارداد داده باشد (*Schwartz & Wilde, 1979, p. 630*). این ابهام در زمانی نیز بیشتر می‌شود که بسیاری از شبکه‌های اجتماعی شروط مرتبط با ثبت‌نام و رعایت حریم خصوصی خود را به زبان انگلیسی در صفحه ثبت‌نام قرار داده‌اند؛ اما بسیاری از کاربران ایشان به این زبان مسلط نیستند و نمی‌توانند به‌صورت دقیق و کامل شرایط مربوط به حریم رعایت حریم خصوصی را مطالعه نمایند. درنتیجه با توجه به موارد مذکور، پذیرفتن این موضوع که همیشه کاربران با اراده واقعی شرایط مربوط به حریم خصوصی را می‌پذیرند دارای ابهام و تردید است.

ثانیاً در شرایط فعلی و گسترش روزافزون شبکه‌های اجتماعی، عضویت در شبکه‌های اجتماعی به امری ضروری تبدیل شده است. به‌نحوی‌که عدم عضویت در یک یا چند شبکه اجتماعی زندگی روزمره شهروندان را دچار اختلال می‌کند. ازاین‌روی نمی‌توان عضویت کاربران با اراده واقعی و آزاد و بدون هیچ فشار محیطی‌ای در شبکه‌های اجتماعی را پذیرفت.

ثالثاً کاربران در هنگام پذیرفتن شرایط عضویت در شبکه‌های اجتماعی و رعایت حریم خصوصی، به نحوی مجبورند که تمامی شرایط را قبول کنند و امکان مذاکره و چانه‌زنی در خصوص شرایط برای کاربران وجود ندارد. ازاین‌رو این قراردادها در حالت کاملاً منصفانه خارج شده و در وضعیت تردید نسبت به منصفانه یا غیرمنصفانه بودن، قرار می‌گیرند *(ابهری و فلاح خاریکی، ۱۳۹۹، ص.۱۷؛ کاظم‌پور، ۱۳۸۹، ص.۱٤٥)*. با توجه به این تردید و امکان غیرمنصفانه بودن شروط شبکه‌های اجتماعی، ماده ٤٦ قانون تجارت الکترونیکی اعمال شروط غیرمنصفانه در قراردادهای الکترونیکی به ضرر مصرف‌کننده را صحیح

[DOI: 10.22034/5.2.119]

نمی‌داند. در این شـرایط با توجه به اینکه اراده آزاد کاربر وجود ندارد و منصـفانه بودن شروط مذکور مورد تردید است، دولت‌ها وظیفه دارند که با بررسی شروط مذکور، شبکه اجتماعی را ملزم به اعمال شـــروط منصـــفانه نمایند. همچنین دادگاه‌ها نیز می‌توانند در هنگام رسیدگی به پرونده‌های شکایت نقض حریم خصوصی کاربران توسط شبکه‌های اجتماعی به غیرمنصفانه بودن آن توجه نمایند.

با توجه به موارد مذکور به‌نظر می‌رســـد که اگرچه که در شـــرایط آزادانه و برابر پذیرفتن تمامی شرایط عضویت و رعایت حریم خصوصی توسط کاربران نقض حریم خصوصی آنان نیست و پذیرفتن «تمامی شرایط شرکت‌های ارائه‌کننده خدمات» هنگام عضـویت در شـبکه‌های اجتماعی به معنای رضـایت کامل کاربران در انتشـار و فروش اطلاعات ایشان است؛ اما با توجه به برابر نبودن طرفین در هنگام عضویت در شبکه‌های اجتماعی باید شـروط اعمال شـده منصـفانه باشـد و در غیراین‌صـورت انتشـار و فروش داده‌های کاربران نقض حریم خصوصی آنان است و صحیح نیست. ازاین‌روی نیاز است که دولت‌ها اقدامات مختلفی را در جهت حمایت از داده‌های کاربران انجام دهند.

جمع‌آوری و فروش اطلاعات کاربران، درآمد هنگفتی را برای شـبکه‌های اجتماعی به همراه دارد و به علت ماهیت تخصصی شبکه‌های اجتماعی، کشف این موارد دشوار است و به‌راحتی نمی‌توان از جمع‌آوری اطلاعات کاربران جلوگیری کرد؛ لذا جهت حفاظت از اطلاعات کاربران در شبکه‌های اجتماعی، قواعد سنتی مربوط به «حفظ حریم خصوصی» کفایت نمی‌کند و باید مقررات و راهکارهای متناسب با اوصاف شبکه‌های اجتماعی اتخاذ گردد.

با توجه به اهمیت بالای شـبکه‌های اجتماعی در زندگی روزمره جوامع کنونی، نمی‌توان ممنوعیت کلی برای اسـتفاده از اطلاعات کاربران توسـط شـبکه‌های اجتماعی وضـع نمود. بهترین رویکرد آن است که استفاده شبکه‌های اجتماعی از اطلاعات کاربران ضابطه‌مند و دارای قواعد مشـخص باشد. دراین‌راستا، صـرف وضـع قانون و مجازات اسـتفاده‌کنندگان از داده‌های خصـــوصـــی کاربران شـــبکه‌های اجتماعی کافی نیســـت. در ادامه مهم‌ترین راهکارهای پیشـنهادی جهت نظام‌مند کردن اسـتفاده از شـبکه‌های اجتماعی و حفظ حریم خصوص افراد مورد مداقه و بررسی قرار می‌گیرند.

[DOI: 10.22034/5.2.119]

۳-۱- اخذ مالیات از داده‌ها

یکی از راهکاری حفاظت از اطلاعات کاربران در شبکه‌های اجتماعی آن است که بابت استفاده تبلیغاتی از این‌گونه اطلاعات، مالیات از شبکه‌های اجتماعی اخذ شود. برخی از محققان، جهت انتشار اطلاعات کاربران، مالیاتی در حدود ۰.۸ تا ۱ درصد را پیشنهاد کرده‌اند. بدیهی است که هر شخصی بابت درآمد خود باید مالیات بپردازد و شبکه‌های اجتماعی نیز باید بخشی از درآمد خود، بابت فروش اطلاعات کاربران را به‌عنوان مالیات هزینه کنند. با توجه به درآمد بالای فروش داده‌های کاربران در شبکه‌های اجتماعی، دریافت این میزان مالیات، مبلغی معقولانه برای شبکه‌های اجتماعی است. همان‌طور که سابقاً بیان گردید، امکان سوءاستفاده از داده‌های کاربران توسط شبکه‌های اجتماعی همیشه وجود دارد. دریافت مالیات، این امکان را به دولت‌ها می‌دهد که در صورت سوءاستفاده شبکه‌های اجتماعی از داده‌های کاربران از محل مبالغ دریافتی، خسارت واردشده به کاربران را جبران نمایند. طبق گزارش لس‌آنجلس تایمز، صنعت فروش اطلاعات کاربران در سال ۲۰۱۹ حدود ۲۰۰ میلیارد دلار درآمد داشته است که با اخذ ۱ درصد مالیات از آن حدود ۲ میلیارد دلار درآمد برای کشورها ایجاد می‌شود. مبلغ مذکور می‌تواند برای حفاظت از اطلاعات کاربران در شبکه‌های اجتماعی و جبران خسارات وارد به آن‌ها هزینه شود. درواقع با توجه به این که منبع اصلی درآمد شبکه‌های اجتماعی از طریق فروش اطلاعات کاربران است؛ پس می‌توان گفت مبلغ مالیات پرداخت شده در این روش امری فراتر از مالیات‌های پرداختی شرکت‌ها نخواهد بود؛ اما در این روش بیان می‌شود که مالیات پرداختی شرکت‌ها می‌بایست در راستای حفاظت از داده‌های کاربران، تقویت امنیت شبکه‌ها و جبران خسارات وارده به افراد از طریق فروش اطلاعات شخصی آنان مصرف شود (*Dembrow, 2022, p. 337*).

نقدی که به راهکار مذکور وارد می‌شود آن است که مقر اصلی شبکه‌های اجتماعی در کشوری مشخص است و مالیات مذکور توسط همان کشور دریافت می‌شود؛ اما مخاطبان شبکه‌های اجتماعی در تمام دنیا حضور دارند و نمی‌توانند از مالیات دریافتی بهره‌مند شوند؛ به‌عنوان‌مثال مقر اصلی اینستاگرام در کشور ایالات متحده آمریکا است و اگر

[DOI: 10.22034/5.2.119]

مخاطبی که در ایران حضـور دارد از افشـای اطلاعات خود خسـارت ببیند، نمی‌تواند از مالیات‌های پرداختی شـبکه اجتماعی مذکور بهره‌مند شـود. در این شـرایط و با فقدان یک نظام مالیات جهانی، کاربران مسـتقر در کشـورهای دیگر چگونه می‌توانند از این مالیات سـود ببرند؟ در این شـرایط سـایر کشـورها نیز بر آن شـبکه اجتماعی قدرت و تسـلطی ندارند که امکان دریافت مالیات برای آن‌ها وجود داشـته باشـد. همچنین اطلاعاتی که در اختیار شـبکه‌های اجتماعی اسـت، کالاهای اعتباری هسـتند که کاربران از سـرتاسـر دنیا آن‌ها را در اختیار این شـبکه‌های اجتماعی قرار می‌دهند؛ لذا اخذ مالیات در هنگام ارائه اطلاعات ممکن نیسـت؛ زیرا اطلاعات کاربران کالای فیزیکی نیسـت که بتوان در هنگام تحویل کالا از آن مالیات اخذ نمود. علاوه‌براین، حتی اگر کشـور مقر شـبکه‌های اجتماعی بر اسـتفاده آن‌ها از داده‌ها مالیات وضـع کند، آن شـبکه اجتماعی به‌راحتی می‌تواند محل اصلی فعالیت خود را به کشور دیگری که مالیات کمتری دارد، منتقل کند (*Dembrow, 2022, pp.337-338*).

با توجه به ایراد فوق، به‌نظر می‌رسد که نمی‌توان از مبالغ مالیاتی دریافتی از شبکه‌های اجتماعی، برای جبران مؤثر خسارات وارده به کاربران بهره برد؛ زیرا مخاطبان شبکه‌های اجتماعی بین‌المللی هسـتند؛ اما سـاختار مالیاتی بین‌المللی وجود ندارد؛ البته باید توجه داشـت که دولت دریافت‌کننده مالیات می‌تواند از این مبالغ جهت نظارت بر عملکرد شبکه‌های اجتماعی و تأمین بودجه سازمان‌های ناظر استفاده کند.

۳-۲- استانداردهای حفاظت از اطلاعات

یکی از راه‌های حفاظت از داده‌های کاربران، قانون‌گذاری در سـطح داخلی و بین‌المللی اسـت. با توجه به رشـد روزافزون شـبکه‌های اجتماعی، قانون‌گذاری روش مناسـبی برای جلوگیری از سـوءاسـتفاده از اطلاعات کاربران اسـت. برای قانون‌گذاری و اجرای سـیاسـت‌های حفاظت از داده‌ها، دو رویکرد حداکثری و حداقلی وجود دارد. در رویکرد حداکثری، تمامی اقدام‌های شـبکه‌های اجتماعی موضـوع مقررات تنظیمی قرار می‌گیرد. به علت ماهیت پویای شـبکه های اجتماعی و توسـعه هر روزه آنان، اعمال این رویکرد به دلیل اینکه نمی‌تواند همه ابعاد فعالیت‌های شـبکه‌های اجتماعی را دربرگیرد، عملاً

[DOI: 10.22034/5.2.119]

امکان‌پذیر نبوده و از طرفی در برخی موارد مقررات وضع شده کارایی خود را از دست خواهند داد. علاوه‌براین، در قوانین باید منافع تمامی طرفین درگیر در نظر گرفته شود و وضع قانون سخت‌گیرانه بدون توجه به منافع شبکه‌های اجتماعی، منجر به برهم خوردن تعادل در قانون می‌شود. به همین دلیل به‌نظر می‌رسد، اتخاذ رویکرد حداقلی مؤثرتر است. به این معنا که محدوده حداقلی رعایت حریم خصوصی و جمع‌آوری و فروش داده‌های کاربران تعیین شود و استفاده از داده‌های کاربران در خارج از آن چهارچوب، تنها با اخذ رضایت از کاربران در هنگام عضویت در شبکه اجتماعی مجاز باشد.

در وضع قوانین مربوط به حفاظت از اطلاعات کاربران، باید به چند ملاحظه اصلی توجه نمود:

۱. یکی از دغدغه‌های اصلی در هنگام وضع قوانین، رعایت حریم خصوصی کاربران در شبکه‌های اجتماعی است. فارغ از بحث حمایت از حریم خصوصی کاربران در هنگام استفاده از شبکه اجتماعی، نحوه طرح دعوی کاربران علیه شبکه‌های اجتماعی به‌صورت انفرادی یا از طریق دادستان همچنان مسئله با اهمیتی است. در صورت تجویز طرح دعوای شخصی علیه شبکه‌های اجتماعی، دعاوی زیادی در دادگستری مطرح می‌شود که رسیدگی به آن‌ها دشوار است. در صورت عدم تجویز اقامه دعوای شخصی نیز ممکن است حق داشتن حریم خصوصی و دادرسی اشخاص نقض شود و امکان طرح دعوا منتفی گردد. در این شرایط، قوانین مختلف روش‌های مختلفی را پیش گرفته‌اند؛ مثلاً در مقررات حریم خصوصی مشتریان در کالیفرنیا (CCPA) [1] در خصوص طرح دعوی در موضوعات دسترسی غیرمجاز، نفوذ، سرقت یا افشای اطلاعات شخصی رمزگذاری نشده کاربران، این امکان را به آنان می‌دهد که ابتدا دعوای خود را نزد همان شبکه اجتماعی مطرح کنند و در صورت عدم حل موضوع ظرف ۳۰ روز، امکان طرح دعوا نزد مراجع قضایی را خواهند داشت.

۲. در هنگام تصویب قوانین مرتبط بر حفظ حریم خصوصی کاربران، دغدغه شرکت‌های تجاری نیز باید مورد بررسی قرار بگیرد. منبع اصلی درآمد شبکه‌های اجتماعی،

1. California Consumer Privacy Act

[DOI: 10.22034/5.2.119]

استفاده از داده‌های کاربران است و تصویب قانون بدون در نظر گرفتن منافع شبکه‌های اجتماعی، باعث قطع منبع اصلی درآمد آن‌ها شده و در نتیجه ممکن است ادامه فعالیت آن‌ها با اختلال روبه‌رو شود. در این شرایط کشورها و مردم از خدمات آن‌ها محروم می‌شوند که با توجه به استفاده گسترده کاربران از اینترنت و شبکه‌های اجتماعی، این امر امکان‌پذیر نیست (*Dembrow, 2022, pp. 338-339*).

۳. مسئله مهم دیگر آن است که مقر اصلی شبکه‌های اجتماعی ممکن است در کشوری متفاوت از اقامتگاه کاربران باشد. در این صورت طرح دعوای کاربر علیه شبکه اجتماعی، نزد مراجع قضایی کشور مقر شبکه اجتماعی محتمل نیست. جهت حل این مشکل دو راهکار وجود دارد: ۱- وضع مقررات بین‌المللی در خصوص شبکه‌های اجتماعی یا تنظیم قوانین نمونه در این خصوص، تا با وضع آن‌ها در قوانین داخلی کشورها وحدت رویه‌ای ایجاد شود تا کاربر بتواند در اقامتگاه خود طرح دعوا کند. ۲- کشور مقر شبکه اجتماعی، با وضع مقررات قانونی، شبکه اجتماعی را ملزم کند که بدون نیاز به رسیدگی قضایی، ساختار حل اختلاف داخلی ایجاد کرده و به شکایات و اعتراضات کاربران رسیدگی نماید. این روش که موسوم به خودتنظیمی است در بخش بعدی موردمطالعه قرار می‌گیرد (*Dembrow, 2022, p.340*).

درنهایت می‌توان گفت، قوانین در تلاش هستند که با افزایش مسئولیت شبکه‌های اجتماعی نسبت به داده‌های کاربران، استفاده از داده‌های آنان را به حداقل برسانند. قوانین حمایت از حریم خصوصی کاربران، معمولاً از یک طرف حقوق فردی کاربران را به رسمیت می‌شناسند و از طرف دیگر مشخص کردن چهارچوب جمع‌آوری، استفاده و اشتراک‌گذاری داده‌ها توسط شبکه‌های اجتماعی و حفظ حقوق و منافع آن‌ها می‌شود. در این قوانین، عمدتاً راهکاری جهت نحوه اعلام رضایت کاربر در خصوص جمع‌آوری و انتشار داده‌های حساس خود وجود دارد که در خصوص برخی از داده‌ها، صرف اعلام رضایت اولیه در شرایط عضویت در شبکه‌های اجتماعی کافی نبوده و کاربر باید به‌صراحت نسبت به جمع‌آوری و انتشار داده‌های حساس خود نظرش را اعلام نماید (*Dembrow, 2022, p.340*).

[DOI: 10.22034/5.2.119]

در خصوص وضع قوانین به‌عنوان راهکار حمایت از حریم خصوصی کاربران این نکته وجود دارد که تجربه کشورها در خصوص وضع قوانین نشان داده است که علی‌رغم وضع قانون در بسیاری از کشورها، همچنان نقض حریم خصوصی کاربران وجود دارد و قوانین نتوانسته است به نحو مطلوبی از نقض حریم خصوصی کاربران و انتشار داده‌های آنان بدون رضایت و مجوز قانونی جلوگیری نماید.

۳-۳- خودتنظیمی شبکه‌های اجتماعی

مقررات قانونی در خصوص حفاظت از اطلاعات کاربران در شبکه‌های اجتماعی، نتوانسته‌اند تأثیر زیادی داشته باشند. با توجه به اینکه که مخاطبان شبکه‌های اجتماعی در کشورهای مختلفی اقامت دارند، طرح دعوا علیه شبکه اجتماعی در کشور مقر آن، دشوار یا محال است. به‌همین‌دلیل، برخی از شبکه‌های اجتماعی، راهکارهای خودتنظیمی را پیش‌گرفته‌اند؛ زیرا درصورتی‌که راهکارهایی برای حفاظت از اطلاعات کاربران وجود نداشته باشد، استقبال کاربران از آن شبکه اجتماعی کاهش می‌یابد؛ لذا با توجه به نارسایی مقررات قانونی، خود شبکه‌های اجتماعی تمایل دارند که با اتخاذ سیاست‌های مقتضی، به کاربران این اطمینان را بدهند که اطلاعات آن‌ها موردحفاظت قرار می‌گیرد. در اجلاس حفظ حریم خصوصی کاربران در سال ۲۰۲۱، شرکت اپل اعلام کرد که نرم‌افزاری را ارائه خواهد داد که بر مبنای آن سیاست‌های جدید حفظ حریم خصوصی کاربران اعمال خواهد شد. درواقع در این اجلاس اعلام شد که برخی شرکت‌ها با استفاده از روش‌های تولید محتوا و الگوریتم خود آشکارا کاربران را گمراه می‌کنند؛ مثلاً در برخی شبکه‌های اجتماعی به تبلیغات علیه واکسن و کاهش اعتماد عمومی نسبت به آن یا تبلیغات گروه‌های خشن و افراطی دامن زده می‌شود. شرکت مذکور، با این سیستم جدید نرم‌افزاری خود در تلاش است که به این‌گونه تبلیغات پایان دهد. بر اساس نرم‌افزار جدید شرکت اپل، این شرکت از تمامی کاربران خود قبل از به اشتراک‌گذاری داده‌های آنان سؤال می‌کند که آیا تمایل دارند که داده‌های خود را در سایر شبکه‌های اجتماعی به‌اشتراک بگذارند یا خیر. بر اساس این سیاست‌ها، وقتی کاربری برای اولین‌بار

[DOI: 10.22034/5.2.119]

نرم‌افزاری را در تلفن همراه یا سایر دستگاه‌های خود نصب می‌کند، اعلانی برای کاربر ارسال می‌شود و دسترسی‌های نرم‌افزار به داده‌های کاربر توضیح داده می‌شود. در این شرایط کاربر می‌تواند انتخاب کند که آیا تمایل دارد که اطلاعات مذکور را به آن نرم‌افزار بدهد یا خیر. شرکت مایکروسافت نیز پس از تصویب و اجرای مقررات حفاظت از داده‌های عمومی خود را با آن هماهنگ کرده است و در چهارچوب آن از داده‌های کاربران محافظت می‌نماید (*Dembrow, 2022, pp.343-344*).

این سیاست‌ها در تمامی شرکت‌ها و شبکه‌های اجتماعی وجود ندارد؛ بلکه سیاست‌های اخیر فیس‌بوک و شرکت متا جهت حفظ حریم خصوصی کاربران خود، بیش از اینکه از حریم خصوصی کاربران حفاظت کند به ترجیحات تبلیغ‌کنندگان و مشتریان توجه می‌نماید. کاربران با عضویت در این شبکه اجتماعی، تأیید شرایط عضویت و نصب نرم‌افزار فیس‌بوک بر تلفن همراه خود، اجازه استفاده از داده‌ها و اطلاعاتشان را در زمینه‌هایی مثل منطقه زمانی، اپراتور تلفن همراه، زبان، موقعیت مکانی دسترسی به فیس‌بوک می‌دهد. طبق سیاست‌های جدید، پیام کاربران در پیام‌رسان واتس‌اپ جمع‌آوری می‌شود و با داده‌های فیس‌بوک تجمیع می‌گردد و در این نهایت این داده‌های تجمیعی در جهت اهداف بازاریابی و تبلیغات استفاده می‌شود؛ اما باوجوداین محتوای چت‌های کاربران در واتساپ همچنان رمزگذاری شده باقی خواهد ماند. در شبکه اجتماعی اینستاگرام، کاربر ضمن ثبت‌نام در این شبکه، به‌طور کامل می‌پذیرد که تمامی تصاویر و ویدئوهای آنان حتی بدون تأیید قبلی کاربران توسط شرکت‌های تبلیغاتی قابل استفاده و دریافت است. این درحالی است کاربران گاهی تصاویر خصوصی خود را در اینستاگرام منتشر می‌کنند که نسبت به انتشار آن رضایت ندارند؛ اما بنا به شرایط عضویت در این شبکه اجتماعی، اینستاگرام از این اطلاعات جهت اهداف تبلیغاتی خود استفاده می‌کند (*Soussan & Trovati, 2021, pp.3-4*).

نتیجه‌گیری

حضور اینترنت و شبکه‌های اجتماعی در دنیای فعلی امری ضروری و لازم است. تصور دنیای بدون اینترنت، تصوری دور از ذهن و تقریباً ناممکن است. حضور اینترنت مانند

[DOI: 10.22034/5.2.119]

سایر پدیده‌های بشری دیگر، در کنار فایده‌های بسیاری که برای جامعه داشته است، با معایب و ضررهایی همراه بوده است. یکی از این معایب، در دسترس بودن اطلاعات کاربران در شبکه‌های اجتماعی است. این موضوع هنگامی‌که شبکه‌های اجتماعی با دسترسی به اطلاعات جمع زیادی از کاربران، آن اطلاعات را تجمیع و دسته‌بندی می‌کنند، به یک مشکل جدی تبدیل می‌شود؛ زیرا که شبکه‌های اجتماعی می‌توانند این اطلاعات تجمیعی را در اهداف مختلف نظیر فعالیت‌های تبلیغاتی استفاده نمایند.

در شرایط فعلی با توجه به اینکه نمی‌توان به صورت مطلق، پذیرفتن تمامی شروط هنگام ثبت‌نام کاربران در شبکه‌های اجتماعی را به‌معنای رضایت کاربر مبنی بر انتشار داده‌های خود دانست و در این زمینه باید به منصفانه یا غیرمنصفانه بودن شروط توجه نمود و علاوه‌براین با عنایت به چندین مورد افشای اطلاعات کاربران از شبکه‌های اجتماعی، مردم و دولت‌ها در تلاش‌اند که به‌نحوی استفاده از اطلاعات کاربران در شبکه‌های اجتماعی را ضابطه‌مند نمایند و از سوءاستفاده‌های بیشتر اطلاعات کاربران جلوگیری نمایند.

برای جلوگیری از سوءاستفاده اطلاعات کاربران، معمولاً اولین راهکار کشورها وضع قانون و تعیین چهارچوب‌های حفظ حریم خصوصی کاربران در شبکه‌های اجتماعی بوده است؛ اما این روش به نتیجه مطلوب خود نرسیده است. ازاین‌رو، روش‌های مختلف دیگری نظیر وضع مالیات بر استفاده شبکه‌های اجتماعی از داده‌های کاربران پیشنهاد شده است. در این خصوص نیز به‌نظر می‌رسد این روش در صورتی مؤثر است که منابع درآمدی حاصل از مالیات مذکور در راه جبران خسارت افراد آسیب‌دیده از سوءاستفاده‌های شبکه‌های اجتماعی از داده‌های آنان، توسعه امنیت دیجیتال، حمایت از سازمان‌های مردم‌نهاد که در راستای حمایت از حریم خصوصی کاربران در اینترنت فعالیت می‌کنند، مصرف شود. به علت اینکه بسیاری از شبکه‌های اجتماعی در کشورهای مختلف دفتر یا شعبه‌ای ندارند، دریافت مالیات از این شرکت‌ها بسیار دشوار خواهد بود و تنها در صورت برقراری سازوکار نظام مالیاتی جهانی، امکان اجراشدن مطلوب این پیشنهاد وجود خواهد داشت.

[DOI: 10.22034/5.2.119]

در کنار راه‌های تنظیم‌گری نهادهای خارج از فضای اینترنت و شبکه‌های اجتماعی نظیر دولت‌ها، شبکه‌های اجتماعی می‌توانند در داخل مجموعه خود، تنظیم‌گری داشته باشند و از این طریق، داده‌ها و حریم خصوصی کاربران محافظت شود. حمایت شبکه‌های اجتماعی از داده‌های کاربران، بهترین راه حفاظت از حریم خصوصی است؛ اما این امر مستلزم وجود نفع یا جلوگیری از ضرر شدید برای شبکه‌های اجتماعی است که در شرایط فعلی چنین وضعی وجود ندارد. با توجه به موارد مذکور اگرچه که امروزه در راستای حمایت از داده‌های کاربران، گام‌های بلندی در سطح بین‌المللی برداشته شده است؛ اما به‌نظر می‌رسد که هیچ‌یک از راهکارهای بیان‌شده نتواند به‌تنهایی از حریم خصوصی کاربران حفاظت نماید. در این شرایط بهترین روش، استفاده از چندین راه مختلف جهت حمایت از داده‌های کاربران است که با این روش بتوان حداقل از بخش زیادی از سوءاستفاده‌ها در فضای اینترنت جلوگیری کرد.

در ایران نیز قوانینی که بتوانند به‌طور کامل از اطلاعات کاربران در شبکه‌های اجتماعی حمایت نمایند، وجود ندارد. باوجوداین امروزه با توسعه روزافزون شبکه‌های اجتماعی داخلی، این نیاز حس می‌شود که دولت جهت حمایت از داده‌های کاربران داخلی، قانون متناسب با حمایت از کاربران و اطلاعات ایشان در شبکه‌های اجتماعی وضع نماید. علی‌رغم اینکه وضع قوانین مختلف می‌تواند موثر باشد؛ اما موثرترین روش در این راستا وضع مالیات بر شبکه‌های اجتماعی و صرف این مبالغ در جهت توسعه امنیت دیجیتال و حمایت از داده‌های کاربران است که این امر می‌تواند شبکه‌های اجتماعی داخلی را به‌سمت خود تنظیم‌گری و حمایت از داده‌ها و حریم خصوصی کاربران هدایت نماید و علاوه بر این در صورت سوءاستفاده شبکه‌های اجتماعی از داده‌ها و اطلاعات کاربران، دولت می‌تواند از محل مالیات پرداخت شده، خسارت وارده به کاربران را جبران نماید.

منابع و مآخذ

ابهری، حمید و فلاح خاریکی، مهدی (۱۳۹۹). شروط غیرمنصفانه در قراردادهای تجاری الکترونیکی در حقوق ایران و اروپا. *پژوهشنامه حقوق تطبیقی، ٤(۱)*، صص.۹–۳٤.

[DOI: 10.22034/5.2.119]

اکبری، علی، فلاحیان، مهدی (۱٤۰۰). حریم خصوصی در نظام حقوقی ایران و اسلام. *تمدن حقوقی، ٤(۹)*، صص.۳٦۱-۳۸۲.

انصاری، باقر (۱۳۸۳). حریم خصوصی و حمایت از آن در حقوق اسلام تطبیقی و ایران. *مجله دانشکده حقوق و علوم سیاسی*. ٦٦*(۰)*. صص.۱-۵۳.

انصاری، باقر (۱٤۰۱). مطالعه حقوقی تبعیض الگوریتمی. *فصلنامه دانش حقوقی. ۱۱(۳۸)*. صص.۱۷۰-۱٤۱.

انصاری، باقر (۱٤۰۲). *حقوق داده‌ها: اصول پردازش داده‌های شخصی*. تهران: شرکت سهامی انتشار.

انصاری، باقر و دیگران (۱٤۰۱). *مطالعه تطبیقی حمایت از داده‌های شخصی در اروپا، آمریکا، چین و ایران*. تهران: شرکت سهامی انتشار.

انصاری، باقر و عطار، شیما (۱٤۰۲). *حقوق کاربران فضای مجازی*، تهران: شرکت سهامی انتشار.

جعفری، علی و رهبرپور، محمدرضا (۱۳۹٦). مسئولیت مدنی ناشی از نقض حریم خصوصی داده‌ها در فقه امامیه و حقوق موضوعه. *پژوهش حقوق خصوصی. ۵(۱۸)*. صص.٤۳-۷٤.

حدادپور، جواد (۱٤۰۱). حریم خصوصی افراد در فقه امامیه و حقوق موضوعه. *آرا، ۲۵*، صص.٤۳-۵٦.

زند، حسین (۱٤۰۱). *حمایت از داده‌ها در حقوق موضوعه ایران*. تهران: شرکت سهامی انتشار.

شهباز قهفرخی، سجاد (۱۳۹٤). حریم خصوصی معنوی افراد در فقه امامیه و حقوق اساسی جمهوری اسلامی ایران. *مجله اندیشه‌های حقوق عمومی، ۲(۷)*، صص.۱۱۰-۹۳.

قناد، فاطمه و علیقلی، امیره. (۱۳۹۹). مفهوم و اهمیت داده‌های شخصی و حریم خصوصی و انواع حمایت از آن در فضای مجازی. *حقوق فناوری‌های نوین (حقوق قراردادها و فناوری‌های نوین)، ۱(۱)*، صص.۲۹۷-۳۲۲.

کاظم‌پور، سیدجعفر (۱۳۸۹). بررسی تطبیقی حمایت از طرف ضعیف قرارداد در ایتالیا و

[DOI: 10.22034/5.2.119]

«دکترین نامعقول بودن» در ایالات متحده آمریکا. *مجله حقوقی دادگستری، ۷۴(۷۱)*، صص.۱۳۹–۱۸۰.

لطیف‌زاده، مهدیه و دیگران (۱۴۰۲). حمایت از دادهٔ شخصی در حقوق اتحادیهٔ اروپا و امکان‌سنجی آن در نظام حقوقی ایران. *مطالعات حقوق عمومی دانشگاه تهران. ۵۳(۲)*. صص.۹۸۱–۱۰۰۵.

نعیمی، حامد (۱۳۹۴). بررسی حفظ حریم خصوصی افراد در رسانه از دیدگاه فقه امامیه، مشهد: دانشگاه فردوسی.

واعظی، سیدحسین و همتی فارسانی، تورج (۱۳۹۵). تجسس و تحلیل آیات فقهی و اخلاقی آن. *نشریه قرآنی کوثر، ۵۷*، صص.۱۶۱–۱۸۲

واعظی، سیدمجتبی و علی‌پور، سیدعلی (۱۳۸۹). بررسی موازین حقوقی حاکم بر حریم خصوصی و حمایت از آن در حقوق ایران. *مجله حقوق خصوصی، ۷(۱۷)*، صص.۱۳۳–۱۶۳.

ولی‌پور، یوسف (۱۳۹۷). فلسفه فقه اطلاعات و مفهوم واژه حریم خصوصی. *نشریه پژوهش‌های فقه اسلامی و مبانی حقوق*، ۱، صص.۷۹–۱۰۶.

Bucher, Taina (2018). *If...Then: Algorithmic Power and Politics.* New York: Oxford Studies in Digital Politics.

Dembrow, Brett (2022). Investing in Human Futures: How Big Tech and Social Media Giants Abuse Privacy and Manipulate Consumerism. *University of Miami Business Law Review, vol. 30, no. 3,* pp. 324-349.

Hoofnagle, Chris Jay, Sloot, Bart van der, Zuiderveen Borgesius, Frederik (2019). The European Union general data protection regulation: what it is and what it means. *Information & Communications Technology Law, 28(1)*, pp 65-98.

Hunt, Robert & McKelvey, Fenwick (2019). Algorithmic Regulation in Media and Cultural Policy: A Framework to Evaluate Barriers to Accountability. *Journal of Information Policy, 9,* pp 307–335.

Schwartz, Alan & Wilde, Louis. L. (1979). Intervening in Markets on the Basis of Imperfect Information: A Legal and Economic Analysis. *University of Pennsylvania Law Review, 127(3)*, 630–682.

Soussan, Tariq, Trovati, Marcello. (2021). Social Media Data Misuse. available at https://www.preprints.org/manuscript/202103.0331/v1. Accessed in 18 october 2023.

Tiwari, Prakhar (2023). Misuse of personal data by social media giants. *Jus Corpus Law Journal, 3(2),* pp 1041-1064.

[DOI: 10.22034/5.2.119]