فصلنامه علمی جامعه‌شناسی فرهنگ و هنر
دوره سوم – شماره سوم – پاییز ۱۴۰۰
صص: ۱۲۳-۹۹

نقش هویت فناوری اطلاعات در رفتار خودافشایی کاربران شبکه اجتماعی اینستاگرام: پیمایشی پیرامون دانشجویان دانشگاه تهران

بابک سهرابی [1*]
حمید رضا یزدانی [2]
امیر مانیان [3]
حسین مسافر [4]

چکیده

ازآنجاکه افراد امروزه بیش از هر زمان دیگری از سایت‌های شبکه‌های اجتماعی استفاده می‌کنند، افشای اطلاعات شخصی تبدیل به مسئله‌ای با اهمیت فزاینده در پژوهش و عمل شده است. به‌رغم وجود دغدغه‌های حریم خصوصی، افراد در رفتاری متناقض به افشای اطلاعات شخصی خود می‌پردازند. ادبیات رشته سیستم‌های اطلاعاتی توضیحی نسبی برای این تناقض ارائه کرده است. بااین‌حال، مطالعات اخیر توجه به رفتارهای ناخودآگاه مرتبط با حریم خصوصی را توصیه کرده است. تحقیقات نوظهور در زمینه هویت فناوری اطلاعات[5] پنجره جدیدی برای توضیح بهتر رفتارهای مربوط به استفاده از فناوری باز کرده است. هویت فناوری اطلاعات در واقع، هویت فردیِ نشأت‌گرفته از فناوری اطلاعات است و به معنای «میزانی است که یک فرد در حسش نسبت به خود و در تعریفش از خود فناوری اطلاعات را جدانشدنی می‌بیند». هدف این پژوهش بررسی نقش هویت فناوری اطلاعات در رفتار خودافشایی کاربران شبکه‌های اجتماعی است. بدین‌منظور، در مرداد ماه ۱۴۰۰ پیمایشی با مشارکت ۴۶۷ دانشجوی دانشگاه تهران که کاربر شبکه اجتماعی اینستاگرام نیز بودند، انجام شد. نتایج این تحقیق نشان می‌دهد که هویت فناوری اطلاعات ارتباطی مثبت با خودافشایی در شبکه‌های اجتماعی دارد و همچنین هویت فناوری اطلاعات به طور غیرمستقیم و از طریق سازه‌های اعتماد، مزایا و مخاطرات ادراک‌شده با رفتار خودافشایی اطلاعات مرتبط است. یافته‌های این پژوهش به توضیح بهتر پدیده تناقض حریم خصوصی کمک می‌کند و نقش هویت فناوری اطلاعات را برای پیش‌بینی رفتارهای مربوط به حریم خصوصی در نظر می‌گیرد.

کلید واژگان: هویت فناوری اطلاعات، دغدغه‌های حریم خصوصی، رفتار خودافشایی، تناقض حریم خصوصی.

دریافت مقاله: ۱۴۰۰/۰۲/۲۸ – 2021/05/18

پذیرش مقاله: ۱۴۰۰/۰۵/۰۴ – 2021/07/26

---

۱ . استاد گروه مدیریت فناوری اطلاعات، دانشکده مدیریت دانشگاه تهران، تهران، ایران. (نویسنده مسئول)
(bsohrabi@ut.ac.ir)

۲-استادیار گروه مدیریت بازرگانی و کسب وکار، دانشکده مدیریت و حسابداری، پردیس فارابی دانشگاه تهران، قم، ایران.

[3]- استاد گروه مدیریت فناوری اطلاعات، دانشکده مدیریت دانشگاه تهران، تهران، ایران.

[4]-دانشجوی دکتری، گروه مدیریت فناوری اطلاعات ، دانشکده مدیریت دانشگاه تهران، تهران، ایران.

[5]-Information Technology Identity (ITID)

مقدمه و طرح مسئله

فناوری اطلاعات تقریباً در همه جنبه‌های زندگی ما نفوذ کرده و «به‌طور فزاینده‌ای با روال‌های شخصی و اجتماعی ما آمیخته‌شده است» (کارتر و گروور[1]، ۲۰۱۵). ازجمله پرکاربردترین فناوری‌های اطلاعات، سایت‌های شبکه‌های اجتماعی[2] هستند، به‌طوری که تا سال ۲۰۲۰، بیش از ۳٫۶ میلیارد نفر در سراسر جهان از شبکه‌های اجتماعی استفاده می‌کردند (استاتیستا[3]،۲۰۲۰). از آنجاکه افراد برای برقراری روابط و حفظ ارتباط با خانواده و دوستان، بیشتر با رسانه‌های اجتماعی مشغول‌اند، با افشای اطلاعات قابل شناسایی شخصی و سایر اطلاعات خصوصی با دوستان خود و حتی غریبه‌ها مانند علایق، احساسات عاطفی، برنامه‌های تعطیلات و روابط خود، ردپایی دیجیتال از افکار، شناخت‌ها و رفتارهای خود به جا می‌گذارند. این مساله به‌نوبه‌خود می‌تواند سطح نگرانی‌های مربوط به حریم خصوصی را افزایش دهد؛ یعنی نگرانی در مورد نحوه جمع‌آوری اطلاعات، آن‌چه با آن انجام می‌شود و آسیب‌هایی که ممکن است ایجاد کند. (اسمیت و همکاران[4]، ۱۹۹۶). این نگرانی برخاسته از دلایل متعددی است:

نخست این‌که با ظهور فناوری‌های پیشرفته اطلاعاتی و ارتباطاتی، می‌توان داده‌ها را بسیار سریع تر از هر زمان دیگری، حتی در حجم بیشتر، جمع‌آوری، ترکیب و تجزیه‌وتحلیل کرد. با استفاده از چنین فناوری‌هایی، چندین ذی‌نفع مانند کسب‌وکارها، بنگاه‌های تبلیغات، و خود ارائه‌دهندگان زیرساخت‌های شبکه اجتماعی، عمداً اطلاعات به اشتراک گذاشته شده در شبکه‌های اجتماعی را جمع‌آوری، ذخیره و پردازش می‌کنند، که این امر می‌تواند نگرانی‌های مختلفی ایجاد کند (العاشور و همکاران[5]، ۲۰۱۷). نتایج یک نظرسنجی توسط مادن و همکاران در سال ۲۰۰۷ نشان می‌دهد که ۸۵ درصد از بزرگسالان معتقدند «کنترل دسترسی به اطلاعات شخصی آن‌ها بسیار مهم است». **دوم،** افزایش روزافزون نقض حریم خصوصی و امنیت در شبکه‌های اجتماعی، حریم خصوصی اطلاعات را برای صاحبان شبکه‌ای اجتماعی و همچنین برای کاربران به یک مسأله مهم تبدیل می‌کند. در رسوایی تاریخی کمبریج آنالیتیکا[6]، که یکی از بزرگ‌ترین مصادیق نقض حریم خصوصی در تاریخ شبکه‌های اجتماعی است، از نمایه[7] بیش از ۷۰ میلیون کاربر فیس‌بوک در تبلیغات سیاسی انتخابات ریاست جمهوری ۲۰۱۶ ایالات متحده سوءاستفاده شد و میزان نگرانی‌کاربران در خصوص حریم خصوصی را تشدید کرد (روزنبرگ و همکاران[8]، ۲۰۱۸). سرانجام، اطلاعات شخصی که به صورت آنلاین افشا

[1] Carter & Grover
[2] Social Networking Sites (SNS)
[3] Statista
[4] Smith et al.
[5] Alashoor et al.
[6] Cambridge Analytica
[7] Profile
[8] Rosenberg et al

می‌شود، می‌تواند توسط مجرمان آنلاین، کلاه‌برداران و قلدرها یا حتی دوستان مورد سوء استفاده قرار گیرد (هوگبن[1]، ۲۰۰۷).

علیرغم تهدیدهای موجود و نگرانی‌های مربوط به حریم خصوصی، افراد به‌طور متناقضی به افشای حجم عظیمی از اطلاعات شخصی خود ادامه می‌دهند که از این پدیده با عنوان «تناقض حریم خصوصی»[2] یاد می‌شود (نوربرگ و همکاران[3]، ۲۰۰۷). پژوهش‌های پیشین مربوط به حریم خصوصی اطلاعات عمدتاً رفتار کاربران را نتیجه یک فرایند تصمیم‌گیری منطقی می‌داند که برخاسته از نگرانی آن‌ها برای حفاظت از اطلاعات شخصی‌شان است (بلانجر و کراسلر[4]، ۲۰۱۱ ؛ لی[5]، ۲۰۱۱ ؛ اسمیت و همکاران، ۲۰۱۱). یکی دیگر از جریان‌های پژوهشی که این پدیده را توضیح می‌دهد، «محاسبه حریم خصوصی» است که مورد پذیرش گسترده پژوهشگران این حوزه است و طرفداران زیادی دارد (به عنوان مثال ، مالهوترا و همکاران[6] (۲۰۰۴) و کراسنوا و همکاران[7] (۲۰۱۰)) ، که فرض می‌کند رفتارهای مربوط به حریم خصوصی کاربران (مانند افشای اطلاعات شخصی) نتیجه یک محاسبه عقلانی ذهنی از مخاطرات ادراک‌شده حریم خصوصی در کنار مزایای ادراک‌شده مربوط به تصمیم افشای اطلاعات باشد.

اگرچه ادبیات نظری این حوزه در توضیح رفتارهای مرتبط با حریم خصوصی مفید بوده است، اما مطالعات اخیر فرض غالب تقریباً همه‌ی تحقیقات سیستم‌های اطلاعاتی[8] مربوط به حریم خصوصی را زیر سوال برده است: «پاسخ به محرک‌های خارجی منجر به تجزیه و تحلیلی فکر شده می‌شود که نگرش‌ها و رفتارهایی کاملاً آگاهانه در خصوص حریم خصوصی در پی خواهد داشت.» (دینو و همکاران[9]، ۲۰۱۵، ص ۱). آن‌ها معتقدند که وقتی صحبت از رفتارهای مربوط به حریم خصوصی به میان می‌آید، بسیاری از کاربران خودجوش و بی‌اندیشه عمل می‌کنند و تأمل کمی در این رابطه انجام می‌دهند. این ادعا با یافته‌های مطالعات برجسته جامعه‌شناسی و روانشناسی در مورد ارتباط بین هویت و رفتار مطابقت دارد که شواهدی قوی بر تأثیر هویت بر رفتار ارائه می‌دهند (به عنوان مثال، گرانبرگ و هولمبرگ[10] (۱۹۹۰) و استتس و بیگا[11] (۲۰۰۳)). به طور خاص، مطالعات نشان می‌دهد که در رفتارهای تکرارشونده (مانند رفتار خود افشایی کاربران در شبکه‌های اجتماعی)، هویت نقش اصلی را در پیش‌بینی نتایج رفتاری ایفا می‌کند (استتس و بیگا، ۲۰۰۳).

---

[1] Hogben
[2] Privacy Paradox
[3] Norberg et al.
[4] Bélanger and Crossler
[5] Li
[6] Malhotra et al.
[7] Krasnova et al.
[8] Information systems
[9] Dinev et al.
[10] Granberg and Holmberg
[11] Stets and Biga

هویت فناوری اطلاعات[1] به عنوان یک جریان تحقیقاتی در حال ظهور در رشته سیستم‌های اطلاعاتی ، یک دیدگاه نظری برای بازتاب بهتر مرزهای مبهم فناوری اطلاعات با تقریباً همه جنبه‌های زندگی روزمره ما فراهم می‌کند. هویت فناوری اطلاعات، در واقع هویت [فردی نشأت‌گرفته از] فناوری اطلاعات است و به معنای «میزانی است که یک فرد در حسش نسبت به خود [و در تعریفش از خود] فناوری اطلاعات را جدانشدنی می‌بیند» (کارتر و گروور، ۲۰۱۵). از نظر کارتر و گروور (۲۰۱۵) ، از آنجا که مردم بیشتر از قبل از فناوری اطلاعات استفاده می‌کنند، این فناوری‌ها به بخشی جدایی‌ناپذیر از آن‌ها تبدیل می‌شود که انتخاب‌های رفتاری آن‌ها را هدایت می‌کند و کسانی که خود را بیشتر در نسبت با فناوری اطلاعات تعریف می‌کنند، احتمالاً بیشتر مشغول استفاده از فناوری اطلاعات خواهند شد. همان‌طور که از ابتدا توسط کارتر و گروور (۲۰۱۵) ادعا شد، تجزیه و تحلیل تحقیقات مهم قبلی در زمینه هویت فناوری اطلاعات توسط مسافر و سرآبادانی (۲۰۲۱) نشان می‌دهد که هویت فناوری اطلاعات در ارائه پایه نظری برای تحقیقات رفتاری در زمینه‌های مختلف فناوری اطلاعات مفید بوده است. با این حال، این سازه هنوز در تحقیقات مربوط به حریم خصوصی و رفتار خود افشایی مورد توجه قرار نگرفته است. بنابراین، این پژوهش در پی پاسخ دادن به این سوال است:

- نقش مستقیم و غیرمستقیم هویت فناوری اطلاعات در رفتار خودافشایی کاربران شبکه‌های اجتماعی چیست؟

پژوهش حاضر برای پر کردن این شکاف نظری، به بررسی نقش هویت فناوری اطلاعات به عنوان سازوکاری جدید در کنار حساب حریم خصوصی می‌پردازد. این مطالعه با تکیه بر مدل کلان بهبودیافته «پیش‌آیند و پیامدهای دغدغه‌های حریم خصوصی[2]» (دینو و همکاران[3]، ۲۰۱۵) ، هویت فناوری اطلاعات را به عنوان یک لنز نظری برای توضیح پدیده تناقض حریم خصوصی و رفتارهای مربوط به حریم خصوصی مانند خودافشایی اطلاعات شخصی در شبکه‌های اجتماعی استفاده می‌کند.

در ادامه این مقاله، ابتدا خلاصه‌ای از پژوهش‌های مربوط به دغدغه‌های حریم خصوصی اطلاعات، مدل پیش‌آیند و پیامدهای دغدغه‌های حریم خصوصی، حساب حریم خصوصی، رفتار خودافشایی و هویت فناوری اطلاعات مورد بحث و بررسی قرار می‌گیرد تا براساس شکاف‌های نظری موجود، مدل نظری این تحقیق مطرح شود. در ادامه، روش تحقیق مورد استفاده در آزمودن فرضیه‌های تحقیق و نتایج تجربی این پژوهش آمده است. در پایان، نتایج کسب‌شده تحلیل شده و دلالت‌های نظری و عملی آن در کنار محدودیت‌های تحقیق بیان می‌شود.

[1] IT identity
[2] Antecedents, Privacy Concerns, Consequences (APCO)
[3] Dinev et al.

چارچوب نظری

دغدغه‌های حریم خصوصی اطلاعات

دغدغه‌های حریم خصوصی اطلاعات به معنای نگرانی افراد در مورد نحوه گردآوری اطلاعات، کاری که با آن انجام می‌شود و آسیب‌هایی است که ممکن است ایجاد کند. (اسمیت و همکاران، ۱۹۹۶). به عبارت دیگر، دغدغه‌های حریم خصوصی اطلاعات بیانگر ادارک افراد از پیامدهایی است که ممکن است در نتیجه انتشار اطلاعاتشان در اینترنت به‌وجود آید (دینو و هارت، ۲۰۰۶). در این پژوهش منظور از دغدغه‌های حریم خصوصی میزان نگرانی افراد در خصوص بروز رفتارهای فرصت‌طلبانه در برابر اطلاعاتی است که توسط آن‌ها در شبکه‌های اجتماعی منتشر شده است. دغدغه‌های حریم خصوصی اطلاعات نیز در بین بسیاری از محققان رشته سیستم‌های اطلاعاتی بسیار مهم تلقی شده است (بلانجر و کراسلر، ۲۰۱۱ ؛ لی، ۲۰۱۱ ؛ پاولو، ۲۰۱۱؛ اسمیت و همکاران، ۲۰۱۱)، که تاجایی که محققان این پژوهش اطلاع دارند، در بین آن‌ها هیچ‌کدام سازه هویت فناوری اطلاعات را در بروز دغدغه‌های حریم خصوصی اطلاعات در نظر نگرفته‌اند.

در برخی از پژوهش‌های مربوط به دغدغه‌های حریم خصوصی مشاهده شده است که افراد علی‌رغم تهدیدهای موجود و نگرانی‌های مربوط به حریم خصوصی، همچنان به طور متناقضی به افشای حجم عظیمی از اطلاعات شخصی خود ادامه. این پدیده می‌دهندکه از این پدیده «تناقض حریم خصوصی» نامیده می‌شود. (نوربرگ و همکاران ۲۰۰۷). در پدیده تناقض حریم خصوصی، افراد دغدغه و نگرانی زیادی درخصوص حریم خصوصی خود دارند ولی رفتارشان متفاوت با این دغدغه‌ها است (پاولو[1]، ۲۰۱۱). همچنین تحقیقات قابل توجهی برای توضیح پدیده تناقض حریم خصوصی انجام شده است (بارت و دیونگ[2]، ۲۰۱۷ ؛ گربر، گربر و ولکامر[3]، ۲۰۱۸؛ کوکولاکیس[4]، ۲۰۱۷)، اما تا آنجا که محققان اطلاع دارند هیچ کدام به بررسی نقش هویت فناوری اطلاعات در توضیح تناقض حریم خصوصی نپرداخته‌اند.

مدل بهبودیافته پیش‌آیند و پیامدهای دغدغه‌های حریم خصوصی

اسمیت و همکاران (۲۰۱۱) به منظور مطالعه دغدغه‌های مربوط به حریم خصوصی اطلاعات، به محققان توصیه می‌کنند که یک مدل کلان جامع با ترتیب زیر را مد نظر قرار دهند: پیش‌آیندها، دغدغه‌های حریم خصوصی و پیامدها که نهایتاً تحت عنوان (APCO) از آن یاد می‌کنند. این مدل کلان، محاسبه حریم خصوصی، دغدغه‌های حریم خصوصی و سایر سازه‌ها را به نحوی به‌کار می‌گیرد که بتوان رفتارهای مرتبط با حریم خصوصی را توضیح داد. مدل اولیه APCO با جمع‌بندی و تجمیع

[1] Pavlou
[2] Barth & de Jong
[3] Gerber, Gerber, & Volkamer
[4] Kokolakis

یافته‌های پژوهش‌های مختلف، حریم خصوصی اطلاعات، محاسبه حریم خصوصی و دغدغه‌های حریم خصوصی را به عنوان عوامل مؤثر در تصمیم‌گیری‌های خودافشایی در نظر می‌گیرد. مدل اولیه APCO، رفتارهای حریم خصوصی کاربران را نتیجه یک فرآیند تصمیم‌گیری منطقی (تفکر پرتلاش) می‌دانست و تأثیر فرایندهای ابتکاری پیش‌فرض (فرایندهای شناختی کم‌تلاش و سوگیری‌ها) را نادیده می‌گرفت (دینو و همکاران، ۲۰۱۵). این پژوهش بر اساس پیشنهادهایی که در APCO بهبودیافته توسط دینو و همکاران (۲۰۱۵) ارائه شده است، هویت فناوری اطلاعات را به‌عنوان پیش‌آیندی برای رفتارهای مرتبط با حریم خصوصی در نظر می‌گیرد.

خودافشایی در شبکه‌های اجتماعی

خودافشایی در معنای سنتی خود، «هر پیامی است که یک شخص درباره خود به دیگری مخابره می‌کند» (ویلس و گروتز[1]، ۱۹۷۶). کاربران شبکه‌های اجتماعی علاوه بر اطلاعات شخصی، اطلاعات خصوصی دیگری را هم افشا می‌کنند؛ مانند سرگرمی‌ها، سلیقه خود در گوش دادن به موسیقی، دیدن فیلم و مطالعه کتاب، وضعیت تاهل و حتی تمایلات جنسی خود (گروس و آکویستی[2]، ۲۰۰۵). با درنظر گرفتن میزان اطلاعاتی که یک فرد درباره خودش در یک پلتفرم در معرض دید قرار می‌دهد، خودافشایی در شبکه‌های اجتماعی زمانی اتفاق می‌افتد که یک کاربر جزئیات شخصی، اخبار، احوالات، عقاید، نظرات و باورهای خود را مستقیماً بر روی صفحه‌اش یا در فرآیند ارتباطات عمومی با دیگران به اشتراک می‌گذارد (کراسنوا، ولتری و گانتر، ۲۰۱۲).

ماهیت ارتباطات شبکه‌های اجتماعی به نحوی مشوق و مستلزم رفتارهای خودافشایی است(العاشور، هان و ژوزف[3]، ۲۰۱۷). شبکه‌های اجتماعی فرصت‌های ارزشمندی را برای تعاملات اجتماعی به وجود می‌آورند و کاربران خود را قادر می‌سازند تا تعامل کنند، ارتباط بگیرند و اطلاعاتی را با دیگران به اشتراک بگذارند (آکویستی و گراس[4]، ۲۰۰۶). بدون افشای اطلاعات، کاربران به ندرت منافعی در استفاده از شبکه‌های اجتماعی می‌بینند. در نتیجه، کاربران تمایل پیدا می‌کنند که تا با اشتراک اطلاعات شخصی، در شبکه‌های اجتماعی مشارکت [یا مشغولیت] داشته باشند (العاشور و همکاران، ۲۰۱۷).

برای توضیح تمایل افراد به اشتراک اطلاعات، تاکنون رویکردهای مختلفی اتخاذ شده است. برخی مطالعات به بررسی نقش عوامل جمعیت‌شناختی پرداخته‌اند (مانند فوگل و نهماد[5]، ۲۰۰۹). در این دسته از مطالعات به نقش جنسیت توجه ویژه‌ای شده است؛ به طوری که عمده پژوهش‌ها حاکی از آن است که احتمال خودافشایی کاربران مؤنث در شبکه‌های اجتماعی بیشتر از کاربران مذکر است

[1] Wheeless & Grotz
[2] Gross & Acquisti
[3] Alashoor, Han, & Joseph
[4] Acquisti & Gross
[5] Fogel & Nehmad

(برای مثال توفکچی[1]، ۲۰۰۸). دسته دیگر از پژوهش‌ها، تصمیم‌های خودافشایی را تابعی از باورهای فردی می‌دانند؛ مانند چیو، سو و وانگ[2] (۲۰۰۶) و سو و لین[3]، (۲۰۰۸). نهایتاً در دسته‌ای دیگر از پژوهش‌ها به نقش دغدغه‌های حریم خصوصی اطلاعات در تصمیمات خودافشایی پرداخته شده است (مانند بولگارچو، کاووس‌اغلو و بن‌باسات[4]،۲۰۱۰)؛ چرا که امروزه آگاهی کاربران شبکه‌های اجتماعی از مخاطرات احتمالی افشای اطلاعات بیشتر شده است (کراسنوا و همکاران، ۲۰۱۲).
پژوهش حاضر در بررسی رفتار خودافشایی اطلاعات، رویکرد آخر را اتخاذ می‌کند و خودافشایی اطلاعات را یک رفتار مرتبط با حوزه دغدغه‌های حریم خصوصی اطلاعات درنظر می‌گیرد.

نظریات هویت و پیدایش هویت فناوری اطلاعات

بسیار از پژوهش‌ها هویت را به عنوان پاسخی به سوال «من کیستم؟» در نسبت با یک دسته اجتماعی (یا یک شیئ) مفهوم‌سازی می‌کنند (مک‌کال[5]، ۲۰۰۳؛ ویگنولز و همکاران[6]، ۲۰۱۱). دسته‌های اجتماعی مانند گروه‌ها، نقش‌ها، ویژگی‌های شخصی یا ابزارهای مادی تنها زمانی بخشی از هویت می‌شوند که افراد از آن‌ها برای پاسخ به سؤال فوق استفاده کنند (ویگنولز و همکاران،۲۰۱۱). در طی زمان، این مفهوم‌سازی در روانشناسی اجتماعی مورد اقبال قرار گرفته و منجر به ایجاد دو منظر کلی در مورد ماهیت و تأثیر هویت شده است (اوونز[7]، ۲۰۰۶؛ استرایکر و برک[8]، ۲۰۰۰).

در سطح جمعی، تمرکز نظریه هویت اجتماعی (تاجفل و ترنر[9]، ۲۰۰۴) بر شکل‌گرفتن هویت براساس عضویت فرد در گروه‌های اجتماعی یا دسته‌ها است. در این منظر دسته‌بندی افراد از خودشان به عنوان اعضای گروه به آن‌ها انگیزه می‌دهد که شبیه اعضای درونِ گروه (در مقابل افراد خارج از گروه) باشند، مانند آن‌ها رفتار کنند و دنیا را از منظر افراد درون گروه ببینند (استتس و برک، ۲۰۰۰). در نتیجه، رویکردهای نظری در این سطح بر فرآیندهای گروه و روابط میان‌گروهی متمرکز می‌شوند (ویگنولز و همکاران ۲۰۱۱).

در سطح فردی، نظریه‌های هویت تعامل‌گرایی نمادین ساختاری[10] مانند نظریه هویت (استرایکر، ۱۹۸۰)، نظریه هویت نقش (مک‌کال و سیمونز[11]، ۱۹۷۸) و نظریه کنترل هویت (برک و استتس، ۲۰۰۹؛ برک و ریتزس[12]، ۱۹۹۱) مطرح می‌شوند. این نظریه‌ها توضیح می‌دهند که چگونه شبکه

[1] Tufekci
[2] Chiu, Hsu, & Wang
[3] Hsu & Lin
[4] Bulgurcu, Cavusoglu, & Benbasat
[5] McCall
[6] Vignoles et al.
[7] Owens
[8] Stryker & Burke
[9] Tajfel & Turner
[10] Structural symbolic interactionist identity theories
[11] McCall & Simmons
[12] Burke & Reitzes

نقش‌ها و روابطی که افراد در آن قرار دارند، بر هویت فردی یا هویت ناشی از نقش آن‌ها و متعاقبا بر تفکر و رفتار آن‌ها در نسبت با دیگران تأثیر می‌گذارد (برک و استتس، ۲۰۰۹؛ استرایکر و برک، ۲۰۰۰). هویت ناشی از نقش (برای مثال نقش کاری، نقش والدین) به انتظارات درونی افراد از معنای شایسته بودن در انجام برخی نقش‌ها برمی‌گردد (برک و استتس، ۲۰۰۹). هویت فردی شامل خصوصیات، ارزش‌ها و هنجارهای فرهنگی مشخصی است که افراد برای تعریف خود به عنوان هویت‌های متمایز از آن‌ها استفاده می‌کنند (برک و استتس، ۲۰۰۹) و در نهایت، نوعی از هویت که در عین اهمیت، کمتر مورد مطالعه قرار گرفته است، هویتی است که پیوند با اشیاء مادی تعریف می‌شود؛ مانند محیط طبیعی، مکان‌ها یا اموال شخصی (شامل فناوری اطلاعات) (ویگنولز و همکاران، ۲۰۱۱؛ کلایتون و اپوتو[1]، ۲۰۰۳). هویت‌های مادی، مانند هویت‌های شخصی و ناشی از نقش تمرکزشان بر تفکر و رفتار افراد است تا بر فرآیندهای گروهی و روابط میان‌گروهی. بنابراین دسته از نظریان هویت، کارتر و گرورِ (۲۰۱۵) هویت فناوری اطلاعات را به عنوان شکل جدیدی از هویت مادی مطرح می‌کنند.

با تعریف فناوری اطلاعات به عنوان «واحدی از فناوری (وسیله سخت‌افزاری، نرم‌افزار کاربردی یا محیط نرم‌افزار کاربردی) که افراد آگاهانه با آن مشغول می‌شوند»، هویت فناوری اطلاعات، در واقع هویت [فردی نشأت‌گرفته از] فناوری اطلاعات است و به معنای «میزانی است که یک فرد در حسش نسبت به خود [و در تعریفش از خود] فناوری اطلاعات را جدانشدنی می‌بیند» (کارتر و گروور، ۲۰۱۵). سازه هویت فناوری اطلاعات سازه‌ی مرتبه‌ی دوم است و خود شامل سه بعد وابستگی، انرژی هیجانی و مرتبط‌بودن می‌شود.

به منظور مطابقت بهتر هویت فناوری اطلاعات در زمینه شبکه‌های اجتماعی و همچنین مانند مطالعات قبلی که سازه هویت فناوری اطلاعات را استفاده کرده‌اند (به عنوان مثال آگبانوفه و گرهارت[2]، ۲۰۲۰) ، در این پژوهش سازه هویت فناوری اطلاعات را در قالب هویت شبکه‌های اجتماعی متناظرسازی می‌کنیم. منظور از هویت شبکه اجتماعی، «میزانی است که یک فرد در حسش نسبت به خود و در تعریفش از خود شبکه‌های اجتماعی را جدانشدنی می‌بیند». بنابراین در زمینه شبکه‌های اجتماعی، «مرتبط‌بودن» احساس پیوند داشتن با شبکه‌های اجتماعی را نشان می‌دهد؛ «انرژی هیجانی» نشان دهنده احساس شدید دلبستگی هیجانی کاربر در رابطه با شبکه‌های اجتماعی است و «وابستگی»، احساس وابسته‌بودن کاربر به شبکه‌های اجتماعی را نشان می‌دهد.

[1] Clayton, S., & Opotow
[2] Ogbanufe and Gerhart

مدل مفهومی و فرضیه‌ها

مطابق با مدل مفهومی اولیه هویت فناوری اطلاعات (کارتر و گروور ۲۰۱۵)، چندین مطالعه (مانند اسماعیل زاده (۲۰۲۰) و اوگبانوفه و گرهارت (۲۰۲۰)) نشان می‌دهد که افراد وقتی خود را بیشتر با فناوری اطلاعات شناسایی می‌کنند، استفاده بیشتری از مصنوعات سیستم‌های اطلاعاتی خواهند داشت. به عبارت دیگر، افرادی که هویت فناوری اطلاعات قوی‌تری دارند، از فناوری‌های اطلاعاتی بیشتر، طولانی‌تر و عمیق‌تر استفاده خواهند کرد. علاوه بر این، تحقیقات قبلی نشان می‌دهند که وابستگی به رسانه‌های اجتماعی (یک بعد فرعی از هویت فناوری اطلاعات) با به اشتراک‌گذاری اطلاعات در شبکه‌های اجتماعی ارتباطی مثبت دارد (لی و همکاران، ۲۰۱۹). بنابراین، به منظور انجام این مطالعه فرض می‌کنیم میزانی که کاربران خود را با شبکه‌های اجتماعی تعریف می‌کنند، ارتباطی مثبت دارد با استفاده طولانی مدت و به تبع آن با افزایش افشای اطلاعات شخصی در شبکه‌های اجتماعی. بنابراین، فرضیه اول تحقیق به این شکل صورت‌بندی می‌شود:

- **فرضیه اول**. هویت فناوری اطلاعات با احتمال خودافشایی ارتباط مثبت دارد.

یافته‌های اوگبانوفه و گرهارت (۲۰۲۰) ، به عنوان مرتبط‌ترین تحقیقات هویت فناوری اطلاعات در زمینه حریم خصوصی، تا حدی رابطه منفی بین «هویت ساعت هوشمند» و دغدغه‌های حریم خصوصی را تائید می‌کند. البته آن‌ها دغدغه‌های حریم خصوصی را پیش‌آیند هویت فناوری اطلاعات می‌دانند. فرض پژوهش حاضر آن است که وقتی کاربران ارتباطی قوی، تعلقی هیجانی و وابستگی به شبکه‌های اجتماعی دارند، به احتمال زیاد هنگام استفاده از شبکه‌های اجتماعی از دغدغه‌های حریم خصوصی خود چشم‌پوشی می‌کنند. بنابراین، فرض می‌کنیم:

- **فرضیه دوم**. هویت فناوری اطلاعات با دغدغه‌های حریم خصوصی ارتباط منفی دارد.

کارتر و گروور (۲۰۱۵) از ابتدا «مزایای خالص» را در کنار «لذت» و «رضایت» به عنوان ابعاد فرعی پاداش‌های محقق‌شده در مدل اولیه هویت فناوری اطلاعات در نظر گرفتند. نتایج اسماعیل‌زاده[1] (۲۰۲۰) نیز رابطه مثبت بین پاداش‌های محقق‌شده و هویت فناوری اطلاعات را تائید می‌کند. بر اساس این یافته‌های اولیه، پیشنهاد می‌کنیم میزانی که کاربران یک شبکه اجتماعی را در حسشان نسبت به خود مهم تلقی می‌کنند رابطه مستقیمی دارد با میزان مفید تلقی کردن افشای اطلاعات در شبکه‌های اجتماعی. در این تحقیق قصد داریم این فرض را مطالعه کنیم؛ بنابراین فرض می‌کنیم که:

- **فرضیه سوم**. هویت فناوری اطلاعات با مخاطرات ادراک‌شده رابطه منفی دارد.
- **فرضیه چهارم**. هویت فناوری اطلاعات با مزایای ادراک‌شده رابطه مثبت دارد.
- **فرضیه پنجم**. هویت فناوری اطلاعات با اعتماد رابطه مثبت دارد.

[1] Esmaeilzadeh

همان‌طور که در مطالعات پیشین حریم خصوصی اطلاعات (مانند دینو و هارت، ۲۰۰۶؛ ملهوترا و همکاران[1]، ۲۰۰۴) به‌خوبی تائید شده است، کاربرانی که بیشتر نگران حریم خصوصی خود هستند کمتر احتمال دارد که مشغول رفتارهای خودافشایی شوند (یون و همکاران[2]، ۲۰۱۴). بر این اساس، فرض بر این است که:

- **فرضیه ششم**. نگرانی‌های حریم خصوصی با احتمال خودافشایی ارتباط منفی دارد.

مطالعات قبلی در مورد محاسبه حریم خصوصی شواهدی محکم در مورد تأثیر مخاطرات و مزایای ادراک‌شده بر خودافشایی ارائه کرده است، به این صورت که مزایای ادراک‌شده استفاده از شبکه‌های اجتماعی رابطه‌ای مستقیم با رفتار خودافشایی و مخاطرات ادراک‌شده حریم خصوصی رابطه‌ای منفی با آن دارد (به عنوان مثال، ملهوترا و همکاران، ۲۰۰۴؛ کراسنوا و همکاران،۲۰۱۰). بنابراین، وقتی مزایای ادراک‌شده بیشتر از مخاطرات حریم خصوصی باشد، کاربران به احتمال زیاد اطلاعات شخصی خود را به اشتراک می‌گذارند یا افشا می‌کنند. بنابراین، فرض ما آن است که:

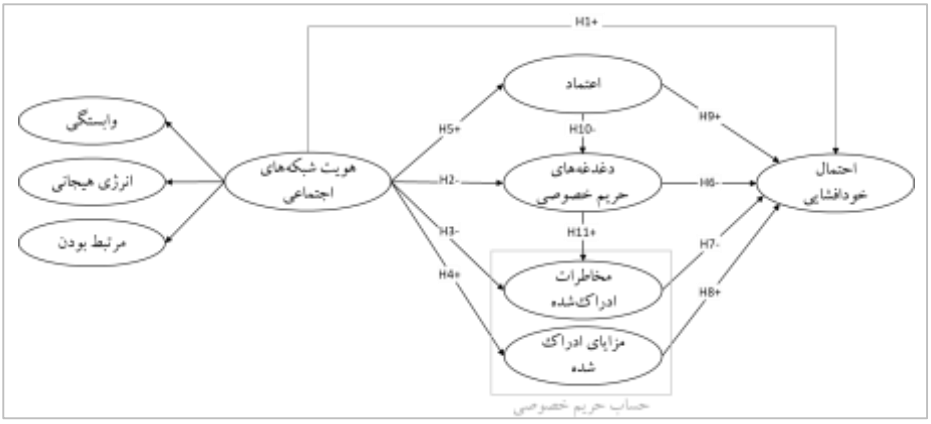
- **فرضیه هفتم**. خطرات درک شده از حریم خصوصی با احتمال افشای خود ارتباط منفی دارد
- **فرضیه هشتم**. مزایای درک شده با احتمال افشای خود ارتباط مثبت دارد

پژوهش‌هایی که ادبیات حوزه حریم خصوصی اطلاعات را به طور نظام‌مند و روش‌مند بررسی کرده‌اند، ارتباط میان سازه‌های کلیدی این حوزه مانند حریم خصوصی اطلاعات، اعتماد، مخاطرات ادراک‌شده و رفتارهای مرتبط با حریم خصوصی را به خوبی تبیین کرده‌اند (بلانجر و کراسلر، ۲۰۱۱ ؛ لی، ۲۰۱۱ ؛ پاولو، ۲۰۱۱؛ اسمیت و همکاران، ۲۰۱۱؛ دینو و همکاران، ۲۰۱۵). بنابراین، فرضیه‌های این بخش صرفا برای بررسی نقش غیرمستقیم هویت فناوری اطلاعات در رفتار خودافشایی بیان شده‌اند، چراکه این روابط در پژوهش‌های قبلی تائید شده است. سایر فرضیه‌های این پژوهش عبارتند از:

- **فرضیه نهم**. اعتماد با احتمال خودافشایی رابطه مثبت دارد.
- **فرضیه دهم**. اعتماد با دغدغه‌های حریم خصوصی اطلاعات رابطه منفی دارد.
- **فرضیه یازدهم**. دغدغه‌ها بر حریم خصوصی اطلاعات با مخاطرات ادراک شده رابطه مثبت دارد.

شکل ۱. مدل پیشنهادی تحقیق را به همراه فرضیه‌ها نشان می‌دهد.

[1] Malhotra et al.
[2] Yun



شکل ۱. مدل پیشنهادی تحقیق براساس مدل کلان APCO

روش‌شناسی

گردآوری داده‌ها

پژوهش حاضر با هدف مطالعه ادراک افراد و با استفاده از سازه‌هایی که در ادبیات سیستم‌های اطلاعاتی و روانشناسی به خوبی تثبیت شده است، انجام می‌شود. برای تحقق هدف پژوهش و آزمایش مدل پیشنهادی تحقیق، پیمایشی برای سنجش ادراک کاربران شبکه‌هایی اجتماعی از نحوه استفاده از فناوری اطلاعات و رفتار خودافشایی آن‌ها انجام شد. جامعه مورد مطالعه در این پژوهش شامل دانشجویان دانشگاه تهران است که در طی ۶ ماه گذشته از شبکه اجتماعی اینستاگرام استفاده کرده‌اند. برای دسترسی به مخاطبان پژوهش، فراخوان مشارکت در پیمایش به همراه لینک پرسشنامه آنلاین در ۲۲ کانال و گروه دانشجویان دانشگاه تهران در تلگرام و همچنین در ۳ صفحه دانشجویی دانشگاه تهران در اینستاگرام منتشر شد. برای اطمینان از واجد شرایط بودن پاسخ‌دهندگان، دو سوال زیر در ابتدای پیمایش از شرکت‌کنندگان پرسیده شد:

- آیا در دانشگاه تهران مشغول به تحصیل هستید؟
- آیا در ۶ ماه اخیر از شبکه اجتماعی اینستاگرام استفاده کرده‌اید؟

به طور کلی ۷۴۲ نفر در پیمایش شرکت کردند که از این تعداد، ۲۶۴ نفر با در نظر گرفتن پاسخ دو پرسش نخست و به دلیل واجد شرایط نبودن، به انتهای پرسشنامه هدایت شدند. نهایتاً، ۴۷۸ پاسخ معتبر از شرکت‌کنندگان دریافت شد.

سازه‌ها و سنجه‌ها

سنجه‌های پژوهش از مقیاس‌های موجود اقتباس‌شده است. هویت فناوری اطلاعات براساس سنجه‌های معرفی شده توسط کارتر و همکاران (۲۰۲۰) اندازه‌گیری شده است و دغدغه های حریم خصوصی با استفاده از مقیاس دینو و هارت (۲۰۰۶). پیامدهای رفتاری (یعنی متغیرهای وابسته) تحت عنوان احتمال خودافشایی تعریف عملیاتی می‌شود (کراسنوا و همکاران ۲۰۱۰). در اندازه‌گیری پدیده تناقض حریم خصوصی نیز از سنجه‌های مخاطرات ادراک‌شده حریم خصوصی (ملهوترا و همکاران، ۲۰۰۴) و مزایای ادراک‌شده (لین و لو، ۲۰۱۱) اقتباس شده است. تعریف عملیاتی کلیه سازه‌های استفاده شده در این پژوهش در جدول ۱ آمده است.

جدول۱. تعریف سازه‌های استفاده‌شده در این پژوهش

سازه	تعریف عملیاتی
هویت شبکه‌های اجتماعی (متناظرسازی شده براساس هویت فناوری اطلاعات)	میزانی است که یک فرد در حسش نسبت به خود [و در تعریفش از خود] شبکه‌های اجتماعی را جدانشدنی می‌بیند. این سازه، از نوع مرتبه دوم و خود شامل ۳ سازه انعکاسی وابستگی، انرژی هیجانی و مرتبط‌بودن است.
دغدغه‌های حریم خصوصی	میزان نگرانی افراد در خصوص بروز رفتارهای فرصت‌طلبانه در برابر اطلاعاتی که توسط آن‌ها در شبکه‌های اجتماعی منتشر شده است.
احتمال خودافشایی	میزانی که احتمال می‌رود افراد اطلاعات شخصی خود (مانند عکس، تجارب، احساسات و...) را در شبکه‌های اجتماعی منتشر کرده و در خصوص اطلاعات منتشر شده توسط دوستانشان علاقمندی و نظرات خود را ابراز کنند.
مخاطرات ادراک‌شده حریم خصوصی	میزانی که کاربران فکر می‌کنند انتشار اطلاعات شخصی خود در شبکه‌های اجتماعی مخاطره‌آمیز است، زیان‌های بالقوه‌ای دارد، موجب عدم اطمینان می‌شود و مسائل پیش‌بینی نشده‌ای را به همراه می‌آورد.
مزایای ادارک شده	میزانی که کاربران فکر می‌کنند شبکه‌های اجتماعی علاوه بر اینکه سرگرم‌کننده و لذت‌بخش هستند، برای کسب اطلاعات، ارتباط با دوستان، یافتن دوستان جدید و به اشتراک‌گذاری کارآمد اطلاعات نیز مفید هستند.
اعتماد	میزانی که کاربران مطمئن هستند که شبکه‌های اجتماعی اطلاعات آن‌ها را با اطمینان، امن و با صلاحیت مدیریت می‌کنند.

شیوه تحلیل داده‌ها

در نهایت، مدل پیشنهادی تحقیق با استفاده از مدل‌سازی معادلات ساختاری و با استفاده از نرم‌افزار اسمارت پی اِل اِس[1] نسخه ۳,۳,۳ (رینگل و همکاران[2]، ۲۰۱۵) آزمایش می‌شود. در رشته سیستم‌های اطلاعاتی، مدل‌سازی مسیر زمانی توصیه می‌شود که پژوهش به جای تأیید یک مدل ساختاری مبتنی بر نظریه، در پی آزمایش فرضیه‌هایی با مسیر مشخص باشد (گیفن و همکاران[3]، ۲۰۰۰). بر این اساس، معادلات ساختاری با روش حداقل مربعات جزئی، یک تکنیک مناسب برای درک روابط بین سازه‌های مدل تحقیق در نظر گرفته شد.

یافته‌های پژوهش

اطلاعات توصیفی و جمعیت‌شناختی پاسخ‌دهندگان

در مجموع ۴۷۸ پاسخ معتبر از شرکت‌کنندگان دریافت شد. پاسخ‌دهندگان زن ۶۴٪ نمونه مطالعه را تشکیل می‌دهند، در حالی که مردان ۳۶٪ پاسخ‌دهندگان را شامل می‌شوند. همچنین، طبقه‌بندی گروه‌های سنی به شرح زیر است: کمتر از ۲۰ سال (۱۰٪)، ۲۰ تا۳۰ سال (۶۷٪)، ۳۰ تا ۴۰ سال (۱۸٪)، ۴۰ تا ۵۰ سال (۴٪) و نهایتا افراد بالای ۵۰ سال (۱٪). نتایج توصیفی سطح تحصیلات نشان می‌دهد که حدود ۴۷ درصد از پاسخ‌دهندگان دانشجوی مقطع کارشناسی، ۴۲ درصد دانشجوی مقطع کارشناسی ارشد و ۱۱ درصد دانشجوی مقطع دکتری هستند. تجزیه و تحلیل ترجیحات کاربران در استفاده از شبکه‌های اجتماعی نشان می‌دهد که علاوه بر اینستاگرام، ۱۵ درصد از آن‌ها از فیس بوک ، ۴۶ درصد از توییتر و ۳۴ درصد از لینکدین استفاده می‌کنند. علاوه بر این، در این مطالعه سابقه کار با شبکه‌های اجتماعی در بین پاسخ‌دهندگان نیز اندازه‌گیری شده است. کمتر از ۱ درصد از پاسخ‌دهندگان سابقه استفاده کمتر از ۶ ماه، ۲ درصد بین ۶ ماه تا ۱ سال و ۴ درصد ۱ تا ۲ سال سابقه استفاده از شبکه‌های اجتماعی را دارند. ۲۶,۸٪ کاربران ۲ تا ۵ سال است که شبکه‌ای اجتماعی استفاده می‌کنند و نهایتاً ۵۱٪ بین ۵ تا ۱۰ سال و ۱۵,۸٪ بیش از ۱۰ سال است که کاربر شبکه‌های اجتماعی هستند. علاوه بر این، از پاسخ‌دهندگان درباره تناوب ارسال پست در شبکه‌های اجتماعی پرسیده شد. ۶۰ درصد از پاسخ‌دهندگان گزارش داده‌اند که به ندرت در شبکه‌های اجتماعی مطلب ارسال می‌کنند (یعنی هر چند ماه یک بار یا کمتر)، ۲۵ درصد چند بار در ماه ، ۱۱ درصد چند بار در هفته و ۴ درصد به صورت روزانه در شبکه‌های اجتماعی پست ارسال می‌کنند. سرانجام، هدف اساسی استفاده از شبکه‌های اجتماعی، به عنوان یک سؤال چند گزینه‌ای ، نشان می‌دهد که اکثر مردم از شبکه‌های اجتماعی برای «حفظ ارتباط با دوستان و اطلاع از احوال آن‌ها» استفاده می‌کنند (۷۴٪) ، و پس از آن برای «پر کردن اوقات فراغت» (۷۲٪)، «در جریان بودن از اخبار و رویدادهای روز» (۷۰٪)

[1] Smart PLS
[2] Ringle et al.
[3] Gefen et al.

و نهایتاً برای «یافتن مطالب خنده‌دار یا سرگرم‌کننده» (۴۹٪). اطلاعات کامل جمعیتی در جدول ۲ ارائه شده است.

جدول ۲. اطلاعات توصیفی نمونه تحقیق (حجم ۴۶۷ نفر)

	توصیف نمونه	تعداد	درصد
جنسیت	– خانم	۲۹۷	٪۶۴
	– آقا	۱۷۰	٪۳۶
سن	– کمتر از ۲۰ سال	۴۸	٪۱۰
	– ۲۰ تا ۳۰ سال	۳۱۲	٪۶۷
	– ۳۰ تا ۴۰ سال	۸۴	٪۱۸
	– ۴۰ تا ۵۰ سال	۱۸	٪۴
	– ۵۰ سال و بیشتر	۵	٪۱
تحصیلات	– دانشجوی کارشناسی	۲۲۰	٪۴۷
	– دانشجوی کارشناسی ارشد	۱۹۵	٪۴۲
	– دانشجوی دکتری	۵۲	٪۱۱
شبکه‌های اجتماعی مورد استفاده به جز اینستاگرام	– فیسبوک	۷۰	٪۱۵
	– توییتر	۲۱۳	٪۴۶
	– لینکدین	۱۵۷	٪۳۴
سابقه کار با شبکه‌های اجتماعی	– کمتر از ۶ ماه	۲	٪۰,۴
	– بین ۶ ماه تا ۱ سال	۱۰	٪۲,۱
	– ۱ تا ۲ سال	۱۸	٪۳,۹
	– ۲ تا ۵ سال	۱۲۵	٪۲۶,۸
	– ۵ تا ۱۰ سال	۲۳۸	٪۵۱
	– بیش از ۱۰ سال	۷۴	٪۱۵,۸
تناوب ارسال پست در شبکه‌های اجتماعی	– به‌ندرت: هر چند ماه یک بار یا کمتر	۲۷۹	٪۶۰
	– چند بار در ماه	۱۱۸	٪۲۵
	– چند بار در هفته	۵۱	٪۱۱
	– روزانه	۱۹	٪۴
هدف از استفاده شبکه‌های اجتماعی	– حفظ ارتباط با دوستان و اطلاع از احوال آن‌ها	۳۴۵	٪۷۴
	– در جریان بودن از اخبار و رویدادهای روز	۳۲۶	٪۷۰
	– پر کردن اوقات فراغت	۳۳۸	٪۷۲
	– برای یافتن مطالب خنده‌دار یا سرگرم‌کننده	۲۳۰	٪۴۹
	– ارتباط عمومی با افراد دیگر	۱۷۴	٪۳۷
	– چون دوستانم آنجا هستند	۱۹۶	٪۴۲
	– به‌اشتراک‌گذاشتن عکس یا فیلم با دیگران	۱۵۵	٪۳۳
	– به‌اشتراک‌گذاشتن نظرات و عقایدم	۱۴۲	٪۳۰

– تحقیق درباره‌ی خرید محصولات جدید	۱۷۰	٪۳۶
– آشنایی و ملاقات با آدم‌های جدید	۱۰۲	٪۲۲

روایی و پایایی

روایی همگرا و واگرا[1] قبل از ارزیابی مدل ساختاری، ضرایب مسیر[2] و واریانس تبیین‌شده[3]، برای همه‌ی سازه‌ها بررسی‌شده است. همه سازه‌های مرتبه اول مورد استفاده در مدل، از نوع انعکاسی[4] بودند. هر یک از سازه‌های انعکاسی دارای روایی بالا و میانگین واریانس استخراج شده[5] قابل قبول هستند. بار عاملی هر یک از سنجه‌های پرسشنامه به جز در یک مورد همه بالای ۰,۶ است. یکی از سنجه‌های «مزایای ادراک‌شده استفاده از شبکه‌های اجتماعی» دارای بار عاملی ۰,۵۷۸ بوده که از پرسشنامه حذف شد. میانگین واریانس استخراج شده که بیش از ۰,۵ توصیه‌شده است نیز روایی سازه‌ها را تائید می‌کند. بارگذاری‌های متقاطع[6] نیز همگی کمتر از بارگذاری‌ها[7] بودند و آزمون فارنل-لارکر[8] هم در سنجش روایی واگرا رابطه کم سازه‌ها را تائید می‌کند (جدول ۳). برای بررسی دقیق‌تر، مقادیر نسبت روایی یگانه-دوگانه[9] را بررسی کردیم. همه مقادیر نسبت روایی یگانه-دوگانه کمتر از ۰,۹ بود. بنابراین، پایایی و روایی واگرا پژوهش مورد تائید است. سنجه‌های پرسشنامه و میزان بار عاملی هر یک از آن‌ها در پیوست ۱ آمده است.

جدول ۳ . نتایج آزمون روایی فارنل-لارکر

	Benefit	Disclosure	ITID	PC	Risk	Trust
Benefit						
Disclosure	0.545					
ITID	0.788	0.491				
PC	0.091	0.129	0.085			
Risk	0.205	0.353	0.228	0.776		
Trust	0.528	0.428	0.444	0.459	0.617	

Benefit = مزایای ادراک‌شده، Disclosure = احتمال خودافشایی، ITID = هویت فناوری اطلاعات، PC = دغدغه‌های حریم خصوصی، Risk = مخاطرات ادراک‌شده، Trust = اعتماد

[1] Convergent and Discriminant Validity
[2] Path Coefficients
[3] Variance Explained
[4] Reflective Construct
[5] Average Variance Extracted (AVE)
[6] Cross Loadings
[7] Loadings
[8] Fornell-Larcker
[9] Heterotrait-Monotrait (HTMT)

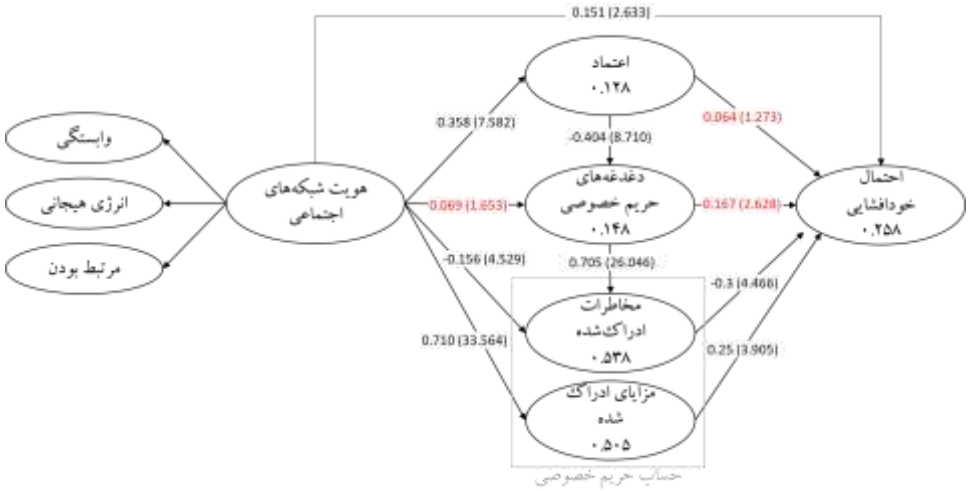
آزمون فرضیه‌ها و مدل پژوهش

نتایج به‌دست آمده نشان می‌دهد که هویت فناوری اطلاعات با احتمال خودافشایی رابطه مثبت معنادار دارد (b = ۰,۱۵۱، p = ۰,۰۰۶) که اولین فرضیه پژوهش را تائید می‌کند. این در حالی است که رابطه هویت فناوری اطلاعات با دغدغه‌های حریم خصوصی قابل توجه نیست (b = ۰,۰۶۹، ۰,۱۳۷ = p) و بنابراین فرضیه دوم پژوهش رد می‌شود. نتایج تحلیل مدل ساختاری نشان می‌دهد که فرضیه سوم پژوهش تائید می‌شود، چرا که هویت فناوری اطلاعات با مخاطرات ادراک شده حریم خصوصی رابطه‌ای منفی و معناداری دارد (b = - ۰,۱۵۶، p < ۰,۰۰۰). در خصوص فرضیه‌های چهارم و پنجم، هویت فناوری اطلاعات رابطه مثبت و معناداری با مزایای ادراک شده استفاده از شبکه‌های اجتماعی (b = ۰,۷۱۰، p < ۰,۰۰۰) و اعتماد (b = ۰,۳۵۸، p < ۰,۰۰۰) دارد و بر همین اساس فرضیه‌های چهارم و پنجم نیز تایید می‌شوند. نتایج پژوهش نشان می‌دهد که دغدغه‌های حریم خصوصی ارتباط مثبت و معناداری با احتمال خودافشایی دارد (b = ۰,۱۶۷، p = ۰,۰۱۰) در حالی که فرضیه ششم این رابطه را منفی درنظر گرفته بود؛ بدین ترتیب فرضیه ششم رد می‌شود. مخاطرات ادراک شده رابطه منفی و معناداری با احتمال خودافشایی کاربران دارد (b = - ۰,۳۰۰، p < ۰,۰۰۰) و این نتیجه فرضیه هفتم را تائید می‌کند. به طور مشابهی، مزایای ادراک شده استفاده از شبکه‌های اجتماعی نیز با احتمال خودافشایی رابطه مثبت و معناداری دارد (b = ۰,۲۵۰، p < ۰,۰۰۰) ؛ به عبارت دیگر، فرضیه هشتم نیز تایید می‌شود. با این حال، اعتماد رابطه معناداری با احتمال خودافشایی ندارد (b = ۰,۰۶۴، p = ۰,۲۱۱) و بدین ترتیب فرضیه نهم رد می‌شود. در نهایت، نتایج بررسی‌ها نشان می‌دهد که اعتماد با دغدغه‌های حریم خصوصی اطلاعات رابطه‌ای منفی و معنادار (b = - ۰,۴۰۴، p < ۰,۰۰۰) و دغدغه‌های حریم خصوصی اطلاعات نیز با مخاطرات ادراک‌شده رابطه‌ای مثبت و معنادار (b = ۰,۷۰۵، p < ۰,۰۰۰) دارد. این نتایج فرضیه‌های دهم و یازدهم را تائید می‌کند.

به طور کلی، این مدل ۲۵,۸٪ واریانس خودافشایی، ۵۳,۸٪ واریانس مخاطرات ادراک‌شده، ۵۰,۵٪ واریانس مزایای ادراک‌شده استفاده از شبکه‌های اجتماعی، ۱۴,۸٪ واریانس دغدغه‌های حریم خصوصی اطلاعات و ۱۲,۸٪ واریانس اعتماد را تبیین می‌کند. شکل ۲ نتایج مدل ساختاری را نشان می‌دهند.

بحث و نتیجه‌گیری

مقاله حاضر رفتار خودافشایی کاربران شبکه‌های اجتماعی را مورد بررسی قرار داده است. در این مقاله نقش مستقیم و غیرمستقیم هویت فناوری اطلاعات را بر احتمال خودافشایی بررسی کردیم. نتایج این پژوهش در خصوص تائید فرضیه اول، نشان می‌دهد که هویت فناوری اطلاعات ارتباطی مثبت با رفتار خودافشایی اطلاعات در شبکه‌های اجتماعی دارد. این بدین معناست که هرچه کاربران در تعریفشان از خود و در حسشان نسبت به خود شبکه‌های اجتماعی را جدانشدنی ببینند، احتمال بیشتری می‌رود که اطلاعات شخصی خود را در شبکه‌های اجتماعی افشا کنند. این یافته با نتایج



شکل ۲. مدل تخمین استاندارد و اعداد معناداری

مطالعات برجسته جامعه‌شناسی و روانشناسی در مورد ارتباط بین هویت و رفتار مطابقت دارد (مانند گرانبرگ و هولمبرگ (۱۹۹۰) و استتس و بیگا (۲۰۰۳)). به طور خاص، ازآنجایی‌که رفتار خودافشایی کاربران در شبکه‌های اجتماعی جزو رفتارهای تکرارشونده است، هویت می‌تواند نقش کلیدی در پیش‌بینی این نتایج رفتاری ایفا می‌کند (استتس و بیگا، ۲۰۰۳). علاوه بر این، پژوهش‌های قبلی نیز نشان می‌دهد که وابستگی به رسانه‌های اجتماعی که خود یک بعد فرعی از هویت فناوری اطلاعات است، با اشتراک گذاشتن اطلاعات در شبکه‌های اجتماعی ارتباطی مثبت دارد (لی و همکاران، ۲۰۱۹).

نتایج این پژوهش در خصوص رد فرضیه دوم نشان می‌دهد میزانی که افراد در تعریفشان از خود و در حس‌شان نسبت به خود شبکه‌های اجتماعی را جدانشدنی ببینند، رابطه‌ای با میزان دغدغه‌های آن‌ها درمورد حریم خصوصی‌شان ندارد. یکی از دلایل این مشاهده می‌تواند به تفاوت در ماهیت اثرگذاری هویت فناوری اطلاعات و به‌وجود آمدن دغدغه‌های حریم خصوصی برگردد. بدین ترتیب که هویت فناوری اطلاعات از طریق یک فرآیند شناختی و سوگیری به اصطلاح کم‌تلاش بر رویکردها، احساسات و رفتارها تاثیر می‌گذارد. به عبارت دیگر، شیوه اثرگذاری هویت برخاسته از تفکری آگاهانه نیست و افراد بدون تفکری آگاهانه و به صورت شهودی و خودبه‌خود از هویت خود تأثیر می‌پذیرند. این در حالی است که به‌وجود آمدن دغدغه‌های حریم خصوصی اطلاعات در نتیجه فکر کردن (یا یک فرآیند شناختی پرتلاش) است. در پژوهش اوگبانوفه و گرهارت (۲۰۲۰) نیز رابطه منفی بین «هویت ساعت هوشمند» و دغدغه‌های حریم خصوصی به طور کامل تائید نشده بود؛ البته آن‌ها دغدغه‌های حریم خصوصی را به عنوان پیش‌آیندی بر هویت فناوری اطلاعات درنظر گرفته بودند.

علاوه براین، تائید فرضیه‌های سوم، چهارم، پنجم، هفتم و هشتم نشان می‌دهد که هویت فناوری اطلاعات به طور غیرمستقیم و از طریق سازه‌های اعتماد، مزایا و مخاطرات ادراک شده با رفتار خودافشایی اطلاعات مرتبط است. به عبارت دیگر، هر چه کاربران ارتباطی قوی، تعلقی هیجانی و وابستگی بیشتری به شبکه‌های اجتماعی داشته باشند، این امر باعث می‌شود که آن‌ها مزایای بیشتری برای استفاده از شبکه‌های اجتماعی درنظر گرفته و مخاطرات استفاده از شبکه‌های اجتماعی را کمتر مورد توجه قرار می‌دهند. این موضوع نهایتاً منجر به بروز رفتار خودافشایی در کاربران شبکه‌های اجتماعی خواهد شد. علاوه بر این، خودشناسایی[1] با شبکه‌های اجتماعی (یا هویت فناوری اطلاعات قوی‌تر) باعث می‌شود که افراد اعتماد بیشتری به شبکه‌های اجتماعی داشته باشند و در نتیجه این اعتماد، دغدغه‌های آن‌ها در خصوص حریم خصوصی‌شان کاهش یافته و مزایای بیشتری برای استفاده از شبکه‌های اجتماعی در نظر گرفته و مخاطرات استفاده از آن را نادیده بگیرند. این موضوع نهایتاً احتمال خودافشایی کاربران را افزایش خواهد داد. با توجه به نوظهور بودن نظریه هویت فناوری اطلاعات، درخصوص رابطه هویت فناوری اطلاعات با اعتماد، مزایا و مخاطرات ادراک‌شده استفاده از شبکه اجتماعی، مطالعات مرتبطی یافت نشد. تنها پژوهش‌های مرتبط با این حوزه کارتر و گروور (۲۰۱۵) و اسماعیل‌زاده (۲۰۲۰) است که رابطه مثبت میان پاداش‌های محقق‌شده و هویت فناوری اطلاعات را تائید می‌کنند.

رد فرضیه‌های ششم نشان می‌دهد که دغدغه‌های کاربران ایرانی شبکه اجتماعی اینستاگرام در خصوص حریم خصوصی‌شان ارتباطی مثبت با احتمال بروز رفتار خودافشایی در آن‌ها دارد. به عبارت دیگر، رد شدن این فرضیه حاکی از وجود پدیده تناقض حریم خصوصی در میان کاربران ایرانی شبکه اجتماعی اینستاگرام است. یعنی کاربران علی‌رغم داشتن دغدغه‌های حریم خصوصی و اعتماد باز هم خودافشایی می‌کنند. این پدیده در برخی از پژوهش‌های پیشین نیز مشاهده شده است (مانند نوربرگ و همکاران، ۲۰۰۷؛ پاولو، ۲۰۱۱؛ بارت و دیونگ، ۲۰۱۷؛ گربر، گربر و ولکامر، ۲۰۱۸ و کوکولاکیس، ۲۰۱۷). البته معنادار شدن رابطه مثبت میان دغدغه‌های حریم خصوصی و رفتار خودافشایی یافته‌ای بحث‌برانگیز بوده و می‌بایست در یک پژوهش کیفی به طور عمیق‌تری مورد بررسی قرار گیرد؛ چراکه این یافته نشان می‌دهد کاربران ایرانی اینستاگرام هر چه دغدغه‌های بیشتری در خصوص حریم خصوصی خود داشته باشند، میزان خودافشایی آن‌ها نیز بیشتر می‌شود.

رد فرضیه نهم نشان می‌دهد که اعتماد افراد به شبکه‌های اجتماعی ارتباطی با احتمال خودافشایی آن‌ها در شبکه‌های اجتماعی ندارد؛ بلکه این اعتماد منجر به کاهش دغدغه‌های افراد در خصوص حریم خصوصی‌شان شده (تایید فرضیه دهم) و درنتیجه افراد با کاهش دغدغه‌های حریم خصوصی، مخاطرات شبکه‌های اجتماعی را کم‌تر مورد توجه قرار می‌دهند (تایید فرضیه یازدهم) که این موضوع منجر به

[1] Self-identification

افزایش احتمال خودافشایی کاربران درشبکه‌های اجتماعی خواهد شد. این یافته‌ها (به جز رد فرضیه نهم) همسو با جمع‌بندی نتایج مطالعات پیشین در خصوص حریم خصوصی اطلاعات (بلانجر و کراسلر، ۲۰۱۱ ؛ لی، ۲۰۱۱ ؛ پاولو، ۲۰۱۱؛ اسمیت و همکاران، ۲۰۱۱؛ دینو و همکاران، ۲۰۱۵) است. رد شدن فرضیه نهم، نشان می‌دهد که احتمال خودافشایی در شبکه‌های اجتماعی ارتباطی با میزان اعتماد افراد به آن شبکه اجتماعی ندارد. این یافته می‌تواند به نحوی دلالت بر وجود پدیده تناقض حریم خصوصی در میان کاربران شبکه‌های اجتماعی در ایران داشته باشد.

کاربردهای عملی و نظری

از بعد عملی، خودافشایی اطلاعات می‌تواند به نقض حریم خصوصی اطلاعاتی افراد و متعاقباً به پیامدهای منفی بسیاری منجر شود. با این حال، نتایج این پژوهش نشان‌دهنده وجود پدیده «تناقض حریم خصوصی» در بافت اجتماعی و فرهنگی جامعه ایران و به‌ویژه جامعه مورد مطالعه این پژوهش (یعنی دانشگاه تهران) است. به عبارت دیگر، دانشجویان دانشگاه تهران علیرغم وجود دغدغه‌هایی در خصوص حریم خصوصی خود، اقدام به خودافشایی اطلاعات شخصی خود می‌کنند. آگاهی از این‌که رفتارهای مربوط به حریم خصوصی اطلاعات در بسیاری مواقع خودجوش و بدون تأمل بوده و به طور مستقیم و غیرمستقیم با هویت فناوری اطلاعات آن‌ها مرتبط است، می‌تواند منجر به ایجاد خودآگاهی و در نتیجه افزایش حساسیت به این موضوع در میان دانشجویان و مسئولان دانشگاه شود. نتایج این تحقیق، خودآگاهی این افراد از رفتارهای خودافشاگرانه‌شان را ارتقا می‌دهد.

علاوه بر این، در کشور ایران در هیچ یک از اصول قانون اساسی، نه تنها به «حریم خصوصی اطلاعاتی» که حتی به حریم خصوصی و حق بر حریم خصوصی به عنوان یک حق اساسی پرداخته نشده است (احمدلو، ۱۳۹۲: ۱۶۷-۱۶۸). مطالعه قوانین اختصاصی این حوزه نیز نشان می‌دهد که بر خلاف بسیاری از کشورهای جهان اولاً، قانونی اختصاصی برای «حمایت از داده و یا صیانت از حریم خصوصی اطلاعاتی» در ایران وجود ندارد و ثانیاً، سایر قوانین موجود نیز توجه محدودی به حفظ حریم خصوصی افراد دارند؛ مانند بندهای ۵۸ تا ۶۱ قانون تجارت الکترونیک (تقوی‌فرد و جمشیدی، ۱۳۹۷: ۱۶۲). از این رو، هرچند پژوهش حاضر به بررسی رفتار خودافشایی اطلاعات در سطح فردی می‌پردازد، اما نتایج آن می‌تواند حساسیت پژوهشگران رشته حقوق، فعالان مدنی و قانون‌گذاران کشور را به حریم خصوصی اطلاعاتی افزایش داده و مورد استفاده آن‌ها قرار گیرد. علاوه بر این، قانون‌گذران و دولت‌ها نیز با کسب بینش در خصوص عوامل مؤثر بر رفتارهای مربوط به حریم خصوصی، مانند خودافشایی اطلاعات، می‌توانند قوانین بهتری در این حوزه وضع کرده و اجرا نمایند.

از بعد نظری، علیرغم اینکه بررسی رفتار خودافشایی کاربران در شبکه‌های اجتماعی می‌تواند موضوع پژوهش در رشته‌های مختلف دانشگاهی مانند جامعه‌شناسی، روانشناسی، علوم ارتباطات، مدیریت رسانه و مدیریت فناوری اطلاعات باشد، در جامعه دانشگاهی ایران مطالعات اندکی با هدف

بررسی رفتار خودافشایی کاربران درشبکه‌های اجتماعی انجام شده است (به عنوان مثال سماواتیان، ۱۳۹۷ و محمدیان و همکاران، ۱۳۹۳). از این‌رو، نتایج این تحقیق می‌تواند به توسعه ادبیات موجود در این زمینه کمک کند و مبنایی برای انجام مطالعات بیشتر باشد.

علاوه بر این، نتایج این پژوهش می‌تواند کاربردهایی نظری برای جامعه دانشگاهی بین‌المللی هم داشته باشد. اول این‌که، با افزودن سازه هویت فناوری اطلاعات به مدل کلان پیش‌آیندها و پیامدهای حریم خصوصی، به غنای بیشتر این مدل و ادبیات موضوعی سیستم‌های اطلاعاتی در این زمینه کمک کرده و توضیحی بدیع در خصوص پدیده تناقض حریم خصوصی ارائه می‌دهد. دوم این‌که، با درنظر گرفتن سازه هویت فناوری اطلاعات برای پیش‌بینی رفتارهای مرتبط با حریم خصوصی و استفاده از هویت فناوری اطلاعات در یک بافت موضوعی جدید، به پیشبرد تحقیقات هویت فناوری اطلاعات نیز کمک می‌کند.

محدودیت‌های پژوهش و پیشنهاد برای پژوهش‌های آتی

نویسندگان اذعان دارند که به عنوان یک محدودیت ذاتی برای مطالعات پیمایشی، هرگونه روابط علی متقابل در بین سازه‌ها قابل تعیین نیست. علاوه بر این، یافته‌ها پژوهش حاضر صرفاً نشان‌دهنده ادراک کاربران است، نه رفتار واقعی آن‌ها. به این معنا که، نتایج این پژوهش صرفاً براساس خوداظهاری کاربرانی است که در پیمایش مربوطه شرکت کرده‌اند و ممکن است رفتار واقعی آن‌ها در شبکه‌های اجتماعی متفاوت از اظهارات آن‌ها در پیمایش انجام شده باشد. پژوهش‌های آتی می‌توانند با گردآوری داده‌ها از طریق طراحی و اجرای آزمایش تجربی، کلیه این محدودیت‌ها را رفع نمایند. به‌علاوه، از آنجا که خودافشایی اطلاعات با پیامدهای منفی برای کاربران شبکه‌های اجتماعی همراه است، مطالعه‌ای دیگر می‌تواند عوامل تقلیل‌دهنده بر رابطه میان هویت فناوری اطلاعات و رفتار خودافشایی اطلاعات را مورد بررسی قرار دهد. نهایتاً، رد فرضیه ششم و تائید آن در خلاف جهت فرض اولیه محققان، یافته‌ای چالش‌برانگیز است و می‌تواند در یک پژوهش کیفی به طور عمیق‌تری مورد بررسی و مطالعه قرار گیرد.

منابع

احمدلو، مونا. (۱۳۹۲). *حریم خصوصی در فقه و حقوق ایران*. تهران: انتشارات مجد.

تقوی‌فرد، محدتقی؛ جمشیدی، محمدجواد. (۱۳۹۷). *اصول و مبانی حریم خصوصی اطلاعاتی*. تهران: انتشارات چراغ دانش.

سماواتیان، اکرم (۱۳۹۷). بررسی خودافشایی در شبکه‌های اجتماعی؛ مجازی مورد مطالعه: شهر همدان. *فصلنامه مطالعات فرهنگی پلیس*. ۵ (۱)، ۱-۲۸.

محمدیان, بهزاد, شعله, مهدی, بابائیان مهابادی, سمیه. (۱۳۹۳). تأثیر خودافشایی در شبکه‌های اجتماعی بر توسعه سرمایه اجتماعی (بررسی نقش سرمایه معنوی). *مجله علمی "مدیریت سرمایه اجتماعی"*, ۱(۲), ۲۲۵-۲۴۵.

Acquisti, A., & Gross, R. (2006, June). Imagined communities: Awareness, information sharing, and privacy on the Facebook. In *International workshop on privacy enhancing technologies* (pp. 36-58). Springer, Berlin, Heidelberg.

Alashoor, T., Han, S., & Joseph, R. C. (2017). Familiarity with big data, privacy concerns, and self-disclosure accuracy in social networking websites: An APCO model. *Communications of the Association for Information Systems*, *41*(1), 4.

Barth, S., & De Jong, M. D. (2017). The privacy paradox–Investigating discrepancies between expressed privacy concerns and actual online behavior–A systematic literature review. *Telematics and informatics*, *34*(7), 1038-1058.

Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: a review of information privacy research in information systems. *MIS quarterly*, 1017-1041.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Understanding emergence and outcomes of information privacy concerns: A case of Facebook.

Burke, P. J., & Stets, J. E. (2009). *Identity theory*. Oxford University Press.

Burke, P. J., & Reitzes, D. C. (1991). An identity theory approach to commitment. *Social psychology quarterly*, 239-251.

Carter, M., & Grover, V. (2015). Me, My Self, And I (T). *Mis Quarterly*, *39*(4), 931-958.

Carter, M., Petter, S., Grover, V., & Thatcher, J. B. (2020). IT Identity: A measure and empirical investigation of its utility to IS research. *Journal of the Association for Information Systems*, *21*(5), 2.

Chiu, C. M., Hsu, M. H., & Wang, E. T. (2006). Understanding knowledge sharing in virtual communities: An integration of social capital and social cognitive theories. *Decision support systems*, *42*(3), 1872-1888.

Clayton, L. W. (2003). Identity and the natural environment: The psychological significance of nature. Mit Press. Retrieved from https://psycnet.apa.org/record/2004-14744-000.

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information systems research*, *17*(1), 61-80.

Dinev, T., McConnell, A. R., & Smith, H. J. (2015). Research commentary—informing privacy research through information systems, psychology, and behavioral economics: thinking outside the "APCO" box. *Information Systems Research*, *26*(4), 639-655.

Esmaeilzadeh, P. (2021). How does IT identity affect individuals' use behaviors associated with personal health devices (PHDs)? An empirical study. *Information & Management*, *58*(1), 103313.

Fogel, J., & Nehmad, E. (2009). Internet social network communities: Risk taking, trust, and privacy concerns. *Computers in human behavior*, *25*(1), 153-160.

Gefen, D., Straub, D., & Boudreau, M. C. (2000). Structural equation modeling and regression: Guidelines for research practice. *Communications of the association for information systems*, *4*(1), 7.

Gerber, N., Gerber, P., & Volkamer, M. (2018). Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers & security*, *77*, 226-261.

Granberg, D., & Holmberg, S. (1990). The intention-behavior relationship among US and Swedish voters. *Social Psychology Quarterly*, 44-54.

Gross, R., & Acquisti, A. (2005). Information revelation and privacy in online social networks. In *Proceedings of the 2005 ACM workshop on Privacy in the electronic society* (pp. 71-80).

Hogben, G. (2007). Security Issues and Recommendations for Online Social Networks. Retrieved March 1.

Hsu, C. L., & Lin, J. C. C. (2008). Acceptance of blog usage: The roles of technology acceptance, social influence and knowledge sharing motivation. *Information & management*, *45*(1), 65-74.

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & security*, *64*, 122-134.

Krasnova, H., Spiekermann, S., Koroleva, K., & Hildebrand, T. (2010). Online social networks: Why we disclose. *Journal of information technology*, *25*(2), 109-125.

Krasnova, H., Veltri, N. F., & Günther, O. (2012). Self-disclosure and privacy calculus on social networking sites: the role of culture. *Business & Information Systems Engineering*, *4*(3), 127-135.

Li, Y. (2011). Empirical studies on online information privacy concerns: Literature review and an integrative framework. *Communications of the Association for Information Systems*, *28*(1), 28.

Li, Y., Yang, S., Zhang, S., & Zhang, W. (2019). Mobile social media use intention in emergencies among Gen Y in China: An integrative framework of gratifications, task-technology fit, and media dependency. *Telematics and Informatics*, *42*, 101244.

Lin, K. Y., & Lu, H. P. (2011). Why people use social networking sites: An empirical study integrating network externalities and motivation theory. *Computers in human behavior*, *27*(3), 1152-1161.

Madden, M., Smith, A., & Vitak, J. (2007). Digital footprints: Online identity management and search in the age of transparency.

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information systems research*, *15*(4), 336-355.

McCall, G. J. (2003). The me and the not-me. In *Advances in identity theory and research* (pp. 11-25). Springer, Boston, MA.

McCall, G. J., & Simmons, J. L. (Jerry L. (1978). Identities and interactions: an examination of human associations in everyday life. Free Press.

Mosafer, H., & Sarabadani, J. (2021, January). Identity in the Digital Age: A Review of Information Technology Identity (ITID) Research in Information Systems. In *Proceedings of the 54th Hawaii International Conference on System Sciences* (p. 2627).

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of consumer affairs*, *41*(1), 100-126.

Ogbanufe, O., & Gerhart, N. (2020). The mediating influence of smartwatch identity on deep use and innovative individual performance. *Information Systems Journal*, *30*(6), 977-1009.

Owens, T. J. (2006). Self and identity. In *Handbook of social psychology* (pp. 205-232). Springer, Boston, MA. https://doi.org/10.1007/0-387-36921-X_9.

Pavlou, P. A. (2011). State of the information privacy literature: Where are we now and where should we go?. *MIS quarterly*, 977-988.

Ringle, C. M., Wende, S., & Becker, J. M. (2015). SmartPLS 3. *Boenningstedt: SmartPLS GmbH*.

Rosenberg, M., Confessore, N., & Cadwalladr, C. (2018). How Trump consultants exploited the Facebook data of millions. *The New York Times*, *17*(3), 2018.

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: an interdisciplinary review. *MIS quarterly*, 989-1015.

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: Measuring individuals' concerns about organizational practices. *MIS quarterly*, 167-196.

Statista. (2020). Number of Global Social Network Users 2017-2025.

Stets, J. E., & Biga, C. F. (2003). Bringing identity theory into environmental sociology. *Sociological Theory*, *21*(4), 398-423.

Stets, J. E., & Burke, P. J. (2000). Identity Theory and Social Identity Theory. Social Psychology Quarterly, 63(3), 224. https://doi.org/10.2307/2695870.

Stryker, S. (1980). *Symbolic interactionism: A social structural version*. Benjamin-Cummings Publishing Company.

Stryker, S., & Burke, P. J. (2000). The Past, Present, and Future of an Identity Theory. Social Psychology Quarterly, 63(4), 284. https://doi.org/10.2307/2695840.

Tajfel, H., & Turner, J. C. (2004). The Social Identity Theory of Intergroup Behavior. In Political Psychology (pp. 276–293). https://doi.org/10.4324/9780203505984-16.

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.

Vignoles, V. L., Schwartz, S. J., & Luyckx, K. (2011). Introduction: Toward an integrative view of identity. In *Handbook of identity theory and research* (pp. 1-27). Springer, New York, NY.

Wheeless, L. R., & Grotz, J. (1976). Conceptualization and measurement of reported self-disclosure. *Human communication research*, *2*(4), 338-346.

The Role of IT Identity in Self-disclosure Behavior of Instagram Users: A Survey of Students in University of Tehran

Babak Sohrabi[1*], Hamidreza Yazdani[2], Amir Manian[3], Hossein Mosafer[4]

Abstract

As people use social networking sites (SNS) more than ever before, disclosing personal information continues to be an issue of increasing concern both for practice and research. In spite of existing privacy concerns, people paradoxically continue to disclose personal information. Information Systems (IS) literature has provided partial explanations for this paradox. However, recent studies have recommended the consideration of spontaneous privacy-related behaviors. The emerging research on IT identity (ITID) – the extent to which an individual views use of an IT as integral to his or her sense of self – has opened a new window on better explaining IT use behaviors. This study aims to investigate the role of ITID in self-disclosure behavior of SNS users. To meet this end, in August 2021, a survey was administered among 467 students at University of Tehran who were also Instagram users. The results of this research, shows that ITID is positively associated with self-disclosure behavior on SNS. Furthermore, it also shows that ITID is indirectly associated with self-disclosure behavior through the mediating constructs of trust, perceived benefits and risks. This study contributes to the research by providing a better explanation of privacy paradox phenomenon and considering the role of ITID in predicting privacy-related behaviors.

Keywords: IT identity, Privacy concerns, Self-disclosure behavior, Privacy paradox

1 . Professor, Department of Information Technology Management, Faculty of Management, University of Tehran, Tehran, Iran. (Corresponding Author). (bsohrabi@ut.ac.ir)

2 . Assistant Professor, Department of Business Administration, Faculty of Management and Accounting, Farabi Campus, University of Tehran, Qom, Iran.

3 . Professor, Department of Information Technology Management, Faculty of Management, University of Tehran, Tehran, Iran

4 . PhD Student, Department of Information Technology Management, Faculty of Management, University of Tehran, Tehran, Iran.