



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

فرزانه سیاسی راد<sup>۱</sup>، عبدالله بیجرانلو<sup>۲\*</sup>

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 خودافشایی 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 خودافشایی بررسی شده و سپس بر اساس سواد حریم خصوصی آنلاین، برخی از راهبردهای اجتماعی و فناوریانه برای حل «تناقض حریم خصوصی» معرفی شده‌اند. در بخش یافته‌ها پس از توصیف مهم‌ترین مزایا و خطرهای خودافشایی برای کاربران دختر، الگوهای فعلی چگونگی به‌کارگیری راهبردهای اجتماعی و فناوریانه برای حل این تضاد استخراج و درباره آن‌ها بحث شده است. این بررسی به روش مردم‌نگاری و با مصاحبه نیمه‌ساخت‌یافته و مشاهده غیرمشارکتی صفحات ۲۰ کاربر دختر اینستاگرام صورت گرفته است.

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

۱. دانشجوی کارشناسی ارشد مطالعات فرهنگی و رسانه، دانشکده علوم اجتماعی، دانشگاه تهران، تهران، ایران. [fsiasirad@yahoo.com](mailto:fsiasirad@yahoo.com)

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

گسترش استفاده از اینترنت در زمینه کار و زندگی فرصت‌های جدیدی برای برقراری ارتباط با دیگران در سراسر جهان فراهم کرده است. از این رو، ظهور اجتماعات مجازی فراهم‌کننده امکان ارتباط میان افرادی است که ممکن است لزوماً یکدیگر را نشناسند و صرفاً با واسطه شبکه‌های الکترونیکی امکان مبادله اطلاعات برایشان فراهم شده باشد (گیتیکر و همکاران<sup>۱</sup>، 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 درباره 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<sup>۲</sup>، تلاش می‌کند این مزایا، خطرها و نحوه مدیریت فرایندهای بهینه‌سازی حریم خصوصی را (آلتمن<sup>۳</sup>، ۱۹۷۷) از سوی کاربران دختر در شبکه‌های اجتماعی بررسی کند.

در متن استفاده از شبکه‌های اجتماعی مانند هر رابطه 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 نظریه 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 به سمت خودافشاگری می‌کشاند (درلگا و همکاران<sup>۴</sup>، ۲۰۰۸، ۱۵۷). در نتیجه 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<sup>۵</sup>، ۲۰۰۶). این تناقض که با عنوان دوگانه نگرش یا رفتار<sup>۶</sup> (اکویستی و کراسکیچ<sup>۷</sup>، 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<sup>۸</sup>، 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،<sup>۱</sup> ۲۰۱۶). به‌زعم تربت و همکاران<sup>۲</sup> (۲۰۱۴، ۳۳۳) برخورداری افراد از سواد حریم خصوصی آنلاین به آن‌ها برای حل کردن این تناقض کمک خواهد کرد.

نظریه حریم ارتباطات<sup>۳</sup> ساندارا پترونیو<sup>۴</sup> (۲۰۰۲) از جمله نظریاتی است که عوامل فردی را بر شکل‌گیری نگرانی‌های حریم خصوصی تأثیرگذار می‌داند (لی<sup>۵</sup>، 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 دوسویه 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 (فناورانه و اجتماعی)

استفاده می‌کنند؟

(۴) با توجه به تأکید کاربران بر مزایا، توجه و آگاهی از خطرها و سهم به‌کارگیری هر یک از

راهبردهای فناورانه و یا اجتماعی، الگوهای کاربران برای دستیابی به حد بهینه 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 مسئله حریم خصوصی آنالین، 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 به معنای «هر پیام راجع به خود که فرد به واسطه آن با فرد دیگری ارتباط برقرار می‌کند» است (ویلس و گروتز<sup>۱</sup>، ۱۹۷۶، ۳۳۸؛ به نقل از تدیکن<sup>۲</sup>، ۲۰۱۲، ۲۵۶). آلتمن و تیلور<sup>۳</sup> (۱۹۷۳) در نظریه نفوذ اجتماعی<sup>۴</sup> به تأثیر خودافشاگری بر روابط میان فردی اشاره کرده‌اند و ضمن توصیف شکل‌گیری، حفظ و انحلال روابط نزدیک، خودافشاگری را لازمه توسعه روابط نزدیک می‌دانند (به نقل از برگ و درلگا<sup>۵</sup>، ۱۹۸۷، ۵). امارزو<sup>۶</sup> (۲۰۰۰) با طراحی مدل تصمیم‌گیری افشا<sup>۷</sup> جزئیات بیشتری را در فرایند خودافشاگری معرفی می‌کند. او خودافشاگری را رفتاری چندبعدی می‌داند و بر اساس این مدل توضیح می‌دهد که افراد برای توسعه 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<sup>۸</sup>، ۲۰۱۳). با وجود این، چنانچه ذکر شد، پیامد خودافشاگری فقط پاداش‌های اجتماعی نیست، بلکه برای فرد به صورت همزمان خطرهای اجتماعی را نیز در پی خواهد داشت (امارزو، ۲۰۰۰).

با وجود دشوار بودن ارائه تعریفی مشخص از حریم خصوصی به دلیل 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. Wheelless & 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<sup>۱</sup> در یک گروه» تعریف می‌کند. بر اساس نظر آلتمن حریم خصوصی فرایند پویای بهینه‌سازی بین نیاز به حفظ حریم خصوصی از یک سو 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 به سمت 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 به سوی دیگران می‌کشایند و گاهی بالعکس. اگرچه سازوکارهای آلتمن و پترونو شامل رفتارهای کلامی و فراکلامی، کنترل فضاهای شخصی و سازوکارهای فرهنگی، برای دستیابی به حریم خصوصی بهینه در زندگی روزمره و در هر موقعیتی در محیط‌های آنلاین قابل استفاده نیستند، رویکرد آنها به حریم خصوصی به مثابه «کنترل انتخابی دسترسی به خود» برای مذاکره مرزهای خودافشاگری و عدم خودافشاگری در سایت‌های شبکه‌های اجتماعی نیز قابل استفاده است (توفچی، ۲۰۰۸؛ لیت<sup>۲</sup>، ۲۰۱۳).

#### ۱-۱. مزایا و خطرهای خودافشاگری

پترونو در نظریه مدیریت حریم ارتباطات بر این باور است که نحوه 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 (پترونو، ۲۰۰۲، ۲۶). پنج مزیت اصلی خودافشاگری عبارت است از: بیان<sup>۳</sup>، شفاف سازی خود<sup>۴</sup>، اعتباریابی اجتماعی<sup>۵</sup>، توسعه روابط<sup>۶</sup> روابط<sup>۶</sup> و کنترل اجتماعی<sup>۷</sup>. 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 به سمت تقویت دیدگاه‌ها و ارزش‌های فرد سوق دهد و اعتبار اجتماعی او را افزایش دهد. توسعه 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 گرزلاک<sup>۱</sup>، ۱۹۷۹؛ به نقل از پترونو، ۲۰۰۲، ۶۶-۶۷).

سطوح خطرهای خودافشاگری ممکن است بالا، متوسط یا پایین باشد. خطرهای بالا ناشی از افشای موضوعاتی است که شرم‌آور و تهدیدکننده‌اند، مثل رازهای فرد. خطرهای متوسط رویدادها، نگرش‌ها، ارزش‌ها و تجربیاتی است که بیان آن‌ها برای دیگران موجب آزرده‌گی فرد می‌شود و خطرهای پایین بیان مسائل تناقض‌آمیز یا دروغ‌های مصلحتی است. علاوه بر سطوح، خطرهای خودافشاگری انواعی دارد، از جمله خطر امنیتی، خطر انگ، خطر وجهه، خطر رابطه و خطر نقش<sup>۲</sup>. خطرهای امنیتی دسته‌ای از افشاهاست که ممکن است امنیت فرد یا دیگران را به خطر اندازد. خطر انگ مبتنی بر فرضیاتی است که گویای ارزیابی منفی دیگران از رفتار و عقیده فرد است و بیشتر مربوط به خود درونی و هویت فردی است. خطر وجهه حالت کلی‌تری دارد و مربوط به پیش‌بینی فرد از افشاهایی است که موجب شرمساری فرد یا گروهی می‌شود که در آن عضویت دارد. خطر رابطه تهدیدکننده رابطه فرد با دیگران است و خطر نقش موجب به خطر افتادن جایگاه فرد و نقش و وظایف او می‌شود. خطرهای مذکور حالت نسبی دارند و در نتیجه آنچه برای یک فرد خطر است، ممکن است برای فرد دیگر تهدید نباشد (پترونو، ۲۰۰۲، ۷۱-۶۷).

## ۱-۲. تناقض میان خودافشاگری و حریم خصوصی

اساس نظریه مدیریت حریم ارتباطات این است که خودافشاگری امری دیالکتیکی است. به بیان روشن‌تر، اگر خودافشاگری فرایند در میان نهادن اطلاعات شخصی فرد با دیگران و نیز ضرورتی برای توسعه روابط فرد باشد، تعریف حریم خصوصی در مقابل این تعریف قرار می‌گیرد؛ بدین معنا که افراد حق دارند به صورت فردی یا گروهی اطلاعات شخصی خود را محفوظ نگه دارند (پترونو، ۲۰۰۲، ۶). برای روشن‌تر شدن این وضعیت می‌توان تصور کرد که هر فرد، منطقه‌ای اطلاعاتی با تعریف مرزهای مشخص در اطراف خود دارد که تعیین می‌کند چه اطلاعاتی را می‌توان با دیگران به اشتراک گذاشت. بر حسب عوامل موقعیتی یا فردی، تلاش نهادی خارجی برای نفوذ به این مرز می‌تواند تهدید قلمداد شود (لی، ۲۰۱۲).

این تناقض در روابط آنلاین اگرچه در نگاه نخست به دلیل امکان پنهان کردن اطلاعات خصوصی و کاهش آسیب‌پذیری کاربران چندان مطرح نیست، اما حضور کاربران در فضای 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 رابطه دیاکتیکی میان حفظ حریم خصوصی و خودافشاگری را در روابط برخط نیز به اندازه زندگی واقعی مطرح کند. این تناقض خصوصاً زمانی که روابط مجازی ادامه روابط فرد در زندگی واقعی باشند یا به زندگی واقعی فرد نیز تسری یابند، می تواند از توانایی فضای مجازی برای کاهش این تقابل بکاهد (بنزیو،<sup>۱</sup> ۲۰۰۳).

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

اگرچه پژوهش های صورت گرفته در زمینه رابطه میان خودافشاگری و جنسیت گویای یافته های متناقضی است (هیل و استال<sup>۲</sup>، ۱۹۸۷، ۸۲)، بر اساس نظریه حریم خصوصی ارتباطات، جنسیت افراد از شاخص های تأثیرگذار بر تعریف مرزهای حریم خصوصی و به کارگیری قواعد گوناگون برای قاعده مند کردن آن است. این نظریه ریشه این تفاوت را فرآیندهای اجتماعی شدن و انتظارات فرهنگی متفاوت برای زنان و مردان می داند (پترونیو، ۲۰۰۲، ۲۴).

مدل «حریم خصوصی جنسیتی وب اجتماعی»<sup>۳</sup> مایک سلوال<sup>۴</sup> (۲۰۱۱) از بهترین نظریات توضیح تناقض حریم خصوصی و راهبردهای رفع آن در شبکه های اجتماعی با توجه به متغیر جنسیت است. بر اساس این مدل استفاده زنان از شبکه های مجازی به شدت تحت تأثیر نیروهای دوگانه افشا و حفظ حریم خصوصی است. با وجود اینکه زنان فشارهای بیشتری برای دوری از شبکه های مجازی و حفظ حریم خصوصی خود متحمل می شوند، این شبکه ها برای بسیاری از فعالیت های زنان جایگزین های آنلاین مناسبی فراهم می کنند و بسیاری از نیازهای زنان به ارتباطات اجتماعی را برآورده می کنند. زنان به این دلیل که در زندگی واقعی خود دغدغه های بیشتری در خصوص امنیت فیزیکی خود و مواجهه با آزار و اذیت دارند، استفاده از شبکه های مجازی نیز می تواند خطری برای حریم خصوصی این گروه باشد، مثلاً بسیار محتمل تر است که زنان قربانی جرایم مجازی و مزاحمت های سایبری باشند. بنابراین پیش بینی می شود که زنان با احتیاط تر و با استراتژی های حفاظتی بیشتری از شبکه های اجتماعی استفاده می کنند (سلوال، ۲۰۱۱، ۲۵۵-۲۵۲).

با وجود ضرورت به کارگیری استراتژی های حفاظتی بیشتر به منظور رسیدن به سطح بهینه حریم خصوصی برای زنان، برخی صاحب نظران تفاوت های جنسیتی را از عوامل مهم کسب مهارت های حفظ حریم خصوصی دانسته اند (هارجیتایی<sup>۵</sup>، ۲۰۰۲). از این رو جنسیت می تواند به مثابه 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 بهره‌مندی از مزایا در همه حوزه‌های اینترنت شود (پارک<sup>۱</sup>، ۲۰۱۵)، به‌ویژه در شرایطی که در فضای مجازی نیز تحت تأثیر زندگی واقعی، فرایندهای اجتماعی شدن متمایز زنان و مردان در آموزش و پرورش، سازمان‌ها و مناسبات شغلی، موجب هدایت آن‌ها به مسیرهای گوناگونی از انتخاب‌ها و ارزش‌ها شده و در نهایت موجب اتخاذ تصمیمات متفاوت در محیط‌های اطلاعاتی می‌شود (لالی<sup>۲</sup>، ۲۰۰۲؛ به نقل از پارک، ۲۰۱۵). با این حال یافته‌های تجربی فعلی درباره تأثیر جنسیت بر توانایی کنترل حریم خصوصی یک‌دست نیست؛ برخی از یافته‌ها بیانگر کنترل بیشتر زنان و استفاده بیشتر آن‌ها از ابزارهای فناوریانه است (لیت، ۲۰۱۳؛ فوگل و نهمد، ۲۰۰۹؛ لوئیس و همکاران<sup>۳</sup>، ۲۰۰۸). اما نتایج حاصل از تحقیقات دیگر گویای آن است که مردها به مراتب بهتر از زنان از امکانات فنی استفاده می‌کنند و به علت مرد بودنشان اعتماد به نفس بالاتری در حفاظت از حریم خصوصی خود دارند. البته این شکاف در به‌کارگیری استراتژی‌های تکنیکی پررنگ‌تر از ابعاد اجتماعی ملاحظه شده است (پارک، ۲۰۱۱؛ پارک، ۲۰۱۵). در نهایت بوید و هارجیتایی<sup>۴</sup> (۲۰۱۰) به تفاوت‌های اندکی در رفتارهای مرتبط با حریم خصوصی این دو گروه اشاره کرده‌اند، که البته به مرور زمان برای زنان افزایش اندکی داشته است.

#### ۴-۱. سواد حریم خصوصی و راهبردهای حفظ حریم خصوصی

سواد حریم خصوصی آنلاین که خود یکی از ابعاد سواد دیجیتال است و در برخی منابع از آن تحت عنوان سواد اجتماعی عاطفی<sup>۵</sup> و سواد اخلاقی اجتماعی نیز یاد شده است (اشت‌الکالای و آمیچی‌هامبورگر<sup>۶</sup>، ۲۰۰۴؛ بودن<sup>۷</sup>، ۲۰۰۸، ۳۰)، به معنای فهم رفتار درست و معقول در محیط‌های محیط‌های دیجیتال و دربرگیرنده مسائل حریم خصوصی و امنیتی است (بودن، ۲۰۰۸، ۳۰). برخورداری از دانش استراتژی‌های کنترل فردی حریم خصوصی از سوی کاربران در برخی مقیاس‌ها از الزامات برخورداری افراد از سواد حریم خصوصی آنلاین قلمداد شده است (ترپت و همکاران، ۲۰۱۴، ۳۳۳). این استراتژی‌ها که خود ترکیبی از مهارت‌های اجتماعی و فنی است (ترپت و همکاران، ۲۰۱۴، ۳۵۰؛ پارک، ۲۰۱۱)، با توجه به سؤالات مطرح‌شده در این مقاله، راهی برای فهم 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 به صورت کلی ممکن است به صورت منفعلانه و فعالانه صورت گیرد. از این رو، راهبردهای حفظ حریم خصوصی به دو بُعد هنجاری و قانونی و بُعد رفتاری و اجتماعی تفکیک می شود؛ بُعد رفتاری راهبردهایی است که کاربران به صورت رفتارهای برنامه ریزی شده و آگاهانه به کار می گیرند. بدین منظور کاربران باید دانش و مهارت های تکنیکی فضای مجازی را داشته باشند تا بتوانند خطرهای این فضا را به درستی ارزیابی کنند. در مقابل، بُعد هنجاری یا منفعلانه حفاظت های دولت یا دیگران است و فرد کنترل مستقیمی بر آن ها ندارد (یائو<sup>۱</sup>، ۲۰۱۱، ۱۱۵). این حفاظت ها که با توجه ویژه قانونگذاران در کشورهای گوناگون همراه بوده است، اغلب به دلیل نداشتن انعطاف پذیری کافی اجازه استفاده مؤثر از فناوری را به کاربران نمی دهند (پرایس و همکاران<sup>۲</sup>، ۲۰۰۵).

در رویکرد رفتاری مورد نظر این مقاله، دانشمندان اجتماعی چگونگی حفاظت افراد از حریم خصوصی خود در زمینه های گوناگون اجتماعی را مطالعه می کنند. محافظت های رفتاری را می توان در درجه 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 استراتژی های مدیریت مرزی نیاز دارد (یائو، ۲۰۱۱، ۱۱۵). استراتژی های رفتاری را نیز می توان به دو دسته استراتژی های اجتماعی و فناوریانه تقسیم کرد؛ استراتژی های فناوریانه حفظ حریم خصوصی استراتژی هایی است که کاربران از طریق آن ها از ویژگی ها یا امکانات یک سایت برای حفظ حریم خصوصی خود استفاده می کنند، مانند ایجاد فهرست دوستان، آن تگ<sup>۳</sup> کردن پست ها و تصاویر و حذف محتوای پست شده (لیت، ۲۰۱۳). در حالی که استراتژی های اجتماعی شامل ایجاد محدودیت های ذهنی در افشا می شود که با کمک آن کاربر فقط اطلاعاتی را افشا می کند که برای همه اعضای شبکه مناسب باشد (هانگ، ۲۰۱۰، به نقل از استاتزمن و همکاران<sup>۴</sup>، ۲۰۱۲).

الیسون و همکاران<sup>۵</sup> (۲۰۱۱، ۲۹) بر اساس یافته های پژوهش خود بر این باورند که استراتژی های فناوریانه و اجتماعی به مثابه 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 به دلیل اهمیت دادن به جزئیات و نمایش تکثر فعلی هر مسئله در این مقاله استفاده شده است (فلیک<sup>۱</sup>، ۱۳۸۷). تحقیقات مردم‌نگارانه شامل مطالعهٔ اطلاع‌رسانان، کنش‌ها و اقداماتشان در لحظهٔ عمل و در محل طبیعی زندگی می‌شوند (برجس<sup>۲</sup>، ۱۹۸۱). در هم‌تیدگی فضاها برخط و واقعی در سال‌های اخیر موجب شده است تا ضرورت جدا کردن این فضاها در مطالعات مردم‌نگارانه کم‌رنگ‌تر شود (هالت و باربر<sup>۳</sup>، 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<sup>۴</sup>، ۲۰۱۴). سرعت افزایش کاربران و استفاده از این نرم‌افزار به گونه‌ای بوده که بر اساس آمار<sup>۵</sup> 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 به دست آمد. کیفیت برخی سؤالات مطرح‌شده در این مرحله به گونه‌ای است که تفکیک آن‌ها از مصاحبهٔ یادداشت روزانه<sup>۶</sup> 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 یادداشت‌روانه<sup>۱</sup> 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 یادداشت‌روانه بر نوعی مطالعه اکتشافی و امیک تأکید دارند و امکان امتداد مرزهای پژوهش در غیاب پژوهشگر را فراهم می‌کنند (برجس، ۱۹۸۱؛ مارکهام و کولدري<sup>۲</sup>، ۲۰۰۷؛ هال<sup>۳</sup>، ۲۰۰۸).

در این مقاله، از آنجا که درک چگونگی ایجاد تناقضات خودافشاگری و نحوه عبور از آن در لحظه 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»<sup>۴</sup> یا موضوعی موضوعی تحلیل شده‌اند. تحلیل تماتیک روشی سیستماتیک برای شناسایی، سازماندهی و ارائه 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 مرحله عمل معمولاً از سه مرحله اصلی ایجاد کدهای اولیه، جست‌وجوی تم‌های کلی‌تر و تعریف و نام‌گذاری تم‌ها تشکیل شده است (برون و کلارک<sup>۵</sup>، 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<sup>۶</sup> از راهبردهای رایج در پژوهش‌های کیفی است که طیف گسترده‌ای از کیفیت‌ها، ویژگی‌ها، موقعیت‌ها، یا اتفاقات را در چارچوب مسئله پژوهش بررسی می‌کند. در این روش، پژوهشگر فقط در پی یافتن نمونه‌هایی است که ویژگی‌های متنوعی داشته باشند (لیندلف و تیولور<sup>۷</sup>، ۱۳۸۸، ۱۷۳). به دلیل 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 دغدغه‌حریم خصوصی دارد، برای مصاحبه معرفی کنند. در انتخاب اطلاع‌رسانان تلاش شده است تا افرادی انتخاب شوند که علاوه بر داشتن نسبی دغدغه‌حریم خصوصی، به لحاظ روابط اجتماعی، میزان اعتقادات مذهبی، شرایط خانوادگی و تعداد پست‌های به اشتراک گذاشته‌شده نیز متنوع باشند. ضمناً همه اعضای نمونه حاضر در مصاحبه در صفحه اینستاگرام خود از نام واقعی استفاده کرده‌اند و دوستان و نزدیکان خود را نیز در لیست دنبال‌کنندگان<sup>۱</sup> در صفحه خود داشته‌اند. مشخصات شرکت‌کنندگان در جدول ۱ آمده است.

جدول ۱. مشخصات اطلاع‌رسانان

ردیف نام	سن	رشته 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 فناوری 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	تقریباً ۱
۱۵ مهسا	۲۷	دانشجوی کارشناسی ارشد مهندسی آی.تی	۲	۲۰۲	۹۸	۲-۱
۱۶ فاطمه	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	۲ تا ۱
۱۸ پرینسا	۲۶	دانشجوی کارشناسی ارشد گرافیک	تقریباً ۲	۲۵۰	۶۱	کمتر از ۱
۱۹ سحر	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



## 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 حدیه عکس وقتی این صحنه حس خوبی بهم میده، به کسانی که می‌بینن هم همین حس خوب رو بده».

«تخلیه 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 منطقی 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 صفحه خود احساسات مثبت حاصل از آن را به دیگر زمان‌ها نیز توسعه دهند. پریسا در این باره می‌گوید: «دوست دارم اینستاگرام واقعاً مثل یه 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»، «توسعه 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 دوستای همفکرم توی اینستا فعال‌اند و راجع به 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 به دست می‌آورد. آمنه در این زمینه چنین بیان می‌کند: «مثلاً به 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 پیججت 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 راجع به طرز فکرم چیه؟ حتی به 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:

«بین از به نظر خوبه که دوستایی که به مدت طولانی نمی‌بینیشون ازشون بی‌خبر نیستی، مثلاً این ۲۰۷ نفر توی به 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».

«توسعه روابط» در اینجا به مزایای حاصل از خودافشاگری‌هایی اشاره می‌کند که به گسترش دایره 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: «به شعری بخونم یا کتابی بخونم که به قسمتش رو دوست داشته باشم یا آهنگی گوش بدم که دوستش داشته باشم، دوست دارم که دوستامم بدونن».



«بازنمایی خود» مزیتی است که کاربر از طریق افشای خود آن گونه که دوست دارد، مثلاً فردی شاد، ثروتمند، خوشبخت به دست می آورد. راحله در این باره چنین بیان می کند: «جایی برم یا اتفاق خاصی بیافته حتماً می دارم، دلیل اصلیش پز دادنه، اینکه نشون بدم حالم خوبه، خوشحالم، زندگی بر وفق مراده، آگه نباشه نمی دارم، فقط راجع به اتفاقات خوبش می دارم. دوست ندارم کسی بدونه ناراحتم».

## ۲. خطرهای خودافشاگری

خطرهای حاصل از خودافشاگری نیز که پیش از این در قالب مجموعه خطرهای امنیتی، خطر انگ، خطر وجهه، خطر رابطه و خطر نقش معرفی شد، در نتیجه یافته های حاصل از مصاحبه ها توسعه یافته اند و مجدداً ذیل دو تم کلی «خطرهای روانشناختی» و «خطرهای اجتماعی» قرار گرفته اند. «خطرهای روانشناختی» خطرهایی است که منشأ فردی دارند و این خود کاربر است که در گذر زمان و با کنترل نکردن افشاهای عاطفی خود زمینه ساز ایجاد چنین خطرهایی برای خود می شود. در حالی که در «خطرهای اجتماعی» دوستان، دنبال کنندگان صفحه کاربر و در برخی موارد مالکان شبکه موجب تبدیل افشا به خطر برای کاربر می شوند. اغلب کدها تحت تم «خطرهای اجتماعی» قرار دارند، شامل «خطر وجهه»، «خطر سطحی شدن»، «خطر سوء تفاهم»، «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 توسعه احساسات منفی این حوادث به دیگر مقاطع زندگی فرد می شوند و در نهایت به پشیمانی فرد از افشا می انجامد. امروز به این خطر اشاره کرده است: «توی دوره که حالم بود یه عکس گذاشتم، فقط چشم معلوم بود، داشتم گریه می کردم و دوستم ازم عکس گرفته بود. عکس سیاه و سفید بود و اشکم ریمبل داشت، ولی بعد هر موقع اینو می دیدم یاد اون موقع می افتادم، سر همون پشیمون شدم».

«خطر وجهه» به خطرهایی اشاره می کند که جایگاه فرد را آن طور که خود خواهان آن است، مثلاً در جایگاه فردی قانون مدار، تحصیل کرده و متدین تهدید می کند. این خطرها همچنین می توانند حاصل نوعی شرمندگی از افشاهای بسیار شخصی مرتبط با جایگاه شغلی، تحصیلی، خانوادگی و یا دوستانه فرد باشد که گویای حقایقی از کوتاهی ها و نقصان های فرد در این موقعیت هاست. فهمیه درباره این خطر می گوید:

«یه بار از خانمی که تویی. آر. تی نشسته بود، عکس گذاشتم حس خوبی بهم داده بود، بعد یکی از بچه ها 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 پرس و جو کردم گفتن به لحاظ قانونی حق نداری عکسش رو بدون اجازه پنخش کنی. منم گفتم پاکش کنم بهتر از اینه که بهم بگن خلاف قانون عمل کردی».

«خطر سطحی شدن» ناشی از افشاهایی است که به دلیل همه گیر شدن مزایای چندانی برای فرد ندارد و کاربرد فقط به دلیل علاقه شخصی ممکن است دست به چنین افشایی بزند. انتشار تصاویر مرتبط با غذا و دیگر امور روزمره اغلب زمینه ساز این نوع از خطرها برای کاربران شده است. فاطمه با اشاره به این خطر می گوید: «یه دوره می با دوستات داری از سفره ای چیزی عکس می گیری، می خوای بذاری با خودت فکر می کنی که چه دلیلی داره عکس غذایی که من خوردم رو بقیه بخوان ببینن».

«خطر سوء تفاهم» چنانچه از عنوان آن نیز مشخص است حاصل بدفهمی دنبال کنندگان از افشای فرد است که می تواند «خطر دور» را نیز به دنبال داشته باشد و کاربرد را مجبور به ارائه توضیحات اضافه، مکرر و بی نتیجه کند. مینا به این دو خطر اشاره می کند: «من یه بار یه پست گذاشتم راجع به مرگ و بعد یکی نوشت که این چیه؟ با این چیزها همه رو افسرده می کنی. کل روز با طرف بحث می کردم که مرگ هم جزئی از زندگیه».

«خطر قضاوت شدن» که تا حدودی به خطر انگ پترونیو (۲۰۰۲) نزدیک است، مربوط به افشاهایی است که زمینه ساز نسبت دادن صفات، ویژگی ها یا اعمال ناخوشایند به فرد می شوند، تا آنجا که می تواند تهدیدکننده آبروی کاربر باشد. فاطمه در این مورد می گوید:

«چون تو فامیلا یه مقداری فضولی هست، ترجیحاً اد نمی کنم اونم نه به خاطر پستیایی که من می دارم بیشتر به خاطر کامنتایی که زیرش گذاشته می شه. وای فلان پسر فلان حرف رو زده حالا اون پسر هم آزمایشگاهی منه و من باهاش روزی ده ساعت توی یه آزمایشگاهم. ولی اون آدم با دید دو دهه قبل یه جور دیگه برداشت می کنه».

«خطر رابطه» چنانچه از عنوان این کد نیز مشخص است، تهدیدکننده رابطه کاربر با نزدیکانش است.

«خیلی کم پست می دارم، چون همون اطرافیان که من رو فالو می کنن با کوچک ترین عکسی که می دارم میان سریع واکنش نشون میدن. خیلی حساسن رو من. بیشتر می گن مواظبتیم بعد خب چون حق دارن به گردنم اصلاً دوس ندارم جلوشون بایستم یا جوابی بدم» (آنیس).

«خطر نقش» مشخصاً گویای تهدیدی برای جایگاه شغلی و تحصیلی اطلاع رسانی در این



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 به جای ضوابط در خصوص همکاران و دوستان خود موجب ایجاد خطر نقش برای آن‌ها نیز شده باشند.

دوس ندارم همکارام پیجم رو ببین، چون چندتا پست دارم که خیلی از اوضاع شرکت گلایه کردم واسه همین ترجیح میدم نبین، 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 نتیجه آن فرد افشا در هر زمینه‌ای را تهدیدکننده امنیت خود به دلیل عدم توانایی کنترل اطلاعات شخصی و امکان سوءاستفاده اشخاص و یا مالکان اینستاگرام از آن‌ها می‌داند. زهرا تنها اطلاع‌رسانی است که به دلیل 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 همه چی تو حافظشون می‌مونه».

### ۳. راهبردهای کاربران

لیت (۲۰۱۳) راهبردهای رفتاری یا فردگرایانه در حفظ حریم خصوصی را در دو دسته راهبردهای اجتماعی و فناورانه 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 عاشقانه 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 میان فردی کاربران می شود. مهسا این گونه به این راهبرد اشاره می کند: «مسائل خیلی شخصی و خانوادگی نمی دارم کلاً. یا اینکه بخوام بقیه رو در جریان زندگی شخصیم بذارم، این جور عکس نمی دارم».

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 نمی کند. مینا می گوید: «صفحه بعضی از دخترا خیلی خزه، مثلاً تو بیوگرافی شون می نویسن خوشبختی یعنی داشتن من. به نظرم دختر باید صفحه اش خیلی متین باشه».

تعدادی از کاربران در صفحات خود هیچ گونه تصویری از خود یا نزدیکانشان را منتشر نکرده اند، چرا که انتشار چنین تصاویری را فاقد هرگونه مزایا برای خود دانسته اند. فهیمه که خود از این راهبرد استفاده کرده در این رابطه می گوید: «عکسام رو که دیدی چه جوریه! عکس صورت و اینا نمی دارم. عکس خودم رو از زاویه های مختلف بگیرم و بذارم خوشم نیواد. بقیه بیان لایک کنن یا کامنت بذارن اینجوری خوشم نیواد» (فهیمه).

«مطابقت با عرف و باورهای عامه» به این معنا که کاربر از انتشار تصاویر یا بیان مطالب مناقشه برانگیز خصوصاً خارج از جریان اصلی در جامعه خودداری می کند. پریسا می گوید: «مثلاً اینکه بخوام در مورد قضیه سیاسی یا مذهبی بحث کنم، نه اصلاً! مثلاً من حتی از علاقه ام به حیوانات چیزی نمی گم صرفاً به عکس می دارم».

کاربران با «رعایت مرزهای پوشش» که البته در هر مصاحبه شونده به صورت متفاوت تعریف شده است، تلاش می کنند تا بتوانند مزایای حاصل از افشا را برای خود تقویت کنند. یکی از اطلاع رسانیان می گوید: «عکسای من عکسایی نیست که احساس کنم اشکالی داشته باشه، نهایت عکسی که از من مشخصه، گردیه صورتم» (فاطمه ۲).

کد «بیان غیر مستقیم افشا» به راهبردهایی اشاره می کند که کاربر با استفاده از اشعار، جملات قصار و نمادها دست به افشا می زند. مینا به این راهبرد اشاره کرده و می گوید: «اگه ناراحت باشم، میرم عکس پاییز می دارم».

«اضافه کردن توضیحات» بدین معناست که کاربر خطرهای حاصل از یک افشا را با افزودن توضیحاتی کاهش می دهد. مریم در این باره می گوید: «شده مثلاً سخنی گذاشتم از نویسنده ای 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 می داند با واکنش

منفی دیگران مواجه می‌شود و در عین حال جزئی از شرایط زندگی یا روحی فرد است، به صورت 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 بگذروم، عکس می‌ذارم بعد یه سری هستن که هرازگاهی میان میگن خوش می‌گذره؟ یه کم درس بخون. بعد حس می‌کنم این عکس رو آگه بذارم اونا میان دوباره این کامنتا رو می‌ذارن. برا همین نمی‌ذارم یا مثلاً صبر می‌کنم که یه کم از عکس قبلم بگذره بعدش می‌ذارم تا فکر نکنن من هر روز در حال خوش گذرونی ام».

#### ۲-۳. راهبردهای فناوریانه

کدها در این راهبرد طبیعتاً با امکانات ارائه شده برای حفظ حریم خصوصی در اینستاگرام مرتبط اند و برای اطلاع‌رسانان در این مقاله به ترتیب و برحسب بیشترین فراوانی شامل «انتخاب هدف (خصوصی بودن صفحه<sup>۱</sup>)»، «بلاک کردن<sup>۲</sup>»، «رد درخواست»، «حذف پست»، «حذف کامنت»، «ارسال پیام خصوصی<sup>۳</sup>»، «آن تگ کردن»، «عمومی نکردن کامنت‌ها» و «استفاده همزمان از چند اکانت» می‌شوند. نکته قابل ذکر، تفاوت قابل ملاحظه کاربران دختر در میزان آشنایی و استفاده از راهبردهای فناوریانه است. درحالی که برخی کاربران تقریباً با همه قابلیت‌های فناوریانه اینستاگرام آشنای اند و تجربه 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 جور می‌شه یه کامنت رو حذف کرد؟» (فریده).

بچه‌ها یه صفحه 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» (فهمیه).

#### ۴. الگوهای استفاده از راهبردهای سواد حریم خصوصی

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



1. private
2. block
3. direct message

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

#### ۴-۱. راهبردهای فناوریانه 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 فناوریانه 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 خطرهای 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 جمع‌آوری شده 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 خطرهای 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 این باره می‌گوید: «اینستا خوبی هم داره، مثلاً دوستان میان خودشون رو تخلیه می‌کنن، غیر مستقیم می‌نویسن، اینا اشکالی نداره، ولی من از همه اینا صرف نظر کردم».

#### ۴-۲. راهبردهای فناوریانه بالا، راهبردهای اجتماعی پایین

این الگوی به‌کارگیری راهبردها شامل کاربرانی است که معمولاً در استفاده 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 به دلیل بی‌توجهی به راهبردهای اجتماعی خطرهای بیشتری را نیز تجربه کرده‌اند که البته به دلیل تسلط بر راهبردهای فناوریانه خطرهای به‌صورت کوتاه‌مدت بوده و کاربر معمولاً توانسته خطرهای کنترل کند. این الگو دربرگیرنده 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 فناوریانه و اجتماعی بالا

این دسته از کاربران اگرچه در استفاده از راهبردهای فناوریانه تسلط کافی دارند، به دلیل نگرانی زیاد از خطرهای و در نتیجه استفاده فراوان از راهبردهای اجتماعی و محدودیت‌های ذهنی باز هم ممکن است در مواردی به شدت تضاد حریم خصوصی را احساس کرده و خصوصاً برای دستیابی به مزایای روانشناختی از رفع آن به ایده‌آل‌ترین شکل مورد نظر خود بازمانده باشند. با این حال، در مقایسه با الگوی نخست به دلیل تسلط و آگاهی نسبتاً بیشتر از امکانات فناوریانه اینستاگرام، شناخت دقیق مرزهای حریم خصوصی خود و مزایایی که به دنبال آن هستند، رضایت بیشتری در استفاده 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 محتوای 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 پیام خودم رو بشناسونم بهشون. برا همین راجع به خصوصیاتم نمی‌ذارم. فقط در حد گردش و ایناست».

### ۴-۴. راهبردهای فناوریانه و اجتماعی پایین

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



شامل کاربرانی است که برای دستیابی به مزایا به ویژه مزایای روانشناختی تا حدود زیادی از خطرهای بالقوه چشم‌پوشی کرده‌اند. کاربران در این الگو تنها کاربرانی‌اند که با خطر پشیمانی مواجه شده‌اند و این بدین معناست که بی‌توجهی به راهبردهای اجتماعی و فناوریانه برای دستیابی 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 سریع پست می‌دارم، ولی از اون‌ور خیلی پیش اومده که پست گذاشتم و بعد یه مدت پاکش کردم، مثلاً پیش اومده تو یه شب ده تا پست هم پاک کردم چون دیگه بهشون حس خوبی نداشتم». با این حال، این کاربران کمتر در الگوی استفاده خود از اینستاگرام تغییری ایجاد می‌کنند و خطرهای پیش‌آمده را اتفاقاتی محدود قلمداد می‌کنند که تا حدودی بیانگر دغدغه پایین‌تر حریم خصوصی در این کاربران بوده است. چهار نفر از اطلاع‌رسانان در این الگو قرار گرفته‌اند.

#### ۵-۴. راهبردهای فناوریانه و اجتماعی متوازن

این گروه از اطلاع‌رسانان که بر اساس اظهارات خود بیشترین میزان رضایت در استفاده خود از اینستاگرام را دارند، فقط شامل دو نفر از مصاحبه‌شوندگان می‌شود. برای این گروه استفاده از اینستاگرام جزء جدایی‌ناپذیر از زندگی روزمره است و معمولاً این نرم‌افزار را منشأ بسیاری از پیامدهای مثبت برای خود می‌دانند. فریبا در مورد اینستاگرام می‌گوید:

«از برنامه‌های اجتماعی کلاً خوشم نمیاد، ولی اینستاگرام رو به خاطر فلسفه‌اش که می‌تونیه چیزای روزمره زندگی رو با دوستان به اشتراک بذاری، دوست دارم. اینکه بایه عده‌ای در ارتباطی، کامنتایی از دوستان می‌گیری، عکس الان دوستایی رو که چند ساله ندیدی‌شون می‌بینی، اینکه چیزی تودلت باشه میگی، اینا جذابه».

این دسته از کاربران که با اطمینان بیشتری از این نرم‌افزار استفاده می‌کنند، افشاهای بالاتری دارند و در عین حال با خطرهای پشیمانی‌های کمتری در افشای خود مواجه‌اند و از این‌رو موفق‌ترین الگوی دستیابی به حد بهینه حریم خصوصی هستند. این دسته از کاربران هر دو گونه مزایای اجتماعی و روانشناختی را تجربه کرده‌اند و بر حسب تعداد کدها به میزان تقریباً برابر به راهبردهای اجتماعی و فناوریانه در حفظ حریم خصوصی خود اشاره کرده‌اند. مشخصه دیگر این گروه از کاربران حرکت آرام و پیوسته ایشان در دستیابی به حد بهینه حریم خصوصی با تسلط بر راهبردهای فناوریانه است. به این معنا نگرانی‌ها و استفاده کاربران از راهبردهای اجتماعی با افزایش مهارت‌های فناوریانه ایشان کاهش یافته تا در شرایط کنونی به حد متوازن و رضایت‌بخش از نظر خود دست یافته‌اند. مینا از کاربرانی است که به این مسئله اشاره کرده است:



«اوایلش که اوادم اینستا نمی دونستم تگ کردن چیه بعد یه پسره بود رو عکسش منم تگ می کرد. داداش منم یه کم حساسه اومد به من گفت چرا آن تگش نمی کنی، بعد بهم گفت چه جوریه رفتم آن تگش کردم. ولی الان هر سری آپدیت میشه و یه قابلیت بهش اضافه میشه سریع میرم چند و چونش رو در میارم دیگه».

## نتیجه

دستیابی به حد بهینه حریم خصوصی برای کاربران شبکه‌های اجتماعی مستلزم برقراری ارتباطات مؤثر و مسئولانه (بارچ و دیلن، ۲۰۱۶) از سوی آنهاست؛ ارتباطی که با به‌کارگیری راهبردهای مبتنی بر سواد حریم خصوصی بتواند ضمن کنترل خطرها، مزایای حاصل از خود افشاگری را نیز برای کاربر در پی داشته باشد و آنها را در رفع این تناقض یاری کند. ایجاد درکی از وضعیت و میزان موفقیت کاربران دختر اینستاگرام در دستیابی به این حد بهینه هدف اصلی این مقاله بوده است. نتایج حاصل از مصاحبه با ۲۰ اطلاع‌رسان در نهایت با شناسایی دو تم کلی مزایا و خطرهای «روانشناختی» و «اجتماعی» چنین تناقضی را برای کاربران دختر تأیید کرد. این تضاد به‌ویژه در دستیابی به مزایای روانشناختی بیشتر بوده است. به این معنا کاربران در اغلب موارد در دستیابی به مزایای روانشناختی، مانند «بیان (تسکین پریشانی) و بهبود احساسات فردی»، «تخلیه هیجانات فردی» و «شفاف‌سازی خود» خطرهای بیشتری را احساس کرده‌اند. صرف نظر کردن از همین دسته از مزایا نیز در اغلب موارد با ابراز نارضایتی بیشتر اطلاع‌رسانان به وضعیت کاربری خود همراه بوده است. نکته دیگر آنکه وجود این تناقض برای همه کاربران یکسان نبوده است؛ برای برخی کاربران به‌حدی بوده است که آنها را به صرف نظر کردن از خودافشاگری و مزایای حاصل از آن واداشته است و برخی دیگر چنین تضادی را کم‌تر احساس کرده و با بی-توجهی به خطرها، کسب مزایای بیشتر را در اولویت قرار داده‌اند.

همچنین یافته‌ها در مجموع گویای استفاده بیشتر کاربران از «راهبردهای اجتماعی» و محدودیت‌های ذهنی در مقایسه با «راهبردهای فناورانه» بوده است. این مسئله بیانگر تسلط کافی نداشتن برخی کاربران بر راهبردهای فناورانه است که خود گویای نیاز به آموزش‌های بیشتر در این راستاست. در طول مصاحبه‌ها موارد فراوانی از ناآشنایی کاربران با راهبردهای فناورانه و ابهام در نحوه به‌کارگیری آنها ملاحظه شد. بی‌توجهی به راهبردهای اجتماعی نیز در برخی موارد به‌اندازه بی‌اطلاعی از راهبردهای فناورانه موجب مواجهه کاربران دختر با تهدیدات حریم خصوصی شده است. بر اساس یافته‌ها استفاده متوازن و تکمیلی از راهبردهای فناورانه و اجتماعی به رضایت



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

اگرچه حد بهینه حریم خصوصی امری نسبی است و برای هر کاربر کاملاً متفاوت است، از میان الگوهای معرفی شده 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 بهینه حریم خصوصی هستند. علاوه بر این، نتایج نیز گویای تجربه 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 استفاده صحیح از راهبردها برای رفع تضاد حریم خصوصی خود بوده است، و در نتیجه در بدترین شرایط برخی مجبور به صرف نظر کردن از مزایا و برخی دیگر در اثر بی‌توجهی به خطرها از حد بهینه 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 فناوریانه‌ای دارد که مصاحبه‌شوندگان حتی کسانی که در رفع تناقض حریم خصوصی خود نسبتاً موفق بوده‌اند، نیز بدان‌ها اشاره کرده‌اند، اما به دلیل 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 این رو اجرای پژوهش‌های کمتی مکمل در این زمینه به لحاظ 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: 10.1191/1478088706qp0630a
- 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. Zigers, *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 Presented 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 Presented at the *Sixth International AAAI Conference on Weblogs and Social Media*, June 4-8, 2012, Dublin, Ireland. Retrieved 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.