Journal of Iran Cultural Research, 10(2), 125-151, Autumn 2017

Siasirad, F., & Bicharanlou, A. (2017). The models of applying online privacy literacy strategies; A case study of Instagram girl users. *Journal of Iran Cultural Research*, 10(3), 125-151. doi: 10.22631/JICR.2017.1534.2230

Doi: https://www.doi.org/10.22631/JICR.2017.1534.2230 URL: http://www.jicr.ir/article_345.html

The Models of Applying Online Privacy Literacy Strategies: A Case Study of Instagram Girl Users

Farzaneh Siasirad[1], **Abdollah Bicharanlou**[*2]

Received: Mar. 15, 2017; Accepted: Aug. 13, 2017

Extended Abstract

Social networks affect remarkably in the lives of virtual space users. These networks like most human relations involve compromising between self-disclosure and privacy protection. A process which is realized through improving privacy and empowering the user at the personal level. This study aimed to assess strategies based on online privacy literacy. In particular, strategies that Instagram young girls users should employ to achieve the optimum level of privacy. For this purpose, firstly the paradox of privacy, benefits and risks of self-disclosure are explained, then according to online privacy literacy, some social and technological strategies are introduced by which users can solve the "paradox of privacy." In the result section, after describing the main benefits and risks of self-disclosure by girl users, the current models of using these social and technological strategies to solve the mentioned paradox are discussed. The research method is ethnography based on non-collaborative observation of Instagram pages and semi-structured interviews with 20 girl users of social networks.

Keywords: Online privacy literacy, privacy, self-disclosure, social virtual networks

1. M.A. Student of Cultural Studies and media, faculty of social Sciences, University of Tehran, Tehran, Iran.
fsiasirad@yahoo.com

2. Assistant Professor of Social Communications, faculty of Social Sciences, University of Tehran, Tehran, Iran (Corresponding Author).
✉ bikaranlou@ut.ac.ir

Introduction

The increasing use of virtual networks and communities in recent years has brought up many arguments on the benefits and risks of these communities and how to reach the optimum level of user`s privacy. According to the literature, achieving an optimal level of privacy (Altman, 1977) requires the elimination of conflict between self-disclosure and privacy and is, in fact, subject to the calculation of the self-disclosure`s risk-benefit ratio by users (Petronio, 2002, 26). The users' mastery of technological and social strategies based on online privacy literacy will help them to overcome this contradiction and achieve optimal level in defining the privacy boundaries (Trepte et al., 2014; Park, 2011).

Purpose

The main purpose of this research was to assess the benefits and risks of self-disclosure with regard to girl users as well as their degree of mastery on social and technological strategies to manage their privacy.

Methodology

The study was conducted by ethnography method through a semi-structured interview and non-collaborative observation of 20 Instagram girls' pages. The samples were selected purposefully and in most cases with prior acquaintance and privacy concerns. The sample included users with maximum dispersion of social relationships, beliefs, family circumstances, and number of shared posts.

Results

The results of ethnographic study are provided in three sections: 1) describing the most important benefits and risks of self-disclosure for the girls, 2) various types of employed social and technological strategies, and 3) the patterns available on how to apply these strategies.

Social and psychological benefits and risks are the four main themes describing the paradox of privacy for informants. Psychological benefits emphasizing the centrality of emotions in self-disclosure comprised these codes: "expression (distress relief) and improvement of individual emotions", "evacuation of individual emotions", "self-clarification", and "recording the positive and memorable moments". The codes of "having voice", "acquiring awareness", "knowing oneself and others", "relationships restoration and maintenance", "relationship development", "social control" and "representing oneself" are subsets of the social benefits theme. Risks of self-disclosure are often subsets of social risks, i.e., other people turn a disclosure into a risk. These risks included "face risk", "superficiality risk", "misunderstanding risk", "round risk", "judgment risk", "relationship risk", "role risk for oneself or another" and "security risk", "Regret risk" is the only code which is the subset of psychological risk.

Strategies for managing the privacy boundaries are summarized in technological and social strategies themes. Codes for "not expressing mental states", "not expressing personal issues", "emphasis on keeping personal identity", "not publishing personal and family images", "conforming to custom and public beliefs", "defining the coverage limits", "indirect expression of disclosure", "anonymity", "adding caption" and "creating exposure intervals" represent social strategies or content control. The technology strategies related to the privacy

Iran Cultural Research

Vol. 10
No. 3
Autumn 2017

management features in Instagram, according to the most widely used informants included "target selection (private page)", "blocking", "rejecting request", "deleting post", "deleting comment", "direct message", "un tagging", "not publicizing comments" and "using multiple accounts simultaneously".

Based on the effects of each benefit, risk, social and technological strategy employed by the girl users, their achievement in optimal online privacy level is divided into five patterns. These patterns include "using low technological strategies and high social strategies", "using high technological strategies and low social technological", "using high technological and social strategies", "using low technological and social strategies", and "balanced use of technological and social strategies".

Conclusion

According to the findings, all girl users experienced some privacy paradox. This contradiction is seen more in the area of psychological benefits, which users felt more at risk in achieving them. Disregarding these benefits often results in more dissatisfaction of the users. However, this contradiction was not the same for all users. It was disturbing for some users to the point of neglecting self-disclosure and its benefits. However, others feel this contradiction less harming, disregard the risks, and take the benefits. The findings also indicate that users apply "social strategies" more than "technological strategies". Therefore, some users are not sufficiently skilled in applying the technological strategies and need further training in this regard. Ignoring social strategies and lack of knowledge on technological privacy strategies have exposed girls to privacy threats in some cases. Although the optimal level of privacy is relative and can be quite different for various users, among the patterns introduced in this article, the users in the last category can be considered as the most successful group in achieving the highest level of online privacy based on their reported degree of satisfaction. In addition, the results indicate that these users experience the highest level of benefits and the lowest risks, as well as the balanced and complementary use of technological and social strategies. However, a few numbers of users are in this category which indicates the relative failure of other users to correctly use the strategies in resolving their privacy conflicts. Therefore, in the worst case scenario, some people have to ignore the benefits and others have gone away from privacy due to neglecting risks.

Bibliography

Acquisti, A., & Grossklags, J. (2005). Privacy and rationality in individual decision making. *IEEE Security & Privacy*, 3(1), 24-30. doi: 10.1109/MSP.2005.22

Altman, I. (1977). Privacy regulation: Culturally universal or culturally specific?. *Journal of Social Issues*, 33(3), 66-84. doi: 10.1111/j.1540-4560.1977.tb01883.x

Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. *First Monday*, 11(9). doi: 10.5210/fm.v11i9.1394

Bartsch, M., & Dienlin, T. (2016). Control your Facebook: An analysis of online privacy literacy. *Computers in Human Behavior*, 56, 147-154. doi: 10.1016/j.chb.2015.11.022

Bawden, D. (2008). Origins and concepts of digital literacy. In C. Lankshear, & M. Knobel, *Digital Literacies: Concepts, Policies and Practices* (pp. 17-32), New York: Peter Lang.

Ben-Ze'ev, A. (2003). Privacy, emotional closeness, and openness in cyberspace. *Computers in Human Behavior*, 19(4), 451–467. doi: 10.1016/S0747-5632(02)00078-X

Berg, J. H., & Derlega, V. J. (1987). Themes in the study of self-disclosure. In V. J. Derlega, & J. H. Berg, *Self-Disclosure: Theory, Research, and Therapy* (pp. 1-8), New York: Plenum Press.

Boyd, D., & Hargittai, E. (2010). Facebook privacy settings: Who cares?. *First Monday*, 15(8). doi: 10.5210/fm.v15i8.3086

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2), 77-101. doi: 10.1191/1478088706qp063oa

Burgess, R. G. (1981). Keeping a research diary. *Cambridge Journal of Education*, 11(1), 75-83. doi: 10.1080/0305764810110106

Derlega, V. J., Winstead, B. A., & Greene, K. (2008). Self-disclosure and starting a close relationship. In S. Sprecher, A. Wenzel, & J. Harvey, (Eds.). *Handbook of Relationship Initiation* (pp. 153–174), New York: Psychology Press.

Ellison, N. B., Vitak, J., Steinfield, C., Gray, R., & Lampe, C. (2011). Negotiating privacy concerns and social capital needs in a social media environment. In S. Trepte, & L. Reinecke, *Privacy Online: Perspectives on Privacy and Self-Disclosure in the Social Web* (pp. 19-32), Berlin: Springer.

Eshet-Alkali, Y., & Amichai-Hamburger, Y. (2004). Experiments in digital literacy. *CyberPsychology & Behavior*, 7(4), 421-429. doi: 10.1089/cpb.2004.7.421

Flick, U. (2008). *Darāmadi bar tahqiq-e keyfi* [An introduction to qualitative research] (H. Jalili, Trans.). Tehran, Iran: Našr-e Ney. (Original work published 2006)

Fogel, J., & Nehmad, E. (2009). Internet social network communities: Risk taking, trust, and privacy concerns. *Computers in Human Behavior*, 25(1), 153-160. doi: 10.1016/j.chb.2008.08.006

Gattiker, U. E., Perlusz, S., Bohmann, K., & Sørensen, C. M. (2001). The virtual community: Building on social structure, relations and trust to achieve value. In L. Chidambaram, & I. Zigurs, *Our Virtual World: The Transformation of Work, Play and Life via Technology* (pp. 165-187), Hershey; USA & London; Uk: Idea Group Publishing.

Hall, G. (2008). An ethnographic diary study. *ELT Journal*, 62(2), 113-122. doi: 10.1093/elt/ccm088

Hallett, R. E., & Barber, K. (2013). Ethnographic research in a cyber era. *Journal of Contemporary Ethnography*, 43(3), 306-330. doi: 10.1177/0891241613497749

Hargittai, E. (2002). Second-level digital divide: Differences in people's online skills. *First Monday*, 7(4). doi: 10.5210/fm.v7i4.942

Hill, C. T., & Stull, D. E. (1987). Gender and self-disclosure: Strategies for exploring the issues. In V. J. Derlega, & J. H. Berg, *Self-Disclosure: Theory, Research, and Therapy* (pp. 81-100), New York: Plenum Press.

Hu, Y., Manikonda, L., & Kambhampati, S. (2014). What we Instagram: A First analysis of Instagram photo content and user types. Paper be Peresented at The *8th International AAAI Conference on Weblogs and Social Media*, June 1-4, 2014, *USA, Michigan*. Retrived from https://www.aaai.org/ocs/index.php/ICWSM/ICWSM14/paper/viewFile/8118/8087

Lee, H., Park, H., & Kim, J. (2013). Why do people share their context information on social network services? A qualitative study and an experimental study on users' behavior of balancing perceived benefit and risk. *Human-Computer Studies*, 71, 862–877. doi: 10.1016/j.ijhcs.2013.01.005

Lewis, K., Kaufman, J., & Christakis, N. (2008). The taste for privacy: An analysis of college student privacy settings in an online social network. *Journal of Computer-Mediated Communication*, 14(1), 79-100. doi: 10.1111/j.1083-6101.2008.01432.x

Li, Y. (2012). Theories in online information privacy research: A critical review and an integrated framework. *Decision Support Systems*, 54(1), 471-481. doi: 10.1016/j.dss.2012.06.010

Lindlof, T. R., & Taylor, B. C. (2009). *Raveshā-ye tahqiq-e keyfi dar olum-e ertebātāt* [Qualitative communication research methods] (A. Guivian, Trans). Tehran, Iran: Hamšahri. (Original work published in 2002)

Litt, E. (2013). Understanding social network site users' privacy tool use. *Computers in Human Behavior*, 29, 1649–1656. doi: 10.1016/j.dss.2012.06.010

Markham, T., & Couldry, N. (2007). Tracking the reflexivity of the (Dis) Engaged citizen some methodological reflections. *Qualitative Inquiry*, 13(5), 675-695. doi: 10.1177/1077800407301182

Omarzu, J. (2000). A disclosure decision model: Determining how and when individuals will self-disclose. *Personality and Social Psychology Review*, 4(2), 174-185. doi: 10.1207/S15327957PSPR0402_05

Park, Y. J. (2011). Digital literacy and privacy behavior online. *Communication Research*, 1-22. doi: 10.1177/0093650211418338

Park, Y. J. (2015). Do men and women differ in privacy? Gendered privacy and (in) equality in the internet. *Computers in Human Behavior*, 50, 252-258. doi: 10.1016/j.chb.2015.04.011

Petronio, S. (2002). *Boundaries of privacy: Dialectics of disclosure.* New York: State University of New York Press.

Price, B. A., Adam, K., & Nuseibeh, B. (2005). Keeping ubiquitous computing to yourself: A practical model for user control of privacy. *International Journal of Human-Computer Studies*, 63(1), 228-253. doi: 10.1016/j.ijhcs.2005.04.008

Stutzman, F., Vitak, J., Ellison, N. B., Gray, R., & Lampe, C. (2012). Privacy in interaction: Exploring disclosure and social capital in Facebook. Paper Peresented at the *Sixth International AAAI Conference on Weblogs and Social Media,* June 4-8, 2012, Dublin, Irland. Retrived from https://www.aaai.org/ocs/index.php/ICWSM/ICWSM12/paper/viewFile/4666/5000

Taddicken, M. (2012). Privacy, surveillance, and self-disclosure in the social web. In C. Fuchs, K. Boersma, A. Albrechtslund, & M. Sandoval, (Eds.). *Internet and Surveillance: The Challenges of Web 2.0 and Social Media* (pp. 255-272), New York: Routledge Publication.

Thelwall, M. (2011). Privacy and gender in the social web. In S. Trepte, & L. Reinecke, *Privacy Online: Perspectives on Privacy and Self-Disclosure in the Social Web* (pp. 251-265), Berlin: Springer.

Trepte, S., Teutsch, D., Masur, P. K., Eicher, C., Fischer, M., Hennhöfer, A., & Lind, F. (2014). Do people know about privacy and data protection strategies? Towards the "Online Privacy Literacy Scale" (OPLIS). In S. Gutwirth, R. Leenes, & P. D. Hert, *Reforming European Data Protection Law* (pp. 333-365), Netherlands: Springer.

Tufekci, Z. (2008). Can you see me now? Audience and disclosure regulation in online social network sites. *Bulletin of Science, Technology & Society*, 28(1), 20-36.

Yao, M. Z. (2011). Self-protection of online privacy: A behavioral approach. In S. Trepte, & L. Reinecke, *Privacy Online: Perspectives on Privacy and Self-Disclosure in the Social Web* (pp. 111-125), Berlin: Springer.

فصلنامه تحقیقات فرهنگی ایران، ۱۰(۳)، ۱۵۱-۱۲۵، پاییز ۱۳۹۶

سیاسی‌راد، فرزانه؛ و بیچرانلو، عبدالله (۱۳۹۶). الگوهای به‌کارگیری راهبردهای سواد حریم خصوصی آنلاین؛ مطالعه موردی کاربران دختر اینستاگرام. فصلنامه تحقیقات فرهنگی ایران، ۱۰(۳)، ۱۵۱-۱۲۵. doi: 10.22631/JICR.2017.1534.2230

شاپا: ۱۸۴۷-۲۰۰۸ URL: http://www.jicr.ir/article_345.html Doi: https://www.doi.org/10.22631/JICR.2017.1534.2230

الگوهای به‌کارگیری راهبردهای سواد حریم خصوصی آنلاین؛ مطالعهٔ موردی کاربران دختر اینستاگرام

فرزانه سیاسی راد[۱]، عبدالله بیچرانلو*[۲]

دریافت: ۱۳۹۵/۱۲/۲۵ پذیرش: ۱۳۹۶/۰۵/۲۲

چکیده

امروزه شبکه‌های اجتماعی در زندگی کاربران حضوری پُررنگ دارند، اما بهره‌مندی کاربران از مزایای آن‌ها، مانند اغلب تعاملات میان‌فردی در زندگی واقعی مستلزم حل تناقض میان خودافشاگری و حفظ حریم خصوصی کاربر است. این بهره‌مندی با فرایندهای بهینه‌سازی حریم خصوصی و با تأکید بر توانایی‌های کاربر در سطح فردی محقق می‌شود. هدف اصلی این نوشتار ایجاد درکی از چگونگی به‌کارگیری راهبردهای مبتنی بر سواد حریم خصوصی آنلاین برای دستیابی کاربران دختر اینستاگرام به سطح بهینه حریم خصوصی است. به این منظور ابتدا تناقض حریم خصوصی، مزایا و خطرهای خودافشاگری بررسی شده و سپس بر اساس سواد حریم خصوصی آنلاین، برخی از راهبردهای اجتماعی و فنّاورانه برای حل «تناقض حریم خصوصی» معرفی شده‌اند. در بخش یافته‌ها پس از توصیف مهم‌ترین مزایا و خطرهای خودافشاگری برای کاربران دختر، الگوهای فعلی چگونگی به‌کارگیری راهبردهای اجتماعی و فنّاورانه برای حل این تضاد استخراج و دربارهٔ آن‌ها بحث شده است. این بررسی به روش مردم‌نگاری و با مصاحبهٔ نیمه‌ساخت‌یافته و مشاهدهٔ غیرمشارکتی صفحات ۲۰ کاربر دختر اینستاگرام صورت گرفته است.

کلیدواژه‌ها: سواد حریم خصوصی آنلاین، حریم خصوصی، خودافشاگری، شبکه‌های اجتماعی مجازی

---

۱. دانشجوی کارشناسی ارشد مطالعات فرهنگی و رسانه، دانشکده علوم اجتماعی، دانشگاه تهران، تهران، ایران.
fsiasirad@yahoo.com

۲. استادیار علوم ارتباطات اجتماعی، دانشکده علوم اجتماعی، دانشگاه تهران، تهران، ایران (نویسنده مسئول).
bikaranlou@ut.ac.ir ✉

مقدمه

گسترش استفاده از اینترنت در زمینهٔ کار و زندگی فرصت‌های جدیدی برای برقراری ارتباط با دیگران در سراسر جهان فراهم کرده است. از این‌رو، ظهور اجتماعات مجازی فراهم‌کنندهٔ امکان ارتباط میان افرادی است که ممکن است لزوماً یکدیگر را نشناسند و صرفاً با واسطهٔ شبکه‌های الکترونیکی امکان مبادلهٔ اطلاعات برایشان فراهم شده باشد (گیتیکر و همکاران[1]، ۲۰۰۱، ۱۶۶). حضور در این شبکه‌ها و اجتماعات مجازی در سال‌های اخیر با استقبال فراوانی از سوی کاربران در سراسر جهان روبه‌رو شده است. با وجود این و به موازات این رشد، مباحث فراوانی دربارهٔ مزایا، خطرها و تبعات حضور در این محیط‌ها برای حریم خصوصی کاربران طرح شده است. نوشتار پیش‌رو با تأکید بر سطوح فردی و نظریات مرتبط با این سطح در ادبیات حریم خصوصی و سواد حریم خصوصی آنلاین[2]، تلاش می‌کند این مزایا، خطرها و نحوهٔ مدیریت فرایندهای بهینه‌سازی حریم خصوصی را (آلتمن[3]، ۱۹۷۷) از سوی کاربران دختر در شبکه‌های اجتماعی بررسی کند.

در متن استفاده از شبکه‌های اجتماعی مانند هر رابطهٔ اجتماعی جدید دیگری دیالکتیکی جاری است. این دیالکتیک در آغاز هر رابطه میان خودافشاگری از یک‌سو، و حفظ حریم خصوصی از سوی دیگر رخ می‌دهد. بنابر نظریهٔ تنظیم حریم خصوصی آلتمن در هر مرحله از رشد روابط میان افراد نیروهای متناقضی وجود دارد که از یک‌سو موجب حفظ حریم خصوصی و فاصله از دیگران می‌شود و از سوی دیگر فرد را به‌سمت خودافشاگری می‌کشاند (درلگا و همکاران[4]، ۲۰۰۸، ۱۵۷). در نتیجهٔ این تناقض که با عنوان «تناقض حریم خصوصی» شناخته می‌شود، کاربران ممکن است با وجود اطمینان از تهدید، برای حفظ حریم خصوصی خود اقدامی نکنند (بارنز[5]، ۲۰۰۶). این تناقض که با عنوان دوگانهٔ نگرش یا رفتار[6] (اکویستی و کراسکیج[7]، ۲۰۰۵) نیز شناخته می‌شود، در محیط شبکه‌های اجتماعی بدین معناست که کاربر با وجود نگرانی فراوان در مورد حفظ حریم خصوصی خود (نگرش) همچنان به‌گونه‌ای فعال اطلاعات خود را در شبکه‌های اجتماعی به اشتراک می‌گذارد (رفتار) (لی و همکاران[8]، ۲۰۱۳). درحالی‌که

1. Gattiker et al
2. online privacy literacy
3. Altman
4. Derlega et al
5. Barnes
6. Attitude /behavior dichotomy
7. Acquisti & Grossklags
8. Lee et al

برای ارتباطات مؤثر و مسئولانه در شبکه‌های اجتماعی کاربران باید این تناقض میان افشای اطلاعات و حریم خصوصی خود را حل کند (بارچ و دیلن،[1] ۲۰۱۶). به‌زعم ترپت و همکاران[2] (۲۰۱۴، ۳۳۳) برخورداری افراد از سواد حریم خصوصی آنلاین به آن‌ها برای حل کردن این تناقض کمک خواهد کرد.

نظریهٔ حریم ارتباطات[3] ساندارا پترونیو[4] (۲۰۰۲) از جمله نظریاتی است که عوامل فردی را بر بر شکل‌گیری نگرانی‌های حریم خصوصی تأثیرگذار می‌داند (لی[5]، ۲۰۱۲). این نظریه تلاشی است برای تبیین همین واقعیت که افراد چگونه به‌صورت هم‌زمان بر دیالکتیک میان خودافشاگری و حفظ حریم خصوصی خود فائق می‌آیند. بنابراین، با استفاده از این نظریه و در گام اول، مزایا و خطرهای شبکه‌های اجتماعی از نظر دختران جوان روشن شده است تا از این طریق ابعاد دوسویهٔ این تناقض، شناسایی و میزان دغدغه‌مندی دختران برای حل چنین تناقضی مشخص شود. در گام بعد و با توجه به نقشی که سواد حریم خصوصی آنلاین می‌تواند در کنترل اطلاعات شخصی، افزایش مزایا و کاهش خطرهای آنلاین ایفا کند، الگوهای به‌کارگیری راهبردهای سواد حریم خصوصی آنلاین برای دستیابی کاربران دختر به سطح بهینه حریم خصوصی استخراج شده است.

بنابراین، سؤالات اصلی این پژوهش عبارت‌اند از:

۱) مزایای خودافشاگری و به اشتراک گذاشتن اطلاعات شخصی در شبکه‌های اجتماعی مجازی از نظر دختران جوان چیست؟

۲) مهم‌ترین خطرها و تهدیدهایی که کاربران دختر در اثر خودافشاگری متوجه حریم خصوصی خود می‌دانند چیست؟

۳) دختران جوان برای غلبه بر ضرورت خودافشاگری و بهره‌مندی از مزایای این محیط‌ها از یک‌سو و حفظ حریم خصوصی خود از سوی دیگر از چه راهبردهایی (فنّاورانه و اجتماعی) استفاده می‌کنند؟

۴) با توجه به تأکید کاربران بر مزایا، توجه و آگاهی از خطرها و سهم به‌کارگیری هر یک از راهبردهای فنّاورانه و یا اجتماعی، الگوهای کاربران برای دستیابی به حد بهینهٔ حریم خصوصی چیست؟

---

1. Bartsch & Dienlin
2. Trepte et al
3. the Communication Privacy Management theory
4. Sandra Petronio
5. Li

یافته‌های این پژوهش ضمن تشریح دقیق وضعیت و رویکرد دختران جوان به مسئلهٔ حریم خصوصی آنلاین، به نهادهای فرهنگی و سیاست‌گذار برای تدوین قوانین و تسهیل آموزش‌های این گروه و بهبود استراتژی‌های دختران جوان برای حفاظت از حریم خصوصی خود کمک خواهد کرد.

ادبیات نظری

۱. خودافشاگری و حریم خصوصی

خودافشاگری جزء جدایی‌ناپذیر هر تعامل اجتماعی است که به‌معنای «هر پیام راجع‌به خود که فرد به‌واسطهٔ آن با فرد دیگری ارتباط برقرار می‌کند» است (ویلس و گروتز[1]، ۱۹۷۶، ۳۳۸؛ به‌نقل از تدیکن[2]، ۲۰۱۲، ۲۵۶). آلتمن و تیلور[3] (۱۹۷۳) در نظریه نفوذ اجتماعی[4] به تأثیر خودافشاگری بر روابط میان‌فردی اشاره کرده‌اند و ضمن توصیف شکل‌گیری، حفظ و انحلال روابط نزدیک، خودافشاگری را لازمهٔ توسعهٔ روابط نزدیک می‌دانند (به نقل از برگ و درلگا[5]، ۱۹۸۷، ۵). اُمارزو[6] (۲۰۰۰) با طراحی مدل تصمیم‌گیری افشا[7] جزئیات بیشتری را در فرایند خودافشاگری معرفی می‌کند. او خودافشاگری را رفتاری چندبُعدی می‌داند و بر اساس این مدل توضیح می‌دهد که افراد برای توسعهٔ روابط و پیش از خودافشاگری از فرایند تصمیم‌گیری استفاده می‌کنند و متغیرهایی را تعیین می‌کنند که بر عمق، وسعت و مدت افشا آثار پیش‌بینی‌پذیری خواهد داشت. وسعت، مدت و عمق اطلاعات افشاشده از متغیرهای اساسی برای نفوذ بیشتر بر دیگران و برقراری ارتباط گسترده‌تر با آن‌هاست (لی و همکاران[8]، ۲۰۱۳). با وجود این، چنانچه ذکر شد، پیامد خودافشاگری فقط پاداش‌های اجتماعی نیست، بلکه برای فرد به‌صورت همزمان خطرهای اجتماعی را نیز در پی خواهد داشت (اُمارزو، ۲۰۰۰).

با وجود دشوار بودن ارائهٔ تعریفی مشخص از حریم خصوصی به‌دلیل آشفتگی‌های مفهومی و شمول معنایی وسیع، در این مقاله با توجه به اتخاذ دیدگاه فردی در حفاظت از حریم خصوصی بر تعریف آلتمن از حریم خصوصی تأکید شده است. آلتمن (۱۹۷۷) حریم خصوصی را «کنترل

1. Wheeless & Grotz
2. Taddicken
3. Altman and Taylor
4. social penetration theory
5. Berg & Derlega
6. Omarzu
7. disclosure decision model
8. Lee & et al

انتخابی دسترسی به خود[1] در یک گروه» تعریف می‌کند. بر اساس نظر آلتمن حریم خصوصی فرایند پویای بهینه‌سازی بین نیاز به حفظ حریم خصوصی از یک‌سو و نیاز به تعامل اجتماعی از سوی دیگر است؛ بدین معنا حریم خصوصی در بهینه‌ترین حالت هنگامی محقق می‌شود که هر دو نیاز با هم یکی شده و در تناظر با یکدیگر قرار گیرند و بدیهی است که دور شدن از سطح بهینه به‌سمت هر یک از نیازها موجب نارضایتی فرد خواهد شد. از این منظر، حریم خصوصی فرایندی پویاست که در آن افراد گاهی مرزهای حریم خصوصی خود را به‌سوی دیگران می‌گشایند و گاهی بالعکس. اگرچه سازوکارهای آلتمن و پترونیو شامل رفتارهای کلامی و فراکلامی، کنترل فضاهای شخصی و سازوکارهای فرهنگی، برای دستیابی به حریم خصوصیِ بهینه در زندگی روزمره و در هر موقعیتی در محیط‌های آنلاین قابل استفاده نیستند، رویکرد آنها به حریم خصوصی به‌مثابه «کنترل انتخابی دسترسی به خود» برای مذاکرهٔ مرزهای خودافشاگری و عدم خودافشاگری در سایت‌های شبکه‌های اجتماعی نیز قابل استفاده است (توفچی، ۲۰۰۸؛ لیت[2]، ۲۰۱۳).

۱-۱. مزایا و خطرهای خودافشاگری

پترونیو در نظریهٔ مدیریت حریم ارتباطات بر این باور است که نحوهٔ محاسبات ذهنی افراد برای آشکار کردن اطلاعات خصوصی خود در هر موقعیت، به میزان بسیار زیاد تحت تأثیر نسبت هزینه به سود حاصل از افشا عمل می‌کند (پترونیو، ۲۰۰۲، ۲۶). پنج مزیت اصلی خودافشاگری عبارت است از: بیان[3]، شفاف سازی خود[4]، اعتباریابی اجتماعی[5]، توسعهٔ روابط[6] روابط[6] و کنترل اجتماعی[7]. بیان گویای این واقعیت است که بیان برخی مسائل شخصی باعث افزایش توانایی فرد در پذیرش اطلاعات می‌شود. با شفاف‌سازی خود افراد درک افکار و مسائلی که برایشان مهم است، راحت‌تر می‌شود. از سوی دیگر، بیان احساسات خود به دیگران می‌تواند آنان را به‌سمت تقویت دیدگاه‌ها و ارزش‌های فرد سوق دهد و اعتبار اجتماعی او را افزایش دهد. توسعهٔ روابط بیانگر این است که افراد با افشای خود می‌توانند ماهیت روابط خود با دیگران را بهبود بخشند. همچنین، افشای اطلاعات خصوصی تأثیرگذاری بر توجه دیگران به

1. selective control of access to the self
2. Tufekci; Litt
3. expression
4. self-clarification
5. social validation
6. relationship development
7. social control

یک مسئله و کنترل اجتماعی بر موقعیت را برای فرد ممکن می‌کند (درلگا و گـرزلاک[1]، ۱۹۷۹؛ به نقل از پترونیو، ۲۰۰۲، ۶۶-۶۷).

سطوح خطرهای خودافشاگری ممکن است بالا، متوسط یا پایین باشد. خطرهـای بـالا ناشـی از افشای موضوعاتی است که شرم‌آور و تهدیدکننده‌اند، مثل رازهای فرد. خطرهای متوسـط رویـدادها، نگرش‌ها، ارزش‌ها و تجربیاتی است که بیـان آن‌هـا بـرای دیگـران موجـب آزردگـی فـرد می‌شـود و خطرهای پایین بیان مسائل تناقض‌آمیز یا دروغ‌های مصـلحتی اسـت. عـلاوه بـر سـطوح، خطرهـای خودافشاگری انواعی دارد، از جمله خطر امنیتی،خطر انگ، خطر وجهه، خطر رابطه و خطـر نقـش[2]. خطرهای امنیتی دسته‌ای از افشاهاست که ممکن است امنیت فرد یا دیگران را به خطر انـدازد. خطـر انگ مبتنی بر فرضیاتی است که گویای ارزیابی منفی دیگـران از رفتـار و عقیـدۀ فـرد اسـت و بیشـتر مربوط به خود درونی و هویت فردی است. خطر وجهه حالت کلی‌تری دارد و مربـوط بـه پـیش‌بینـی فرد از افشاهایی است که موجب شرمساری فرد یا گروهی مـی‌شـود کـه در آن عضـویت دارد. خطـر رابطه تهدیدکنندۀ رابطه فرد با دیگران است و خطر نقش موجب به خطر افتادن جایگاه فـرد و نقـش و وظایف او می‌شود. خطرهای مذکور حالت نسبی دارند و در نتیجه آنچه برای یک فـرد خطـر اسـت، ممکن است برای فرد دیگر تهدید نباشد (پترونیو، ۲۰۰۲، ۷۱-۶۷).

۲-۱. تناقض میان خودافشاگری و حریم خصوصی

اساس نظریۀ مدیریت حریم ارتباطات این است که خودافشاگری امری دیـالکتیکی اسـت. بـه‌بیان روشن‌تر، اگر خودافشاگری فرایند در میان نهادن اطلاعات شخصی فرد با دیگـران و نیـز ضـرورتی برای توسعۀ روابط فرد باشد، تعریف حریم خصوصی در مقابل این تعریف قـرار مـی‌گیـرد؛ بـدین معنا که افراد حق دارند به‌صورت فردی یا گروهی اطلاعات شخصی خـود را محفـوظ نگـه دارنـد (پترونیو، ۲۰۰۲، ۶). برای روشن‌تر شدن این وضعیت می‌توان تصور کرد که هـر فـرد، منطقـه‌ای اطلاعاتی با تعریف مرزهای مشخص در اطراف خود دارد که تعیین می‌کند چه اطلاعاتی را مـی‌توان با دیگران به اشتراک گذاشت. بر حسب عوامل موقعیتی یا فردی، تلاش نهادی خارجی بـرای نفوذ به این مرز می‌تواند تهدید قلمداد شود (لی، ۲۰۱۲).

این تناقض در روابط آنلاین اگرچـه در نگـاه نخسـت بـه‌دلیل امکـان پنهـان کـردن اطلاعـات خصوصی و کاهش آسیب‌پذیری کاربران چندان مطـرح نیسـت، امـا حضـور کـاربران در فضـای مجازی با هویت واقعی شامل نام و نام خانوادگی، محل زندگی و سایر اطلاعات زمینه‌ای می‌تواند

1. Derlega and Grzelak
2. security risks, stigma risks, face risks, relational risks, role risks

مجدداً رابطهٔ دیالکتیکی میان حفظ حریم خصوصی و خودافشاگری را در روابط برخط نیز به‌اندازهٔ زندگی واقعی مطرح کند. این تناقض خصوصاً زمانی که روابط مجازی ادامهٔ روابط فرد در زندگی واقعی باشند یا به زندگی واقعی فرد نیز تسری یابند، می‌تواند از توانایی فضای مجازی برای کاهش این تقابل بکاهد (بنزیو،[1] ۲۰۰۳).

۳-۱. جنسیت، خودافشاگری و سواد حریم خصوصی آنلاین

اگرچه پژوهش‌های صورت گرفته در زمینهٔ رابطهٔ میان خودافشاگری و جنسیت گویای یافته‌های متناقضی است (هیل و استال[2]، ۱۹۸۷، ۸۲)، بر اساس نظریه حریم خصوصی ارتباطات، جنسیت افراد از شاخص‌های تأثیرگذار بر تعریف مرزهای حریم خصوصی و به‌کارگیری قواعد گوناگون برای قاعده‌مند کردن آن است. این نظریه ریشهٔ این تفاوت را فرآیندهای اجتماعی شدن و انتظارات فرهنگی متفاوت برای زنان و مردان می‌داند (پترونیو، ۲۰۰۲، ۲۴).

مدل «حریم خصوصی جنسیتی وب اجتماعی[3]» مایک سلوال[4] (۲۰۱۱) از بهترین نظریات توضیح تناقض حریم خصوصی و راهبردهای رفع آن در شبکه‌های اجتماعی با توجه به متغیر جنیست است. بر اساس این مدل استفادهٔ زنان از شبکه‌های مجازی به‌شدت تحت تأثیر نیروهای دوگانهٔ افشا و حفظ حریم خصوصی است. با وجود اینکه زنان فشارهای بیشتری برای دوری از شبکه‌های مجازی و حفظ حریم خصوصی خود متحمل می‌شوند، این شبکه‌ها برای بسیاری از فعالیت‌های زنان جایگزین‌های آنلاین مناسبی فراهم می‌کنند و بسیاری از نیازهای زنان به ارتباطات اجتماعی را برآورده می‌کنند. زنان به این دلیل که در زندگی واقعی خود دغدغه‌های بیشتری در خصوص امنیت فیزیکی خود و مواجهه با آزار و اذیت دارند، استفاده از شبکه‌های مجازی نیز می‌تواند خطری برای حریم خصوصی این گروه باشد، مثلاً بسیار محتمل‌تر است که زنان قربانی جرایم مجازی و مزاحمت‌های سایبری باشند. بنابراین پیش‌بینی می‌شود که زنان با احتیاط‌تر و با استراتژی‌های حفاظتی بیشتری از شبکه‌های اجتماعی استفاده می‌کنند (سلوال، ۲۰۱۱، ۲۵۵-۲۵۲).

با وجود ضرورت به‌کارگیری استراتژی‌های حفاظتی بیشتر به‌منظور رسیدن به سطح بهینه حریم خصوصی برای زنان، برخی صاحب‌نظران تفاوت‌های جنسیتی را از عوامل مهم کسب مهارت‌های حفظ حریم خصوصی دانسته‌اند (هارجیتایی[5]، ۲۰۰۲). از این‌رو جنسیت می‌تواند به‌مثابه خطی

1. Ben-Ze'ev
2. Hill & Stull
3. social web gendered privacy model
4. Mike Thelwall
5. Hargittai

تمایزبخش مانع از مشارکت برابر و بهره‌منـدی از مزایـا در همـهٔ حـوزه‌هـای اینترنـت شـود (پـارک[1]، ۲۰۱۵)، به‌ویژه در شرایطی که در فضای مجازی نیز تحت تأثیر زندگی واقعی، فراینـدهای اجتمـاعی شدن متمایز زنان و مردان در آموزش و پرورش، سازمان‌ها و مناسبات شغلی، موجـب هـدایت آن‌هـا به مسیرهای گوناگونی از انتخاب‌ها و ارزش‌ها شده و در نهایت موجب اتخاذ تصمیمات متفـاوت در محیط‌های اطلاعاتی می‌شود (لالی[2]، ۲۰۰۲؛ به نقل از پارک، ۲۰۱۵). با این حال یافته‌های تجربـی فعلی درباره تأثیر جنسیت بر توانایی کنترل حریم خصوصی یک‌دست نیست؛ برخی از یافته‌ها بیانگر کنترل بیشتر زنان و استفاده بیشـتر آن‌هـا از ابزارهـای فنّاورانـه اسـت (لیـت، ۲۰۱۳؛ فوگـل و نهمـد، ۲۰۰۹؛ لوئیس و همکاران[3]، ۲۰۰۸). اما نتایج حاصل از تحقیقات دیگر گویای آن است که مردهـا به مراتب بهتر از زنان از امکانات فنّی استفاده می‌کنند و به علت مرد بودنشان اعتماد به نفس بـالاتری در حفاظت از حریم خصوصی خود دارند. البته این شکاف در بـه‌کـارگیری اسـتراتژی‌هـای تکنیکـی پررنگ‌تر از ابعاد اجتماعی ملاحظه شـده اسـت (پـارک، ۲۰۱۱؛ پـارک، ۲۰۱۵). در نهایـت بویـد و هارجیتایی[4] (۲۰۱۰) به تفاوت‌های اندکی در رفتارهای مرتبط با حریم خصوصی این دو گـروه اشـاره کرده‌اند، که البته به مرور زمان برای زنان افزایش اندکی داشته است.

٤-١. سواد حریم خصوصی و راهبردهای حفظ حریم خصوصی

سواد حریم خصوصی آنلاین که خود یکی از ابعاد سواد دیجیتال است و در برخی منـابع از آن تحـت عنوان سـواد اجتماعی ـعاطفی[5] و سـواد اخلاقی ـاجتماعی نیـز یـاد شـده اسـت (اِشت ـالکالای و آمیچی‌ـهامبورگر[6]، ۲۰۰۴؛ بودن[7]، ۲۰۰۸، ۳۰)، به‌معنای فهم رفتار درست و معقول در محیط‌های محیط‌های دیجیتال و دربرگیرنـدهٔ مسـائل حـریم خصوصـی و امنیتـی اسـت (بـودن، ۲۰۰۸، ۳۰). برخورداری از دانش استراتژی‌های کنترل فردی حریم خصوصی از سوی کاربران در برخی مقیاس‌هـا از الزامات برخورداری افراد از سواد حریم خصوصی آنلاین قلمداد شده اسـت (ترپـت و همکـاران، ۲۰۱۴، ۳۳۳). این استراتژی‌ها که خـود ترکیبـی از مهـارت‌هـای اجتمـاعی و فنّـی اسـت (ترپـت و همکاران، ۲۰۱۴، ۳۵۰؛ پارک، ۲۰۱۱)، با توجه به سؤالات مطرح‌شده در این مقاله، راهی برای فهـم چگونگی حل کردن تناقض حریم خصوصی از سوی کاربران دختر به‌کار گرفته شده است.

1. Park
2. Lally
3. Fogel & Nehmad; Lewis et al
4. Boyd & Hargittai
5. socio-emotional skills
6. Eshet-Alkali & Amichai-Hamburger
7. Bawden

محافظت از حریم خصوصی به‌صورت کلی ممکن است به‌صورت منفعلانه و فعالانه صورت گیرد. از این‌رو، راهبردهای حفظ حریم خصوصی به دو بُعد هنجاری و قانونی و بُعد رفتاری و اجتماعی تفکیک می‌شود؛ بُعد رفتاری راهبردهایی است که کاربران به‌صورت رفتارهای برنامه‌ریزی‌شده و آگاهانه به‌کار می‌گیرند. بدین منظور کاربران باید دانش و مهارت‌های تکنیکی فضای مجازی را داشته باشند تا بتوانند خطرهای این فضا را به درستی ارزیابی کنند. در مقابل، بُعد هنجاری یا منفعلانه حفاظت‌های دولت یا دیگران است و فرد کنترل مستقیمی بر آن‌ها ندارد (یائو[1]، ۲۰۱۱، ۱۱۵). این حفاظت‌ها که با توجه ویژهٔ قانونگذاران در کشورهای گوناگون همراه بوده است، اغلب به‌دلیل نداشتن انعطاف‌پذیری کافی اجازهٔ استفادهٔ مؤثر از فنّاوری را به کاربران نمی‌دهند (پرایس و همکاران[2]، ۲۰۰۵).

در رویکرد رفتاری مورد نظر این مقاله، دانشمندان اجتماعی چگونگی حفاظت افراد از حریم خصوصی خود در زمینه‌های گوناگون اجتماعی را مطالعه می‌کنند. محافظت‌های رفتاری را می توان در درجهٔ نخست فرایند مدیریت مرزی با ابزارهای گوناگون کنترل حریم خصوصی و اطلاعات شخصی دانست. چنین حفاظتی به تشخیص تهدیدات بیرونی، سنجش میزان تهدیدات در برابر ترجیحات حفظ حریم خصوصی و سپس اتخاذ استراتژهای مدیریت مرزی نیاز دارد (یائو، ۲۰۱۱، ۱۱۵). استراتژی‌های رفتاری را نیز می‌توان به دو دسته استراتژی‌های اجتماعی و فنّاورانه تقسیم کرد؛ استراتژی‌های فنّاورانه حفظ حریم خصوصی استراتژی‌هایی است که کاربران از طریق آن‌ها از ویژگی‌ها یا امکانات یک سایت برای حفظ حریم خصوصی خود استفاده می‌کنند، مانند ایجاد فهرست دوستان، آن‌تگ[3] کردن پست‌ها و تصاویر و حذف محتوای پست‌شده (لیت، ۲۰۱۳). درحالی‌که استراتژی‌های اجتماعی شامل ایجاد محدودیت‌های ذهنی در افشا می‌شود که با کمک آن کاربر فقط اطلاعاتی را افشا می‌کند که برای همهٔ اعضای شبکه مناسب باشد (هانگ، ۲۰۱۰، به نقل از استاتزمن و همکاران[4]، ۲۰۱۲).

الیسون و همکاران[5] (۲۰۱۱، ۲۹) بر اساس یافته‌های پژوهش خود بر این باورند که استراتژی‌های فنّاورانه و اجتماعی به‌مثابه بخشی از راهبردهای حفظ حریم خصوصی در ارتباط با

1. Yao
2. Price et al
3. untag
4. Hogan, Stutzman et al
5. Ellison et al

یکدیگر عمل می‌کنند. آن‌ها بر اساس یافته‌های خود توضیح می‌دهند که چطور ناآشنایی کاربران با تنظیمات حریم خصوصی چه به عدم افشا برای ایشان بیانجامد و چه به خودافشاگری، برای کاربران تجربه‌های منفی را در پی خواهد داشت و آنها را در دستیابی به سرمایه‌های اجتماعی با دشواری مواجه خواهد کرد. از سوی دیگر آن‌ها همچنین با نارضایتی کاربرانی مواجه شده‌اند که به دلیل نگرانی بالا از حفظ حریم خصوصی خود و با تأکید صرف بر راهبردهای اجتماعی از افشا صرف نظر کرده‌اند. این دسته از کاربران اغلب وضعیت دیگر کاربران را بر شرایطی که خود در شبکه‌های اجتماعی دارند، ترجیح داده‌اند (۲۰۱۱، ۲۸).

روش تحقیق

برای پاسخ به پرسش‌های تحقیق از روش کیفی مردم‌نگاری استفاده شده است. روش تحقیق کیفی به‌دلیل اهمیت دادن به جزئیات و نمایش تکثر فعلی هر مسئله در این مقاله استفاده شده است (فلیک[1]، ۱۳۸۷). تحقیقات مردم‌نگارانه شامل مطالعهٔ اطلاع‌رسانان، کنش‌ها و اقداماتشان در لحظهٔ عمل و در محل طبیعی زندگی می‌شوند (برجس[2]، ۱۹۸۱). در هم‌تنیدگی فضاهای برخط و واقعی در سال‌های اخیر موجب شده است تا ضرورت جدا کردن این فضاها در مطالعات مردم‌نگارانه کم‌رنگ‌تر شود (هالت و باربر[3]، ۲۰۱۳). میدان مطالعهٔ آنلاین در این مقاله صفحات کاربران دختر جوان در اینستاگرام است. اینستاگرام سرویس به اشتراک‌گذاری تصاویر (و ویدئوهای) گرفته‌شده با تلفن همراه است. این نرم‌افزار امکان گرفتن، ویرایش و اشتراک سریع تصاویر و فیلم‌های لحظات زندگی را فراهم کرده است (هو و همکاران[4]، ۲۰۱۴). سرعت افزایش کاربران و استفاده از این نرم‌افزار به گونه‌ای بوده که بر اساس آمار[5] منتشرشده در ۲۰۱۶ تعداد کاربران آن به ۵۰۰ میلیون نفر رسیده است.

روش اصلی گردآوری داده‌ها در این مقاله مصاحبه است؛ ابتدا از طریق مصاحبهٔ نیمه‌ساخت‌یافته از کاربران دختر جوان شبکه‌های اجتماعی سؤالاتی پرسیده شد و فهم دقیق‌تر موضوع با مشاهدهٔ غیرمشارکتی صفحات این کاربران به‌دست آمد. کیفیت برخی سؤالات مطرح‌شده در این مرحله به‌گونه‌ای است که تفکیک آن‌ها از مصاحبهٔ یادداشت روزانه[6] دشوار

1. Flick
2. Burgess
3. Hallett & Barber
4. Hu & et al
5. https://www.instagram.com/press/
6. diary-interview

است، اگرچه اصول این‌گونه مصاحبه در این پژوهش عیناً به‌کار گرفته نشده است. این نوع از مصاحبه اغلب برای تکمیل مطالعات یادداشت روزانه[1] در مردم‌نگاری به‌کار می‌روند و بیشتر مختص میدان‌هایی است که مردم‌نگار خود امکان حضور دائم در میدان را ندارند و در نتیجه افراد حاضر در میدان در جایگاه مشاهده‌گر مشارکتی ظاهر می‌شوند و مشاهدات، تجربیات و احساسات خود را بر حسب ترتیب زمانی به شکل‌های گوناگون شفاهی و کتبی و به صورت آشکارا و صادقانه ثبت می‌کنند. بدین معنا مطالعات یادداشت روزانه بر نوعی مطالعهٔ اکتشافی و امیک تأکید دارند و امکان امتداد مرزهای پژوهش در غیاب پژوهشگر را فراهم می‌کنند (برجس، ۱۹۸۱؛ مارکهام و کولدری[2]، ۲۰۰۷؛ هال[3]، ۲۰۰۸).

در این مقاله، از آنجا که درک چگونگی ایجاد تناقضات خودافشاگری و نحوهٔ عبور از آن در لحظهٔ مبادرت به افشا در شبکه‌های مجازی دشوار بود، در طول مصاحبه‌ها از مصاحبه‌شوندگان خواسته شد تا با مراجعه به صفحه اینستاگرام خود تجربیات خود را درباره افشاهایشان خصوصاً در شرایط حساس بیان کنند. یافته‌های حاصل از مصاحبه‌ها با تکنیک «تحلیل تماتیک»[4] یا موضوعی موضوعی تحلیل شده‌اند. تحلیل تماتیک روشی سیستماتیک برای شناسایی، سازماندهی و ارائهٔ الگوهای معنایی از کل داده‌هاست که با تمرکز بر معنا در مجموعه‌ای از داده‌ها امکان دستیابی به معانی یا تجارب مشترک یا جمعی را فراهم می‌کند. این تحلیل در مرحلهٔ عمل معمولاً از سه مرحلهٔ اصلی ایجاد کدهای اولیه، جست‌وجوی تم‌های کلی‌تر و تعریف و نام‌گذاری تم‌ها تشکیل شده است (برون و کلارک[5]، ۲۰۰۶)، که در این تحقیق نیز عیناً به‌کار گرفته شده است.

نمونه اطلاع‌رسانان حاضر در این مطالعه ۲۰ نفر از دختران جوان ساکن تهران است. برای انتخاب نمونه از منطق نمونه‌گیری هدفمند و راهبرد دستیابی به حداکثر پراکندگی استفاده شده است. انتخاب نمونه‌هایی با بیشترین اختلاف[6] از راهبردهای رایج در پژوهش‌های کیفی است که طیف گسترده‌ای از کیفیت‌ها، ویژگی‌ها، موقعیت‌ها، یا اتفاقات را در چارچوب مسئلهٔ پژوهش بررسی می‌کند. در این روش، پژوهشگر فقط در پی یافتن نمونه‌هایی است که ویژگی‌های متنوعی داشته باشند (لیندلف و تیلور[7]، ۱۳۸۸، ۱۷۳). به‌دلیل حساسیت سؤالات مطرح‌شده در مصاحبه

1. diary Study
2. Markham & Couldry
3. Hall
4. Thematic Analysis
5. Braun & Clarke
6. maximum variation sampling
7. Lindlof & Taylor

و ضرورت ورود به مسائل بسیار شخصی مصاحبه‌شوندگان، اغلب اطلاع‌رسانان با شناخت قبلی انتخاب شده‌اند و فقط در مواردی از نمونه‌گیری گلوله‌برفی استفاده شده است. به این معنا که از مصاحبه‌شوندگان خواسته شده است تا یکی از دوستان خود را که عضو شبکه‌های مجازی است و در عین حال دغدغهٔ حریم خصوصی دارد، برای مصاحبه معرفی کنند. در انتخاب اطلاع‌رسانان تلاش شده است تا افرادی انتخاب شوند که علاوه بر داشتن نسبی دغدغهٔ حریم خصوصی، به‌لحاظ روابط اجتماعی، میزان اعتقادات مذهبی، شرایط خانوادگی و تعداد پست‌های به اشتراک گذاشته‌شده نیز متنوع باشند. ضمناً همهٔ اعضای نمونه حاضر در مصاحبه در صفحه اینستاگرام خود از نام واقعی استفاده کرده‌اند و دوستان و نزدیکان خود را نیز در لیست دنبال‌کنندگان[1] در صفحهٔ خود داشته‌اند. مشخصات شرکت‌کنندگان در جدول ۱ آمده است.

جدول ۱. مشخصات اطلاع‌رسانان

ردیف	نام	سن	رشتهٔ تحصیلی یا شغل	مدت عضویت (برحسب سال)	تعداد دنبال‌کنندگان	تعداد پست	متوسط ساعت استفاده روزانه
۱	فریده	۲۵	کارمند	تقریباً ۲	۱۰۰	۳۰	کمتر از ۱
۲	زینت	۲۵	کارمند	تقریباً ۲	۱۰۰	۸۶	۲-۱
۳	فاطمه	۲۶	دانشجوی دکتری شیمی	۱	۱۰۰	۵	کمتر از ۱
۴	فریبا	۲۸	کارمند	تقریباً ۳	۲۱۱	۳۳۵	۲
۵	افروز	۲۵	دانشجوی دامپزشکی	تقریباً ۲	۲۸۰	۱۴۵	۱
۶	فهیمه	۲۵	دانشجوی کارشناسی ارشد مهندسی نفت	تقریباً ۱	۴۱۸	۴۳	۱
۷	سحر	۲۳	دانشجوی کارشناسی ارشد پلیمر	تقریباً ۳	۲۰۷	۹۰	۲
۸	زهرا	۲۴	دانشجوی کارشناسی ارشد مدیریت رسانه	تقریباً ۱	۳۰	۰	کمتر از ۱
۹	مینا	۲۴	دانشجوی کارشناسی ارشد آرشیو	۱	۵۲۴	۲۷۰	۱
۱۰	مریم	۲۴	دانشجوی کارشناسی ارشد فنّاوری اطلاعات	کمتر از ۱	۱۵۰	۱۳	کمتر از ۱
۱۱	پگاه	۲۳	دانشجوی کارشناسی ارشد مدیریت جهانگردی	تقریباً ۲	۱۲۲	۱۰۵	۱
۱۲	آمنه	۲۳	دانشجوی کارشناسی ارشد علم اطلاعات و دانش‌شناسی	۱	۶۵	۹۰	کمتر از ۱
۱۳	مینو	۳۰	دانشجوی کارشناسی ارشد تصویرسازی	تقریباً ۲	۴۶۹	۱۲۶	۱
۱۴	انیس	۲۱	دانشجوی کارشناسی تربیت بدنی	تقریباً ۲	۱۳۱	۱۷	تقریبا ۱
۱۵	مهسا	۲۷	دانشجوی کارشناسی ارشد مهندسی آی.تی	۲	۲۰۲	۹۸	۲-۱
۱۶	فاطمه۲	۲۷	دانشجوی کارشناسی ارشد مهندسی آی.تی	تقریباً ۱	۲۱۲	۷۲	کمتر از ۱
۱۷	مریم	۲۶	دانشجوی کارشناسی ارشد زبان روسی	کمتر از ۱	۵۰	۲۳	۱ تا ۲
۱۸	پریسا	۲۶	دانشجوی کارشناسی ارشد گرافیک	تقریباً ۲	۲۵۰	۶۱	کمتر از ۱
۱۹	سحر۲	۲۳	دانشجوی کارشناسی ارشد اقتصاد	تقریباً ۲	۲۱۴	۲۰	۱
۲۰	راحله	۲۵	دانشجوی کارشناسی ارشد مدیریت منابع انسانی	تقریباً ۲	۱۶۰	۱۵۳	۲-۱

1. follower

یافته‌ها

۱. مزایای خودافشاگری

این مزایا به‌طور کلی در دو تم جای گرفته‌اند که از دل ۱۱ کد استخراج شده‌اند؛ تم نخست «مزایای روانشناختی» است. در مزایای روانشناختی کاربران برای دستیابی به رضایت روانی اطلاعاتی را درباره احساسات و افکار خود افشا می‌کنند. آنچه کدهای ذیل «مزایای روانشناختی» را به یکدیگر متصل می‌کند، بیشتر نوعی مرکزیت احساسات در این نوع خودافشاگری‌هاست. «بیان (تسکین پریشانی) و بهبود احساسات فردی» مرکزی‌ترین کد در این تم است. در این مورد کاربران با بیان مسئله‌ای اغلب منفی تلاش می‌کنند تا آرامش خاطر بیشتری برای خود فراهم کنند و از سوی دیگر با بیان رویدادی خوشایند و به اشتراک گذاشتن آن با دیگران تلاش می‌کنند تا احساس مثبت حاصل از آن را برای خود پررنگ کنند. فریبا در این باره می‌گوید: «مثلاً من صبح دارم میرم طلوع خورشید رو می‌بینم دوست دارم در حد یه عکس وقتی این صحنه حس خوبی بهم میده، به کسایی که می‌بینن هم همین حس خوب رو بده».

«تخلیهٔ هیجانات فردی» و «شفاف‌سازی خود» از دیگر کدهای این تم است. فرد پس از مواجهه با حادثه‌ای استثنایی با افشای آن در قالب یک پست، هیجانات خود را کاهش می‌دهد و با شفاف‌سازی خود سعی می‌کند تا برخی اتفاقات را برای خود قابل تحمل کند.»

در ادامه، نظر برخی شرکت‌کنندگان که این مزایا را حائز اهمیت دانسته‌اند، ارائه شده است:

«نخل طلای اصغر فرهادی رو گذاشتم چون خیلی هیجان‌زده شده بودم؛ گفتم خوشحالیم رو به اشتراک بذارم» (سحر)؛ «خیلی وقتا پیش میاد که آدم منطق خیلی چیزا رو نمی‌فهمه، مثلاً گاهی از رفتار بعضیا اینقد تعجب می‌کنی که همش با خودت میگی این یعنی چی الان؟ اینجور موقع‌ها حرفای دلم رو میام مثلاً پست می‌ذارم» (فریبا)

«ثبت لحظات مثبت و خاطره‌انگیز» آخرین کد در این تم است؛ کاربران دختر تلاش می‌کنند با ثبت اتفاقی خوشایند و خاطره‌انگیز در صفحهٔ خود احساسات مثبت حاصل از آن را به دیگر زمان‌ها نیز توسعه دهند. پریسا در این باره می‌گوید: «دوست دارم اینستاگرام واقعاً مثل یِه آلبوم شخصی باشه که مثلاً در گذر زمان بعضی لحظات ثبت بشه و بعداً خاطرات برام زنده بشه».

دومین تم در مزایای حاصل از خودافشاگری «مزایای اجتماعی» است؛ «برخورداری از صدا»، «کسب آگاهی»، «شناخت خود و دیگران»، «احیا و حفظ روابط»، «توسعهٔ روابط»، «کنترل اجتماعی» و «بازنمایی خود» مجموعه کدهایی است که ذیل این تم قرار می‌گیرند. دستیابی به هر یک از این مزایا بدون وجود دیگران یا اصطلاحاً دنبال‌کنندگان ممکن نخواهد بود.

«برخورداری از صدا» مزیتی است که برای فرد امکان طرح دغدغه‌های مشترک خود با همفکرانش را فراهم می‌کند، مثلاً سحر یکی از اطلاع‌رسانان بر این باور است که «خیلی از دوستایِ همفکرم توی اینستا فعال‌اند و راجع‌به خیلی از دغدغه‌های مشترکمون مثل وضعیت بد بازار کار رشته‌مون پیش اومده که اونجا بحث کردیم».

«کسب آگاهی» مزیتی است که فرد از طریق افشاهایی در قالب پرسش یا مسئله‌ای مناقشه‌برانگیز امکان آگاهی از نظرهای دیگران را به‌دست می‌آورد. آمنه در این زمینه چنین بیان می‌کند: «مثلاً یه اتفاقی افتاده، اینکه چطور میشه تحلیل کرد؟ چطور تو آینده قرار اثر داشته باشه؟ ما باید چیکار کنیم؟ بقیه دارن چیکار می‌کنن؟ این‌ها مسائلیه که با مطرح کردنش توی پیجت میتونی نظر بقیه رو هم راجع بهش بدونی».

به اشتراک گذاشتن اطلاعات خود با دیگران در برخی موارد برای کاربران دختر راهی برای «شناخت خود و دیگران» است. زینت می‌گوید: «بعضی پست‌ها رو می‌ذارم برای اینکه ببینم نظر بقیه راجع‌به طرز فکرم چیه؟ حتی یه بار پرسیدم که بهترین و بدترین ویژگی من به نظرشون چیه؟» (زینت)

«احیا و حفظ روابط» به امکان پیدا کردن دوستان یا آشنایان قدیمی و تجدید یا تقویت ارتباط با آن‌ها از طریق شبکه‌های مجازی اشاره دارد. سحر به این مزیت اشاره کرده است:

> «ببین از یه نظر خوبه که دوستایی که یه مدت طولانی نمی‌بینیشون ازشون بی‌خبر نیستی، مثلاً این ۲۰۷ نفر توی یه تایمی دوستای من بودن، ولی الان دیگه اینطوری نیست که باهاشون در ارتباط باشی و ازشون خبر داشته باشی، مثلاً پست می‌ذاره می‌بینی طرف ازدواج کرده یا بچه‌اش به دنیا اومده».

«توسعهٔ روابط» در اینجا به مزایای حاصل از خودافشاگری‌هایی اشاره می‌کند که به گسترش دایرهٔ روابط فرد با کسانی می‌انجامد که پیش از این با آن‌ها در ارتباط نبوده است و از این جهت کمتر به ماهیت روابط اشاره می‌کند، مثلاً زینت می‌گوید: «توی بیوگرافیم دانشگاه و رشته‌ام رو نوشتم، واسه همین خیلی از بچه‌های دانشکده و حتی دانشگاه که قبلاً اصلاً نمی‌شناختمشون الان پیجم رو فالو می‌کنن».

برخی کاربران دختر با افشای علایق خود تلاش می‌کنند دیگران را نیز به انجام دادن عملی مشابه اعم از تماشای فیلمی، شنیدن موسیقی یا بازدید از یک مکان دعوت کنند و از این طریق به مزیت «کنترل اجتماعی» دست یابند، مثلاً فریبا می‌گوید: «یه شعری بخونم یا کتابی بخونم که یه قسمتش رو دوست داشته باشم یا آهنگی گوش بدم که دوسش داشته باشم، دوست دارم که دوستامم بدونن».

«بازنمایی خود» مزیتی است که کاربر از طریق افشای خود آن‌گونه که دوست دارد، مثلاً فردی شاد، ثروتمند، خوشبخت به‌دست می‌آورد. راحله در این باره چنین بیان می‌کند: «جایی برم یا اتفاق خاصی بیافته حتماً می‌ذارم، دلیل اصلیش پز دادنه، اینکه نشون بدم حالم خوبه، خوشحالم، زندگی بر وفق مراده، اگه نباشه نمی‌ذارم، فقط راجع‌به اتفاقات خوبش می‌ذارم. دوست ندارم کسی بدونه ناراحتم».

۲. خطرهای خودافشاگری

خطرهای حاصل از خودافشاگری نیز که پیش از این در قالب مجموعهٔ خطرهای امنیتی، خطر انگ، خطر وجهه، خطر رابطه و خطر نقش معرفی شد، در نتیجهٔ یافته‌های حاصل از مصاحبه‌ها توسعه یافته‌اند و مجدداً ذیل دو تم کلی «خطرهای روانشناختی» و «خطرهای اجتماعی» قرار گرفته‌اند. «خطرهای روانشناختی» خطرهایی است که منشأ فردی دارند و این خود کاربر است که در گذر زمان و با کنترل نکردن افشاهای عاطفی خود زمینه‌ساز ایجاد چنین خطرهایی برای خود می‌شود. درحالی‌که در «خطرهای اجتماعی» دوستان، دنبال‌کنندگان صفحهٔ کاربر و در برخی موارد مالکان شبکه موجب تبدیل افشا به خطر برای کاربر می‌شوند. اغلب کدها تحت تم «خطرهای اجتماعی» قرار دارند، شامل «خطر وجهه»، «خطر سطحی شدن»، «خطر سوءتفاهم»، «خطر دور»، «خطر قضاوت شدن»، «خطر رابطه»، «خطر نقش برای خود یا دیگری» و «خطر امنیتی». تنها «خطر روانشناختی» «خطر پشیمانی» است.

«خطر پشیمانی» اغلب حاصل افشای اتفاقات ناگواری است که موجب توسعهٔ احساسات منفی این حوادث به دیگر مقاطع زندگی فرد می‌شوند و در نهایت به پشیمانی فرد از افشا می‌انجامد. افروز به این خطر اشاره کرده است: «تو یه دوره که حالم بود یه عکس گذاشتم، فقط چشام معلوم بود، داشتم گریه می‌کردم و دوستم ازم عکس گرفته بود. عکس سیاه و سفید بود و اشکم ریمل داشت، ولی بعد هر موقع اینو می‌دیدم یاد اون موقع می‌افتادم، سر همون پشیمون شدم».

«خطر وجهه» به خطرهایی اشاره می‌کند که جایگاه فرد را آن‌طور که خود خواهان آن است، مثلاً در جایگاه فردی قانون‌مدار، تحصیل‌کرده و متدین تهدید می‌کند. این خطرها همچنین می‌توانند حاصل نوعی شرمندگی از افشاهای بسیار شخصی مرتبط با جایگاه شغلی، تحصیلی، خانوادگی و یا دوستانهٔ فرد باشد که گویای حقایقی از کوتاهی‌ها و نقصان‌های فرد در این موقعیت‌هاست. فهمیه درباره این خطر می‌گوید:

«یه بار از خانمی که تو بی.آر.تی نشسته بود، عکس گذاشتم حس خوبی بهم داده بود، بعد یکی از بچه‌ها اومد گفت اجازه گرفتی عکس گرفتی ازش؟ گفتم نه، بعد دوباره گفت کارت خیلی زشت و

خلاف قانون بوده بعد یکی دیگه هم اومد گفت قبول کن کارت زشت بود. بعد پرس‌وجو کـردم گفـتن بـه لحاظ قانونی حق نداری عکسش رو بدون اجازه پخش کنی. منم گفتم پاکش کنم بهتر از اینه که بهم بگـن خلاف قانون عمل کردی».

«خطر سطحی شدن» ناشی از افشاهایی است که به دلیل همه‌گیر شدن مزایای چنـدانی بـرای فرد ندارد و کاربر فقط به‌دلیل علاقهٔ شخصی ممکن است دست بـه چنـین افشـایی بزنـد. انتشـار تصاویر مرتبط با غذا و دیگر امور روزمره اغلب زمینه‌ساز این نـوع از خطرهـا بـرای کـاربران شـده است. فاطمه با اشاره به این خطر می‌گوید: «یه دورهمی با دوستات داری از سفره‌ای چیزی عکس می‌گیری، می‌خوای بذاری با خودت فکر می‌کنی که چه دلیلی داره عکس غذایی که من خوردم رو بقیه بخوان ببینن».

«خطر سوءتفاهم» چنانچه از عنوان آن نیز مشخص است حاصـل بـدفهمی دنبال‌کننـدگان از افشای فرد است که می‌تواند «خطر دور» را نیز به دنبـال داشـته باشـد و کـاربر را مجبـور بـه ارائـهٔ توضیحات اضافه، مکرر و بی‌نتیجه کند. مینا به این دو خطر اشاره می‌کند: «من یـه بـار یـه پسـت گذاشتم راجع‌به مرگ و بعد یکی نوشت که این چیه؟ با این چیزا همه رو افسرده می‌کنـی. کـل روز با طرف بحث می‌کردم که مرگ هم جزئی از زندگیه».

«خطر قضاوت‌شدن» که تا حدودی به خطر انگ پترونیو (۲۰۰۲) نزدیـک اسـت، مربـوط بـه افشاهایی است که زمینه‌ساز نسبت دادن صفات، ویژگی‌ها یا اعمال ناخوشایند به فـرد مـی‌شـوند، تا آنجا که می‌تواند تهدیدکنندهٔ آبروی کاربر باشد. فاطمه در این مورد می‌گوید:

«چون تو فامیلا یه مقداری فضولی هست، ترجیحاً اد نمی‌کنم اونم نه بـه‌خاطر پسـتایی که من می‌ذارم بیشتر به‌خاطر کامنتایی که زیرش گذاشته می‌شـه. وای فـلان پسـر فـلان حرف رو زده حالا اون پسر هم‌آزمایشگاهی منه و من باهاش روزی ده سـاعت تـوی یـه آزمایشگاهم. ولی اون آدم با دید دو دهه قبل یه‌جور دیگه برداشت می‌کنه».

«خطر رابطه» چنانچه از عنـوان ایـن کـد نیـز مشـخص اسـت، تهدیدکننـدهٔ رابطـهٔ کـاربر بـا نزدیکانش است.

«خیلی کم پست می‌ذارم، چون همون اطرافیان که من رو فالو مـی‌کـنن بـا کوچـک‌ترین عکسی که می‌ذارم میان سریع واکنش نشون میدن. خیلی حساسن رو من. بیشتر می‌گـن مواظبتیم بعد خب چون حق دارن به گردنم اصلاً دوس ندارم جلوشون بایستم یا جـوابی بدم» (اَنیس).

«خطر نقش» مشخصاً گویای تهدیدی برای جایگاه شغلی و تحصیلی اطـلاع‌رسـانان در ایـن

تحقیق بوده است. همچنین، در برخی موارد کاربران ممکن است دست به افشاهایی زده باشند که با پرده برداشتن از صداقت نداشتن، ناراستی، کوتاهی و تن دادن به روابط به‌جای ضوابط در خصوص همکاران و دوستان خود موجب ایجاد خطر نقش برای آن‌ها نیز شده باشند.

«دوس ندارم همکارام پیجم رو ببینن، چون چندتا پست دارم که خیلی از اوضاع شرکت گلایه کردم واسه همین ترجیح میدم نبینن، چون حتماً تو روابط کاریم تأثیر می‌ذاره؛ هم واسه خودم بد میشه، هم بعضی همکارا شاید» (زینت)

«خطر امنیتی» آخرین کد در تم «خطرهای اجتماعی» است که در نتیجهٔ آن فرد افشا در هر زمینه‌ای را تهدیدکنندهٔ امنیت خود به‌دلیل عدم توانایی کنترل اطلاعات شخصی و امکان سوءاستفاده اشخاص و یا مالکان اینستاگرام از آن‌ها می‌داند. زهرا تنها اطلاع‌رسانی است که به‌دلیل نگرانی از این خطر تاکنون هیچ پستی را در اینستاگرام به اشتراک نگذاشته است: «خودم پست نمی‌ذارم. اصلاً من به هیچ‌کدوم از فضاهای شبکه‌های مجازی اعتماد ندارم، چون اصلاً مخصوص ایران نیست و اکثراً دست اونوریاست و همه‌چی تو حافظشون می‌مونه».

۳. راهبردهای کاربران

لیت (۲۰۱۳) راهبردهای رفتاری یا فردگرایانه در حفظ حریم خصوصی را در دو دستهٔ راهبردهای اجتماعی و فنّاورانه قرار می‌دهد که در اینجا نیز استفاده شده است:

۳-۱. «راهبردهای اجتماعی» یا «کنترل محتوا»

«راهبردهای کنترل محتوا»ی کاربران دختر برای حل تضاد حریم خصوصی بر اساس نتایج حاصل از مصاحبه‌ها شامل ۱۳ کد می‌شوند. این راهبردها به‌طور کلی مرزها و محاسباتی است که خود فرد به‌صورت ذهنی برای محتواهایی که قصد افشای آن‌ها را در شبکه‌های مجازی دارد، تعریف می‌کند و با پایبندی به آن‌ها سعی می‌کند خطرهای حاصل از افشا را به حداقل برساند.

کدهای «عدم بیان حالات روحی»، «عدم بیان مسائل شخصی»، «تأکید بر حفظ هویت شخصی»، «عدم انتشار تصاویر شخصی و خانوادگی»، «مطابقت با عرف و باورهای عامه»، «تعریف مرزهای پوشش»، «بیان غیرمستقیم افشا»، «گمنامی»، «اضافه کردن توضیحات» و «ایجاد فواصل زمانی در افشا» ذیل این تم قرار می‌گیرند. «عدم بیان حالات روحی» به این معناست که کاربر تمایلی به افشای احساسات خود از قبیل غم، احساسات عاشقانه، عصبانیت، دلتنگی و تنهایی ندارد. مینو می‌گوید: «اصولاً احساسات عاشقانهٔ آدم به کسی مربوط نیست، ناراحتی و عصبی بودن و اینام همین‌طور».

«عدم بیان مسائل شخصی» پُرکاربردترین راهبرد اجتماعی برای کاربران دختر است و بیشتر

شامل مسائل خانوادگی و روابط میان‌فردی کاربران می‌شود. مهسا این‌گونه به این راهبرد اشاره می‌کند: «مسائل خیلی شخصی و خانوادگی نمی‌ذارم کلاً. یا اینکه بخوام بقیه رو در جریان زندیگی شخصیم بذارم، این‌جوری عکس نمی‌ذارم».

در راهبرد «حفظ هویت شخصی» کاربر آنچه ممکن است هویتش را در جایگاه دختر، دانشجو، دوست، و کارمند نزد دوستان و همکارانش تحت تأثیر قرار دهد، افشا نمی‌کند. مینا می‌گوید: «صفحه بعضی از دخترا خیلی خزه، مثلاً تو بیوگرافی‌شون می‌نویسن خوشبختی یعنی داشتن من. به نظرم دختر باید صفحه‌اش خیلی متین باشه».

تعدادی از کاربران در صفحات خود هیچ‌گونه تصویری از خود یا نزدیکانشان را منتشر نکرده‌اند، چرا که انتشار چنین تصاویری را فاقد هرگونه مزایا برای خود دانسته‌اند. فهیمه که خود از این راهبرد استفاده کرده در این رابطه می‌گوید: «عکسام رو که دیدی چه جوریه! عکس صورت و اینا نمی‌ذارم. عکس خودم رو از زاویه‌های مختلف بگیرم و بذارم خوشم نمیاد. بقیه بیان لایک کنن یا کامنت بذارن اینجوری خوشم نمیاد» (فهیمه).

«مطابقت با عرف و باورهای عامه» به این معنا که کاربر از انتشار تصاویر یا بیان مطالب مناقشه‌برانگیز خصوصاً خارج از جریان اصلی در جامعه خودداری می‌کند. پریسا می‌گوید: «مثلاً اینکه بخوام در مورد قضیه سیاسی یا مذهبی بحث کنم، نه اصلاً! مثلاً من حتی از علاقه‌ام به حیوانات چیزی نمی‌گم صرفاً یه عکس می‌ذارم».

کاربران با «رعایت مرزهای پوشش» که البته در هر مصاحبه‌شونده به‌صورت متفاوت تعریف شده است، تلاش می‌کنند تا بتوانند مزایای حاصل از افشا را برای خود تقویت کنند. یکی از اطلاع رسانان می‌گوید: «عکسای من عکسایی نیست که احساس کنم اشکالی داشته باشه، نهایت عکسی که از من مشخصه، گردیه صورتمه» (فاطمه ۲).

کد «بیان غیرمستقیم افشا» به راهبردهایی اشاره می‌کند که کاربر با استفاده از اشعار، جملات قصار و نمادها دست به افشا می‌زند. مینا به این راهبرد اشاره کرده و می‌گوید: «اگه ناراحت باشم، میرم عکس پاییز می‌ذارم».

«اضافه کردن توضیحات» بدین معناست که کاربر خطرهای حاصل از یک افشا را با افزودن توضیحاتی کاهش می‌دهد. مریم در این باره می‌گوید: «شده مثلاً سخنی گذاشتم از نویسنده‌ای بعد اومدن نظر دادن که نه اینجوری نیست، بعد توضیح دادم که من منظورم این بوده و حالا این نویسنده از یه نظر دیگه نگاه کرده و اینجوری نبود که این نظر خودم باشه».

«ایجاد فواصل زمانی در افشا» راهبردی است که در آن کاربر افشاهایی را که می‌داند با واکنش

منفی دیگران مواجه می‌شود و در عین حال جزئی از شرایط زندگی یا روحی فرد است، به‌صورت پشت سر هم قرار نمی‌دهد بلکه آن‌ها را با رعایت فواصل زمانی افشا می‌کند تا واکنش‌های منفی را از این طریق به حداقل کاهش دهد. راحله می‌گوید:

«وقتی که میرم خوش بگذرونم، عکس می‌ذارم بعد یه سری هستن که هرازگاهی میان میگن خوش می‌گذره؟ یه‌کم درس بخون. بعد حس می کنم این عکس رو اگه بذارم اونا میان دوباره این کامنتا رو می‌ذارن. برا همین نمی‌ذارم یا مثلاً صبر می‌کنم که یه‌کم از عکس قبلیم بگذره بعدش می‌ذارم تا فکر نکنن من هر روز در حال خوش‌گذرونی‌ام».

۲-۳. راهبردهای فنّاورانه

کدها در این راهبرد طبیعتاً با امکانات ارائه‌شده برای حفظ حریم خصوصی در اینستاگرام مرتبط‌اند و برای اطلاع‌رسانان در این مقاله به‌ترتیب و برحسب بیشترین فراوانی شامل «انتخاب هدف (خصوصی بودن صفحه[1])»، «بلاک کردن[2]»، «رد درخواست»، «حذف پست»، «حذف کامنت»، «ارسال پیام خصوصی[3]»، «آن‌تگ کردن»، «عمومی نکردن کامنت‌ها» و «استفاده همزمان از چند اکانت» می‌شوند. نکتهٔ قابل ذکر، تفاوت قابل ملاحظهٔ کاربران دختر در میزان آشنایی و استفادهٔ از راهبردهای فنّاورانه است. درحالی‌که برخی کاربران تقریباً با همهٔ قابلیت‌های فنّاورانهٔ اینستاگرام آشنای‌اند و تجربهٔ استفاده از آن‌ها را داشته‌اند، برخی صرفاً با چند قابلیت آشنا هستند و برای رفع مشکلات خود به دیگران مراجعه می‌کنند. تجربه‌های برخی اطلاع‌رسانان در ادامه قابل ملاحظه است:

«شده پستی گذاشتم که قشنگ از کامنت میشه فهمید که طرف نفهمیده چی شده، ولی متأسفانه نمی‌دونم چه جوری میشه یه کامنت رو حذف کرد؟» (فریده).

بچه‌ها یه صفحهٔ خزی دارن عکسای خز و عجیب غریبمون رو می‌ذارن بعد منم تگ می‌کنن. بهشون گفتم چرا من رو تگ کردی؟ خب من نمی‌خوام ببینن. بعد گفتن نگران نباش پیج ما چون پرایوته، فقط دوستای مشترکمون می‌بینن» (فهیمه).

۴. الگوهای استفاده از راهبردهای سواد حریم خصوصی

در این بخش سعی شده است وضعیت کاربران دختر در دستیابی به حد بهینهٔ حریم خصوصی بر اساس سهم و انواع مزایا، خطرها و راهبردهای فنّاورانه و اجتماعی مورد استفادهٔ آنها در قالب

1. private
2. block
3. direct message

الگوهایی تفکیک شود. الگوها حالت کلی دارند و ممکن است کاربری در میانهٔ دو الگو قرار گیرد، اما بر اساس نزدیکی بیشتر به هر یک از الگوهای مذکور در آن طبقه قرار داده باشد.

۱-۴. راهبردهای فنّاورانه پایین، راهبردهای اجتماعی بالا

این دسته از کاربران بیشترین میزان تأکید بر راهبردهای اجتماعی و محدودیت‌های ذهنی را دارند و از سوی دیگر بیش از سایر کاربران از قابلیت‌های فنّاورانه اینستاگرام اظهار بی‌اطلاعی می‌کنند. همچنین نارضایتی این گروه از وضع کاربری خود در اینستاگرام بیش از سایر اطلاع‌رسانان بوده است. این گروه به دلیل نگرانی زیاد از خطرها از مزایای آن صرف نظر می‌کنند تا آنجا که افشا نکردن و استفاده‌های مبتنی بر سرگرمی و آگاهی از فعالیت‌های دیگران را بر فعال بودن خود ترجیح می‌دهند. این کاربران با مشخصه‌هایی مانند دوستان بسیار محدود، پست‌های کم، پست‌های غیرشخصی مانند تصاویر جمع‌آوری‌شده از پیج‌های دیگران و در نهایت صفحات عمومی، از دیگر مصاحبه‌شوندگان تفکیک می‌شوند و شامل چهار نفر از مصاحبه‌شوندگان می‌شوند. تأکید بیشتر بر مزایای اجتماعی و حذف تقریبی مزایای روانشناختی و بیشتر بودن تعداد کدهای خطرها در مقایسه با کدهای مرتبط با مزایای خودافشاگری از دیگر ویژگی‌های کاربرانی است که در این الگو قرار گرفته‌اند، مثلاً فریده بر آن است که: «اینستا بهت کمک می‌کنه که خیلی بهتر آدمای اطرافت رو بشناسی، ولی می‌گم من به شخصه جرئت نکردم ازش استفاده کنم. یعنی هیچ‌وقت این ریسک رو نکردم که مثلاً پستی بذارم که از روی اون بتونم تشخیص بدم که فیدبکا چه جوریه». همچنین زهرا در این‌باره می‌گوید: « اینستا خوبی هم داره، مثلاً دوستام میان خودشون رو تخلیه می‌کنن، غیرمستقیم می‌نویسن، اینا اشکالی نداره، ولی من از همهٔ اینا صرف‌نظر کردم».

۲-۴. راهبردهای فنّاورانه بالا، راهبردهای اجتماعی پایین

این الگوی به‌کارگیری راهبردها شامل کاربرانی است که معمولاً در استفادهٔ خود از اینستاگرام محدودیت‌های کمتری در مقایسه با گروه قبل دارند و اغلب در تعریف مرزهای حریم خصوصی خود بسیار پرابهام عمل می‌کنند. به این معنا در موقعیت‌های گوناگون ممکن است رفتارهای متفاوتی در این خصوص از آنها دیده شود. این کاربران در مقایسه با گروه قبل ریسک‌پذیری بالاتری برای دریافت مزایا به‌ویژه مزایای روانشناختی دارند. درحالی‌که در برخی موارد به‌دلیل بی‌توجهی به راهبردهای اجتماعی خطرهای بیشتری را نیز تجربه کرده‌اند که البته به دلیل تسلط بر راهبردهای فنّاورانه خطرها به‌صورت کوتاه‌مدت بوده و کاربر معمولاً توانسته خطرها را کنترل کند. این الگو دربرگیرندهٔ سه نفر از کاربران بوده است. برای مثال زینت می‌گوید:

«مثلاً چند وقت پیش یه پست در مورد چالش جذابیت گذاشتن، منم رفتم این رو پُر کردم و بعد یکی به من گفت که تو از ۸۱ درصد خانم‌های جامعه جذاب‌تری. بعد من این رو گذاشتم و یه کپشن هم به طعنه زیرش رفتم که حالا نمردیم یکی به ما گفت جذاب. تبعاتش خیلی شدید شد تا یک ماه ملت من رو دست می‌انداختن. یه پسر زیر همین پست چیزی نوشت که مجبور شدم بلاکش کنم» .

۳-۴. راهبردهای فنّاورانه و اجتماعی بالا

این دسته از کاربران اگرچه در استفاده از راهبردهای فنّاورانه تسلط کافی دارند، به دلیل نگرانی زیاد از خطرها و در نتیجه استفادهٔ فراوان از راهبردهای اجتماعی و محدودیت‌های ذهنی باز هم ممکن است در مواردی به‌شدت تضاد حریم خصوصی را احساس کرده و خصوصاً برای دستیابی به مزایای روانشناختی از رفع آن به ایده‌ال‌ترین شکل مورد نظر خود بازمانده باشند. با این‌حال، در مقایسه با الگوی نخست به‌دلیل تسلط و آگاهی نسبتاً بیشتر از امکانات فنّاورانهٔ اینستاگرام، شناخت دقیق مرزهای حریم خصوصی خود و مزایایی که به دنبال آن هستند، رضایت بیشتری در استفادهٔ خود دارند و در مقایسه با کاربرانی که در الگوی دوم قرار گرفته‌اند، با خطرهای کمتری مواجه شده‌اند. این گروه از کاربران وضعیت بسیار مشخصی در تعریف مرزهای حریم خصوصی خود دارند و معمولاً کیفیت افشاهایشان نوسان کمتری دارد. صفحات این کاربران معمولاً شامل پست‌هایی با محتواهای مشابه، مانند مسافرت‌ها، جمع‌های دوستانه و تفریحات شخص می‌شود که با به اشتراک‌گذاری آن‌ها اغلب دستیابی به مزایای اجتماعی را دنبال می‌کنند. هفت نفر از اطلاع‌رسانان در این الگو قرار گرفته‌اند که گویای بیشترین فراوانی در مقایسه با سایر الگوها است. پریسا در همین راستا می‌گوید:

«من این مدلی که هستم دوس دارم. یه بی‌اعتمادی توش هست دیگه. امنیت نیست. مثلاً از اینکه این همه فالور دارم، دوستایی که نمی‌شناسم، خب احساس خوبی ندارم. دلیلی نداره بیام خودم رو بشناسونم بهشون. برا همین راجع‌به خصوصیاتم نمی‌ذارم. فقط در حد گردش و ایناست».

۴-۴. راهبردهای فنّاورانه و اجتماعی پایین

کاربران در این الگو اغلب به‌دلیل به‌کارگیری راهبردهای کنترل محتوا و محدودیت‌های ذهنیِ کم مشخصهٔ افشاهای بالا را دارند و از این جهت با خطرهایی مواجه شده‌اند و از آنجا که چندان در استفاده از راهبردهای اجتماعی و فنّاورانه ضرورتی ندیده‌اند و یا تسلط کافی بدان نداشته‌اند، وجود فاصلهٔ زمانی در لحظهٔ برخورد با تضاد تا به‌کارگیری راهبرد را تجربه کرده‌اند و این مسئله خود منجر به جدی شدن خطرها برای آن‌ها شده است. این گروه دقیقاً عکس الگوی نخست

شامل کاربرانی است که برای دست‌یابی به مزایا به‌ویژه مزایـای روانشـناختی تـا حـدود زیـادی از خطرهای بالقوه چشم‌پوشی کرده‌اند. کاربران در این الگو تنها کاربرانی‌اند کـه بـا خطـر پشـیمانی مواجه شده‌اند و این بدین معناست که بی‌توجهی به راهبردهای اجتماعی و فنّاورانه بـرای دسـتیابی به مزایای روانشناختی در برخی موارد به تبعات منفی روانشناختی برای خود کاربران و پشیمانی از افشا برای آن‌ها انجامیده است. سحر به این مسئله اشاره کرده و بیان می‌کند: «خیلی سـریع پسـت می‌ذارم، ولی از اون‌ور خیلی پیش اومده که پست گذاشتم و بعد یه مدت پاکش کردم، مـثلاً پـیش اومده تو یه شب ده تا پست هم پاک کردم چون دیگه بهشون حس خوبی نداشتم». با این‌حال، این کاربران کمتر در الگوی استفادهٔ خود از اینستاگرام تغییری ایجاد می‌کنند و خطرهـای پیش‌آمـده را اتفاقاتی محدود قلمداد می‌کنند که تا حدودی بیانگر دغدغـهٔ پـایین‌تـر حـریم خصوصـی در ایـن کاربران بوده است. چهار نفر از اطلاع‌رسانان در این الگو قرار گرفته‌اند.

۵-۴. راهبردهای فنّاورانه و اجتماعی متوازن

این گروه از اطلاع‌رسانان که بر اساس اظهارات خود بیشترین میـزان رضـایت در اسـتفادهٔ خـود از اینستاگرام را دارند، فقط شامل دو نفر از مصاحبه‌شوندگان مـی‌شـود. بـرای ایـن گـروه اسـتفاده از اینستاگرام جزء جدایی‌ناپذیر از زندگی روزمره است و معمـولاً ایـن نـرم‌افـزار را منشـأ بسـیاری از پیامدهای مثبت برای خود می‌دانند. فریبا در مورد اینستاگرام می‌گوید:

«از برنامه‌های اجتماعی کلاً خوشم نمیاد، ولی اینستاگرام رو به‌خاطر فلسـفه‌اش کـه می‌تـونی چیزای روزمرهٔ زندگی رو با دوسـتات بـه اشـتراک بـذاری، دوسـت دارم. اینکـه بـا یـه عـده‌ای در ارتباطی، کامنتایی از دوستات مـی‌گیـری، عکـس الان دوسـتایی رو کـه چنـد سـاله ندیدی‌شـون می‌بینی، اینکه چیزی تو دلت باشه میگی، اینا جذابه».

این دسته از کاربران که با اطمینان بیشتری از این نرم‌افزار استفاده می‌کننـد، افشـاهای بـالاتری دارند و در عین حال با خطرها و پشیمانی‌های کمتری در افشای خود مواجه‌اند و از ایـن‌رو موفـق‌ترین الگوی دستیابی به حد بهینهٔ حریم خصوصی هستند. این دسته از کاربران هر دو گونهٔ مزایـای اجتماعی و روانشناختی را تجربه کرده‌اند و بر حسب تعداد کدها به میزان تقریباً برابر به راهبردهای اجتماعی و فنّاورانه در حفظ حریم خصوصی خود اشاره کـرده‌انـد. مشخصـهٔ دیگـر ایـن گـروه از کاربران حرکت آرام و پیوسـته ایشـان در دسـتیابی بـه حـد بهینـهٔ حـریم خصوصـی بـا تسـلط بـر راهبردهای فنّاورانه است. به این معنا نگرانی‌ها و استفادهٔ کاربران از راهبردهای اجتماعی با افزایش مهارت‌های فنّاورانهٔ ایشان کاهش یافته تا در شرایط کنونی به حد متـوازن و رضـایت‌بخش از نظـر خود دست یافته‌اند. مینا از کاربرانی است که به این مسئله اشاره کرده است:

«اوایلش که اومدم اینستا نمی‌دونستم تگ کردن چیه بعد یه پسره بـود رو عکسـاش مـنم تگ می‌کرد. داداش منم یه‌کم حساسه اومد به من گفت چرا آن‌تگش نمی‌کنی، بعد بهـم گفت چه جوریه رفتم آن‌تگش کردم. ولی الان هر سری آپدیت میشه و یه قابلیـت بهـش اضافه میشه سریع میرم چند و چونش رو در میارم دیگه».

نتیجه

دستیابی به حد بهینهٔ حریم خصوصی برای کاربران شبکه‌های اجتماعی مستلزم برقراری ارتباطـات مؤثر و مسئولانه (بارچ و دیلن، ۲۰۱۶) از سوی آن‌هاست؛ ارتباطی که بـا بـه‌کارگیری راهبردهـای مبتنی بر سواد حریم خصوصی بتواند ضمن کنترل خطرها، مزایای حاصل از خود افشـاگری را نیـز برای کاربر در پی داشته باشد و آن‌ها را در رفع این تناقض یاری کنـد. ایجـاد درکـی از وضـعیت و میزان موفقیت کاربران دختر اینستاگرام در دستیابی به این حد بهینه هدف اصـلی ایـن مقالـه بـوده است. نتایج حاصل از مصـاحبه بـا ۲۰ اطلاع‌رسـان در نهایـت بـا شناسـایی دو تـم کلـی مزایـا و خطرهای «روانشناختی» و «اجتماعی» چنین تناقضی را برای کاربران دختر تأیید کرد. ایـن تضـاد به‌ویژه در دستیابی به مزایای روانشناختی بیشتر بوده است. به این معنا کاربران در اغلـب مـوارد در دستیابی به مزایایی روانشناختی، ماننـد «بیـان (تسـکین پریشـانی) و بهبـود احساسـات فـردی»، «تخلیهٔ هیجانات فردی» و «شفاف‌سازی خود» خطرهای بیشتری را احساس کرده‌انـد. صـرف‌نظر کردن از همین دسته از مزایا نیز در اغلب موارد با ابراز نارضایتی بیشتر اطلاع‌رسـانان بـه وضـعیت کاربری خود همراه بوده است. نکتهٔ دیگر آنکه وجود این تناقض برای همهٔ کـاربران یکسـان نبـوده است؛ برای برخی کاربران به‌حدی بوده است که آن‌هـا را بـه صـرف‌نظر کـردن از خودافشـاگری و مزایای حاصل از آن واداشته است و برخی دیگر چنین تضادی را کم‌تـر احسـاس کـرده و بـا بـی‌توجهی به خطرها، کسب مزایای بیشتر را در اولویت قرار داده‌اند.

همچنین یافتـه‌هـا در مجمـوع گویـای اسـتفادهٔ بیشـتر کـاربران از «راهبردهـای اجتمـاعی» و محدودیت‌های ذهنی در مقایسه با «راهبردهای فنّاورانه» بوده است. این مسئله بیانگر تسلط کـافی نداشتن برخی کاربران بر راهبردهای فنّاوانه است که خود گویای نیاز به آموزش‌های بیشتر در ایـن راستاست. در طول مصاحبه‌ها موارد فراوانی از ناآشنایی کاربران با راهبردهـای فنّاورانـه و ابهـام در نحوهٔ به‌کارگیری آن‌ها ملاحظه شد. بی‌توجهی به راهبردهای اجتماعی نیز در برخی مـوارد به‌انـدازهٔ بی‌اطلاعی از راهبردهای فنّاورانه موجب مواجههٔ کاربران دختر با تهدیدات حریم خصوصـی شـده است. بر اساس یافته‌ها استفادهٔ متوازن و تکمیلی از راهبردهـای فنّاورانـه و اجتمـاعی بـه رضـایت

بیشتر اطلاع‌رسانان از وضعیت کاربری خود انجامیده است. نکتهٔ دیگر آنکه باید میان اطلاع از یک راهبرد و استفادهٔ موفقیت‌آمیز از آن برای رفع تناقض حریم خصوصی تفکیک قائل شد که البته این مسئله در خصوص راهبردهای فنّاورانه پُررنگ‌تر بوده است. بدین معنا برخی مصاحبه‌شوندگان از کنار راهبردهایی که حتی با آن‌ها آشنایی داشتند، عبور کرده و نتوانسته‌اند در رفع تضادهای خود به‌درستی از آن‌ها استفاده کنند.

اگرچه حد بهینهٔ حریم خصوصی امری نسبی است و برای هر کاربر کاملاً متفاوت است، از میان الگوهای معرفی‌شده در این مقاله کاربرانی که در دسته آخر قرار گرفتند بر اساس میزان رضایتی که از وضعیت کاربری خود داشتند، موفق‌ترین گروه در دستیابی به حد بهینهٔ حریم خصوصی هستند. علاوه بر این، نتایج نیز گویای تجربهٔ بیشترین میزان مزایا در برابر کمترین میزان خطرها برای این کاربران بوده است. اما کم بودن تعداد کاربران این دسته بیانگر ناموفقیت نسبی دیگر اطلاع‌رسانان در استفادهٔ صحیح از راهبردها برای رفع تضاد حریم خصوصی خود بوده است، و در نتیجه در بدترین شرایط برخی مجبور به صرف‌نظر کردن از مزایا و برخی دیگر در اثر بی‌توجهی به خطرها از حد بهینهٔ حریم خصوصی دور شده‌اند.

در پایان فارغ از داشتن یا نداشتن سواد حریم خصوصی کاربران باید به این مسئله اشاره کرد که اینستاگرام نیز برای دختران محدودیت‌های فنّاورانه‌ای دارد که مصاحبه‌شوندگان حتی کسانی که در رفع تناقض حریم خصوصی خود نسبتاً موفق بوده‌اند، نیز بدان‌ها اشاره کرده‌اند، اما به‌دلیل خارج بودن از بحث اصلی این مقاله در اینجا آن را بررسی نکرده‌ایم. دیگر آنکه یافته‌های حاصل از مصاحبه‌ها در این مقاله قابلیت تعمیم ندارند و از این‌رو اجرای پژوهش‌های کمّی مکمل در این زمینه به‌لحاظ فراهم کردن درکی فراگیرتر از چگونگی به‌کارگیری راهبردهای سواد حریم خصوصی و نتایج آن برای عبور از «تضاد حریم خصوصی» راهگشا به نظر می‌رسند.

منابع

فلیک، اووه (۱۳۸۷). درآمدی بر تحقیق کیفی (مترجم: هادی جلیلی). تهران: نی. (تاریخ اصل اثر ۲۰۰۶)

لیندلف، تامس آر؛ و تیلور، برایان سی (۱۳۸۸). روش‌های تحقیق کیفی در علوم ارتباطات (مترجم: عبدالله گیویان). تهران: همشهری. (تاریخ اصل اثر ۲۰۰۲)

Acquisti, A., & Grossklags, J. (2005). Privacy and rationality in individual decision making. *IEEE Security & Privacy*, 3(1), 24-30. doi: 10.1109/MSP.2005.22

Altman, I. (1977). Privacy regulation: Culturally universal or culturally specific?. *Journal of Social Issues*, 33(3), 66-84. doi: 10.1111/j.1540-4560.1977.tb01883.x

Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. *First Monday*, 11(9). doi: 10.5210/fm.v11i9.1394

Bartsch, M., & Dienlin, T. (2016). Control your Facebook: An analysis of online privacy literacy. *Computers in Human Behavior*, 56, 147-154. doi: 10.1016/j.chb.2015.11.022

Bawden, D. (2008). Origins and concepts of digital literacy. In C. Lankshear, & M. Knobel, *Digital Literacies: Concepts, Policies and Practices* (pp. 17-32), New York: Peter Lang.

Ben-Ze'ev, A. (2003). Privacy, emotional closeness, and openness in cyberspace. *Computers in Human Behavior*, 19(4), 451–467. doi: 10.1016/S0747-5632(02)00078-X

Berg, J. H., & Derlega, V. J. (1987). Themes in the study of self-disclosure. In V. J. Derlega, & J. H. Berg, *Self-Disclosure: Theory, Research, and Therapy* (pp. 1-8), New York: Plenum Press.

Boyd, D., & Hargittai, E. (2010). Facebook privacy settings: Who cares?. *First Monday*, 15(8). doi: 10.5210/fm.v15i8.3086

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2), 77-101. doi: 10.1191/1478088706qp063oa

Burgess, R. G. (1981). Keeping a research diary. *Cambridge Journal of Education*, 11(1), 75-83. doi: 10.1080/0305764810110106

Derlega, V. J., Winstead, B. A., & Greene, K. (2008). Self-disclosure and starting a close relationship. In S. Sprecher, A. Wenzel, & J. Harvey, (Eds.). *Handbook of Relationship Initiation* (pp. 153–174), New York: Psychology Press.

Ellison, N. B., Vitak, J., Steinfield, C., Gray, R., & Lampe, C. (2011). Negotiating privacy concerns and social capital needs in a social media environment. In S. Trepte, & L. Reinecke, *Privacy Online: Perspectives on Privacy and Self-Disclosure in the Social Web* (pp. 19-32), Berlin: Springer.

Eshet-Alkali, Y., & Amichai-Hamburger, Y. (2004). Experiments in digital literacy. *CyberPsychology & Behavior*, 7(4), 421-429. doi: 10.1089/cpb.2004.7.421

Fogel, J., & Nehmad, E. (2009). Internet social network communities: Risk taking, trust, and privacy concerns. *Computers in Human Behavior*, 25(1), 153-160. doi: 10.1016/j.chb.2008.08.006

Gattiker, U. E., Perlusz, S., Bohmann, K., & Sørensen, C. M. (2001). The virtual community: Building on social structure, relations and trust to achieve value. In L. Chidambaram, & I. Zigurs, *Our Virtual World: The Transformation of Work, Play and Life via Technology* (pp. 165-187), Hershey; USA & London; Uk: Idea Group Publishing.

Hall, G. (2008). An ethnographic diary study. *ELT Journal*, 62(2), 113-122. doi: 10.1093/elt/ccm088

Hallett, R. E., & Barber, K. (2013). Ethnographic research in a cyber era. *Journal of Contemporary Ethnography*, 43(3), 306-330. doi: 10.1177/0891241613497749

Hargittai, E. (2002). Second-level digital divide: Differences in people's online skills. *First Monday*, 7(4). doi: 10.5210/fm.v7i4.942

Hill, C. T., & Stull, D. E. (1987). Gender and self-disclosure: Strategies for exploring the issues. In V. J. Derlega, & J. H. Berg, *Self-Disclosure: Theory, Research, and Therapy* (pp. 81-100), New York: Plenum Press.

Hu, Y., Manikonda, L., & Kambhampati, S. (2014). What we Instagram: A First analysis of Instagram photo content and user types. Paper be Peresented at The *8th International AAAI Conference on Weblogs and Social Media*, June 1-4, 2014, *USA, Michigan.* Retrived from https://www.aaai.org/ocs/index.php/ICWSM/ICWSM14/paper/viewFile/8118/8087

Lee, H., Park, H., & Kim, J. (2013). Why do people share their context information on social network services? A qualitative study and an experimental study on users' behavior of balancing perceived benefit and risk. *Human-Computer Studies*, 71, 862–877. doi: 10.1016/j.ijhcs.2013.01.005

Lewis, K., Kaufman, J., & Christakis, N. (2008). The taste for privacy: An analysis of college student privacy settings in an online social network. *Journal of Computer-Mediated Communication*, 14(1), 79-100. doi: 10.1111/j.1083-6101.2008.01432.x

Li, Y. (2012). Theories in online information privacy research: A critical review and an integrated framework. *Decision Support Systems*, 54(1), 471-481. doi: 10.1016/j.dss.2012.06.010

Litt, E. (2013). Understanding social network site users' privacy tool use. *Computers in Human Behavior*, 29, 1649–1656. doi: 10.1016/j.dss.2012.06.010

Markham, T., & Couldry, N. (2007). Tracking the reflexivity of the (Dis) Engaged citizen some methodological reflections. *Qualitative Inquiry*, 13(5), 675-695. doi: 10.1177/1077800407301182

Omarzu, J. (2000). A disclosure decision model: Determining how and when individuals will self-disclose. *Personality and Social Psychology Review*, 4(2), 174-185. doi: 10.1207/S15327957PSPR0402_05

Park, Y. J. (2011). Digital literacy and privacy behavior online. *Communication Research*, 1-22. doi: 10.1177/0093650211418338

Park, Y. J. (2015). Do men and women differ in privacy? Gendered privacy and (in) equality in the internet. *Computers in Human Behavior*, 50, 252-258. doi: 10.1016/j.chb.2015.04.011

Petronio, S. (2002). *Boundaries of privacy: Dialectics of disclosure.* New York: State University of New York Press.

Price, B. A., Adam, K., & Nuseibeh, B. (2005). Keeping ubiquitous computing to yourself: A practical model for user control of privacy. *International Journal of Human-Computer Studies*, 63(1), 228-253. doi: 10.1016/j.ijhcs.2005.04.008

Stutzman, F., Vitak, J., Ellison, N. B., Gray, R., & Lampe, C. (2012). Privacy in interaction: Exploring disclosure and social capital in Facebook. Paper Peresented at the *Sixth International AAAI Conference on Weblogs and Social Media,* June 4-8, 2012, Dublin, Irland. Retrived from https://www.aaai.org/ocs/index.php/ICWSM/ICWSM12/paper/viewFile/4666/5000

Taddicken, M. (2012). Privacy, surveillance, and self-disclosure in the social web. In C. Fuchs, K. Boersma, A. Albrechtslund, & M. Sandoval, (Eds.). *Internet and Surveillance: The Challenges of Web 2.0 and Social Media* (pp. 255-272), New York: Routledge Publication.

Thelwall, M. (2011). Privacy and gender in the social web. In S. Trepte, & L. Reinecke, *Privacy Online: Perspectives on Privacy and Self-Disclosure in the Social Web* (pp. 251-265), Berlin: Springer.

Trepte, S., Teutsch, D., Masur, P. K., Eicher, C., Fischer, M., Hennhöfer, A., & Lind, F. (2014). Do people know about privacy and data protection strategies? Towards the "Online Privacy Literacy Scale" (OPLIS). In S. Gutwirth, R. Leenes, & P. D. Hert, *Reforming European Data Protection Law* (pp. 333-365), Netherlands: Springer.

Tufekci, Z. (2008). Can you see me now? Audience and disclosure regulation in online social network sites. *Bulletin of Science, Technology & Society*, 28(1), 20-36.

Yao, M. Z. (2011). Self-protection of online privacy: A behavioral approach. In S. Trepte, & L. Reinecke, *Privacy Online: Perspectives on Privacy and Self-Disclosure in the Social Web* (pp. 111-125), Berlin: Springer.