Journal of Interdisciplinary Studies in Marketing Management, Vol.2, No.1, May 2023, pp. 31-45

The Importance of Privacy Concerns in Permission Marketing

Zahra Mohammadzadeh Emamverdikhan[1], Ali Reza Farokhbakht Foumani[2]*, Rahmat Ali Saberi Haghayegh[3]

Received date: 10/04/2023 Acceptance date: 28/05/2023

Abstract

Nowadays, in a very competitive environment with dozens of techniques, business owners are looking for newer ways to introduce and sell more diverse products and services to customers, but they face negative responses from most customers because most of their messages are sent when people are not focused. Sometimes, due to the sensitivity of most customers to the security of personal information, they consider receiving unwanted advertisements with different topics as a nuisance. The present study was a quantitative applied research. First, the data, models and theoretical literature were collected and the appropriate model was selected and distributed in the field by distributing a combined 38-question questionnaire (standard and researcher-made based on Likert's five-point spectrum) in the statistical population with 384 online and offline customers receiving services from the city of Rasht. 7 proposed hypotheses were confirmed. Privacy concerns were explained by 88% and permission by 50%.

Keywords: Perceived Control, Permission Marketing, Personal Relevant, Privacy Concerns, Trust

1. Ph.D. Student in Marketing, Department of Business Management, Rasht Branch, Islamic Azad.University, Rasht, Iran
2. Department of Management, Bandar Anzali Branch, Islamic Azad University, Bandar Anzali, Iran (Corresponding Author) alifoumani59@gmail.com
3. Department of Management, Bandar Anzali Branch, Islamic Azad University, Bandar Anzali, Iran.Saberi118@ut.ac.ir

اهمیت حریم خصوصی در بازاریابی اجازه‌ای

زهرا محمدزاده اماموردیخان [۱]، علیرضا فرخ بخت فومنی [۲*]، رحمتعلی صابری حقایق [۳]

تاریخ دریافت: ۱۴۰۲/۰۱/۲۱ تاریخ پذیرش: ۱۴۰۲/۰۳/۰۷

چکیده

امروزه صاحبان کسب و کارهای دنیا در فضایی بسیار رقابتی با ده‌ها نوع تکنیک بدنبال روشهای جدیدتر معرفی و فروش محصولات و خدمات متنوع‌تر به مشتریان هستند، لیکن با دریافت پاسخ‌های منفی از سوی بیشتر مشتریان روبرو می‌گردند. زیرا اکثرا پیام‌های آنان زمانیکه مردم تمرکز بالایی ندارند، ارسال می‌شود و گاهی بدلیل حساسیت اغلب مشتریان نسبت به امنیت اطلاعات شخصی، دریافت تبلیغات ناخواسته و با موضوعات متفاوت را مزاحمت تلقی می-کنند. گودین ۱۹۹۹ بمعرفی بازاریابی اجازه‌ای در کتاب بازاریابی اجازه‌ای تبدیل غریبه‌ها به دوست و دوستان به مشتری که به فعالیت‌های بازاریابی مستقیمی که نیاز به رضایت مصرف‌کنندگان جهت تماس و معرفی و تبلیغ محصولات و سرویس‌های یک کسب و کار به مشتریان با یک شرکت خاص دارد، پرداخت. مطالعه حاضر پژوهشی کمی کاربردی بود که ابتدا دیتاها، مدلها و ادبیات نظری انجام شده در این زمینه، گردآوری و مدل مناسب انتخاب و بصورت میدانی با توزیع پرسشنامه ۳۸ سوالی ترکیبی (استاندارد و محقق ساخته بر اساس طیف پنجگانه لیکرت) در جامعه آماری با ۳۸۴ مشتری آنلاین و آفلاین دریافت کننده خدمات شهر رشت انجام شد. تمام ۷ فرضیه طرح شده تایید گردیدند. نگرانی های مربوط به حریم خصوصی توسط ۸۸٪ و اجازه ۵۰٪ تبیین شد.

واژگان کلیدی: ارتباط شخصی، اعتماد، بازاریابی اجازه‌ای، کنترل ادراک‌شده، نگرانی‌های حریم خصوصی

۱. دانشجوی دکترای مدیریت بازاریابی، گروه مدیریت بازرگانی، واحد رشت، دانشگاه آزاد اسلامی، رشت، ایران
۲. گروه مدیریت، واحد بندر انزلی، دانشگاه آزاد اسلامی، بندر انزلی، ایران. (نویسنده مسئول) رایانامه: alifoumani59@gmail.com
۳. گروه مدیریت، واحد بندر انزلی، دانشگاه آزاد اسلامی، بندر انزلی، ایران Saberi118@ut.ac.ir

مقدمه

نگرانی درباره حریم خصوصی به مسئله اخلاقی مهمی در عصر اطلاعات تبدیل شده است (مارتین، ۲۰۱۶). این تجربه مصرف‌کننده و رفاه عمومی را تخریب کرده و به یک مانع اساسی برای بازاریابی و فروش آنلاین و آفلاین تبدیل شده و به عبارتی معضلی پایدار است که سیاست‌گذاران باید از عهده آن برآیند (کرافت و همکاران، ۲۰۱۷). در ادبیات پیشین راهنمایی در مورد چگونگی کاهش نگرانی حریم خصوصی مصرف‌کنندگان از طریق ابتکارات شرکتی، ازجمله درخواست رضایت قبلی برای جمع‌آوری داده‌ها و ارائه مزایایی در ازای اطلاعات قابل‌شناسایی شخصی ارائه‌شده است. حریم خصوصی اطلاعات به‌عنوان توانایی کنترل اطلاعات در مورد خود و تعیین اینکه دیگران چه زمانی و به چه هدفی می‌توانند به چنین اطلاعاتی دسترسی داشته باشند تعریف می‌شود (بلانگر و همکاران، ۲۰۱۹). استدلال شده است که پیشرفت‌های چشمگیر فناوری دهه اخیر، مفهوم و ابعاد حریم خصوصی را تغییر داده است. افراد به‌طور مداوم درگیر رسانه‌های اجتماعی هستند و از طریق دستگاه‌های تلفن همراه جهت ایجاد سرمایه اجتماعی، ارتقا، عزت‌نفس و اعتمادبه‌نفس خود و تأمین نیازهای لذت بردن از آن‌ها در شبکه‌های اجتماعی آنلاین[1] با دیگران ارتباط برقرار می‌کنند (هیراوی[2] و همکاران، ۲۰۱۸). بااین‌وجود، مطالب به اشتراک گذاشته‌شده در این سیستم‌عامل‌ها می‌تواند توجه طیف وسیعی از افراد، سازمان‌های شخص ثالث و سازمان‌های دولتی را به خود جلب کند (اکواستی و همکاران، ۲۰۱۵). لذا، هنگام تصمیم‌گیری برای افشای اطلاعات، کاربران باید سو استفاده احتمالی از اطلاعات خصوصی را توسط: ۱) سازمانی که شبکه‌های اجتماعی آنلاین و شرکای آن را اداره می‌کند (نگرانی حریم خصوصی نهادی) و (۲) سایر کاربران یا اشخاص موجود در سیستم‌عامل (حریم خصوصی اجتماعی) را در نظر بگیرند (رینز-گولدیه[3]، ۲۰۱۰). علاوه بر این افشای اطلاعات کاربر با داده‌های تولیدشده در دستگاه (مثلاً شناسه دستگاه، مکان و لیست تماس کاربر) تکمیل می‌گردد (برانگر، کراسلر، ۲۰۱۹). زمانی که کاربران درخواست مجوز را قبول می‌نمایند چنین داده‌هایی به‌طور خودکار با توسعه‌دهنده به اشتراک گذاشته می‌شوند (دوگرویل[4] و همکاران، ۲۰۱۷). بعلاوه، بیشتر توسعه‌دهندگان برای ردیابی و تبلیغات، داده‌های کاربر را با اشخاص ثالث به اشتراک می‌گذارند. برخلاف وب‌سایت‌های سنتی یا برنامه‌های دسکتاپ، برنامه‌های تلفن همراه می‌توانند به‌طور مداوم فعالیت‌های کاربران خود را تماشا کنند (ورتریچ[5] و همکاران، ۲۰۱۸). بنابراین، پویایی اشتراک و افشای داده‌ها باعث گردیده است که مطالعات مربوط به حفظ حریم خصوصی در عصر موبایل اجتماعی بیش از گذشته پیچیده شده باشد (برانگر و همکاران، ۲۰۱۹). بررسی‌ها و مقالات زیادی درباره نقش حریم خصوصی اطلاعات مشتریان در تجارت الکترونیکی صورت گرفته است همانند: رسانه‌های اجتماعی (جوزانی و همکاران، ۲۰۲۰)، پوشیدنی‌ها (لیدنیا و همکاران، ۲۰۱۷) و اینترنت اشیا (پائول و همکاران، ۲۰۲۰) و نشان‌دهنده این مطلب هستند که: حریم خصوصی مشتریان و نگرانی‌های مربوط به آن در برقراری ارتباطات بازاریابی و اجازه مشتریان از اهمیت بالایی برخوردارند. لذا باید توجه داشت که حفاظت از داده‌های شخصی و حریم خصوصی همه کاربران مهم است و حفاظت از اطلاعات شخصی آن‌ها در کاهش خطر آسیب بیشتر به تهدید یا استفاده نامناسب از داده‌های بیومتریک در اولویت اصلی قرارداد (گری، ۲۰۱۸). باک و موریموتو (۲۰۱۲) عنوان کردند که نگرانی درباره حفظ حریم خصوصی منجر به افزایش بدبینی تبلیغات و ممانعت از تبلیغات می‌شود. بر اساس این استدلال‌ها و یافته‌های آشکار مشاهده می‌گردد که

1 . Online Social Netwoks
2 . Heravi
3 . Raynes-Goldie
4. Dogruel
5. Wottrich

نگرانی‌های مربوط به حریم خصوصی یک متغیر مهم در بسیاری از تصمیمات مربوط به ارائه اطلاعات است. اثرات متقابل بین نگرانی‌های حریم خصوصی و مزایای ادراک‌شده مصرف‌کنندگان بهمراه نگرانی‌های شدید درباره حریم خصوصی نگرش کلی منفی نسبت به همه اشکال ارتباطات شخصی‌سازی‌شده دارند (مارتین و همکاران، ۲۰۱۷). مشتریان ترس شدیدی دارند که داده‌هایشان به‌اشتباه استفاده شود و معمولاً به نیت خیر شرکت‌ها نیز اعتماد ندارند. با توجه به این‌ها، تأثیر مستقیم و منفی نگرانی درباره حریم خصوصی در تصمیم‌گیری برای مجوز را پذیرفته‌ایم. براین اساس ما بینشی را از بحث درباره رویکردهای نظری، ادبیات مربوط به ارتباطات شخصی و نگرانی‌های مربوط به حریم خصوصی، درک نفوذ، مزایای ادراک‌شده، هزینه‌های احتمالی، میزان کنترل بر ارائه داده‌ها درنظرگرفته و ادغام می‌کنیم تا چارچوب مفهومی خود را اثبات کنیم.

مبانی نظری

بازاریابی اجازه‌ای

بازاریابی اجازه‌ای[1]از مصرف‌کنندگان جهت ارسال ارتباطات بازاریابی مجوز می‌گیرد. مصرف‌کنندگان اطلاعاتی را در مورد انواع پیام‌های تبلیغاتی که می‌خواهند دریافت کنند، به بازاریابان علاقه‌مند می‌دهند. بازاریابان نیز از این اطلاعات برای هدف قرار دادن مشتریان و تبلیغات استفاده می‌کنند. هدف: شروع، حفظ و توسعه گفت‌وگو با مشتریان، ایجاد اعتماد و در طول زمان بالا بردن سطح مجوز و تبدیل آن به دارایی‌های باارزش‌تر می‌باشد (کنت و همکاران، ۲۰۰۳). گودین (۱۹۹۹) بیان می‌کند که مصرف‌کنندگان امروزه مایل‌اند تا برای صرفه‌جویی در زمان هزینه گزافی را بپردازند درحالی‌که بازاریابان نیز مشتاق به پرداخت بسته‌های مختلف برای جلب توجه هستند. بازاریابی مجوز است که به مصرف‌کننده فرصتی جهت داوطلب شدن برای بازاریابی صرفاً با صحبت کردن با داوطلبان ارائه می‌دهد. اجازه بازاریابی تضمین می‌کند که مصرف‌کنندگان توجه بیشتری را به پیام بازاریابی داشته باشند. مطالعات نشان می‌دهند که اگرچه کاربران کنترل کمی بر نحوه جمع‌آوری و به اشتراک‌گذاری داده‌های خود دارند لیکن استفاده از درخواست‌های صریح اجازه و اعلان‌های روشن حریم خصوصی می‌تواند احساس کنترل ایجاد نماید و نگرانی‌های مربوط به حریم خصوصی آن‌ها را کاهش دهد (ویدجاجا و همکاران، ۲۰۱۹).

هنجار ذهنی[2]

نظریه کنش منطقی، هنجار ذهنی یک فرد نسبت به نظرات همسالان در مورد رفتار موردنظر را به‌عنوان یک پیش‌بینی کننده مهم قصد رفتاری شناسایی می‌کند (فیشبین و همکاران، ۲۰۱۱) واینکه اعضای گروه‌های اجتماعی وظیفه‌دارند رفتار خود را مطابق با هنجارهای اجتماعی موجود در گروه بزرگ‌تر تنظیم کنند. از طرفی استفاده از برنامه‌های تعاملی همانند فیس‌بوک اطلاعات شخصی را از دوستان فرد (درحالی‌که از برداشت اطلاعات شخصی‌شان بی‌اطلاع‌اند) جمع‌آوری می‌کنند و بنابراین آسیب‌پذیری فرد را در برابر نقض حریم خصوصی افزایش می‌دهند.

نگرانی حریم خصوصی

نگرانی از حریم خصوصی به احساس اضطراب در مورد حریم خصوصی شخصی اشاره دارد. مصرف‌کنندگان نگرانی‌های زیادی در مورد حفظ حریم خصوصی دارند و نسبت به جمع‌آوری و استفاده از داده‌های شخصی‌شان توسط شرکت‌ها دلهره و ناراحتی نشان

1. Permission marketing
2. Normative belief

می‌دهند. درحالی‌که نگرانی حفظ حریم خصوصی در درک رفتار مصرف‌کننده حیاتی تلقی می‌شود، اختر در (۲۰۱۴) اشاره‌کرده است که نگرانی‌های حفظ حریم خصوصی مصرف‌کنندگان، در معاملات آنلاین خرید، بانکداری و سرمایه‌گذاری آنلاین، خودکارآمدی اینترنتی نقش مهمی دارند و هسته اصلی این خودکارآمدی، توانایی/شایستگی و اعتمادبه‌نفس درک شده مصرف‌کنندگان برای انجام موفقیت‌آمیز فعالیت آنلاین است. درزمینه تبلیغات رفتاری موبایلی نیز، با توانایی افراد جهت مدیریت ابزارها و تنظیمات حریم خصوصی بر روی تلفن همراه خود، به‌منظور افزایش حریم خصوصی شخصی مرتبط می‌باشد. انواع مختلفی از ابزارها و تنظیمات حفظ حریم خصوصی سمت مشتری در تلفن‌های همراه برای کمک به افراد برای کنترل حریم خصوصی خود ازجمله توانایی مسدود کردن تبلیغات ایجادشده است. بااین‌حال، ابزارهای تضمین حریم خصوصی گاهی اوقات برای کاربران برای درک و/یا مدیریت مؤثر بسیار پیچیده هستند. همچنین مصرف‌کنندگان ممکن است به اثربخشی ابزارهای مشتری برای کمک به مدیریت مؤثر حریم خصوصی خود اعتماد نداشته باشند. مطابق با نظریه قرارداد اجتماعی، ادراک ناتوانی در محافظت از حریم خصوصی می‌تواند منجر به نگرانی شود (پارک و همکاران، ۲۰۱۸).

فرهنگ

گرچه مرزها و محتوای آنچه حریم شخصی یا حریم خصوصی قلمداد می‌شود در میان فرهنگ‌ها و اشخاص مختلف متفاوت است، اما تم اصلی آن‌ها مشترک است و مفهوم حریم خصوصی بر مفهوم امنیت (از سوءاستفاده گرفته تا امنیت اطلاعات) تأثیر گذاشته و مصونیت از تعرضِ حکومت‌ها، شرکت‌ها، یا افراد به حریم خصوصی، در بسیاری از کشورها را به‌عنوان قوانین حفظ حریم خصوصی کرده است حتی در برخی موارد در قانون اساسی آن‌ها آمده است. هرچند که گاهی افراد اطلاعات خصوصی خود را برای به دست آوردن منافع، تبلیغات، هنگام شرکت در مسابقه‌ها و قرعه‌کشی‌ها و... داوطلبانه افشا می‌کنند و هر فرد، شرکت، فرهنگ یا کشوری تعاریف مختلفی از حریم خصوصی (حریم خصوصی جسمانی، حریم خصوصی اطلاعاتی) دارند، لیکن نگرانی‌ها در مورد حریم خصوصی و ضرورت پاسداشت آن در هنگام جمع‌آوری و نگهداری به‌صورت دیجیتال یا غیر دیجیتال داده‌ها و اطلاعاتی که فردی را به‌صورت خاص بازشناس‌اند، بیشتر نمود می‌یابد و این نشان می‌دهد که ریشه و اساس مشکل حریم خصوصی مربوط به افشاگری نامناسب و بدون کنترل داده‌های شخصی است. لذا نگرانی‌های حریم خصوصی مصرف‌کنندگان ممکن است در فرهنگ‌های مختلف ملی متفاوت باشد (بازم، کافاس،۲۰۲۰).

آگاهی از حریم خصوصی

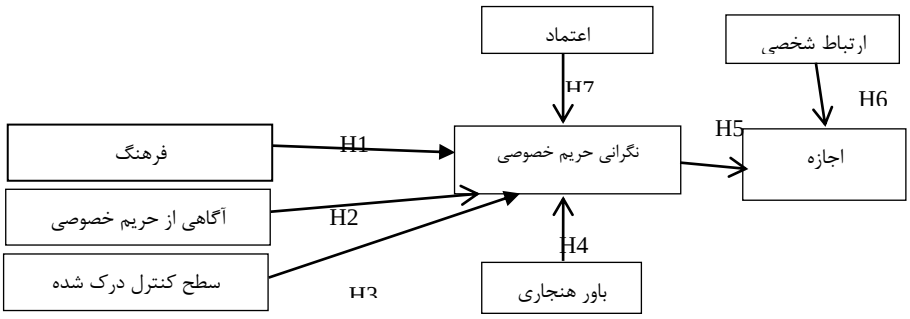
آگاهی از حریم خصوصی به ارزیابی اهمیت حریم خصوصی، تهدیدات برای حریم خصوصی و سیاست‌هایی اشاره دارد که حریم خصوصی را تنظیم می‌کند. بنابراین بر نگرانی درباره حریم خصوصی آنلاین به‌طور مثبت و/یا منفی تأثیر می‌گذارد. به‌عبارت‌دیگر، اگر کاربران احساس امنیت و محافظت کنند، درجه کمتری از نگرانی درباره حریم خصوصی را ابراز می‌نمایند. در چارچوب شبکه‌های اجتماعی، آگاهی کاربر تأثیر مثبتی بر افشای اطلاعات دارد (بن سون و همکاران، ۲۰۱۵). بااین‌حال، اگر کاربران اطلاعات بیشتری در مورد سیاست حفظ حریم خصوصی داشته باشند، اما متوجه نشتی در سیستم شوند، ممکن است بیشتر نگران حفظ حریم خصوصی باشند. افراد بسیار آگاه درزمینه حفظ حریم خصوصی اهمیت بیشتری در مورد حفظ و تمایل به پیروی از مسائل مربوط به حریم خصوصی دارند (دینو و همکاران، ۲۰۰۶).

ارتباط شخصی

نیاز به اطلاعات مرتبط، می‌تواند به‌عنوان یک عامل اصلی که مصرف‌کنندگان را به سمت تعامل با یک شرکت سوق می‌دهد، باشد. با توجه به ارتباطات بازاریابی تعاملی، چنین اطلاعاتی ارزش قابل‌توجهی را نشان می‌دهند و بنابراین، بر تمایل مصرف‌کنندگان بدادن اجازه تأثیر می‌گذارند. فراتر از آن، شخصی‌سازی ادراک‌شده با تردید تبلیغاتی و جلوگیری از تبلیغات ارتباط منفی دارد و میزان شخصی‌سازی باعث کاهش شک و تردید نسبت به رسانه‌های ارتباطی می‌شود (بائک و همکاران، ۲۰۱۲). در رابطه با بازاریابی مبتنی بر موقعیت مکانی، ژائو و همکاران (۲۰۱۲) نشان می‌دهند که شخصی‌سازی، که به‌عنوان یک مزیت بیرونی تعریف می‌شود، تأثیر مثبتی بر قصد مصرف‌کنندگان برای افشای اطلاعات دارد.

اعتماد

اعتماد مانند روح، هرگز از بین نمی‌رود و هرگز برنمی‌گردد. اعتماد کاربران به مؤسسات ممکن است بر اساس نوع محصول یا خدمات سازمان‌ها باشد (پابلیلیوس، ۲۰۱۸). مثلاً در مورد سازمان معروف فیس‌بوک که رسانه‌ای اجتماعی است و خدمات ارتباطی و شبکه‌های اجتماعی با بیش از ۱/۷ میلیارد کاربر (شیااو و همکاران، ۲۰۱۸) را ارائه می‌دهد، اعتماد ممکن است تصور کاربران در مورد ذخیره‌سازی، استفاده و محافظت اطلاعات مشترک آن‌ها در بستر این شبکه را تغییر دهد. کاهش اعتماد کاربر به سازمان‌ها منجر به کاهش استفاده از سیستم‌عامل‌ها می‌شود (آنتوسی و همکاران، ۲۰۱۹). در سال ۲۰۱۴، کمبریج آنالیتیکا، که خدمات تغییر رفتار مخاطب را ایجاد می‌کند، شروع به برداشت نامناسب اطلاعات و نظرات کاربران فیس‌بوک بدون اجازه آنها کرد (کانفسور، ۲۰۱۸) که باعث افزایش نگرانی درباره حریم خصوصی کاربران و تخریب اعتبار فیس‌بوک شد. نظرسنجی در بازارهای عمده ازجمله ایالات‌متحده و آلمان نشان داد که علیرغم عذرخواهی فیس‌بوک، همچنان کاربران نسبت به حریم خصوصی خود در رسانه‌های اجتماعی (به‌ویژه فیس‌بوک) اعتماد پایین دارند (خان و همکاران، ۲۰۱۸). با توجه به تخلفات مکرر داده‌ها و حریم خصوصی مرتبط با داده‌های دیجیتالی، ماهیت و تأثیرات آن بر عملکرد مارک‌های رسانه‌های اجتماعی یا سازمان‌ها در مقایسه با رسانه‌های سنتی پیچیده‌تر و مخرب‌تر است (یانگ و همکاران، ۲۰۱۶).



شکل (۱) مدل مفهومی تحقیق (محمدزاده و همکاران، ۱۴۰۱)

روش پژوهش

این پژوهش ازنظر هدف کاربردی و از لحاظ راهبرد پژوهشی کمی محسوب می‌گردد. در ابتدا دیتاها، مدل‌ها و ادبیات نظری سایر تحقیقات انجام‌شده در این زمینه، گردآوری گردید. مدل مناسب و جامع (محمدزاده و همکاران، ۱۴۰۱) انتخاب و به‌صورت میدانی با

توزیع تصادفی ساده پرسشنامه ۳۸ سؤالی ترکیبی (استاندارد و محقق ساخته) بر اساس طیف پنج‌گانه لیکرت آزمون شد. جامعه آماری مشتریان آنلاین وآفلاین دریافت کننده خدمات در شهر رشت بوده که به علت نامحدود بودن جامعه آماری و با توجه به واریانس استخراج‌شده از توزیع ۳۰ پرسشنامه پایلوت، بر اساس فرمول کوکران ۳۸۴ نفر درنظرگرفته شد. (لازم به ذکر است ازآنجاکه پیش‌ازاین تحقیقی در زمینه تدوین مدل جامع، مجموعه عوامل و فاکتورهای بازاریابی اجازه‌ای یافت نشده بود، نویسندگان همین مقاله، پژوهشی کیفی در ارتباط با متغیرهای مؤثر در بازاریابی اجازه‌ای و مدل مناسب آن در تبیین نقش حریم خصوصی در دو فاز اجرا نمودند که با اجرای دو مرحله دلفی‌فازی مدل نهایی حاصل آمد و نتایج در مقاله علمی پژوهشی سلامت روان کودک پاییز ۱۴۰۱ منتشر گردید (محمدزاده و همکاران، ۱۴۰۱). تحقیق پیش رو جهت آزمون این مدل به‌صورت کمی اجراشده است).

نتایج

در این پژوهش تجزیه‌وتحلیل داده‌ها در دو قسمت آمار توصیفی و استنباطی ارائه می‌شود. در آمار توصیفی با استفاده از فنون آمار توصیفی چون شاخص‌ها و درصدهای فراوانی، جداول و نمودارها به تجزیه‌وتحلیل جمعیت شناختی نمونه آماری و در قسمت آمار استنباطی با استفاده از آزمون‌های آماری به بررسی فرضیه‌های تحقیق پرداختیم. تجزیه‌وتحلیل استنباطی با استفاده از آزمون‌هایی چون ضریب همبستگی، تحلیل عاملی تأییدی[1]، آزمون برازش مدل، مدل اندازه‌گیری و تحلیل مسیر به کمک نرم‌افزار اسمارت پی ال اس[2] انجام شد.

جدول (۱) جدول ساختارهای توصیفی متغیرهای پژوهش

متغیرهای پژوهش	حداقل	حداکثر	میانگین	انحراف معیار
باور هنجاری	۱	۵	۱,۹۸	۱,۰۰
نگرانی درباره حریم خصوصی	۱	۵	۱,۸۱	۰,۸۱
ارتباط شخصی	۱	۵	۲,۱۳	۰,۸۱
سطح درک شده کنترل	۱	۵	۳,۱۱	۱,۶۵
آگاهی از حریم خصوصی	۱	۵	۱,۶۹	۰,۸۳
اعتماد	۱,۲	۵	۴,۳۲	۰,۹۶
فرهنگ	۱	۵	۲,۳	۰,۷۳
اجازه	۱	۵	۲,۷۲	۰,۸۷

همانطورکه مشاهده می‌گردد بیشترین میزان میانگین متغیر اعتماد با میزان میانگین ۴,۳۲ بوده است.

1. Confirmatory Factor Analysis (CFA)
2. Smrt PLS 2.0

جدول (۲) آزمون کولموگروف-اسمیرنوف جهت بررسی نرمال بودن متغیرهای تحقیق

شاخص‌ها	Z کولموگروف-اسمیرنوف	P-value
باور هنجاری	۴،۵۵۹	۰،۰۰۱
نگرانی درباره حریم خصوصی	۴،۶۷	۰،۰۰۱
ارتباط شخصی	۳،۵۷۴	۰،۰۰۱
سطح درک شده کنترل	۴،۹۷۹	۰،۰۰۱
آگاهی از حریم خصوصی	۴،۷۶۷	۰،۰۰۱
اعتماد	۷،۲۳۶	۰،۰۰۱
فرهنگ	۳،۱۷۹	۰،۰۰۱
اجازه	۳،۴۴۱	۰،۰۰۱

با توجه به اینکه سطح معنی‌داری آزمون کولموگروف- اسمیرنوف که برای متغیرهای پژوهش، کمتر از ۰/۰۵ است، نتیجه می‌شود که توزیع فراوانی متغیرهای تحقیق نرمال نبوده است؛ لذا جهت بررسی فرضیه‌های پژوهش از نرم‌افزار معادلات ساختاری اسمارت پی ال اس استفاده شد. برای آزمودن مدل اندازه‌گیری، از آلفای کرونباخ و پایایی مرکب جهت بررسی پایایی مدل اندازه‌گیری استفاده‌شده و از آزمون روایی همگرا و روایی واگرا جهت بررسی آزمون روایی مدل اندازه‌گیری استفاده گردید. نتایج آن به شرح زیر می‌باشد:

جدول (۳) آلفای کرونباخ متغیرهای پژوهش

متغیر	آلفای کرونباخ	وضعیت متغیر
آگاهی از حریم خصوصی	۰،۸۵۹	قابل‌قبول
اجازه	۰،۸۴۷	قابل‌قبول
ارتباط شخصی	۰،۹۵۳	قابل‌قبول
اعتماد	۰،۹۴۶	قابل‌قبول
سطح درک شده کنترل	۰،۹۷	قابل‌قبول
فرهنگ	۰،۷۱	قابل‌قبول
کنترل اطلاعات مشتری	۰،۷۷۹	قابل‌قبول
نگرانی درباره حریم خصوصی	۰،۹۶۸	قابل‌قبول

مقادیر بالاتر از ۰،۷ بوده، بنابراین آلفای کرونباخ متغیرهای پژوهش تأیید گردید.

جدول (۴) پایایی مرکب متغیرهای پژوهش

متغیر	پایایی مرکب	وضعیت متغیر
آگاهی از حریم خصوصی	۰،۹۱۴	قابل‌قبول
اجازه	۰،۹۲۹	قابل‌قبول
ارتباط شخصی	۰،۹۶۹	قابل‌قبول
اعتماد	۰،۹۶۱	قابل‌قبول
باور هنجاری	۰،۹۷	قابل‌قبول
سطح درک شده کنترل	۰،۹۸	قابل‌قبول
فرهنگ	۰،۸۳۵	قابل‌قبول
نگرانی درباره حریم خصوصی	۰،۹۷۴	قابل‌قبول

پایایی مرکب متغیرهای پژوهش>۰،۷بوده؛ لذا کلیه متغیرهای پژوهش از وضعیت مناسب و قابل قبولی برخوردارند.

جدول (۵) روایی همگرا متغیرهای پژوهش

متغیر	روایی همگراAVE	وضعیت متغیر
آگاهی از حریم خصوصی	۰,۷۸۱	قابل‌قبول
اجازه	۰,۸۶۷	قابل‌قبول
ارتباط شخصی	۰,۹۱۳	قابل‌قبول
اعتماد	۰,۸۳۴	قابل‌قبول
باور هنجاری	۰,۹۱۵	قابل‌قبول
سطح درک شده کنترل	۰,۹۴۳	قابل‌قبول
فرهنگ	۰,۶۳۷	قابل‌قبول
نگرانی درباره حریم خصوصی	۰,۸۶۲	قابل‌قبول

کلیه مقادیر بالاتر از ۰,۵؛ لذا روایی همگرای کلیه متغیرهای پژوهش در حد قابل‌قبول است.

جدول (۶) ضریب تبیین و شاخص متوسط اشتراک متغیرهای پژوهش

متغیر	R Square	Communality	وضعیت متغیر
آگاهی از حریم خصوصی	---	۰,۷۸۱	قابل‌قبول
اجازه	۰,۵	۰,۸۶۷	قابل‌قبول
ارتباط شخصی	---	۰,۹۱۳	قابل‌قبول
اعتماد	---	۰,۸۳۴	قابل‌قبول
باور هنجاری	---	۰,۹۱۵	قابل‌قبول
سطح درک شده کنترل	---	۰,۹۴۳	قابل‌قبول
فرهنگ	---	۰,۶۳۷	قابل‌قبول
نگرانی درباره حریم خصوصی	۰,۸۸۰	۰,۸۶۲	قابل‌قبول

نتایج روایی واگرا و تشخیصی فورنل و لارکر[1] نیز نشان دادند که روایی مدل پژوهش در حد قابل‌قبول می‌باشد. بر اساس آزمون مدل ساختاری که شامل: اعداد معناداری تی[2] و معیار Q^2 است، مدل ساختاری از قدرت پیش‌بینی بالایی برخوردار است. ارزیابی برازش کلی مدل با محاسبه جی او اف صورت گرفت. در این پژوهش جی ا اف= ۰,۶۱ بود و بر اساس نظر وتزلز[3] و همکاران (۲۰۰۹) سطح برازش کلی مدل در حد عالی است.

بحث و نتیجه‌گیری

نتایج آزمون فرضیه‌ها: جدول (۷) نتایج نهایی آزمون فرضیات

فرضیه‌های پژوهش	شدت تأثیر	مقدارT	سطح معناداری	نتیجه
فرضیه۱ – فرهنگ با نگرانی درباره حریم خصوصی ارتباط دارد.	۰,۱۱	۴,۲۸	۰,۰۰۱	تائید
فرضیه۲ – آگاهی از حریم خصوصی با نگرانی حفظ حریم خصوصی مرتبط است.	-۰,۲۴	۶,۴۵	۰,۰۰۱	تائید
فرضیه۳– کنترل حریم خصوصی ادراک‌شده بر نگرانی‌های مربوط به حریم خصوصی مؤثر است.	۰,۳۲۴ -	۱۱,۳۸۴	۰,۰۰۱	تائید
فرضیه۴ – هنجار ذهنی، با نگرانی‌های مربوط به حریم خصوصی شخص ارتباط دارد.	۰,۱۸۵ -	۴,۵۱۹	۰,۰۰۲	تائید
فرضیه ۵– نگرانی‌های حریم خصوصی بر اجازه برنامه‌های بازاریابی تأثیر می‌گذارد.	۰,۱۸۴ -	۳,۶۰۶	۰,۰۰۱	تائید

1. Fornell-Larcker Criterion
2. T-values
3. Wetzels

فرضیه ۶- ارتباط شخصی درک شده با اجازه فعالیت بازاریابی ارتباط دارد.	۰,۲۸۲	۶,۲۰۸	۰,۰۰۱	تائید
فرضیه ۷- اعتماد مشتری بر نگرانی او درباره‌ی حریم خصوصی مؤثر است.	۰,۱۱۶-	۳,۰۲۹	۰,۰۰۸	تائید

با توجه به مباحثی که تاکنون مطرح شد و با عنایت به نتایج محاسبات انجام‌شده:

بررسی فرضیه اول: فرهنگ با نگرانی درباره حریم خصوصی ارتباط دارد. تحقیق ما می‌تواند اثرات مربوط به حریم خصوصی را به‌طور خاص با پرداختن به ارزش‌های فرهنگی ایران کشف کند. فرض بر این است که نگرانی‌های مربوط به حریم خصوصی در جوامع جمعی مثل، چین نسبت به جوامع فردگرا همانند آلمان یا ایالات‌متحده بسیار شدیدتر است (جیو[1] و همکاران، ۲۰۲۰). زمانی ۱۳۹۴دریافت که کاربران در جریان استفاده از شبکه‌های اجتماعی در معرض آسیب‌های فرهنگی مختلفی در حوزه نقض حریم خصوصی قرار دارند که بر روند زندگی خانوادگی و هویت فرهنگی استفاده‌کنندگان بسیار تأثیرگذار است. آگاهی از این آسیب‌ها ضمن کاهش معضلات اجتماعی امکان استفاده بهینه از فناوری‌های نوین را فراهم و مسیر برنامه‌ریزی و سیاست‌گذاری خرد و کلان فرهنگی را برای متولیان امر هموارتر می‌نماید. تحقیقات زیادی نشان دادند که اختلاف فرهنگی، هنجارهای اجتماعی و سیاست حفظ حریم خصوصی می‌تواند بر حریم خصوصی کاربران تأثیر بگذارد (وانگ، ۲۰۱۹). در پژوهش ما این فرضیه تأیید و نشان داد فرهنگ و نگرانی درباره حریم خصوصی ارتباط معنادار دارند.

بررسی فرضیه دوم: آگاهی از حریم خصوصی با نگرانی در مورد حفظ حریم خصوصی ارتباط دارد. زو و همکاران (۲۰۱۶) دریافتند آگاهی از حریم خصوصی، نیاز به درک حریم خصوصی آنلاین را تحت تأثیر قرار می‌دهد و افراد بسیار آگاه حتی به حفظ حریم خصوصی در محیط اجتماعی خود بیشتر اهمیت می‌دهند. تحقیق مک کورماک و همکاران، ۲۰۱۷ بیانگر وجود رابطه مثبت بین آگاهی و امنیت اطلاعات می‌باشد. هیرچپلانگ[2] و همکاران (۲۰۱۶) دریافتند که وقتی افراد دانش لازم را نداشته باشند، تصمیماتشان را بر اساس گمانه‌زنی‌ها قرار می‌دهند. بااین‌حال، هرچه آگاهی و دانش فردی بیشتر باشد، این تصمیمات و رفتار مربوط به آن منطقی‌تر می‌شود. این فرضیه نیز تائید گردید.

بررسی فرضیه سوم: کنترل حریم خصوصی ادراک شده با نگرانی‌های مربوط به حریم خصوصی ارتباط دارد. زلاتولاس و همکاران (۲۰۱۵) دریافتند که کنترل حریم خصوصی تأثیر منفی بر نگرانی‌های مربوط به حریم خصوصی دارد. در مطالعه‌ای بر روی کاربران چهار نوع مختلف وب‌سایت یعنی سایت‌های تجارت الکترونیک، شبکه اجتماعی، مالی و سایت‌های مراقبت‌های بهداشتی دریافتند که کنترل حریم خصوصی یکی از ساختارهای کانونی است که نگرانی‌های مربوط به حریم خصوصی را توضیح می‌دهد. درخواست‌های بیش‌ازحد مجوز برنامه که "فراتر از عملکرد ضروری برنامه است" به دلیل نگرانی‌های مربوط به حفظ حریم خصوصی در مورد اطلاعات شخصی، با احتمال کمتری توسط کاربران تلفن همراه پذیرفته می‌شوند (چین[3] و همکاران، ۲۰۱۸). اثبات شد حریم خصوصی ادراک‌شده بر نگرانی‌های مربوط به حریم خصوصی به‌صورت مستقیم اما معکوس رابطه دارد.

فرضیه چهارم: هنجار ذهنی، با نگرانی‌های مربوط به حریم خصوصی شخص ارتباط دارد.

1 .Guo
2 . Hirschprung
3 . Chin

نتایج تجزیه‌وتحلیل‌ها نشان داد که هنجار ذهنی جهت افشا، با نگرانی‌های مربوط به حریم خصوصی شخص به‌صورت مستقیم اما معکوس رابطه دارد. تانگلو و همکاران (۲۰۱۰) پیشنهاد دادند وقتی فردی احساس کند همتایانش استفاده از آپهای تلفن همراه را تائید و تشویق می‌کنند، آن فناوری را مفید دانسته، ریسک کمتری را در ارائه اطلاعات شخصی درک و افشای اطلاعات بیشتری را انجام می‌دهند. زیرا تشویق دیگران به‌عنوان یک تجربه غیرمستقیم با موبایل عمل می‌کند.

بررسی فرضیه ششم: ارتباط شخصی درک شده با اجازه فعالیت بازاریابی ارتباط دارد. به‌طورکلی شواهد کافی وجود دارد که نشان می‌دهد شخصی‌سازی بیشتر، منجر به پیشنهادات مرتبط با آن در بازاریابی مستقیم شده، بنابراین نرخ پاسخ‌ها را افزایش بیشتری می‌دهد. این فرضیه نیز تائید گردید.

بررسی فرضیه هفتم: اعتماد مشتری بر نگرانی او درباره‌ی حریم خصوصی مؤثر است. همان‌طور که بدیهی است اعتماد ظریف است و تحقیقات قبلی حاکی از آن است که ترمیم اعتماد شکسته در تجارت بسیار سخت، وظیفه‌ای دشوار، زمان‌بر و نیازمند فرایندی طولانی است. نشان داده‌شده است که اعتماد با پذیرش فناوری به‌طورکلی و برنامه‌های تلفن همراه بطورخاص رابطه معناداری دارد (دی دزاندو، ۲۰۲۳). پذیرفته شد اعتماد مشتری بر نگرانی او درباره‌ی حریم خصوصی به‌صورت مستقیم و معکوس مرتبط است.

در انتها لازم به ذکر است: ۸۸٪ متغیر نگرانی درباره حریم خصوصی توسط متغیرهای مستقل و همچنین ۵۰٪ متغیر وابسته اجازه توسط سایر متغیرها تبیین گردیده است. این موضوع اشاره به این دارد که مجموعه عوامل دیگری در تبیین این متغیر وابسته دخالت دارند.

پیشنهادات تحقیق

همان‌طور که نتایج ما تائید می‌کنند ارائه‌دهندگان خدماتی که مشتریان آن‌ها از سطح بالایی از نگرانی‌های مربوط به حریم خصوصی برخوردارند، احتمال درک خرید فریبکارانه[1]، میزان استفاده و افشای اطلاعات، اعتماد مشتری، ارزیابی‌ها و رفتارهای منفی، افزایش درک خطر و نمایش رفتارهای محافظتی بیشتری را در پی خواهند داشت. برای کاهش این اثرات خصمانه، شرکت‌های فعال جهت کاهش نگرانی‌های مربوط به حریم خصوصی مشتری، می‌بایست به طراحی و ارائه استراتژی مناسب اقدام کنند. یک روش می‌تواند توسعه استراتژی‌های حسن نیت جدید یا افزودن به استراتژی‌های مرتبط با حسن نیت موجود همانند فعالیت‌های خیرخواهانه یا مسئولیت اجتماعی شرکت‌ها و ارتقا تصویر و اعتبار شرکت‌ها از طریق تبلیغ در رسانه‌های جمعی و اجتماعی باشد (اوکازاکی و همکاران، ۲۰۲۰).

رویکرد دیگر، توسعه محصولات و خدمات نوآورانه است که به ارائه خدماتی می‌پردازد که کمترین میزان نیاز به داده‌های شخصی و معاملاتی مشتریان را داشته باشد. نگرانی‌های زیاد مشتریان درباره حریم خصوصی‌شان تهدیدات فراوانی را ایجاد می‌کند، افزایش آگاهی از این نگرانی‌ها در بین فروشندگان می‌تواند خطر آن‌ها را کاهش داده و درعین‌حال با محافظت از حریم خصوصی مشتریان از تهدید موجود، فرصت‌های جدیدی برای خود ایجاد کنند. این امر با تقویت بخش ارتباط با مشتریان شرکت و پایش مداوم دغدغه‌ها و نگرانی‌های حریم خصوصی آنان ممکن است حاصل آید. یافته‌ها نشان می‌دهند که ماهیت خاص کانال‌های مختلف فروش تأثیر نگرانی‌های مربوط به حفظ حریم خصوصی مشتری را بر نتایج تغییر می‌دهد. مثلاً کانال‌های وب اثرات مثبتی بر ارزیابی مثبت و رفتارهای استفاده‌شده نشان می‌دهند، درحالی‌که کانال‌های تلفن همراه، اعتماد و رفتارهای محافظتی را کاهش می‌دهند. از طرف دیگر، معاملات در کانال‌های اجتماعی افزایش ریسک، افشا و سو استفاده از رفتارها را نشان می‌دهد. بنابراین شرکت‌هایی که از کانال‌های

1 .faceweaker

اجتماعی استفاده می‌کنند باید از این تأثیرات آگاه بوده و برای دستیابی استراتژیک، ذخیره و از بین بردن داده‌های مشتریان برای محافظت از شهرت آن‌ها فراتر از آگاهی صرف حرکت کنند (پلانگر و همکاران، ۲۰۱۵). با افزایش وقایع عمده سرقت اطلاعات شخصی -مانند حادثه اخیر فیس‌بوک، که در آن ۷۸ میلیون حساب در معرض دید قرار گرفت (روزن، ۲۰۱۸) -نگرانی‌های مربوط به حریم خصوصی مشتری به‌طورکلی در آینده افزایش می‌یابد.

شرکت‌هایی که داده‌های شخصی مشتریان را جمع‌آوری می‌کنند، موظف‌اند با ایجاد موارد محافظتی خاص برای حفاظت و اطمینان از حریم خصوصی اطلاعات مشتریان، خود را برای نقض غیرمنتظره امنیت داده‌های بزرگ آماده کنند و مشتریان در جریان مداوم اقدامات قرار داشته باشند. مثلاً در سایت شرکت تمامی اقدامات انجام‌شده در معرض دید مشتریان قرار داده شود. از طرفی، طراحی و انجام کمپین‌های ارتباطی که سیاست‌های شفاف اعمال‌شده را منتقل می‌کنند، امری حیاتی است. با این کمپین‌ها اقدامات، عملکرد و شفافیت شرکت به اطلاع مشتریان رسیده، همچنین باعث تقویت نیروی پرقدرت باور هنجاری می‌گردد. این کمپین‌ها که با استراتژی‌های مناسب ایجاد و اجرا می‌گردد، موجب تقویت اعتماد و شهرت شرکت و بهبود روابط با مشتریان می‌گردد.

نقض داده‌ها بسته به محل زندگی مشتریان، ممکن است اثرات متفاوتی بر مصرف‌کنندگان داشته باشد. تعریف و اثرات نقض حریم خصوصی در جمعیت‌های مختلف متفاوت بوده و توجه به این امر حتماً باید مدنظر قرار گیرد. همچنین یافته‌های ما حاکی از آن است که طرح‌های موجود جهت درخواست‌های اجازه برنامه نیز مشکل‌ساز هست، بطوریکه مشتریان دریافت‌کننده خدمات به دلیل نگرانی از درخواست‌های اجازه برنامه‌های بازاریابی، از افشای اطلاعات شخصی خود خودداری می‌کنند و یا اطلاعات نادرست و ناقص ارائه می‌کنند.

شرکت‌ها می‌توانند از یافته‌های این مطالعه استفاده کرده و در ارتباط با ویژگی‌های طراحی درخواست‌های اجازه برنامه تجدیدنظر کنند تا نگرانی‌های مشتریان خود را برای پذیرش درخواست اجازه برنامه کاهش دهند. درخواست‌های غیرضروری و بیش‌ازحد مجاز برنامه تأثیر شدیدی در نگرانی درباره حریم خصوصی کاربران دارد و می‌تواند مانع از پذیرش برنامه‌های بازاریابی و ارتباطی توسط مشتریان شود و شرکت و برنامه‌های ارتباطی آن‌ها به‌عنوان مزاحم قلمداد کنند. درنتیجه، ارائه‌دهندگان خدمات باید اطمینان حاصل کنند که فقط در صورت لزوم و به شکلی توجیه شده با خدمات دارای ارزش‌افزوده مانند ردیابی مکان به دلیل اهداف ناوبری، ارائه خدمات ضروری بهداشتی و.... به اطلاعات شخصی ذخیره‌شده دسترسی پیدا می‌کنند و با ارائه این درخواست‌ها در زمان‌های مناسب که با شرایط و مقتضیات مشتریان متناسب باشد به تأثیرات بزرگ نگرانی‌های حریم خصوصی توجه کرده و آن‌ها را جدی بگیرند.

همانطورکه از نتایج برمی‌آید، نگرانی‌های مربوط به افشای اطلاعات، نظرات همتایان مشتری، فرهنگ حاکم بر جامعه، عدم آگاهی از چرایی ارتباط‌گیری و نحوه استفاده از داده‌های شخصی افراد تأثیر بسیار مهمی در نگرانی‌های مربوط به حریم خصوصی مشتریان دارد. درنهایت نتایج این مطالعه به اینجا می‌رسد که به دلیل رشد سریع برنامه‌های ارتباطی بازاریابی و درخواست‌های بیش‌ازحد مجوز پذیرش ناشی از آن، کاهش نگرانی درباره حریم خصوصی مشتریان، بیش از هر زمان دیگری مهم می‌باشد که می‌بایست از طریق نیروهای ستادی مناسب و حرفه‌ای (که در ارتباط مستقیم با مصرف‌کنندگان هستند) با افزایش اعتماد و آگاهی هرچه بیشتر مشتریان از روند جمع‌آوری اطلاعات و نحوه نگه‌داری آن‌ها می‌توانند به ایجاد اعتماد و اطمینان از صحت و امنیت نگهداری داده‌ها همت گمارند و به ایجاد ادراکات مثبت مشتریان در کنترل‌هایشان بر میزان و نحوه‌ی استفاده، اشخاص و زیرساخت‌های دارای دسترسی از داده‌ها پرداخته شود. مثلاً با ایجاد کاربری‌هایی که خود مشتریان در زمان، میزان، نوع ارائه داده و همچنین در قطع ارتباط و عدم ارائه داده‌های

شخصی قدرت و توانایی بیشتری داشته باشند. هر زمان لازم دانستند اطلاعات مدنظران را ارائه و در غیر این صورت مختار به قطع ارتباط و حذف داده‌ها باشند و مهم‌تر اینکه لزوم ارائه خدمات شخصی‌سازی‌شده‌ی بیشتر که باعث کاهش نگرانی‌های مشتریان دریافت‌کننده خدمات شده و ازاین‌رو میزان بیشتری از دریافت اجازه و ارتباطات بازاریابی با رضایتمندی هرچه بیشتر مشتریان فراهم می‌شود. ارائه خدمات و محصولات دقیقاً متناسب با نیاز مشتری از اهداف اصلی هر شرکتی است و دریافت آن‌ها مطابق با آنچه در نظر دارد رویای هر مشتری هست. لذا در این راستا ممکن است از پاره‌ای از چارچوب‌ها و ممانعت‌های خود عدول کرده و سطح نگرانی‌های خود را کاهش و برقراری ارتباط را بیشتر خواهان باشد. در این راستا می‌بایست حتماً به مسائل و نیازهای فرهنگی، مذهبی، اجتماعی جهت ارتباط‌گیری و حریم خصوصی توجه خاص مبذول شود. گاها مشتریان به خاطر همین شرایط و بعضاً ترس از پاره‌ای مسائل و تابوها از ابراز نظرات و دیدگاه‌های خود طفره رفته و نگرانی‌هایشان افزایش می‌یابد که گاها موجب قطع کامل پل ارتباطی با شرکت‌ها می‌شود.

همانند تمام مطالعات تجربی، ما محدودیت‌های خاص مطالعه خود را تأیید می‌کنیم و علاوه بر یافته‌هایمان می‌توان از این موارد برای تحریک تحقیقات بیشتر در زمینه بازاریابی اجازه‌ای و نگرانی‌های مربوط به حریم خصوصی مشتری استفاده کرد. جامعه‌ی آماری این پژوهش محدود به شرکت‌کنندگانی ایرانی با فرهنگ و تعصبات و دیدگاه ایرانی انجام‌شده است. نظرسنجی در کشورهای دیگر ممکن است به نتایج متفاوتی منجر شود. طبق شاخص ابعاد فرهنگی هافستد، ایران یک فرهنگ میانه است (هافستد، مینکوف، ۲۰۱۰) بنابراین، ممکن است مشتریان از کشورهای دیگر با کاربرانی با فرهنگ‌های صرفاً جمع گرایانه یا صرفاً فردگرایانه، به دلیل علایق فردی و جمعی نگرانی‌های متفاوتی در مورد حفظ حریم خصوصی و پذیرش درخواست‌های اجازه داشته باشند.

ملاحظات اخلاقی

حامی مالی: پژوهش حاضر بدون هیچ‌گونه حمایت مالی از جانب سازمان خاصی انجام‌شده است.

نقش هر یک از نویسندگان: در پژوهش حاضر نویسنده اول خانوم زهرا محمدزاده اماموردیخان در نگارش و ایده پردازی مقاله، جمع‌آوری و تحلیل داده‌ها و نویسنده دوم آقای دکتر علیرضا فرخ بخت فومنی به‌عنوان استاد راهنما و نویسنده سوم آقای دکتر رحمتعلی صابری حقایق به‌عنوان استاد مشاور در ویرایش مقاله نقش داشتند.

تضاد منافع: انجام این پژوهش برای نویسندگان هیچ‌گونه تعارض در منافع را به دنبال نداشته است و نتایج آن به‌صورت کاملاً شفاف و بدون سوگیری، گزارش‌شده است.

تقدیر و تشکر: "این مقاله مستخرج از رساله دکترای تخصصی نویسنده اول در واحد رشت، دانشگاه آزاد اسلامی، رشت، ایران می‌باشد."

منابع

زمانی، عباس، (۱۳۹۴)، شبکه‌های اجتماعی تلفن همراه و نقض حریم خصوصی کاربران، *سومین همایش علمی پژوهشی علوم تربیتی و روانشناسی آسیب‌های اجتماعی و فرهنگی ایران*، COI:PSCONF03-051.

Ajzen, I. (2011). The theory of planned behaviour: Reactions and reflections. *Psychology & Health*, 26(9),1113-1127.

Acquisti, A., Brandimarte, L., Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, 347, 509–514.

Antoci, A., Bonelli, L., Paglieri, F., Reggiani, T., & Sabatini, F. (2019). Civility and trust in social media. *Journal of Economic Behavior & Organization*, 160, 83–99.

Baazeem, R., and Qaffas, A. (2020). The relationship between user religiosity and preserved privacy in the context of social media and cybersecurity. In: Emerging Cyber Threats and Cognitive Vulnerabilities. *Elsevier*, pp. 93–116.

Baek, T. H. and Mariko, M. (2012), "Stay Away from Me: Examining the Determinants of Consumer Avoidance of Personalized Advertising," *Journal of Advertising*, 41, 1, 59–76.

Belanger, F., Crossler, and Robert, E. (2019). Dealing with digital traces: Understanding protective behaviors on mobile devices, *Journal of Strategic Information Systems*, https://doi.org/10.1016/j.jsis.2018.11.002.

Chin, A. G., Harris, M. A., & Brookshire, R. (2018). A bidirectional perspective of trust and risk in determining factors that influence mobile app installation. *International Journal of Information Management*, 39, 49–59. https://doi.org/10.1016/j.ijinfomgt.2017.11.010.

Confessore, N. (2018). Cambridge analytica and facebook: The scandal and the fallout so far. *Retrieved from The New York Times* https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html.

Dzandu, M. (2023). Antecedent, behaviour, and consequence (a-b-c) of deploying the contact tracing app in response to COVID-19:Evidence from Europe,Technological Forecasting and Social Change, Volume 187, February 2023, 122217. https://doi.org/10.1016/j.techfore.2022.122217.

Dinev, T., & Hart, P. (2006). An extended privacy Calculus model for E-commerce transactions. *Information Systems Research*, 17(1), 61–80.

Dogruel, L., Joeckel, S., and Vitak, J., (2017). The valuation of privacy premium features for smartphone apps: The influence of defaults and expert recommendations. *Computers in Human Behavior*, 77, 230–239.

Gerrya, F, Muraszki ewiczb J, aIannelli, O. (2018). The drive forvirtual (online) courts and the failure to consider obliganid entification ,protection and privacy of victims. *Journal of computer law & security review*. Pp. 1–8. https://doi.org/10.1016/j.clsr.2018.06.002.

Goodin, S. (1999). *Permission Marketing to Turn Strangers Into Friends and Friends into Customers.* New York: Simon and Schuster Rockefeller. ISBN 0-684-83633-5. www.SimonSats.com.

Guo, J., Li, N., and Wu, Y. (2020). Examining help requests on social networking sites: integrating privacy perception and privacy calculus perspectives. *Electronic Commerce*. Res. Appl. 39, 100828.

Heravi, A., Mubarak, S., and Choo, K.K.R., (2018). Information privacy in online social networks: uses and gratification perspective. *Computers in Human Behavior*, 84, 441–459.

Hirschprung, R., Toch, E., Bolton, F., and Maimon, O. (2016). A methodology for estimating the value of privacy in information disclosure systems. *Computers in Human Behavior*, 61,443–453.

Hofstede, G., Hofstede, G. J., & Minkov, M. (2010). Cultures and organizations: Software of the mind – *Intercultural cooperation and its importance for survival* (3rd ed.). New York:McGraw-Hill.

Jozani, M. Ayaburi, E. Myung, K. Kim-Kwang, C. R. (2020). Privacy Concerns and Benefits of Engagement with Social Media-enabled Apps: A Privacy Calculus Perspective. *Computers in Human Behavior*, https://doi.org/10.1016/j.chb.2020.106260.

Kahn, C., & Ingram, D. (2018). Americans less likely to trust Facebook than rivals on personal data. *Retrieved from Reuters* https://www.reuters.com/article/us-usa-facebook-poll/americans-less-likely-to-trust-facebook-than-rivals-on-personal-data-reuters-ipsospoll-idUSKBN1H10K3.

Kent, R., & Brandal, H. (2003). Improving email response in a permission marketing context. *International Journal of Market Research*, 45(4), 489–503.

Kim, D., Park, K., Park, Y., Ahn, J.H., (2019). Willingness to provide personal information:Perspective of privacy calculus in IoT services. *Computers in Human Behavior*, 92, 273–281.

Krafft, M, A., Christine, M., and Verhoef, P. C. (2017). Permission Marketing and Privacy Concerns — Why Do Customers (Not) Grant Permissions?. *Journal of Interactive Marketing.* 39,39 – 54. http://dx.doi.org/10.1016/j.intmar.

Lidynia, C. , Brauner, P., and Ziefle, M. (2017). A Step in the Right Direction–Understand- ing Privacy Concerns and Perceived Sensitivity of Fitness Trackers. *Springer*, pp. 42–53 .

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., and Pattinson, M. (2017), [Internet]. Individual Differences and Information Security Awareness, 69. Comput Human Behav, pp. 151–156.

Martin, K.D., Borah, A., and Palmatier, R.W. (2017). Data Privacy: effects on Customer and Firm Performance. J. Mark. 81, 36–58. https://doi.org/10.1509/jm.15.0497.

Mohammadzadeh Emamverdikhan, Z., Farokhbakht Fumani A., Saberi Haghayegh R. (2022), Factors affecting parent permission to accept the marketing of companies providing services (kindergartens) with an emphasis on the role of privacy in childrens mental health . *Journal of Child Ment Health*. (2022), 9(3): 136-152. Doi:10.525447/jcmh.9.3.11.

Okazaki, S., Eisend, M., Plangger, K., Ruyter, K. and Dhruv, G. (2020). Understanding the Strategic Consequences of Customer Privacy A Concerns:Meta-Analytic Review. *Journal of Retailing*, -754, https://doi.org/10.1016/j.jretai.2020.05.007.

Paul, C., Scheibe, K.P., and Nilakanta, S. (2020). Privacy Concerns regarding Wearable IoT Devices: how it is Influenced by GDPR? In: Proceedings of the 53rd Hawaii *In- ternational Conference on System Sciences*, p. 10.

Park, J. and Jung, Y. (2018). An investigation of relationships among privacy concerns, affective responses, and coping behaviors in location-based services. *International Journal of Information Management*, 43, 15–24. https://doi.org/10.1016/j.ijinfomgt.2018.05.007.

Plangger, Kirk and Richard T. W. (2015). Balancing customer privacy, secrets, and surveillance: Insights and management,Business Horizons, 58 (6), 625–33.

Publilius, S. (2018). Quotable quote. Retrieved from https://www.goodreads.com/quotes/503006-trust-like-the-soul-never-returns-once-it-is-gone.

Raynes-Goldie, K. (2010). Aliases, creeping, and wall cleaning: Understanding privacy in the age of Facebook. First Monday 15.

Rosen, G. (2018). Security Update, Facebook Newsroom. [available at https://newsroom.fb.com/news/2018/09/security-update/].

Shiau, W.-L., Dwivedi, Y. K., & Lai, H.-H. (2018). Examining the core knowledge on facebook. *International Journal of Information Management*, 43, 52–63.

Tanoglu, I., Basoglu, N., Daim, T., (2010). Exploring technology diffusion: case of information technologies. *International Journal of Information Technology and Decision Making* 9 (2), 195–222.

Widjaja, A. E., Chen, J.V., Sukoco, B.M., and Ha, Q.A. (2019). Understanding users' willingness to put their personal information on the personal cloud-based storage applications: An empirical study. *Computers in Human Behavior* 91, 167–185.

Wottrich, V. M., Reijmersdal, E. A., & Smit, E. G. (2018). The privacy trade-off for mobile app downloads: The roles of app value, intrusiveness, and privacy concerns. *Decision Support Systems*, 106, 44–52. https://doi.org/10.1016/j.dss.2017.12.003.

Xie, Y., Keh, and H.T., (2016). Taming the blame game: using promotion programs to counter product-harm crises. J. Advert. 45 (2), 1–16.

Youn, S., Kim, S. (2019). Understanding ad avoidance on Facebook: antecedents and outcomes of psychological reactance. *Comput. Hum. Behav*. 98, 232–244.

Zhang, R., Chen, J.Q., and Lee, C.J. (2013). Mobile commerce and consumer privacy concerns. *Journal of Computer Information Systems*, 53(4), 31-38.

Zlatolas, L. N., Welzer, T., Heričko, M., & Holbl, M. (2015). Privacy antecedents for SNS self-disclosure: The case of Facebook. *Computers in Human Behavior*, 45, 158–167. https://doi.org/10.1016/j.chb.2014.12.012.