حق بر حریم خصوصی در شبکه‌های اجتماعی

همایون حبیبی*

تاریخ دریافت: ۹۵/۵/۱۹ تاریخ پذیرش: ۹۵/۱۰/۲۸

چکیده

در عصر فناوری اطلاعات و با توسعه فضای مجازی، حریم خصوصی بیش از هر زمان دیگری در خطر است و در این میان شبکه‌های اجتماعی از وضعیت ممتازی در باب أخذ، جمع‌آوری و استفاده از اطلاعات اشخاص در فضای مجازی برخوردارند . این شبکه‌ها با رصد کردن رفتار افراد در شبکه و افزودن این اطلاعات به بانک داده‌های خود، مجموعه‌ای از اطلاعات را جمع‌آوری کرده و از طریق داده‌کاوی، پروفایل‌های شخصی برای اعضا می‌سازند که حاوی اطلاعات بسیار زیادی از زندگی خصوصی افراد است و به این ترتیب به حریم خصوصی تعداد بیشتری از مردم جهان وارد می‌شوند. حساسیت نسبت به نقض حریم خصوصی در فضای دیجیتال در سطح بین‌المللی، منطقه‌ای و ملی ایجاد شده، ولی هنوز مقررات کافی برای حفاظت مناسب از حریم خصوصی وجود ندارد. در ایران این فقر قانونی چشمگیرتر است. و نیاز به تصویب مقررات حمایت کننده از حریم خصوصی با توجه به اصول مورد پذیرش بین‌المللی حس می‌شود.

کلید واژگان

حریم خصوصی، فضای مجازی، شبکه‌های اجتماعی، حقوق بین‌الملل.

*. استادیار حقوق بین الملل عمومی دانشکده حقوق دانشگاه علامه طباطبایی.
homayounhabibi@yahoo.com

مقدمه

حریم خصوصی را باید از حقوق مهم بشری تلقی کرد که با شخصیت انسان ارتباط مستقیم و تنگاتنگی دارد. این حق در ماده ۱۲ اعلامیه جهانی حقوق بشر مورد توجه قرار گرفته است و هرچند حفظ حریم خصوصی در تمامی جهان دارای اهمیت است ولی در فرهنگ‌های مختلف اهمیت یکسانی ندارد. حتی در بین فرهنگ‌هایی که نزدیک به هم به‌نظر می‌رسند تفاوت‌ها گاه چشمگیر است.[۱] در فرهنگ و حقوق اسلامی نیز مجموعه‌ای از مفاهیم و دستورات وجود دارد که به حفظ حریم خصوصی مربوط است، مانند ممنوعیت ورود بدون اجازه به منازل دیگران یا منع تجسس در امور خصوصی آنان[۲]. بنابراین در خصوص مفهوم و مصادیق حریم خصوصی به لحاظ فرهنگی اتفاق نظر وجود ندارد.[۳] و شاید بی‌دلیل نباشد که برخی در امکان تعریف آن تردید کرده‌اند.[۴] به این پیچیدگی در تعریف، باید مشکلات مرتبط با ترجمه از یک زبان حقوقی به زبان دیگر را نیز افزود.[۵]

حق بر حریم خصوصی به کرامت انسان و حق هر شخص به حفاظت از آن مربوط است. و امروزه لزوم احترام به برخی از جنبه‌های حریم خصوصی در قوانین ملی- و از جمله قوانین

۱. برای ملاحظه تحلیلی در خصوص حق بر حریم خصوصی نگاه کنید به: رحمدل، منصور؛ «**حق انسان بر حریم خصوصی**»، دانشکده حقوق و علوم سیاسی(دانشگاه تهران) ش ۷۰ ، ۱۳۸۴، ۴۶- ۱۱۹ و برای مروری بر تئوری‌های حریم خصوصی نگاه کنید به:
Margulis, Stephen T., "**Three Theories of Privacy: un overview**" *in* Privacy Online, Perspectives on Privacy and Self-Disclosure in the Social Web, Sabine Trepte and Leonard Reinecke (eds.) (Dordrecht London New York: springer, 2011), 9–18, doi:10.1007/978-3-642-21521-6.

۲. انصاری، باقر؛ «**حریم خصوصی و حمایت از آن در حقوق اسلام تطبیقی و ایران**»، مجله دانشکده حقوق و علوم سیاسی زمستان ۱۳۹۳، ش ۶۶ (ص‌ص ۱-۵۳).

3. Margulis Stephen T., Op. cit.,

4. Bostwick, Gary L. "**A Taxonomy of Privacy: Repose, Sanctuary, and Intimate Decision**" California Law Review vol. 64, P. 1447, No. 6 (1976) doi:10.2307/3480041.

۵. زیرا، به لحاظ انتخاب لغت معادل ممکن است معانی جدیدی از همان مفهوم استنباط شود. در زبان فارسی برای آنچه در زبان انگلیسی Privacy و در زبان فرانسه la vie privée خوانده می‌شود، معادل حریم خصوصی پیشنهاد شده و همین انتخاب، تعریف و گستره مفهوم را از آنچه در دیگر جوامع فهم می‌شود متفاوت ساخته است. (نگاه کنید به: انصاری، باقر؛ «**واکاوی مفهومی حریم خصوصی و مفاهیم مشابه**»، نشست علمی مورخ ۱۳۹۴/۱۲/۱۵ «مفهوم و قلمروی حریم خصوصی در نظام حقوقی ایران» پژوهشگاه قوه قضائیه،)

اساسی- و اسناد بین‌المللی[۱] مورد تأکید قرار گرفته است. برای مثال اصل ۲۵ قانون اساسی جمهوری اسلامی ایران، جنبه‌هایی از حمایت از حریم خصوصی را دربر دارد.[۲]

به‌رغم این توجه در قوانین اساسی و عادی، زندگی شخصی افراد و حریم خصوصی آنها در دنیای امروز به‌طور فزاینده‌ای مورد تهدید و تحدید قرار گرفته است. فناوری‌های جدید امکان جمع‌آوری و نگهداری اطلاعات در مقیاس بسیار بزرگ را ایجاد کرده و فناوری اطلاعات این امکان را فراهم آورده است که این داده‌ها به انحای مختلف مورد واکاوی قرار گرفته و اطلاعات دقیق و روشنی از زندگی افراد به‌دست آید و خطرات غیرقابل تصوری برای حریم شخصی افراد به همراه داشته باشد. به همین دلیل، امروزه بیشترین تمرکز در ادبیات حقوقی ناظر به حریم خصوصی، بر مباحث مربوط به حفظ و کنترل بر داده‌های شخصی است. و یکی از موضوعاتی که هنوز نیاز به مداقه دارد، مسئله جمع‌آوری اطلاعات و چگونگی بهره‌برداری از آن است. در میان ابزارهای گوناگون جمع‌آوری اطلاعات در دنیای امروز، به‌طور ویژه باید به فضای مجازی توجه کرد و یکی از پیچیده‌ترین و شاید مخرب‌ترین ابزارهای جمع‌آوری و استفاده از اطلاعات شخصی، شبکه‌های اجتماعی هستند.

این مقاله پس از اشاره‌ای به مفهوم شبکه‌های اجتماعی، به انواع تهدیداتی که شبکه‌های اجتماعی بر حریم خصوصی وارد می‌کنند پرداخته و سپس نظام حقوقی موجود برای مقابله با این تهدیدها را مورد بررسی قرار خواهد داد.

---

۱. برای مثال در قطعنامه شماره ۱۶۸/۶۷ مجمع عمومی سازمان ملل مورخ ۱۸ دسامبر ۲۰۱۳ در مورد این حق این‌گونه بیان شده است:

"Reaffirming the human right to privacy, according to which no one shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, and the right to the protection of the law against such interference…"

۲. اصل ۲۵ قانون اساسی: «بازرسی و نرساندن نامه‌ها، ضبط و فاش کردن مکالمات تلفنی، افشای مخابرات تلگرافی و تلکس، سانسور، عدم مخابره و نرساندن آنها، استراق سمع و هرگونه تجسس ممنوع است مگر به حکم قانون.» برخی معتقدند که این اصل به اندازه کافی از حریم خصوصی در نظام حقوقی ایران حمایت نمی‌کند. هرچند این سخن با توجه به سنت قضایی ایران که در آن قاضی از تمسک مستقیم به قانون اساسی اجتناب می‌کند صحیح است، ولی باید دانست که همین اصل نیز می‌تواند تا حدود زیادی مؤثر باشد، کما اینکه در حقوق ایالات متحده آمریکا نیز مبنای حقوقی حمایت از حریم خصوصی را در اصلاحیه چهارم قانون اساسی این کشور می‌یابیم که مقرره‌ای مشابه اصل ۲۵ دارد. این اصلاحیه می‌گوید:
"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, …"

فصل اول: شبکه‌های اجتماعی عامل خطر فزاینده علیه حریم خصوصی در فضای مجازی

کارکرد ا شبکه‌های اجتماعی ایجاد ارتباط بین مردم است و این فعالیت ارتباطی می‌تواند به‌طور طبیعی در جهت خلاف «حفظ حریم خصوصی» عمل کند، زیرا، در طبع این شبکه‌ها نهفته است که مردم اطلاعات شخصی خود را به اشتراک بگذارند.

شبکه‌های اجتماعی در واقع محصول تعاملی شدن وب در اواخر دهه ۹۰ میلادی هستند. البته در خصوص آنکه اصطلاح «شبکه‌های اجتماعی» شامل کدام خدمات اینترنتی می‌شود اختلاف دیدگاه وجود دارد: به شکل حداقلی می‌توان اطلاق این اصطلاح را به شبکه‌های ارتباط کاربران در فضای مجازی محدود دانست که معروف‌ترین نمونه آن فیسبوک است. به این ترتیب اصطلاح مزبور به خدماتی اطلاق می‌شود که محصول «وب۲» است و مبتنی بر محتواهایی است که استفاده‌کنندگان به اشتراک می‌گذارند و در آن افراد و گروه‌ها برای خود در چارچوب خدمات اینترنتی مزبور حساب کاربری و پرونده شخصی تعریف می‌کنند. فعالیت شبکه عبارت از در ارتباط قراردادن این حساب‌های کاربری و تسهیل ایجاد شبکه اجتماعی برای افراد و گروه‌ها است.[۱]

همچنین می‌توان عنوان «شبکه اجتماعی» را شامل طیف وسیع‌تری از پایگاه‌های اینترنتی تعاملی در وب دانست که در آن محتوا به‌وسیله کاربران تولید می‌شود مانند وبلاگ‌ها، تالارهای گفتگو، یا سایت‌های ویکی مثل ویکی‌پدیا[۲]ــ ویلیکلیکس[۳] و ویکیشنری[۴]. فراتر از آن ممکن است که پایگاه‌های اینترنتی که خدمات دیگری ارائه می‌کنند ولی دارای بخش‌های تعاملی بین استفاده‌کنندگان هستند را جزء شبکه‌های اجتماعی تلقی کرد. مثل شبکه‌های خبری که جایی را برای مباحثه بازدیدکنندگان باز گذاشته‌اند یا سایت‌های خرید برخط که در عین حال بخشی از آن پایگاه امکان تعامل بین خریداران را ایجاد کرده‌اند و اشخاص می‌توانند به بحث و مناظره در خصوص کالاها بپردازند.[۵]

1. Obar, Jonathan A. and Wildman, Steven S., "**Social Media Definition and the Governance Challenge: An Introduction to the Special Issue**", SSRN Electronic Journal, 2015, doi:10.2139/ssrn.2647377. p 745.
2. www.Wikipedia.org
3. www.**wikileaks.org**
4. www.wiktionary.org
5. Elovici ,Yuval and Altshuler Yaniv, "**Introduction to Security and Privacy in Social Networks**" *in Security and Privacy in Social Networks* (New York, NY: Springer New York, 2013), 1–6, doi:10.1007/978-1-4614-4139-7_1.

این مقاله بنا ندارد وارد چالش تعریف شبکه‌های اجتماعی شود و به‌ویژه بر شبکه‌هایی متمرکز می‌گردد که کارکرد اصلی آنها ایجاد ارتباطات دوستانه یا حرفه‌ای بین عده‌ای از افراد است. فهرست و تخصص این سایت‌ها هم بسیار مفصل است.[۱] و ما به توصیف آنها نمی‌پردازیم. در ایران نیز تلاش‌هایی برای ایجاد شبکه‌های اجتماعی در سطح ملی صورت گرفته است ولی بخش اصلی بازار ایران نیز با توجه به نوع فعالیت، بین برخی مؤسسات بزرگ جهانی توزیع شده است. در شبکه‌های دوستی فیسبوک با بیش از یک و نیم میلیارد حساب کاربری فعال در رتبه اول تمامی شبکه‌ها قرار دارد[۲] و یا در موضوع اشتراک تصویر اینستاگرام[۳] و فلیکر[۴] قرار دارند. که هر کدام وابسته به یکی از دو مؤسسه بزرگ اینترنتی یعنی گوگل و یاهو هستند. و اخیرا برنامک‌های ویژه گوشی‌های تلفن همراه هوشمند، نسل جدیدی از شبکه‌های اجتماعی را شکل داده که نمونه معروف این شبکه‌ها «تلگرام» است.

مشکلات مرتبط با تهدید حریم خصوصی از سوی شبکه‌های اجتماعی را می‌توان در دو دسته بزرگ تقسیم‌بندی کرد: اول تهدیدات مرتبط با رفتار کاربران است و دیگری تهدیدات مرتبط با عملکرد مستقیم شبکه‌های اجتماعی در قبال جمع‌آوری داده‌های شخصی و چگونگی بهره‌برداری از آنها است.

این مقاله به تهدیدات ناشی از سرقت و افشای اطلاعات کاربران از سوی هکرها یا نحوه فعالیت اشخاص و شرکتهای ثالث نزد شبکه‌های اجتماعی نمی‌پردازد.

---

۱. برای مطالعه‌ای کوتاه در مورد تاریخچه شبکه‌های اجتماعی و فهرستی از مطرح‌ترین آنها نگاه کنید به:
http://www.webdesignerdepot.com/2009/10/the-history-and-evolution-of-social-media/ (last visited :15/mai/2016)

برای مطالعه ای در خصوص تعریف و تاریخچه شبکه‌های اجتماعی همچنین نگاه کنید به:
Boyd, Danah M. And Ellison, Nicole B., "**Social Network Sites: Definition, History, and Scholarship**", Journal of Computer-Mediated Communication 13, No.10 (oct. 2007) PP. 210-230 doi:10.1111/j.1083-6101.2007.00393.x.

برای مرور بر آمارهای مرتبط با استفاده از شبکه اجتماعی نگاه کنید به:
Perrin, Andrew. "**Social Networking Usage: 2005-2015**" Pew Research Center. October 2015. Available at: http://www.pewinternet.org/2015/10/08/2015/Social-Networking-Usage-2005-2015/

2. http://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/ (last visited 7/12/2016).

3. www.instagram.com

این مؤسسه در ژوئن سال ۲۰۱۶ اعلام کرد که تعداد اعضایش به ۵۰۰ میلیون نفر رسیده که ۳۰۰ میلیون نفر از آنها هر روز به آن مراجعه می‌کنند:
http://blog.instagram.com/post/146255204757/160621-news (last accessed 7/13/2016)
و هر روز بیش از ۸۰ میلیون تصویر را به اشتراک می‌گذارند:
http://blog.instagram.com/post/129662501137/150922-400million)) last accessed 13/07/2016

4. flicker.com

اول: تهدیدات مرتبط با رفتار کاربران

اولین مشکل به رفتار کاربران مربوط می‌شود که بسیاری از اوقات بدون آگاهی از گستره عمل خود دست به انتشار عمومی یا نیمه عمومی اطلاعاتی می‌زنند که به‌طور طبیعی جزئی از اطلاعات شخصی و خصوصی محسوب می‌شود. این رفتار غیرمحتاطانه ممکن است ناشی از عدم توجه به ویژگی‌های شبکه‌های اجتماعی و اینترنت باشد. در واقع بسیاری از استفاده‌کنندگان از شبکه‌ها با قیاس ارتباطات رو در رو یا مخابراتی، مانند تلفن، تصور می‌کنند که آنچه در ارتباطات دو یا چندجانبه در اینترنت به اشتراک گذاشته شده است، محرمانگی خود را حفظ خواهد کرد. حال آنکه ماهیت ارتباطات در این شبکه‌ها متفاوت است و چنین پیش‌فرضی از ابتدا نادرست است.[1] شاید به همین دلیل باشد که برخی نویسندگان معتقدند بیش از آنکه وقت خود را صرف تدوین قوانین حفاظت از حریم خصوصی کنیم باید تلاش کنیم تا استفاده‌کنندگان به این ویژگی شبکه‌های اجتماعی پی برند.[2] البته مسئولین شبکه‌ها بی‌تقصیر نیستند: آنها بسیاری اوقات عامدانه و برای اینکه شبکه اجتماعی برد و تأثیر بیشتری پیدا کند سعی بر این دارند که اطلاعات، حتی‌المقدور، به شکلی عمومی منتشر شود، بنابراین شبکه‌ها را طوری طراحی می‌کنند که اطلاعات عمومی باشد و کاربر باید به اطلاعاتی که افشا کرده و در اختیار عموم قرار می‌دهد توجه داشته باشد. گاه لازم است کاربران با انجام تغییرات در تنظیمات پیش فرض شبکه از حریم خصوصی خود حفاظت کنند.

برخی اوقات امکان انجام تنظیماتی که منجر به حفظ بیشتر حریم شخصی می‌شود به‌درستی به اطلاع کاربر نمی‌رسد، یا به‌گونه‌ای دور از دسترس است که تنها کاربران دارای توان فنی بالاتر می‌توانند از آن استفاده کنند. در برخی موارد نیز، امکان انتخاب از کاربر گرفته می‌شود مانند اینکه در بدو ورود به شبکه اجتماعی (ذیل پروانه بهره برداری از امکانات و نرم افزار شبکه) اجازه دسترسی به حساب کاربری و مشخصات تماس‌ها أخذ می‌شود و از این طریق، ورود کاربر به جمع اعضای شبکه اجتماعی را به تمامی آشنایان شخص اطلاع می‌دهند، بدون اینکه او بتواند اجازه صدور چنین اعلامیه‌ای را از آنها سلب کند. در واقع این خبر که کاربری از یک نرم افزار

1. Walther Joseph B., "**Introduction to Privacy Online**", *in* Privacy Online, Perspectives on Privacy and Self-Disclosure in the Social Web, Sabine Trepte و Leonard Reinecke,(eds.) 2011. P 4-5.
2. Ibid.

ارتباط جمعی –مثلا تلگرام استفاده می‌کند، هرچند از دید وی خصوصی باشد، دیگر موضوعی خصوصی نیست. حتی کاربر نمی‌تواند بداند چه کسانی از این خبر مطلع شده‌اند، زیرا، نمی‌داند چه شماری از افراد شماره تلفن وی را در دفتر تلفن خود دارند.

مسئله انتشار عمومی اطلاعات شخصی، در مورد اطفال و اشخاصی که به سن قانونی نرسیده‌اند، می‌تواند مشکلات بیشتری ایجاد کند، زیرا، آنها درک کافی از حریم خصوصی و حفاظت از آن نداشته و عموماً از گستره پخش اطلاعات‌شان بی‌اطلاعند.

کاربران از طریق ارائه متن‌ها، تصاویر و نوشته‌های متعدد در صفحات شخصی خود و همچنین رفتن به صفحه‌های مختلف، و حاشیه زدن به مطالب دیگران اطلاعات ذی‌قیمتی از علایق شخصی و شخصیت‌شان را بر این شرکت‌ها و سایرین برملا می‌کنند. صاحبان شبکه‌ها برای استفاده‌های بعدی، همه این اطلاعات را حفظ کرده و حتی بعد از خروج شخص از عضویت در شبکه، نگه می‌دارند. پس اگر کاربران نسبت به اطلاعاتی که به اشتراک می‌گذارند محتاط باشند، مشکلات مرتبط با نقض حریم خصوصی از سوی شبکه ها کاهش خواهد یافت.

دوم: عملکرد شبکه‌های اجتماعی در قبال داده‌های شخصی

تقریبا همه شبکه‌های اجتماعی نسبت به جمع‌آوری و دسته‌بندی داده‌ها و از جمله داده‌های مرتبط با زندگی شخصی افراد حریص هستند.[1] داده، به انحاء مختلف جمع‌آوری می‌شود: اولاً، این شبکه‌ها به‌طور معمول اطلاعات زیادی را هنگام ثبت نام از افراد درخواست می‌کنند. ثانیاً، انواع مختلفی از اطلاعات مرتبط با افراد از طریق تعقیب رفتارها و فعالیت‌های آنها در شبکه قابل جمع‌آوری است. کافی است این اطلاعات دسته‌بندی شده و در کنار هم قرار گیرند و به این ترتیب می‌توان یک پروفایل کامل از شخصیت هر فرد ایجاد کرد که در آن نقاط قوت و ضعف، علایق سیاسی، اعتقادی، اخلاقی وی مشخص شده باشد. به این ترتیب مدیران شبکه می‌دانند، هر عضو شبکه چه سلیقه موسیقیایی دارد، چه کتاب‌هایی می‌خواند، چه تفریحاتی را دوست دارد، یا حتی اینکه به لحاظ ثروت در کدام طبقه اجتماعی قرار دارد و اگر مایل باشد هزینه کند چه چیزهایی خواهد خرید.

1. Dugain, Marc, et Labbe, Christophe. *L'homme nu La dictature invisible du numérique.* Paris : Plon, 2016. Chapter 1 .

بر اساس اطلاعات جمع‌آوری شده می‌توان اندازهٔ شبکه آشنایان هر شخص و ترکیب فرهنگی آن را ملاحظه کرد یا می‌توان در خصوص تعادل روانی یا سلامت جسمانی فرد اظهار نظر کرد.
چگونگی بهره‌برداری از این اطلاعات مسئله‌ای دیگر است: اگر اطلاعات بدون نام و نشان باشد به‌صورت آماری در مطالعات عمیق جامعه‌شناسی و اقتصادی و بازاریابی و امثال آن به‌کار می‌آید، ولی اگر با نام باشد سوای آنکه می‌تواند به منظور تبلیغات و بازاریابی هدفمند به‌کار گرفته شود، می‌توان آن را به‌عنوان کالایی مستقل به فروش رساند. اطلاعات خصوصی افراد، مانند کالا قابل فروش است. از تجار تا کارفرمایان تا دولت‌ها همه خریدار این کالا هستند.
تشنگی شرکت‌هایی مانند گوگل، اپل، میکروسافت یا فیسبوک به داشتن داده‌های شخصی تا حدی است که اطلاعات غیر اعضا را هم برای اضافه کردن به بانک داده‌شان ردیابی کرده و نگه می‌دارند. برای مثال اگر عضوی در فیسبوک تصویری به اشتراک گذاشته، نام افرادی غیر عضو فیسبوک که در عکس هستند را مشخص کند، آن اطلاعات نیز ذخیره می‌شود و با عکس‌هایی که دیگران گرفته‌اند و آنها هم چهره همان اشخاص را مشخص کرده‌اند در یکجا جمع می‌شود. یعنی ممکن است مادربزرگ‌هایی که کاری با تکنولوژی نوین ندارند هم پرونده‌ای نزد فیسبوک داشته باشند!

این شرکت‌های بزرگ معمولا اعلام می‌کنند که اطلاعات افراد را به‌صورت شخصی و قابل شناسایی در اختیار سایر مؤسسات قرار نمی‌دهند.[۱] اما از یک طرف خودشان در سیاست حریم خصوصی‌شان معترفند که ممکن است خود از آن اطلاعات استفاده کنند: برای مثال حق دارند با تحلیل علایق افراد، تبلیغاتی را به شکل شخصی شده برای افراد ارسال کنند. لذا با اعلام اینکه تبلیغات هدف‌دار و مآلا مفیدتری انجام می‌دهند هزینه بیشتری از صاحبان کالا یا خدمات مطالبه می‌کنند.
و به این ترتیب است که فقط شرکت فیسبوک در سال ۲۰۱۴ میلادی درآمدی بیش از ۱۰ میلیارد دلار داشته که بیش از ۸۵ درصد آن از محل همین تبلیغات بوده است.[۲] اما نباید فراموش کرد که هر دو این رفتارها یعنی جمع‌آوری اطلاعات از طریق کنترل رفتار بر خط استفاده‌کنندگان و ایجاد پروفایل شخصی برای آنها می‌تواند آثار جدی بر زندگی شخصی افراد

۱. برای مثال نگاه کنید به: سیاست جمع‌آوری داده در شرکت فیسبوک به نشانی:
https://www.facebook.com/full_data_use_policy (last accessed 1/6/2016).
2. Fiegerman, Seth, "**Facebook's annual revenue topped $10 billion for the first time in 2014**", Mashable, http://mashable.com/2015/01/28/facebook-q4-earnings-2014/.(last accessed : 10/5/2016) .

داشته باشد. لذا این دو موضوع به‌طور مشخص مورد توجه حقوق‌دانان و قانون‌گذاران قرار گرفته است:

الف) تعقیب رفتار افراد در شبکه

تعقیب رفتارهای برخط (آنلاین) افراد در شبکه در دهه اخیر به‌طور روز افزونی متداول شده است. به‌گونه‌ای که برخی ادعا می‌کنند که این رفتار به پدیده ذاتی «*جامعه اینترنت‌زده*» تبدیل شده است.[1] این رفتار در تمامی سطوح صنعت اینترنت انجام می‌گیرد. و به همین دلیل در برخی نظام‌های حقوقی، در مورد آن قانون‌گذاری صورت گرفته است یا به‌واسطهٔ مقررات موجود، از افراد در قبال چنین رفتارهایی حمایت می‌شود. از جمله در چارچوب اتحادیه اروپا، هرگاه تعقیب رفتار برخط افراد به شناسایی افراد منجر شود یا به‌گونه‌ای باشد که احتمال شناسایی افراد در آن برود «قواعد حمایت از داده‌های شخصی اروپایی»[2] بر موضوع حاکم است.[3] متأسفانه در نظام ملی ما حمایت‌های واضحی از افراد در این خصوص صورت نمی‌گیرد ولی حتی در نظام‌های ملی که حمایت از داده‌های شخصی و حریم خصوصی موضوع مقررات مشخص و جداگانه‌ای است، چه بسا سرعت فناوری و روش‌های تعقیب رفتار افراد به‌ویژه از سوی شبکه‌های اجتماعی نظیر فیسبوک به‌گونه‌ای است که نمی‌توان از حفاظت کافی قانونی سخن گفت. در اتحادیه اروپا، برای مثال، اخیرا بحث‌های جدی برای تدوین مقررات جدید در این خصوص درگرفته و پیش‌نویس مقررات حمایت جدید سعی در حل این معضل دارد.

روش اصلی که مدت‌ها است برای کنترل رفتار افراد در استفاده از اینترنت به‌کار می‌رود استفاده از کوکی‌ها است.[4] البته امروزه ضمن حفظ و توسعه استفاده از کوکی‌ها به‌عنوان چارچوب اصلی

1. Skouma, Georgia and Léonard, Laura, "**On-line Behavioral Tracking: What May Change After the Legal Reform on Personal Data Protection**" *in* Serge Gutwirth, Ronald Leenes, و Paul de Hert (eds.), Reforming European Data Protection Law (Springer, 2015), doi:10.1007/978-94-017-9385-8. P 35.
2. The European personal data protection rules.
3. Ibid.
۴. کوکی (cockie) عبارت است از یک بسته اطلاعاتی که هنگام ارتباط با سرورها (مثل سرور فیسبوک) در کامپیوتر استفاده‌کننده بارگزاری می‌شود و اطلاعات مربوط به نحوه ارتباط و استفاده از آن سرور در آن ذخیره شده و در تماس‌های بعدی با همان سرور مجددا به سرور باز می‌گردد و به این ترتیب ارائه‌دهندگان خدمات اینترنتی می‌توانند ضمن شناسایی استفاده کننده، اطلاعات متنوعی را از فعالیت‌های استفاده‌کننده جمع‌آوری کنند. استفاده از کوکی‌ها ماهیتاً غیرقانونی تلقی نمی‌شود و می‌تواند به تعامل بیشتر و شخصی‌سازی سایت برای استفاده‌کننده بیانجامد ولی با توجه به امکان سوء استفاده و تعرض به حریم خصوصی اخیراً موضوع مقررات‌گذاری‌هایی قرار گرفته است (برای توضیحات تفصیلی‌تر نگاه کنید به: https://www.*cookielaw*.org *or* http://www.aboutcookies.org/cookie-faq/

فنی برای کنترل رفتار افراد، روش‌های کنترل رفتار بسیار دقیق‌تر و کاراتری نیز ابداع شده است. یکی از این روش‌ها تشویق کاربران به زدن برچسب[1] و اعلام علاقه است. برای مثال شرکت فیسبوک با ابداع ابزارک «*لایک*» یا گوگل با ابزارک «*پلاس*» امکان اظهارنظر کردن سریع را برای افراد فراهم کرده‌اند، به‌گونه‌ای که افراد بتوانند با کلیک بر روی شکلک *لایک* نظر مثبت خود را نسبت به یک محتوا اعلام کنند. به این ترتیب هنگامی که فرد در خصوص صفحه‌ای، خبری یا عکسی بر این ابزارک کلیک کرده و به اصطلاح آن را «لایک می‌کند» نه تنها در یک نظرخواهی عمومی شرکت کرده و نظر عموم را درباره آن عکس یا نوشته نشان می‌دهد، بلکه در شبکه رد پایی از دیدگاه‌های خود به‌جای می‌گذارد. در واقع از این طریق دقیقا اعلام می‌کند در صفحه‌هایی که مرور کرده است، از چه چیزهایی خوشش آمده و نقطه علایقش کدام است. زیرا، این لایک‌ها در کوکی‌هایی ذخیره شده و در اختیار شبکه اجتماعی که وی عضو آن است قرار می‌گیرد. بر اساس یک پژوهش انجام شده در بین ۵۸ هزار داوطلب عضو فیسبوک، تنها از طریق اطلاعات مرتبط با لایک‌های ذخیره شده در حساب کاربری فیسبوک می‌توان جهت‌گیری‌های سیاسی، اخلاقی، جنسیتی و حتی ریشه‌های قومی مذهبی و ویژگی‌های اخلاقی افراد را برملا ساخت.[2] متأسفانه هنوز مقررات کافی در محدود کردن شبکه‌های اجتماعی درباره تعقیب برخط افراد وجود ندارد.[3]

ب) پروفایل ایجاد کردن

ایجاد پروفایل در واقع استفاده از داده‌های موجود است برای دسته‌بندی کردن افراد و گروه‌ها و تصمیم‌گیری بر اساس آن. این کار امری جدید نیست و کاربردهای متعددی در حوزه‌های مختلف علوم دارد. از علم پزشکی تا روان‌شناسی و جرم‌شناسی از این فن، استفاده‌های متعددی

1 .Tag.

۲. عطار، شیما؛ «**حمایت از حریم خصوصی در شبکه‌های اجتماعی مجازی**» (پایان‌نامه کارشناسی ارشد، دانشگاه علامه طباطبایی، ۱۳۹۲، (ص ۵۰) به نقل از:

Roosendaal, Arnold, "**Facebook Tracks and Traces Everyone: Like This!**;" *Tilburg Law School Legal Studies Research Paper Series* no. 3 (2011): 3

۳. یکی از تلاش‌های جنجالی در سطح ملی، مقام حفاظت داده‌های بلژیک فیسبوک را بخاطر تعقیب رفتار افرادی که عضو این شبکه اجتماعی نیستند مورد تعقیب قضایی قرار داد و هرچند در مرحله بدوی موفق به محکوم کردن فیسبوک شد در مرحله تجدید نظر در تابستان سال ۲۰۱۶ این رأی نقض شد و به این ترتیب حتی در بلژیک فیسبوک می‌تواند به این رفتار خود ادامه دهد. نگاه کنید به:

http://www.reuters.com/article/us-facebook-belgium-idUSKCN0ZF1VV (last accessed 2/7/2016)

می‌شود. برای مثال با همین روش است که در علم پزشکی دانشمندان بر اساس داده‌های موجود متوجه می‌شوند که وجود ژن خاصی در انسان، باعث بروز نوع خاصی از سرطان می‌شود.

پروفایل ایجاد کردن، هرچند می‌تواند آثار مثبت زیادی، مانند پیش‌گیری زود هنگام از بیماری نزد افراد مستعد به یک بیماری خاص داشته باشد، ولی می‌تواند در عمل باعث تبعیض و نقض حقوق بشری شود. برای مثال اگر از روی پروفایل ژنتیکی یا تعلق نژادی تصمیم گرفته شود که شخصی محتملاً مجرم است یا می‌تواند مجرم باشد و بنابراین رفتار تبعیض‌آمیزی با وی صورت پذیرد با مشکل جدی در حوزه حقوق بشر مواجه خواهیم بود. بنابراین موضوع ایجاد پروفایل برای افراد حتی قبل از دنیای مجازی هم یک مشکل بوده است. و مطالعات و بحث‌هایی در خصوص آن وجود داشته و دارد.[۱] اما اکنون و با تحول فناوری اطلاعات و در عصر «کلان داده»[۲]ها ما با این پدیده به شکل بسیار پیچیده‌تری مواجه هستیم. از طریق «داده کاوی»[۳] در کلان داده‌ها می‌توان، اطلاعات مشخصی در مورد افراد و گروه‌ها به‌دست آورد. بنابراین امکان دسته‌بندی اطلاعات و قرار دادن افراد بر اساس این دسته‌بندی‌ها به آسانی وجود دارد. می‌توان از مجموعه این اطلاعات، پرونده شخصیتی برای افراد و گروه‌ها ایجاد کرد که می‌تواند به جنبه‌های گوناگون هویت آنها مربوط باشد. صاحبان کلان‌داده‌ها امروزه برای استفاده از این داده و ایجاد پروفایل‌ها، الگوریتم‌هایی تعریف می‌کنند. به عبارت دیگر اطلاعات مربوط به هر فرد و رفتارهای وی در شبکه می‌تواند به وسیله الگویی که برنامه‌نویسان تهیه کرده‌اند، تحلیل شود. و فرد یا گروهی از افراد واجد صفات و مشخصاتی تلقی شوند. حتی بر اساس همان الگو و پروفایل‌های ایجاد شده به‌وسیله آن، ممکن است رفتار خاصی در قبال افراد صورت پذیرد و به این ترتیب صاحبان بزرگترین شبکه‌های اجتماعی از مجموعه اطلاعاتی که از افراد در اختیار دارند به انبوهی از پروفایل‌های شخصی و گروهی می‌رسند و در مورد هر فرد یا گروه از طریق برنامه های کامپیوتری تصمیم خاصی می‌گیرند.

پروفایل ایجاد کردن در واقع دو روی سکه دارد: یک روی سکه خود پروفایل است. اینکه افراد متصف به صفات و ویژگی‌های خاص تلقی شوند و این اطلاعات دسته‌بندی شده، یک دانش

۱. در خصوص یک مطالعه نسبتاً جامع در خصوص پروفایل ایجاد کردن برای افراد و آثار حقوقی آن نگاه کنید به:
Hildebrandt, Mireille and Gutwirth, Serge, (eds.), Profiling the European Citizen: Cross-Disciplinary Perspectives (Springer, 2008), doi:10.1007/978-1-4020-6914-7
2. Big data.
3. Data Mining.

قابل استفاده و قابل فروش تلقی شود، خود مسئله‌ای در خور تأمل در حوزه حقوق بشر است. زیرا، از یک طرف فروش این اطلاعات شخصی نقض حریم خصوصی افراد است و طرف دیگر این پروفایل‌ها می‌توانند مبنایی برای رفتار تبعیض‌آمیز باشند.

روی دیگر سکه این است که این افراد بر اساس الگوریتمی از پیش تعریف شده، ولی اطلاع داده نشده، دسته‌بندی می‌شوند. به عبارت دیگر افراد ممکن است به این دلیل متصف به یک ویژگی اخلاقی، سیاسی عقیدتی تلقی شوند که الگوریتم تعریف شده برای ماشین، ارتباط مجموعه‌ای از اطلاعات با یک فرد را این‌گونه تفسیر می‌کند. به عبارت دیگر، پروفایل‌ها به‌صورت اتوماتیک و خودکار ایجاد می‌شوند و لذا بدون اینکه فرد قادر به عکس‌العمل باشد نزد صاحبان شبکه اجتماعی به داشتن تعدادی از ویژگی‌ها شناخته خواهد شد و بدتر آنکه ممکن است بر همین اساس اطلاعات علیه وی تصمیمی گرفته شود. شاید یک مثال بتواند موضوع را روشن‌تر کند: برای هیچ‌کس مطلوب نیست پروفایل یک فرد مظنون به ارتکاب جنایت تروریستی را داشته باشد. ولی حسب تعریفی که برای کامپیوترها شده، ممکن است مجموعه‌ای اطلاعات و رفتارهای شخصی در شبکه اجتماعی، مثلاً مراجعه منظم به سایتهایی خاص، شخصی را در چنین پروفایلی قرار دهد. در حالی‌که شخص هیچ ارتباطی با تروریسم ندارد. سپس تصور کنید مقامات امنیتی تصمیم بگیرند که تمامی کسانی که دارای چنین پروفایلی هستند را زیر نظر بگیرند یا پس از وقوع یک حادثه تروریستی مورد بازجویی قرار دهند. به این ترتیب اشخاص ممکن است بی‌دلیل برچسب مظنونیت خورده و احتمالا به شکل تبعیض‌آمیزی مورد کنترل و بازجویی قرار گیرند و این همه در حالی است که مردم نمی‌دانند ارتکاب کدام رفتارها، افراد را در این فهرست قرار می‌دهند.

مسئله دیگری که می‌تواند مشکل‌آفرین باشد به استفاده تبلیغات‌کنندگان از پروفایل‌ها مربوط می‌شود. یک شخص ممکن است فعالیت‌های در شبکه اینترنت داشته باشد که به جنبه‌های خصوصی زندگی او مربوط بوده و او نخواهد همگان بدانند. ولی با توجه به پروفایل ایجاد شده ممکن است تبلیغاتی از این دست به صفحه او اضافه شود. مثلا شخصی که به لحاظ حرفه‌ای یک دانشمند علوم زیستی است ممکن است به‌طور مخفیانه دیدگاه‌های گروه‌های سیاسی و اجتماعی خاصی را تعقیب کند که نخواهد به‌صورت عمومی برملا شود. ولی با توجه به پروفایلی که از وبگردی او ایجاد شده تبلیغات ذی‌ربطی روی صفحه‌های او به نمایش گذاشته می‌شود.

جدای از مشکل جمع‌آوری اطلاعات و ایجاد پروفایل، نگرانی دیگر مربوط به سیاست نحوه بهره‌برداری از این اطلاعات است. در نبود مقررات محدودکننده، تنها نقطه اتکای استفاده‌کنندگان به قراردادهای بهره‌برداری و سیاست عملی این مؤسسات است. قراردادهای بهره‌برداری که به‌وسیله اغلب استفاده‌کنندگان مطالعه نمی‌شود مانند هر قرارداد الحاقی دیگر بیشترین حقوق را برای صاحبان این شرکت‌ها محفوظ می‌دارند. در نهایت بر اساس عملکرد شرکت‌ها به آنها اعتماد می‌شود. ولی تضمینی در خصوص حفظ سیاست‌ها و عدم تغییر آن وجود ندارد. برای مثال اخیرا مؤسسه فیسبوک که سیاست‌اش این بود که اطلاعات مربوط به پست‌های اعضا را درون شبکه نگه داشته و به موتورهای جستجو ندهد، اعلام کرده است که اطلاعاتی که اشخاص قبلاً به‌صورت عمومی روی صفحه‌های‌شان گذاشته‌اند را در اختیار موتورهای جستجو قرار خواهد داد. به‌عبارت دیگر اگر تا دیروز این اطلاعات (که شامل نوشته و عکس می‌شود) فقط از طریق حساب‌های کاربری فیسبوک قابل بازیابی بود، در آینده از طریق جستجو در گوگل یا یاهو هم قابل دسترس خواهد بود. یا در مثالی دیگر فیسبوک در سال ۲۰۱۳ امکانی را در حوزه حریم خصوصی حذف کرد که بنابر آن شخص می‌توانست انتخاب کند که نامش قابل جستجو نباشد.[1]

فصل دوم: حمایت از حریم خصوصی در مقابل تعدی در شبکه‌های مجازی

در برخی از کشورهای جهان مقررات عام حمایت از حریم خصوصی یا مقررات خاص مرتبط با حریم خصوصی در فضای مجازی، تعدیات شبکه‌های اجتماعی به حریم خصوصی مردم را محدود می‌کنند. با این‌حال باید توجه داشت که هرچند ممکن است برخی شبکه‌های اجتماعی به‌صورت محلی و عمدتا در یک کشور خاص فعالیت کنند، ولی مهم‌ترین شبکه‌های اجتماعی مطرح در جهان اغلب، به‌شکل فراملی عمل می‌کنند و به همین دلیل اعمال محدودیت‌های ملی بر آنها معمولا به تنهایی کافی نیست. لذا حفظ حریم خصوصی در سطح بین‌المللی و منطقه‌ای نیز مورد توجه قرار گرفته و تلاش‌هایی در جهت افزایش حمایت از آن، انجام یافته است. همچنین با توجه به ویژگی‌های فضای مجازی، ما با پدیده دیگری نیز در حمایت از حریم

1. “Facebook Removing Option To Be Unsearchable By Name, Highlighting Lack Of Universal Privacy Controls | TechCrunch,” https://techcrunch.com/2013/10/10/facebook-search-privacy last accesed 10/06/2016.

خصوصی در شبکه‌های اجتماعی مواجه هستیم و آن خود تنظیمی است. ذیلاً این سطوح حمایتی به بحث گذاشته می‌شود:

الف) خود تنظیمی[1]:

خود تنظیمی یکی از روش‌های بسیار متداول در تنظیم روابط در فضای مجازیست. خود تنظیمی در موضوع مورد بحث به شکل کدهای رفتاری و اعلامیه‌های سیاست مؤسسه در قبال حریم خصوصی خودنمایی می‌کند. در برخی موارد دولت‌ها برای تثبیت و تقویت قواعد ناشی از خود تنظیمی با تصویب قوانینی بر کدهای رفتاری اعلام شده از سوی مؤسسات و اتحادیه‌های صنفی صحه می‌گذارند.[2] خود تنظیمی به‌ویژه از آن جهت اهمیت دارد که این شبکه‌های فرامرزی، به‌طور دقیق تحت مقررات ملی کشورها قرار نمی‌گیرند و مقررات ملی هیچ کشوری به‌طور مؤثری آنها را محدود نمی‌کند. منفعت مؤسسات و به‌ویژه مؤسسات بزرگ نیز در آن است که نشان دهند این خود تنظیمی به اندازه کافی کارآمد است. زیرا، از این راه می‌توانند مانع تصویب مقررات دولتی یا بین‌المللی اجباری و محدودکننده شوند. چون هنگامی قانون تصویب می‌شود که نیازی احساس شود و ایجاد نظم حقوقی زمانی لازم می‌آید که بی‌نظمی حس شود.

با این حال باید پذیرفت که خود تنظیمی تابع شرایط حاکم بر روابط ذی‌نفعان است و همواره منتج به بهترین نتایج نمی‌شود. به این معنی که مؤسسات ذی‌نفع در این خود تنظیمی از یک طرف به مقررات موجود در کشور مبدأ خود توجه دارند و از سوی دیگر حساسیت‌های جامعه مدنی در سرزمین کشوری که در آن فعالیت می‌کنند را مورد ملاحظه قرار می‌دهند. برای مثال اگر مؤسسات از سوی جامعه مدنی و سازمان‌های غیردولتی حقوق بشری به‌خاطر سیاست‌های مغایر حریم خصوصی مورد حمله قرار بگیرند، ممکن است آنها را اصلاح کرده و بهبود بخشند.

در نقطه مقابل هرچه یک مؤسسه تجاری خود را در موضع قدرت احساس کند، یعنی بداند که کشش خدماتش به گونه‌ای است که می‌تواند دسترسی به اطلاعات خصوصی و استفاده تجاری از آن را به مشترکین تحمیل کند، در نبود مقررات محدودکننده از این کار دست نخواهد شست. و این وضعیتی است که امروزه شاهد آن هستیم و به‌طور منظم از سوی شبکه‌های اجتماعی

1. Self-regulation.
2. "Internet Self-Regulation: An Overview," accessed July 25, 2016, http://www.law.uni-sofia.bg/Kat/T/IP/T/PM/DocLib/Internet%20Self-Regulation%20An%20Overview.htm: see part 3.1 : respect for privacy.

سیاست‌های محرمانگی اعلامی در حال حک و اصلاح است. با توجه به این شرایط است که این مؤسسات در حوزه حفظ حریم خصوصی گاهی یک قدم به جلو[۱] و گاهی یک قدم به عقب برمی‌دارند[۲].

ب) مقررات بین‌المللی حفاظت از حریم خصوصی و قابلیت اعمال آن بر شبکه‌های اجتماعی

در سطح بین‌المللی اصل لزوم حمایت از حریم خصوصی وجود دارد: یعنی می‌توان با توسل به کلیات موجود در اسناد حقوق بشری مانند ماده ۱۲ اعلامیه جهانی حقوق بشر و ماده ۱۷ میثاق مدنی–سیاسی که می‌گوید: *«هیچ‌کس نباید در زندگی خصوصی ... مورد تعرض قرار گیرد ... و باید در مقابل این تعرضات از حمایت قانون برخوردار باشد»* و مطالب مشابهی که در اسناد دیگر وجود دارد دریافت که حقوق بین‌الملل بشر، در کلیت، حافظ حریم خصوصی است.[۳] ولی به‌طور خاص نمی‌توان سند واحد و مهم جهانی در کنترل شبکه‌های اجتماعی یا حتی حمایت از داده‌های شخصی ملاحظه کرد. البته حساسیت به مقوله «حریم خصوصی در فضای دیجیتال» در سطح بین‌المللی ایجاد شده است، ولی نتیجه این حساسیت ارائه قواعد و توصیه‌های کلی است و مقررات‌گذاری دقیق و تفصیلی بر مبنای این اصول کلی باید در سطح ملی انجام شود. زیرا، با توجه به پیچیدگی‌های موضوع نمی‌توان در این خصوص انتظار مقررات خوداجرای تفصیلی بین‌المللی داشت.

فرای کلیات حمایت از حریم خصوصی در حقوق بین‌الملل بشر، موضوع جمع‌آوری اطلاعات وچگونگی بهره‌برداری از آن با اولین موج عصر دیجیتال توجه مجمع عمومی سازمان ملل را جلب کرده است. یکی از اولین قطعنامه‌های مجمع عمومی سازمان ملل در این خصوص مربوط

۱. برای مثال از سال ۲۰۱۴ فیسبوک برای اعضای جدید اصل را بر این گذاشت که اولین پیام‌ها خطاب به دوستان است و نه به عموم، نگاه کنید به:
"Facebook Introduces Privacy Checkup Tool, And New Default Privacy Settings" https://www.searchenginejournal.com/facebook-introduces-privacy-checkup-tool-new-default-privacy-settings/106717/ (last accessed 10/06/2016).

۲. برای مثال سیاست‌های جدید فیسبوک در سال ۲۰۱۶ از سوی رسانه‌ها اقدامی در جهت تهدید حریم خصوصی تلقی شده است. نگاه کنید به:
http://www.forbes.com/sites/thomasbrewster/2016/06/29/facebook-location-tracking-friend-games/#206063f73348

۳. در خصوص استناد به ماده ۱۷ میثاق مدنی- سیاسی در خصوص حق به احترام حریم خصوصی نگاه کنید به:
CCPR General Comment No. 16: Article 17 (Right to Privacy) The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honor and Reputation, Adopted at the Thirty-second Session of the Human Rights Committee, on 8 April 1988

به سال ۱۹۹۰ است که مهم‌ترین خط‌مشی‌های مربوط به جمع‌آوری اطلاعات شخصی افراد را مشخص می‌کند و در آن از دولت‌ها خواسته شده تا در این چارچوب قانون‌گذاری لازم انجام دهند. مجمع عمومی سازمان ملل در آغاز تحول و همه‌گیرشدن اینترنت و قبل از شکل‌گیری پدیده شبکه‌های اجتماعی در این قطعنامه[1] چند اصل مهم را بنا می‌نهد که به نظر می‌رسد هم اکنون شبکه‌های اجتماعی در حال نقض بسیاری از آنها هستند: این اصول به‌طور خلاصه به شرح زیر هستند:

۱. اصل قانونی بودن و منصفانه بودن[2] یعنی جمع آوری اطلاعات باید به روش قانونی ومنصفانه انجام شود و مغایر این اصول از آن بهره‌برداری نشود.

۲. اصل دقیق بودن مطالب:[3] اطلاعات باید دقیق برداشت شده و به روز باشند تا منشأ اشتباهات در خصوص اشخاص نشوند.

۳. اصل هدف‌دار بودن:[4] جمع‌آوری داده ها باید دلیل داشته باشد، مبنایش مشروع باشد و به نحو مناسب به اطلاع ذی‌نفع هم برسد و اطلاعات هم تا زمانی نگهداری شود که برای رسیدن آن هدف لازم است.

۴. اصل دسترسی شخص ذی‌نفع[5]: هرکس باید بتواند به اطلاعاتی که وی مربوط است در شکلی قابل درک و بدون صرف زمان یا هزینه غیرمعقول دسترسی داشته باشد. همچنین هنگامی که افراد با اطلاعاتی در خصوص خودشان برخورد می‌کنند که اشتباه است، یا به نحو غیرقانونی جمع‌آوری شده است باید حق درخواست اصلاح و پاک کردن این اطلاعات را داشته باشند.

۵. اصل عدم تبعیض[6]: به این معنی که اصولا داده‌هایی که منتهی به اقدامات تبعیض‌آمیز می‌شود نباید جمع‌آوری شود مگر به این دلیل که از این نوع اطلاعات برای رفع تبعیض استفاده شود.

۶. امکان اعمال استثنا[1]: اجازه کنار گذاشتن اصول ۱تا ۴ تنها زمانی می‌تواند صادر شود که امنیت ملی، نظم یا اخلاق عمومی یا بهداشت همگانی ایجاب کرده یا حفاظت از حقوق بشر

1. "Guidelines for the Regulation of Computerized Personal Data Files Adopted by General Assembly resolution 45/95 of 14 December 1990," .
2. Principle of lawfulness and fairness.
3. Principle of accuracy.
4. Principle of the purpose-specification.
5. Principle of interested-person access.
6. Principle of non-discrimination .

سایرین مد نظر باشد. و البته آن هم بشرطی که این استثناها در قانون ملی ذکر شده و قانون محدودیت آن را مشخص کرده باشد و نظام قضایی هم بتواند صحت اِعمال آن را کنترل کند.

۷. اصل امنیت[۲]: باید اقدامات احتیاطی لازم جهت امنیت و حفاظت از داده‌ها اتخاذ شود تا مورد سوء استفاده و دسترسی غیرمجاز یا تخریب به‌وسیله ویروس‌های کامپیوتری یا حتی از بین رفتن در اثر بلایای طبیعی قرار نگیرد.

۸. اصل نظارت و ضمانت اجرا[۳]: قوانین ملی مرتبط با حفاظت از داده‌ها باید مرجع ملی نظارت و مجازات تخطی از اصول پیش‌گفته را مشخص کند. مرجعی که باید بی‌طرف و مستقل از مراجع جمع‌آوری و بهره‌برداری از داده‌ها باشد و صلاحیت فنی کافی نیز داشته باشد.

۹. جریان فرامرزی اطلاعات[۴]: چنانچه «حفاظت از داده‌ها» به شرح اصول گفته شده در بالا در کشورهای ذی‌ربط وجود داشته باشد، باید جریان اطلاعات و داده‌ها آزاد باشد، ولی اگر در یکی از کشورها این تضمین‌ها وجود نداشته باشد، می‌توان به منظور حفاظت از حریم خصوصی افراد، محدودیت‌هایی در جریان و انتقال اطلاعات ایجاد کرد.

قطعنامه ۹۵/۴۵ مجمع عمومی نهایتاً مقرر می‌دارد که این اصول باید: اولاً، بر تمامی فایل‌های انفورماتیک خصوصی و دولتی اعمال شود و ثانیاً، درصورت امکان و به شکل اختیاری در مورد داده‌هایی که به شیوه دستی جمع‌آوری و مورد بهره‌برداری قرار می‌گیرند نیز، اعمال شوند. همچنین با توجه به اینکه این اصول برای حفاظت از اشخاص حقیقی پیش‌بینی شده است، قطعنامه، اجرای چنین حمایت‌هایی را در مورد اشخاص حقوقی، اختیاری تلقی می‌کند.

اما در دهه اخیر، توسعه فناوری‌های رقومی (دیجیتال) و اثری که این توسعه می‌تواند بر حریم خصوصی داشته باشد سازمان ملل را وادار کرد که به‌طور مستقل به مقوله «حق بر حریم خصوصی در فضای دیجیتال» بپردازد.

شورای حقوق بشر سازمان ملل در قطعنامه ژوئیه سال ۲۰۱۲ میلادی،[۵] به لزوم رعایت حقوق بشر در فضای دیجیتال و اهمیت توجه به حقوق بشر در فضای مجازی همچون دنیای واقعی

1. Power to make exceptions.
2. Principle of security.
3. Supervision and sanctions.
4. Transborder data flows.
5. Human Rights Council Resolution 20/8 of 5 July 2012 (A/HRC/28/L.27) .

تأکید کرد. پس از این تاریخ توجه به حقوق بشر در فضای مجازی در سازمان ملل اهمیت خاصی پیدا می‌کند.

کمیسر عالی حقوق بشر سازمان ملل در کمیته‌های کارشناسان که در سپتامبر ۲۰۱۳ و فوریه ۲۰۱۴ در ژنو برگزار شد، زنگ خطر ناشی از کنترل و نظارت بر مردم و خطری که برای حریم خصوصی دارد را به صدا در آورد[1] و در ۱۸ دسامبر ۲۰۱۳ ، قطعنامه مجمع عمومی تحت همین عنوان یعنی «حق بر حریم خصوصی در فضای دیجیتال» با وفاق عام به تصویب رسید. در این قطعنامه مجمع ضمن تأکید مجدد بر وجود حق بر حریم خصوصی، از جمله در فضای دیجیتال، از اثرات منفی نظارت بر ارتباطات و/یا شنود آنها و همچنین جمع‌آوری اطلاعات شخصی افراد– به‌ویژه هنگامی در ابعاد کلان انجام شود– بر اجرا و بهره بردن از حقوق بشر ابراز نگرانی کرده است.

در این قطعنامه مجمع از دولت‌های عضو می‌خواهد:

الف) حق بر حریم خصوصی را (از جمله در فضای دیجیتال) به رسمیت شناخته و مورد حمایت قرار دهند.

ب) اقدامات لازم را جهت خاتمه دادن به نقض این حق انجام داده و شرایط لازم برای پیشگیری از چنین نقض‌هایی را، از جمله از طریق قانون‌گذاری، اتخاذ کنند.

ج) گردش‌کارها و عملکردها و مقررات خود را در خصوص نظارت بر ارتباطات به منظور ارتقای جایگاه حریم خصوصی مورد بازبینی قرار دهند.

د) نهاد مستقل نظارتی ایجاد کنند یا اگر موجود است آن را بکار گیرند تا از شفافیت و پاسخگویی دستگاه‌های دولتی ناظر بر ارتباطات اطمینان حاصل کنند.

این قطعنامه اگر چه در چارچوب نگرانی‌های ناشی از شنود و نظارت بر ارتباطات و اطلاعات از سوی دولت‌ها و به‌ویژه ایالات متحده آمریکا تصویب گردیده است، اما با توجه به تأکیداتی که در خصوص حفظ حریم خصوصی در زندگی برخط مردم و توجهی که به معضل جمع‌آوری اطلاعات در قالب کلان‌داده‌ها دارد، می‌تواند بستری برای محدودسازی شبکه‌های اجتماعی باشد.

[1]. "Opening Remarks by Ms. Navi Pillay United Nations High Commissioner for Human Rights to the Expert Seminar: The right to privacy in the digital age", 24 February 2014, Palais des Nations, Geneva," available at: http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?LangID=E&NewsID=14276
"Opening Remarks by Ms. Navi Pillay, United Nations High Commissioner for Human Rights to the Side-event at the 24th session of the UN Human Rights Council How to safeguard the right to privacy in the digital age?" 20 September 2013, available at : http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=13758&LangID=E

قطعنامه موصوف آغاز اقدامات جدیدی است که مجمع عمومی تصمیم دارد درباره حریم خصوصی اتخاذ کند. کما اینکه ملاحظه می‌شود مجمع همچنان موضوع را در دستور کار خود داشته و در سال بعد یعنی در دسامبر سال ۲۰۱۴ میلادی طی قطعنامه دیگری[1] مجدداً بر مواضع قبلی خود تأکید می‌کند.

شورای حقوق بشر قدم بلندتری در خصوص حریم خصوصی برداشته و در قطعنامه سال ۲۰۱۵ خود[2] اعلام می‌کند که تصمیم دارد گزارشگر ویژه‌ای را به مدت سه سال به امر رصد وضعیت حریم خصوصی در فضای دیجیتال بگمارد و از وی می‌خواهد ضمن انجام تفحص لازم در این امر، موارد تخطی و تخلف از رعایت حق بر حریم خصوصی در جهان را در گزارشات سالانه خویش به شورا اعلام کند. اکنون باید منتظر بازتاب عملکرد شبکه‌های اجتماعی در گزارش گزارشگر ویژه سازمان ملل بود. البته نباید فراموش کرد که شورای حقوق بشر بیش از همه، نگران جمع‌آوری داده‌های شخصی صدها میلیون نفر توسط دولت‌های صاحب قدرت جهان و از جمله جمع‌آوری و شنود فراملی داده‌ها در جهان است.

ج) مقررات در سطح منطقه‌ای:

هرچند در سطح بین‌المللی فعالیت‌هایی در جریان است ولی به دلیل ناهمگن بودن جامعه بین‌المللی پیشرفت‌ها هنوز بطئی است در حالی‌که در سطح منطقه‌ای و به‌ویژه در سطح اروپا پیشرفت‌های بیشتری حاصل شده است. اتحادیه اروپا، شورای اروپا و سازمان همکاری و توسعه اقتصادی OEDC هر کدام مجموعه‌ای از قطعنامه‌ها، توصیه‌نامه‌ها و مقررات را درباره جمع‌آوری داده‌های افراد دارند.[3] ولی جز مقررات اروپایی که امکان اجرای مستقیم در سطح ملی را دارد در خصوص مابقی اسناد، به مدد این رهنمودها مقررات‌گذاری در سطح ملی انجام گرفته و می‌گیرد

1. Resolution 69/166 (18 December 2014).
2. A/HRC/28/L.27 (24 March 2015).

۳. برای مثال نگاه کنید به:
the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (“Convention 108”)
Charter of fundamental rights of the European Union 7 dec 2000
Directive on protection of individuals with regard to the processing of personal Data and on the free movement of such data
Directive 2006 /24/ec 2006 on the retention of data generated ir processed in connection with the provision of publicly available electronic communications services of of public communications networks and amending directive2002/58/EC

و انتظار می‌رود با گسترش قانون‌گذاری در این حوزه، شبکه‌های اجتماعی به نحو بهتری به رعایت حریم خصوصی ترغیب شوند.

در اروپا فعلاً مقررات ناظر به حفاظت از داده‌های سال ۱۹۹۵حاکم است. این مقررات زمانی به تصویب رسیده است که پدیده شبکه‌های اجتماعی در فضای مجازی به شکل فعلی وجود نداشت و اساسا استفاده از اینترنت به هیچ وجه قابل مقایسه با دنیای امروز نبود. ناکافی بودن حمایت‌های ناشی از این مقررات باعث شد تا کمیسیون اروپا طرح مقررات جدید حمایت از داده را پیشنهاد نماید. طرحی که هنوز در جریان تصویب قرار دارد.[1]

د) سطح ملی:

به‌طور طبیعی بیشترین تلاش‌ها در حوزهٔ حمایت از داده‌ها در سطح ملی اتفاق افتاده و می‌افتد. مرور مقررات ملی و تحولات آن در چارچوب این مقاله نمی‌گنجد ولی ناگزیر از یادآوری فقر قانونی ناظر به حمایت از حریم خصوصی در فضای دیجیتال در ایران هستیم.

در ایران به‌طور مشخص موضوع حمایت از حریم خصوصی و محرمانگی اطلاعات شخصی در قانون برنامه چهارم توسعه مورد توجه قرار گرفت و لایحه حمایت از حریم خصوصی نیز در اجرای ماده ۱۰۰ همین قانون[2] تهیه و به مجلس تقدیم شد. ولی متعاقبا به‌وسیله دولت در سال۱۳۸۵ پس گرفته شد و تلاش‌های بعدی در ایجاد یک نظام حقوقی خاص حفاظت از حریم خصوصی، از جمله از طریق تقدیم طرحی قانونی به‌وسیله برخی نمایندگان نیز بجایی نرسید. با این وصف تنها متن رسمی قابل استناد در حوزه حریم خصوصی در کشور همین لایحه است که امید می‌رود با توجه به تحولات در فضای مجازی در یک دهه گذشته، مجددا با اصلاحات لازم، در دستور تقنین قرار گیرد.

در نبود یک قانون جامع حمایت از حریم خصوصی در قوانین کشور بصورت پراکنده وناکافی وجود دارد: طبق ماده ۱۷ قانون جرائم یارانه‌ای، افشای اسرار دیگری در فضای مجازی بدون

1. http://ec.europa.eu/justice/data-protection/reform/index_en.htm

۲. ماده ۱۰۰ برنامه چهارم دولت را موظف می‌کند که به منظور ارتقای حقوق انسانی، استقرار زمینه‌های رشد .. «منشور حقوق شهروندی» را مشتمل بر محورهای ذیل تنظیم و به تصویب مراجع ذی‌ربط برساند:
و) حفظ و صیانت از حریم خصوصی افراد.

رضایتش به‌نحوی که منجر به ضرر یا هتک حیثیت شود، جرم و قابل مجازات کیفری (تا دو سال زندان یا/و چهل میلیون ریال جزای نقدی) دانسته شده است.

در نهایت در حوزه حمایت از داده‌ها در فضای سایبر، قانون تجارت الکترونیک مصوب ۱۳۸۲ توانسته است تا حدودی نبود قانون ویژه حمایت از حریم خصوصی و داده‌ها را جبران کند. این قانون ضمن پیش‌بینی اصولی در مواد ۵۸ و ۵۹ خود که ملهم از اصول بین‌المللی پیش‌گفته است، در ماده ۷۱ نقض این مواد قانون را جرم محسوب کرده و ضمانت اجرای کیفری یک تا سه سال حبس را برای آن مقرر کرده است.

نتیجه‌گیری

شبکه‌های اجتماعی در کنار کارکردهای مثبتی که می‌توانند در توسعه اجتماعی و بهبود حقوق بشر داشته باشند خطری جدی برای حریم خصوصی به‌شمار می‌روند. این مخاطرات، از یک سو به طبیعت این شبکه‌ها و از سوی دیگر به نحوه استفادهٔ آنها از داده‌های مردم باز می‌گردد. ذاتی بودن مخاطرات شبکه‌های اجتماعی، نباید ما را از خطرات ناشی از رفتار مؤسسات و گردانندگان شبکه‌ها غافل دارد. بی دلیل نیست که سازمان ملل و نهادهای منطقه‌ای مانند اتحادیه اروپا بر اصلاح مقررات مرتبط با جمع‌آوری داده و نحوه استفاده از آن متمرکز شده‌اند. با گسترش قدرت شبکه‌های اجتماعی و به‌ویژه با توجه به ماهیت بدون مرز فعالیت‌های آنان، لازم است دولت‌ها در همکاری گسترده‌تری به این مسئله اندیشیده و مقررات محدودکننده‌ای در سطح بین‌المللی در خصوص جمع‌آوری و استفاده از اطلاعات تدبیر کنند. راهی که آغاز شده[1] ولی هنوز تا شکل‌گیری احتمالی یک معاهده بین‌المللی در موضوعاتی نظیر حفاظت از حریم خصوصی در فضای مجازی و حفاظت از داده، در مراحل بسیار ابتدایی بسر می‌برد.

در نبود معاهده‌ای فراگیر، خود تنظیمیِ هدایت شده و حمایت شده از سوی دولت و جامعه مدنی مهمترین عامل کنترل شبکه‌های اجتماعی بشمار می رود. ولی دولتها به آن اکتفا نکرده و به توصیهٔ نهادهای جهانی و منطقه‌ای مقررات‌گذاری و کنترل نحوه جمع‌آوری و استفاده از داده را در دستور کار خود قرار داده‌اند، به‌گونه‌ای که می‌توان ادعا کرد، امروز اصول شناخته‌شده بین‌المللی در خصوص چگونگی جمع‌آوری و بهره‌برداری از داده‌ها محور قانون‌گذاری ملی را تشکیل می‌دهد. در کشور ما نیز، اتخاذ اقدامات قانونی تکمیلی در این جهت، ضروری بنظر می‌رسد.

با این حال نباید فراموش کرد که حفاظت از حریم خصوصی در وهله اول با خود افراد است. نهادهای دولتی و مردمی می‌توانند از طریق آموزش عمومی و بویژه آموزش نسل جوان که بیشترین استفاده را از این شبکه‌ها می‌کند به این خودکنترلی کمک کنند. حفاظت از خود می‌تواند از طریق استفاده از «فناوری‌های تشدید حفاظت از حریم خصوصی» [2] نیز تقویت شود.

---

۱. برای مثال نگاه کنید به:
Joint proposal for a draft of international standards on the protection of privacy with regard to the processing of personal Data of 5 Nov 2009 available at:
http://privacyconference2011.org/htmls/adoptedResolutions/2009_Madrid/2009_M1.pdf (last visited 10/06 2016) .

2. Privacy Enhancing Technologies (PETS) .

فهرست منابع

الف) فارسی

۱. انصاری، باقر؛ «**واکاوی مفهومی حریم خصوصی و مفاهیم مشابه**»، گزارش مورخ ۱۳۹۴/۱۲/۱۵ نشست علمی «مفهوم و قلمروی حریم خصوصی در نظام حقوقی ایران» پژوهشگاه قوه قضائیه،

۲. انصاری، باقر؛ «**حریم خصوصی و حمایت از آن در حقوق اسلام تطبیقی و ایران**»، مجله دانشکده حقوق و علوم سیاسی، زمستان ۱۳۹۳، ش ۶۶ (ص‌ص ۱-۵۳).

۳. رحمدل، منصور؛ «**حق انسان بر حریم خصوصی**» دانشکده حقوق و علوم سیاسی(دانشگاه تهران) ۷۰، ش، ۱۳۸۴، ۱۱۹-۴۶.

۴. عطار، شیما؛ «**حمایت از حریم خصوصی در شبکه های اجتماعی مجازی**» (پایان‌نامه کارشناسی ارشد، دانشگاه علامه طباطبایی، ۱۳۹۲).

ب) لاتین

5. Bostwick Gary L., "**A Taxonomy of Privacy: Repose, Sanctuary, and Intimate Decision**," California Law Review 64, no. 6 (1976): 1447–1483, doi:10.2307/3480041.
6. Boyd, Danah M. and Nicole B. Ellison, "Social Network Sites: "**Definition, History, and Scholarship**", Journal of Computer-Mediated Communication, Vol. 13, no. 1 (October 2007): 210–30, doi:10.1111/j.1083-6101.2007.00393.x.
7. Dugain, Marc, and Christophe Labbe. L'homme nu La dictature invisible du numérique. Paris : Plon, 2016.
8. Elovici Yuval and Yaniv Altshuler, "**Introduction to Security and Privacy in Social Networks**," *in* Security and Privacy in Social Networks , New York, NY: Springer New York, 2013 , 1–6, doi:10.1007/978-1-4614-4139-7_1.
9. Fiegerman, Seth, "**Facebook's annual revenue topped $10 billion for the first time in 2014**", Mashable, available at : http://mashable.com/2015/01/28/facebook-q4-earnings-2014/ (last accessed 10/5/2016).

10. Hildebrandt, Mireille and Serge Gutwirth, (eds.), Profiling the European Citizen: Cross-Disciplinary Perspectives (Springer, 2008), doi:10.1007/978-1-4020-6914-7.
11. Margulis, Stephen T., "**Three Theories of Privacy: Un Overview**" *in* Privacy Online, Perspectives on Privacy and Self-Disclosure in the Social Web, ed. Sabine Trepte and Leonard Reinecke Dordrecht London New York: springer, 2011, 9–18, doi:10.1007/978-3-642-21521-6.
12. Obar, Jonathan A. and Steven S. Wildman, "**Social Media Definition and the Governance Challenge: An Introduction to the Special Issue**" SSRN Electronic Journal, 2015, doi:10.2139/ssrn.2647377. p 745.
13. Perrin, Andrew. "**Social Networking Usage: 2005-2015**", Pew Research Center. October 2015. Available at: http://www.pewinternet.org/2015/10/08/2015/Social-Networking-Usage-2005-2015/
14. Skouma, Georgia and Laura Léonard, "**On-line Behavioral Tracking: What May Change After the Legal Reform on Personal Data Protection**" *in* Serge Gutwirth, Ronald Leenes, and Paul de Hert, (eds.), Reforming European Data Protection Law (Springer, 2015), doi:10.1007/978-94-017-9385-8. P 35.
15. Walther, Joseph B., "**Introduction to Privacy Online**", *in* Privacy Online, Perspectives on Privacy and Self-Disclosure in the Social Web, ed. Sabine Trepte and Leonard Reinecke, 2011. P 4-5.

ج) اسناد بین‌المللی

16. "Opening Remarks by Ms. Navi Pillay United Nations High Commissioner for Human Rights to the Expert Seminar: The right to privacy in the digital age", 24 February 2014, Palais des Nations, Geneva," available at: **http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?LangID=E&NewsID=14276**
17. "Opening Remarks by Ms. Navi Pillay, United Nations High Commissioner for Human Rights to the Side-event at the 24th session of the UN Human Rights Council How to safeguard the right to privacy in the digital age?" 20 September 2013, available at : http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=13758&LangID=E

18. A/68/168 (18 Dec. 2013)
19. A/HRC/28/L.27 (24 March 2015)
20. A/HRC/28/L.27 Human Rights Council Resolution 20/8 of 5 July 2012
21. A/res/45/95 (14 December 1990) : "Guidelines for the Regulation of Computerized Personal Data Files" .
22. CCPR General Comment No. 16: Article 17 (Right to Privacy) The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honor and Reputation, Adopted at the Thirty-second Session of the Human Rights Committee, on 8 April 1988
23. Charter of fundamental rights of the European Union 7 December 2000
24. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ("Convention 108")
25. Directive 2006 /24/EC 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services of public communications networks and amending directive 2002/58/EC
26. Directive on protection of individuals with regard to the processing of personal Data and on the free movement of such data
27. Joint proposal for a draft of international standards on the protection of privacy with regard to the processing of personal Data of 5 Nov 2009 available at: http://privacyconference2011.org/htmls/adoptedResolutions/2009_Madrid/2009_M1.pdf (last visited 10/06 /2016)
28. Opening Remarks by Ms. Navi Pillay United Nations High Commissioner for Human Rights to the Expert Seminar: The right to privacy in the digital age, 24 February 2014, Room XXI, Palais des Nations, Geneva,"
29. Resolution AG/69/166 (18 December 2014)

URLs:

29. http://www.webdesignerdepot.com/2009/10/the-history-and-evolution-of-social-media/(last accessed :15/mai/2016)

30. “Reform of EU data protection rules” http://ec.europa.eu/justice/data-protection/reform/index_en.htm
31. "Internet Self-Regulation: An Overview,”, http://www.law.uni-sofia.bg/Kat/T/IP/T/PM/DocLib/Internet%20Self-Regulation%20An%20Overview.htm (accessed 25/ 5/ 2016)
32. “Facebook Introduces Privacy Checkup Tool, And New Default Privacy Settings - Search Engine Journal,” https://www.searchenginejournal.com/facebook-introduces-privacy-checkup-tool-new-default-privacy-settings/106717/ (last accessed 10/06/2016).
33. http://www.forbes.com/sites/thomasbrewster/2016/06/29/facebook-location-tracking-friend-games/#206063f73348
34. http://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/ (last visited 7/12/2016):
35. http://blog.instagram.com/post/146255204757/160621-news (last accessed 13/7/2016) http://blog.instagram.com/post/129662501137/150922-400million (last accessed 13/7/2016)
36. “Facebook Removing Option To Be Unsearchable By Name, Highlighting Lack Of Universal Privacy Controls,” https://techcrunch.com/2013/10/10/facebook-search-privacy (last accesed 10/06/2016
37. https://www.cookielaw.org
38. http://www.aboutcookies.org/cookie-faq/
39. http://www.reuters.com/article/us-facebook-belgium-idUSKCN0ZF1VV (last accessed 2/7/2016)
40. https://www.facebook.com/full_data_use_policy (last accessed 1/6/2016)