مدیریت دولتی
Journal of Public Administration
دانشکدهٔ مدیریت دانشگاه تهران
دورهٔ ۸، شمارهٔ ۴
زمستان ۱۳۹۵
صص. ۶۴۴- ۶۱۷

الگوی ریسک‌های ورود سازمان‌های عمومی به شبکه‌های اجتماعی

سمیه رمضان لواسانی[۱]، مهدی خیراندیش[۲]

چکیده: از دیدگاه نظری هر فعالیتی با درجه‌ای از ریسک همراه است. ریسک را نمی‌توان به‌طور کامل حذف کرد؛ بنابراین نگرش علمی به مسئلهٔ ریسک چیزی جز مدیریت آن نیست. شبکه‌های اجتماعی مجازی به‌لحاظ عمومیت یافتن میان کاربران در پهنهٔ جغرافیایی درون مرزهای ملی، تبدیل شدن به ابزار ارتباطی خصوصی و فارغ بودن از هر نوع کنترل جامع از سوی مراجع قدرت، به‌وسیله‌ای بی‌بدیل در عرصهٔ ارتباطات تبدیل شده‌اند و زمینه‌های تأثیرگذاری خارج از کنترل دولت‌ها و نهادهای قدرت را در جوامع به‌وجود آورده‌اند. گسترش روزافزون این شبکه‌ها علی‌رغم مزیت‌های انکارناپذیر، آسیب‌هایی را نیز برای سازمان‌های عمومی در صورت عدم مدیریت اثربخش آن به همراه خواهد داشت. هدف پژوهش حاضر شناسایی ریسک‌های ورود سازمان‌های عمومی به شبکه‌های اجتماعی است. این پژوهش از نظر هدف، اکتشافی و از نظر نوع استفاده، کاربردی است. بدین منظور، روی نمونه‌ای از خبرگان، مدیران و کارشناسان شهرداری منطقهٔ ۲۲ تهران مطالعاتی انجام شد. تحلیل داده‌ها به‌کمک تحلیل عاملی اکتشافی، تأییدی و آزمون تی نشان داد ریسک‌های اطلاعاتی، اخلاقی، امنیتی، نظارتی، راهبردی و بهره‌وری از مهم‌ترین ریسک‌های ورود سازمان‌های عمومی به شبکه‌های اجتماعی محسوب می‌شوند.

واژه‌های کلیدی: *ریسک ورود، سازمان‌های عمومی، شبکه‌های اجتماعی، شهرداری منطقهٔ ۲۲ تهران.*

۱. کارشناس ارشد مدیریت دولتی، دانشکدهٔ مدیریت، دانشگاه آزاد اسلامی واحد قزوین، قزوین، ایران
۲. دانشیار مدیریت دولتی، دانشکدهٔ مدیریت، دانشگاه هوایی شهید ستاری، تهران، ایران

تاریخ دریافت مقاله: ۱۳۹۵/۰۶/۰۱
تاریخ پذیرش نهایی مقاله: ۱۳۹۵/۰۹/۰۳
نویسندهٔ مسئول مقاله: مهدی خیراندیش
E-mail: kheirandish@ssau.ac.ir

مقدمه

جوامع مختلف تحت تأثیر تحولات عظیم علمی ـ فنی به‌سمت جامعهٔ اطلاعاتی یا جامعهٔ شبکه‌ای حرکت می‌کنند. جامعهٔ شبکه‌ای، جامعه‌ای است که ساختار آن متأثر از فناوری است. در جامعهٔ شبکه‌ای، جوامع با چالش‌هایی مانند نابرابری اجتماعی، هویت‌های جدید، تمایزپذیری و شالوده‌شکنی نهادهایی نظیر دولت و فرصت‌هایی مانند نقش اینترنت و شبکه‌های اجتماعی در پژوهش، خلاقیت، تعامل و همزیستی جهانی، شکل‌گیری هویت سیال و... روبه‌رو شده‌اند. شبکه‌های اجتماعی مجازی به‌لحاظ عمومیت یافتن میان کاربران در پهنهٔ جغرافیاییِ درون مرزهای ملی، تبدیل شدن به ابزار ارتباطی خصوصی و فارغ بودن از هر نوع کنترل جامع از سوی مراجع قدرت، به‌وسیله‌ای بی‌بدیل در عرصهٔ ارتباطات تبدیل شده‌اند و زمینه‌های تأثیرگذاری خارج از کنترل دولت‌ها و نهادهای قدرت را در جوامع به‌وجود آورده‌اند (معمار، عدلی‌پور و خاکسار، ۱۳۹۱).

شبکه‌های اجتماعی به‌طور روزافزون به‌عنوان ابزارهای مؤثری برای مشارکت فعال شهروندان در فرایندهای تصمیم‌گیری، سیاست‌گذاری و اطلاع‌رسانی در سطوح اجتماعی و سیاسی مدنظر قرار می‌گیرند. این نوع نگرش نسبت به این رسانه‌ها از ویژگی‌های خاص آنها نشئت می‌گیرد که بستر اشتراک‌گذاری اطلاعات و مشارکت فراگیر را فراهم آورده و ارتباط برخط میان سازمان‌های عمومی و شهروندان را تسهیل می‌کند (خان، یون و پارک، ۲۰۱۲). با توجه به مزیت‌های استفاده از فناوری‌های موجود در رسانه‌های جدید، بسیاری از سازمان‌ها نسبت به پیاده‌سازی آنها در زمینه‌هایی مانند ساختار داخلی، سیستم‌های مدیریت و تبلیغات و روابط عمومی اقدام کرده‌اند (گو و یو، ۲۰۱۶). بخش عمومی به‌دلایل گوناگونی چون تسهیل ارتباطات و تعاملات میان دولت و شهروندان، اطلاع‌رسانی و فراهم آوردن شرایط استفاده از برخی خدمات عمومی و مجراهایی جدید برای مشارکت سیاسی افراد از رسانه‌های اجتماعی استفاده می‌کنند (استینکمپ و هیدکلارک، ۲۰۱۴). اما هر فناوری نوین، در کنار مزیت‌هایی خود می‌تواند آسیب‌ها یا ریسک‌هایی را به همراه داشته باشد. اگرچه منافع و نویدهای بسیاری در رسانه‌های اجتماعی (و به‌طور خاص شبکه‌های اجتماعی) و فناوری‌های مرتبط وجود دارد، خطرها و ریسک‌های مختلفی نیز با آنها همراه است (پیکازو، گوترز و لونا، ۲۰۱۲) که شناسایی آنها به‌منظور بهبود مدیریت این روند لازم و ضروری است.

در ایران، به دلیل دید نه چندان مثبتی که در گذشته نسبت به رسانه‌های مدرن وجود داشت، به استفاده از آنها در بخش عمومی زیاد توجه نمی‌شد. این در حالی است که رسانه‌های اجتماعی (در اشکال مختلف آن از جمله شبکه‌های اجتماعی)، قابلیت جذب مجموعهٔ گسترده‌ای از کاربران و

تشویق آنها به مشارکت را دارند. امروزه، کشور ایران در حال توسعهٔ دولت الکترونیک است و بر این اساس، رویکردها نسبت به رسانه‌های اجتماعی در چند سال اخیر تغییر کرده و این امر حضور قدرتمندتر سازمان‌های عمومی در عرصهٔ این رسانه‌ها را در آینده‌ای نزدیک نوید می‌دهد. با وجود این، هر فناوری نوینی در کنار مزیت‌های کم و زیاد خود می‌تواند آسیب‌ها یا ریسک‌هایی را به همراه داشته باشد. کنترل ناکافی احراز هویت، درخواست اتصال به سایت‌های جعلی، کلاهبرداری اینترنتی، نشت (درز) اطلاعات، جریان‌های تزریق کدهای مخرب، صحت نداشتن اطلاعات، کاهش بهره‌وری کارکنان، نشت اطلاعات از سوی کارکنان، نرم‌افزارهای مخرب، بدگویی آزادانه در فضایی باز و کلاهبرداری توسط کلاهبرداران اینترنتی از ریسک‌هایی است که در پژوهش ویلسون (۲۰۰۹) به آنها اشاره شده است. همچنین، نظرهای منفی نوشته‌شده توسط کارمندان، استفادهٔ بیش از حد از رسانه‌های اجتماعی در طول ساعات کار، ناتوانی برخی کارمندان در حفظ امنیت موبایل و تبلت خود، نشر اطلاعات محرمانهٔ سازمان به‌صورت سهوی یا عمدی و کاهش عملکرد کارکنان، از مهم‌ترین ریسک‌های ورود سازمان‌ها به رسانه‌های اجتماعی بر اساس تحقیق فیلد و چلیاه (۲۰۱۲) محسوب می‌شوند. در این رابطه، گریفین (۲۰۱۴) نیز به ریسک‌های مانند نبود نظارت کافی، افشای اطلاعات محرمانه، هدایت نامناسب رسانه‌های اجتماعی توسط مدیران و کارکنان، سیاست‌ها و رویه‌های ضعیف مرتبط با رسانه‌های اجتماعی، ریسک‌های بالقوهٔ عملیاتی رسانه‌های اجتماعی اشاره کرده است.

از آنجا که اغلب فناوری‌هایی که در سازمان‌های عمومی کشور استفاده می‌شوند، وارداتی هستند و نیمهٔ پنهان آسیب‌های احتمالی این گونه فناوری‌ها برای بهره‌وران داخلی ناشناخته است و با توجه به استفادهٔ روزافزون سازمان‌های عمومی کشور از شبکه‌های اجتماعی، آگاهی از ریسک‌های استفاده از این شبکه‌ها لازم و ضروری است تا با شناخت صحیح ریسک‌ها، سازمان‌های عمومی از منافع این فناوری بهره‌مند شوند.

با توجه به پیشرو بودن سازمان شهرداری در استفاده از شبکه‌های اجتماعی در امور جاری خود، این پژوهش تلاش کرده است بر مبنای ادبیات و پژوهش‌های پیشین و با رویکردی جامع، به ارائهٔ الگوی ریسک‌های ورود سازمان‌های عمومی به شبکه‌های اجتماعی در شهرداری منطقهٔ ۲۲ تهران اقدام کند. هدف این پژوهش شناسایی آسیب‌ها و ریسک‌هایی است که سازمان‌های عمومی هنگام استفاده از شبکه‌های اجتماعی در انجام امور و فعالیت‌های خود با آنها روبه‌رو می‌شوند. بررسی جامع ادبیات مرتبط و انجام این تحقیق در مراحل اولیهٔ توجه به موضوع ریسک‌های استفاده از شبکه‌های اجتماعی توسط سازمان‌ها در محافل دانشگاهی و دستگاه‌های اجرایی ایران، می‌تواند از نوآوری این تحقیق محسوب شود.

پیشینهٔ نظری پژوهش

در سال ۱۹۵۴ بارنز برای نخستین بار اصطلاح شبکه‌های اجتماعی را مطرح کرد و از آن پس به‌سرعت به شیوه‌ای کلیدی در مطالعات تبدیل شد. در تئوری شبکهٔ اجتماعی سنتی، یک شبکهٔ اجتماعی به این صورت تعریف می‌شود: مجموعه‌ای از نهادهای اجتماعی شامل مردم و سازمان‌ها که به‌وسیلهٔ مجموعه‌ای از روابط معنادار اجتماعی به هم متصل هستند و با هم در به اشتراک گذاشتن ارزش‌ها تعامل دارند. شکل سنتی خدمت شبکهٔ اجتماعی بر انواع روابط مانند دوستی ها و روابط چهره به چهره متمرکز است؛ اما خدمات شبکهٔ اجتماعی، امروزه بیشتر بر جامعهٔ مجازی آنلاین و ارتباطات رایانه‌ای واسط تمرکز دارند (معمار و همکاران، ۱۳۹۱). شبکه‌های اجتماعی اینترنتی پایگاه یا مجموعهٔ پایگاه‌هایی هستند که امکانی فراهم می‌آورند تا کاربران بتوانند علاقه‌ها، افکار و فعالیت‌های خود را با دیگران به اشتراک بگذارند و دیگران هم در این افکار و فعالیت‌ها با آنان سهیم شوند. هر شبکهٔ اجتماعی، مجموعه‌ای از سرویس‌های مبتنی بر وب است که به اشخاص امکان می‌دهد برای خودشان توصیفات عمومی یا خصوصی ایجاد کنند یا با سایر اعضای شبکه ارتباط برقرار کنند، منابع خود را با آنها به اشتراک بگذارند و از میان توصیفات عمومی سایر افراد برای یافتن ارتباطات جدید استفاده کنند (بئید و والیسون، ۲۰۰۷). به‌طور کلی، در تعریف شبکه‌های اجتماعی می‌توان گفت شبکه‌های اجتماعی سایت‌هایی هستند که از طریق موتور جست‌وجوگر و اضافه‌کردن امکاناتی مانند چت، ایمیل و... ویژگی اشتراک‌گذاری را به کاربران خود ارائه می‌دهند. شبکه‌های اجتماعی، محل گردهمایی صدها میلیون کاربر اینترنت است که بدون توجه به مرز، زبان، جنس و فرهنگ، به تعامل و تبادل اطلاعات می‌پردازند. در واقع، شبکه‌های اجتماعی برای افزایش و تقویت تعاملات اجتماعی در فضای مجازی طراحی شده‌اند. به‌طور کلی، از طریق اطلاعاتی مانند عکس کاربر، اطلاعات شخصی و علایق که روی پروفایل افراد قرار می‌گیرد، برقراری ارتباط تسهیل می‌شود. کاربران می‌توانند پروفایل دیگران را ببینند و از طریق برنامه‌های کاربردی مختلف مانند ایمیل و چت با یکدیگر ارتباط برقرار کنند (پمپک، ۲۰۰۹).

ریسک‌های ورود به شبکه‌های اجتماعی

بررسی‌ها نشان می‌دهد که در زمینهٔ آثار، تبعات و ریسک‌های شبکه‌های اجتماعی، پژوهش‌هایی صورت گرفته است. از جملهٔ این ریسک‌ها می‌توان به افشای غیرعمدی اطلاعات محرمانه (گریفین، ۲۰۱۴؛ اندرسون و اسلمپ، ۲۰۱۱)، انتشار هرزنامه (محکم‌کار و حلاج، ۱۳۹۳)، انتشار اطلاعات کذب، نادرست و بدون منبع موثق (پونجابی، ۲۰۱۴؛ دیستاسو، مک‌کور کیندال و رایت،

۲۰۱۱)، فقدان اعتبار و صداقت داده‌ها (بلبی، ۲۰۱۵)، نقض یا تهدید حریم خصوصی افراد (محکم‌کار و حلاج، ۱۳۹۳؛ روزنبلوم، ۲۰۰۷)، انتشار نرم‌افزارهای مخرب (بلبی، ۲۰۱۵؛ آندرونیکاکیس، ۲۰۱۲؛ ویلسون، ۲۰۰۹)، تهدید حریم خصوصی، برند و اعتبار سازمان (فیلد و چلیاه، ۲۰۱۲؛ دیستاسو و همکاران، ۲۰۱۱)، انتشار ویروس‌های مختلف (آندرونیکاکیس، ۲۰۱۲) و سرقت اطلاعات (آندرونیکاکیس، ۲۰۱۲؛ پیکازو و همکاران، ۲۰۱۲) اشاره کرد. آندرونیکاکیس (۲۰۱۲) خطر استفاده از رسانه‌های اجتماعی را برای سازمان‌ها در سرقت هویت (سرقت داده‌های ورودی، حملهٔ جعل هویت و حملهٔ هجوی)، انتشار تصادفی اطلاعات، انتشار بدافزارها و هرزنامه‌های رسانه‌های اجتماعی، رعایت‌نکردن اخلاق (در شیوه‌های جمع‌آوری داده‌ها و عدم افشای وابستگی به سازمان)، رعایت‌نکردن قوانین و مقررات و تهدید اعتبار (لکه‌دار کردن اعتبار، نتیجهٔ معکوس کمپین‌های رسانه‌های اجتماعی و تبلیغات بد) بیان کرد. از نظر پیکازو و همکارانش (۲۰۱۲)، ریسک‌های رسانه‌های اجتماعی در زمینه‌های عمومی، چارچوب نهادی، مشارکت‌ها و شبکه‌های درون سازمانی، ساختار و فرایندهای سازمانی، اطلاعات و داده‌ها و فناوری خلاصه می‌شود. مطالعات فیلد و چلیاه (۲۰۱۲) نشان داد، نظرهای منفی پست‌شدهٔ کارمند بر شبکهٔ آنلاین در خارج از ساعات کار و استفادهٔ بیش از حد کارکنان از شبکه‌های اجتماعی طی ساعات کار، موجب کاهش تمرکز کاری، کاهش بازدهی و در نهایت کاهش بهره‌وری آنها می‌شود و تنش‌هایی را در محیط کار به‌وجود می‌آورد. وی همچنین استفاده‌نکردن از مزیت‌های شبکه‌های اجتماعی به‌دلیل ترس از مواجهه با شرایط منفی، صدمه به شهرت شرکت با توهین از سوی کارمندان به سایر کاربران در جهت دفاع از شرکت، نظرهای منفی مشتریان (ارباب رجوع)، دسترسی شخص ثالث غیرمجاز به اطلاعات سازمان به‌دلیل ناتوانی کارمند در حفاظت از تلفن همراه یا تبلت خود و افشای اطلاعات محرمانهٔ سازمان به‌صورت سهوی یا عمدی را از مهم‌ترین خطرهای استفادهٔ نادرست از رسانه‌های اجتماعی می‌داند.

چی (۲۰۱۱) در پژوهشی با توجه به گزارش انجمن کسب‌وکار ایمن در سال ۲۰۰۹ بیان می‌کند، تهدیدهای شناسایی‌شده در حوزهٔ استفاده از رسانه‌های اجتماعی توسط سازمان‌ها شامل کنترل ناکافی در احراز هویت، اتصال به اسکریپت‌های (برنامه‌نویسی) سایت، درخواست اتصال به سایت‌های جعلی، فیشینگ (کلاهبرداری اینترنتی)، درز اطلاعات، جریان‌های تزریق کدهای مخرب، صحت‌نداشتن اطلاعات و سامانهٔ امنیتی ناکافی هستند.

ایلانارزی (۲۰۱۰) بر اساس مطالعات گروه‌های نظارت و کنترل فناوری اطلاعات، ریسک‌های رسانه‌های اجتماعی برای سازمان‌ها را ویروس‌ها و بدافزارها، درز یا سرقت اطلاعات، ربودن برند، کنترل نکردن محتوای سازمان، انتظارات غیرواقعی و سوء مدیریت ارتباطات الکترونیکی می‌داند.

بلبی (۲۰۱۵) ریسک‌های دوازده‌گانهٔ رسانه‌های اجتماعی برای سازمان‌ها را در خطای انسانی؛ فرایندهای قانونی؛ جمع‌آوری، حفاظت و امنیت داده‌ها؛ پذیرش؛ مالی؛ عملیاتی؛ اعتبار؛ درصد بازگشت سرمایه‌گذاری؛ هزینه؛ پهنا و عقب‌ماندن می‌داند.

از نظر گریفین (۲۰۱۴) ریسک‌هایی همانند نبود نظارت کافی، افشای اطلاعات محرمانه، هدایت نامناسب رسانه‌های اجتماعی توسط مدیران و کارکنان، سیاست‌ها و رویه‌های ضعیف مرتبط با رسانه‌های اجتماعی، ریسک‌های بالقوهٔ عملیاتی، از رسانه‌های اجتماعی نشئت می‌گیرند.

بر اساس پژوهش اشفورد (۲۰۱۳)، بیشتر افراد و کسب‌وکارها از مزیت‌های این شبکه‌های اجتماعی برای رسیدن به مردم و ارتباط جهانی با آنها استفاده می‌کنند. با وجود این، همراه با این مزیت‌ها، چالش‌ها و ریسک‌های امنیتی روزافزونی نیز پیش روی کاربران شبکه‌های اجتماعی وجود دارد. اغلب این خطرها و تهدیدها به مسائل حریم خصوصی و اشاعهٔ اطلاعات نادرست مربوط می‌شود. غیر از حریم خصوصی زندگی شخصی افراد، نگرانی حریم خصوصی کسب‌وکارها باعث آسیب‌پذیرتر شدن سازمان می‌شود؛ زیرا کارمندان ممکن است به افشای اطلاعات خصوصی سازمان روی شبکه‌های اجتماعی اقدام کنند. علاوه بر این، در زمان استفاده از شبکه‌های اجتماعی، احتمال فاش شدن اطلاعات خصوصی شرکت‌ها به‌صورت عمومی افزایش می‌یابد و باعث قرار گرفتن شرکت‌ها در معرض ریسک‌های امنیتی جدی می‌شود، زیرا اطلاعات به‌راحتی بین شبکه‌های اجتماعی منتقل می‌شوند (پونجابی، ۲۰۱۴).

پیشینهٔ تجربی پژوهش

عبادی (۱۳۹۵) در پژوهشی به بررسی وضعیت بلوغ حکمرانی الکترونیک در پورتال وزارتخانه‌های کشور پرداخت. نتایج مبین آن است که اغلب پورتال‌ها در سطوح اولیهٔ بلوغ مدل‌های خدمات‌رسانی الکترونیکی قرار دارند و اطلاعات را بیشتر از خدمات ارائه می‌دهند.

سهرابی، رئیسی و فروزنده (۱۳۹۵) در تحقیقی به طبقه‌بندی و تحلیل عوامل مؤثر بر استفادهٔ کارآمد از سیستم‌های اطلاعاتی یکپارچه در سازمان‌های دولتی ایران پرداختند. نتیجهٔ نهایی نشان‌دهندهٔ اثرگذاری بسیار زیاد دو عامل میزان تعهد و اشتیاق کارکنان و سطوح مدیریتی دستگاه دولتی و زیرساخت‌های فنی و فرایندی بر استفادهٔ کارآمد از سیستم‌های اطلاعاتی یکپارچه است. یعقوبی، ابراهیم‌پور و شاکری (۱۳۹۵) در پژوهشی الگوی نیازهای کاربران دولت همراه در ایران را ارائه دادند. یافته‌ها حاکی از آن است که تراکنش‌های کارا و اثربخش شامل زمان، امنیت و حریم خصوصی، قابلیت اعتماد و هزینه، مهم‌ترین و ضروری‌ترین بُعد برای دستیابی به خدمات موفق دولت همراه است. به‌دنبال آن کیفیت خدمات شامل ضمانت و تضمین،

مسئولیت‌پذیری و قابلیت اطمینان؛ ارتباط متقابل دولت و شهروندان شامل صحت محتوا و شفاف‌سازی در تراکنش‌های مالی، قابلیت تعامل‌پذیری در سطوح مختلف و شهروندمداری؛ ارزش درک‌شده شامل سودمندی درک‌شدهٔ خدمات و سهولت درک‌شدهٔ استفاده از خدمات و در نهایت عاملیت (کارکردگرایی) شامل قابلیت دسترسی، خودکارآمدی و واسط کاربری از نیازهای کاربران دولت همراه در ایران به‌شمار می‌روند.

سلیمی‌فرد، رضایی و رجبی (۱۳۹۴) در پژوهشی به شناسایی و اولویت‌بندی معیارهای مدیریت ارتباط با شهروندان در سازمان‌های دولتی پرداختند. یافته‌های پژوهش نشان داد معیارهای موقعیتی در رتبهٔ نخست قرار دارد و رتبه‌های بعدی به‌ترتیب به عامل رفتاری، روان‌شناختی و جمعیت‌شناختی اختصاص دارد. محکم‌کار و حلاج (۱۳۹۳) شکل‌گیری و ترویج سریع شایعات و اخبار کذب، تبلیغات ضد دینی و القای شبهات، نقض حریم خصوصی افراد، انزوا و دور ماندن از محیط‌های واقعی اجتماع و تأثیرات منفی رفتاری را از پیامدهای منفی شبکه‌های اجتماعی دانستند.

روزنبلوم (۲۰۰۷) در پژوهش خود نشان داد که در انجمن‌های عمومی، ریسک تهدیدکنندهٔ حریم خصوصی بالقوه برای افراد و شرکت‌ها وجود دارد؛ زیرا دسترسی به این انجمن‌ها به‌نسبت آسان است و محتوای ارسال‌شده را می‌توان به‌راحتی مشاهده کرد.

ویلسون (۲۰۰۹) در پژوهش خود به کاهش بازدهی و بهره‌وری کارکنان، نشت اطلاعات از سوی کارکنان، نرم‌افزارهای مخرب، بدگویی آزادانه در فضایی باز، کلاهبرداری توسط کلاهبرداران اینترنتی اشاره کرد.

بر مبنای تحقیق دیستاسو و همکارانش (۲۰۱۱) بزرگ‌ترین چالش‌ها و بحران‌های مربوط به سازمان‌ها در استفاده از رسانه‌های اجتماعی عبارت‌اند از: کمبود کنترل رسانهٔ اجتماعی، نداشتن اطلاعات کامل از عقیدهٔ افراد دربارهٔ سازمان در این رسانه‌ها، نشت (درز) مالکیت معنوی، انتقاد از مدیریت یا شرکت، رفتار اشتباه کارمندان که نام و اعتبار سازمان را زیر سؤال می‌برد و انتشار اطلاعات اشتباه. اندرسون و اسلمپ (۲۰۱۱) در پژوهشی در این رابطه به ریسک‌های انتشار داده‌های حساس، تبعیت نکردن از قوانین، از دست دادن اعتبار شرکت، زیان مالی، از دست دادن اعتبار و امنیت شخصی اشاره کردند.

بر اساس مطالعات نگارندگان از ادبیات مرتبط، ریسک‌های ورود سازمان‌ها به شبکه‌های مجازی را می‌توان در ۴۴ مورد به‌شرح جدول ۱ خلاصه کرد. شایان ذکر است بیشتر پژوهشگران بر ابعاد هفت‌گانهٔ مطالعهٔ آندرونیکاکیس توافق دارند. بر این اساس تلاش شد ضمن پوشش حداکثری ریسک‌های این مطالعه، سایر موارد در قالب عناوینی تلخیص شوند (جدول ۱).

جدول ۱. ریسک‌های شناسایی‌شده

محقق یا نظریه‌پرداز	ریسک شناسایی‌شده
آندرونیکاکیس (۲۰۱۲)	انتشار تصادفی اطلاعات محرمانه
گریفین (۲۰۱۴)	افشای غیرعمد و سهوی اطلاعات محرمانه
فیلد و چلیاه (۲۰۱۲)	
اندرسون و اسلمپ (۲۰۱۱)	
انجمن کسب‌وکار ایمن (۲۰۰۹)	
ویلسون (۲۰۰۹)	
محکم کار و حلاج (۱۳۹۳)	انتشار هرزنامه‌ها
آندرونیکاکیس (۲۰۱۲)	
محکم کار و حلاج	انتشار اطلاعات کذب، نادرست و بدون منبع موثق
پونجابی (۲۰۱۴)	
اشفورد (۲۰۱۳)	
دیستاسو و همکاران (۲۰۱۱)	
ایلانارزی (۲۰۱۰)	
انجمن کسب‌وکار ایمن (۲۰۰۹)	
بلبی (۲۰۱۵)	فقدان اعتبار و صداقت داده‌ها
پیکازو و همکاران (۲۰۱۲)	
انجمن کسب‌وکار ایمن (۲۰۰۹)	
آندرونیکاکیس (۲۰۱۲)	رعایت‌نکردن مسائل اخلاقی در شیوه‌های جمع‌آوری داده‌ها
آندرونیکاکیس (۲۰۱۲)	رعایت‌نکردن مسائل اخلاقی در عدم افشای وابستگی به سازمان
محکم کار و حلاج (۱۳۹۳)	نقض یا تهدید حریم خصوصی افراد
اندرسون و اسلمپ (۲۰۱۱)	
روزنبلوم (۲۰۰۷)	
پونجابی (۲۰۱۴)	انتشار اطلاعات خصوصی سازمان به‌صورت عمدی و آگاهانه
گریفین (۲۰۱۴)	
فیلد و چلیاه (۲۰۱۲)	
ایلانارزی (۲۰۱۰)	
انجمن کسب‌وکار ایمن (۲۰۰۹)	
ویلسون (۲۰۰۹)	
بلبی (۲۰۱۵)	نشت اطلاعات محرمانه مشتری (ارباب رجوع)
بلبی (۲۰۱۵)	انتشار نرم‌افزارهای مخرب (بدافزارها)
آندرونیکاکیس (۲۰۱۲)	
ایلانارزی (۲۰۱۰)	
ویلسون (۲۰۰۹)	
انجمن کسب‌وکار ایمن (۲۰۰۹)	

ادامهٔ جدول ۱

محقق یا نظریه‌پرداز	ریسک شناسایی‌شده
انجمن کسب‌وکار ایمن (۲۰۰۹)	تغییر و دستکاری اطلاعات کاربر و پایگاه دادهاز طریق نرم افزارهای مخرب (بدافزار)
ایلانارزی (۲۰۱۰)	انتشار ویروس‌ها
بلبی (۲۰۱۵)	تهدید حریم خصوصی، برند و اعتبار سازمان
آندرونیکاکیس (۲۰۱۲)	
فیلد و چلیاه (۲۰۱۲)	
اندرسون و اسلمپ (۲۰۱۱)	
دیستاسو و همکاران (۲۰۱۱)	
ایلانارزی (۲۰۱۰)	
روزنبلوم (۲۰۰۷)	
آندرونیکاکیس (۲۰۱۲)	نتیجهٔ معکوس کمپین‌های رسانه‌های اجتماعی
آندرونیکاکیس (۲۰۱۲)	تبلیغات بد
فیلد و چلیاه (۲۰۱۲)	نظرهای منفی کارمندان ناراضی سازمان
ویلسون (۲۰۰۹)	
فیلد و چلیاه (۲۰۱۲)	نظرات منفی مشتری (ارباب رجوع)
ویلسون (۲۰۰۹)	
بلبی (۲۰۱۵)	هک‌شدن سایت، کانال یا گروه سازمان
انجمن کسب‌وکار ایمن (۲۰۰۹)	
بلبی (۲۰۱۵)	اعتماد نامعقول کارمندان سازمان به کاربران رسانه‌های اجتماعی
گریفین (۲۰۱۴)	هدایت نامناسب رسانه‌های اجتماعی توسط کارکنان سازمان
پیکازو و همکاران (۲۰۱۲)	بی‌عتماد عمومی نسبت به سازمان
پیکازو و همکاران (۲۰۱۲)	انتقاد عمومی نسبت به سازمان یا مدیریت سازمان
دیستاسو و همکاران (۲۰۱۱)	
آندرونیکاکیس (۲۰۱۲)	سرقت اطلاعات
پیکازو و همکاران (۲۰۱۲)	
ایلانارزی (۲۰۱۰)	
آندرونیکاکیس (۲۰۱۲)	حمله به سازمان از طریق جعل هویت آن
پیکازو و همکاران (۲۰۱۲)	
آندرونیکاکیس (۲۰۱۲)	حمله هجوی به سازمان
فیلد و چلیاه (۲۰۱۲)	دسترسی افراد غیرمجاز به اطلاعات سازمانی
انجمن کسب‌وکار ایمن (۲۰۰۹)	
بلبی (۲۰۱۵)	کلاهبرداری اینترنتی
ویلسون (۲۰۰۹)	
انجمن کسب‌وکار ایمن (۲۰۰۹)	

ادامهٔ جدول ۱

محقق یا نظریه‌پرداز	ریسک شناسایی‌شده
بلبی (۲۰۱۵)	رعایت‌نکردن قوانین و مقررات
آندرونیکاکیس (۲۰۱۲)	
اندرسون و اسلمپ (۲۰۱۱)	
بلبی (۲۰۱۵)	نقض قوانین مربوط به حریم خصوصی
بلبی (۲۰۱۵)	نقض مالکیت معنوی
پیکازو و همکاران (۲۰۱۲)	
دیستاسو و همکاران (۲۰۱۱)	
بلبی (۲۰۱۵)	جرایم سایبری و فعالیت‌های غیرمجاز توسط کارمندان سازمان
پیکازو و همکاران (۲۰۱۲)	نقض چارچوب‌های قانونی ملی و بین‌المللی در خصوص امنیت اطلاعات
گریفین (۲۰۱۴)	نبود یا کمبود کنترل و نظارت مناسب بر رسانه‌های اجتماعی
دیستاسو و همکاران (۲۰۱۱)	
گریفین (۲۰۱۴)	سیاست‌ها و رویه‌های ضعیف مرتبط با رسانه‌های اجتماعی
پیکازو و همکاران (۲۰۱۲)	نبود چارچوب قانونی برای فعالیت‌های مربوط به شبکه‌های اجتماعی
پیکازو و همکاران (۲۰۱۲)	عدم تنظیم فرایندی برای سازماندهی، ساختار و توزیع داده‌ها
فیلد و چلیاه (۲۰۱۲)	استفادهٔ بیش از حد کارکنان از رسانه‌های اجتماعی طی ساعات کاری
بلبی (۲۰۱۵)	کاهش بازدهی کارکنان
فیلد و چلیاه (۲۰۱۲)	
ویلسون (۲۰۰۹)	
بلبی (۲۰۱۵)	کاهش تمرکز کارکنان بر کار سازمانی
فیلد و چلیاه (۲۰۱۲)	
بلبی (۲۰۱۵)	کاهش پاسخگویی سازمانی
بلبی (۲۰۱۵)	کاهش کیفیت خدمات‌رسانی سازمان
بلبی (۲۰۱۵)	کاهش سطح رضایتمندی مشتری (ارباب رجوع)
بلبی (۲۰۱۵)	افزایش هزینه‌های سازمانی و اتلاف منابع

روش‌شناسی پژوهش

این پژوهش از نظر هدف، از دسته پـژوهش‌هـای کـاربردی؛ از لحـاظ نحـوهٔ گـردآوری داده‌هـا، اکتشافی و از نظر نوع، پیمایشی است. در این تحقیـق از تحلیـل عـاملی اکتشـافی بـرای تعیـین مؤلفه‌ها استفاده شده است. در پژوهش حاضر، نمونه‌گیری در سه مرحله انجام گرفت؛ در مرحلـهٔ اول برای انجام تحلیل عاملی اکتشافی از ۱۲ خبره که به‌صورت قضاوتی هدفمند انتخاب شـدند، نظرسنجی شد. این افراد شامل ۸ نفر در حوزهٔ شهـرداری (شهردار، مـدیران و رئـیس اداره‌هـای ناحیهٔ ۳ منطقهٔ ۲۲)، ۲ نفر استاد دانشگاه در حوزهٔ روان‌شناسی، ۱ نفر در حوزهٔ فناوری اطلاعات و

۱ نفر در حوزهٔ حقوقی (وکیل پایهٔ یک دادگستری) بودند. در مرحلهٔ دوم که به بررسی میزان آسیب‌پذیری می‌پرداخت، جامعهٔ آماری پژوهش کلیهٔ مدیران و کارشناسان شهرداری منطقهٔ ۲۲ تهران به تعداد ۱۶۲ نفر (۶۱ مدیر و ۱۰۱ نفر کارشناس) بودند که از میان آنها حداقل حجم لازم، یعنی ۱۱۴ نفر (۴۳ مدیر و ۷۱ کارشناس) به روش تصادفی طبقه‌ای برای نمونه انتخاب شدند. در این مرحله برای جمع‌آوری داده‌ها، پرسشنامهٔ محقق‌ساخته‌ای مشتمل بر ۴۸ سؤال طراحی شد که پس از کسب نظر متخصصان و خبرگان حوزهٔ فناوری اطلاعات و اعمال اصلاحات لازم، چهار سؤال از پرسشنامه حذف شد و چند سؤال نیز از لحاظ نگارشی تغییر کرد. پایایی ابزار تحقیق به‌کمک ضریب آلفای کرونباخ در یک نمونهٔ ۳۰ تایی سنجیده شد. نتایج پیش‌آزمون، مقادیر آلفای کرونباخ محاسبه‌شده را بیش از ۰/۷ نشان داد که این رقم گویای پایایی مناسب ابزار تحقیق است. در مرحلهٔ سوم نیز برای دسته‌بندی مؤلفه‌های مرحلهٔ دوم در مقولهٔ کلی‌تر، ۱۵ نفر از حوزه‌های مختلف فناوری اطلاعات، مدیریت دولتی و مدیران و کارشناسان شهرداری منطقهٔ ۲۲ تهران به‌صورت قضاوتی هدفمند انتخاب شدند.

یافته‌های پژوهش

در این پژوهش حدود ۷۲/۸ درصد پاسخ‌دهندگان مرد و ۲۷/۲ درصد آنها زن بودند. همچنین از لحاظ مدرک تحصیلی، ۶۱/۴ درصد پاسخ‌دهندگان مدرک کارشناسی و ۳۸/۶ درصد مدرک کارشناسی ارشد داشتند.

در مرحلهٔ اول بر اساس داده‌های جدول ۱، پرسشنامه‌ای تدوین شد و به‌صورت قضاوتی هدفمند در اختیار ۱۲ نفر از خبرگان قرار گرفت. تحلیل پرسشنامه از طریق تحلیل عاملی اکتشافی به روش مؤلفه‌های اصلی انجام شد. شاخص کفایت نمونه‌برداری ۰/۹۳۸ به دست آمد که نشان‌دهندهٔ کفایت نمونه‌گیری است. همچنین میزان مجذور کای کرویت بارتلت ۶۶۵۰/۹۰۲ با درجهٔ آزادی ۹۴۶ بود. این مقادیر حاکی از مناسب بودن داده‌هاست؛ به این معنا که محقق می‌تواند برای تحلیل عاملی از آنها استفاده کند. ارزش ویژهٔ سه عامل بزرگ‌تر از ۱ به دست آمد. این سه عامل در مجموع ۶۲ درصد کل واریانس بین ۴۴ عامل مورد مطالعه را تبیین می‌کنند. برخی پژوهشگران به‌منظور تحقیق دربارهٔ روابط بین متغیرها و همچنین دستیابی به تعاریف عامل‌ها، ضرایب بیشتر از ۰/۳ و گاهی بیشتر از ۰/۴ را در تعریف عامل‌ها مهم و معنادار می‌دانند و ضرایب کمتر از این حدود را به‌عنوان صفر (عامل تصادفی) در نظر می‌گیرند. در پژوهش حاضر ضریب معنادار ۰/۴ مد نظر قرار گرفت و چهار عامل استخراج شد. برای دانستن اینکه آیا عامل‌ها

از هم مستقل هستند یا خیر، از چرخش واریماکس استفاده شد که داده‌های آن در جدول ۲ درج شده است.

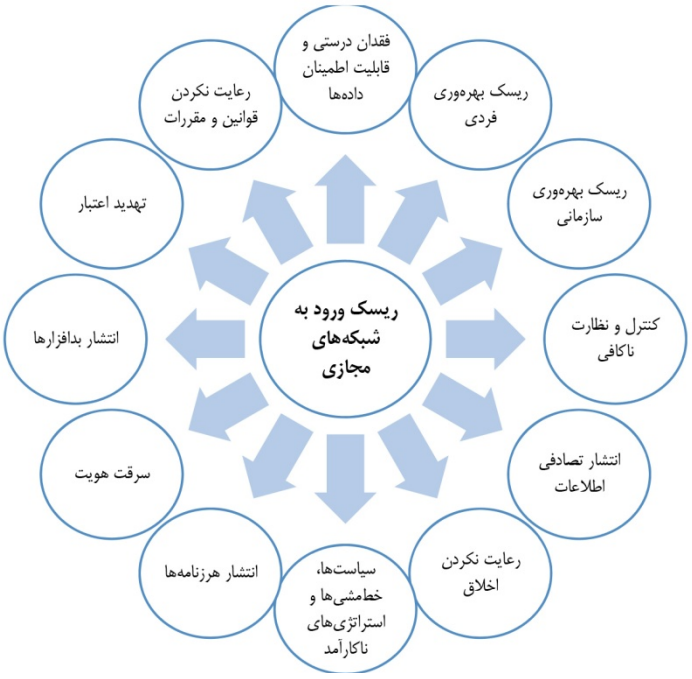
جدول ۲ . چرخش واریماکس متغیرهای پژوهش

سؤال	عامل‌ها						سؤال	عامل‌ها					
	۱	۲	۳	٤	٥	٦		۷	۸	۹	۱۰	۱۱	۱۲
۱	۰/۶۷						۲۳						۰/۶۳
۲	۰/۷۸						۲۴	۰/۵۸					
۳		۰/۷۹					۲۵	۰/۴۵					
۴		۰/۶۲					۲۶	۰/۴۳					
۵			۰/۵۰				۲۷	۰/۵۷					
۶			۰/۵۵				۲۸	۰/۷۰					
۷			۰/۶۸				۲۹		۰/۷۸				
۸			۰/۵۳				۳۰		۰/۸۱				
۹			۰/۶۶				۳۱		۰/۷۵				
۱۰				۰/۷۸			۳۲		۰/۵۴				
۱۱				۰/۶۶			۳۳		۰/۵۸				
۱۲				۰/۶۷			۳۴			۰/۶۶			
۱۳					۰/۴۹		۳۵				۰/۵۵		
۱۴					۰/۵۳		۳۶				۰/۵۳		
۱۵					۰/۴۷		۳۷				۰/۵۳		
۱۶					۰/۶۳		۳۸					۰/۵۷	
۱۷					۰/۵۱		۳۹					۰/۶۲	
۱۸					۰/۵۶		۴۰					۰/۵۳	
۱۹					۰/۵۰		۴۱						۰/۵۲
۲۰					۰/۵۱		۴۲						۰/۸۱
۲۱					۰/۶۶		۴۳						۰/۷۳
۲۲					۰/۵۹		۴۴						۰/۵۵

با توجه به جدول ۲ و بر اساس همبسته‌بودن عامل‌های تمام پرسش‌ها، نام‌های پیشنهادی برای عامل‌ها همراه با تعداد سؤال‌ها در جدول ۳ آمده است. بر اساس نتایج تحلیل عاملی اکتشافی ۴۴ ریسک شناسایی‌شده در قالب ۱۲ عامل به شرح شکل ۱ است.

جدول ۳. عامل‌ها و سؤال‌های پرسشنامه بعد از چرخش واریماکس

عامل‌ها	سؤال‌های پرسشنامه بعد از چرخش واریماکس
انتشار تصادفی اطلاعات	سؤال‌های ۱ تا ۲
انتشار هرزنامه	سؤال ۳
فقدان درستی و قابلیت اطمینان داده‌ها	سؤال‌های ۴ تا ۵
رعایت‌نکردن اخلاق	سؤال‌های ۶ تا ۱۰
انتشار بدافزارها	سؤال‌های ۱۱ تا ۱۳
تهدید اعتبار	سؤال‌های ۱۴ تا ۲۳
سرقت هویت	سؤال‌های ۲۴ تا ۲۸
رعایت‌نکردن قوانین و مقررات	سؤال‌های ۲۹ تا ۳۳
کنترل و نظارت ناکافی	سؤال ۳۴
سیاست‌ها، خط‌مشی‌ها و استراتژی‌های ناکارآمد	سؤال‌های ۳۵ تا ۳۷
بهره‌وری فردی	سؤال‌های ۳۸ تا ۴۰
بهره‌وری سازمانی	سؤال‌های ۴۱ تا ۴۴



شکل ۱. مدل مفهومی استخراج‌شده از تحلیل عاملی اکتشافی

در ادامه بـه ارائـهٔ توضـیح مختصـری در خصـوص هـر یـک از متغیرهـای مـدل مفهـومی استخراج‌شده از تحلیل عاملی اکتشافی پرداخته شده است.

انتشار تصادفی اطلاعات: این مفهوم به‌معنای به اشتراک‌گذاری عمـومی اطلاعـات، داده‌هـا و عقایدی است که باید به‌صورت خصوصی و محرمانه حفظ شوند (آندرونیکاکیس، ۲۰۱۲).

انتشار هرزنامه‌ها: هرزنامه به‌معنای پیام یا نامهٔ الکترونیکی است که بـدون درخواسـت گیرنـده برای افراد بی‌شماری فرستاده می‌شود.

فقدان درستی و قابلیت اطمینان داده‌ها: این مفهوم به‌معنای عدم وجـود داده‌هـای صـحیح، مناسب و معتبر در عرصه‌های مختلف سازمان است (سخایی، ۱۳۹۴).

رعایت‌نکردن اخلاق: این مفهوم به‌معنای استفاده از روش‌های غیراخلاقی توسـط کـاربران در به‌کارگیری رسانه‌های اجتماعی به‌عنوان کانال جدید ارتباطی است (آندرونیکاکیس، ۲۰۱۲).

انتشار بدافزارها: اصطلاح بدافزار در واقع به نرم‌افزاری اشاره دارد که به‌طور اختصاصـی بـرای آسیب‌رسانی به سیستم رایانه‌ای بدون اطلاع و رضایت صاحب سیستم اقدام می‌کند. رسـانه‌هـای اجتماعی کانال جدیدی را برای توزیع انواع گوناگونی از نرم‌افزارهای مخـرب ماننـد ویـروس‌هـا، کرم‌ها یا اسب‌های تروجان فراهم می‌کنند (آندرونیکاکیس، ۲۰۱۲).

تهدید اعتبار: شهرت و اعتبار، منعکس‌کنندهٔ نوع درک و نگرش افکار عمومی از یک شرکت یا سازمان است. ریسک‌های اعتباری و شهرتی در ارتباط با موقعیت‌هایی هستند کـه مـی‌تواننـد از طریق رسانه‌های اجتماعی تأثیرات معکوسی بر وجههٔ عمومی و قابلیت اعتمـاد یـک شـرکت یـا سازمان برجای گذارند (آندرونیکاکیس، ۲۰۱۲).

سرقت هویت: بر مبنای بیانیهٔ کمیتهٔ تجارت فدرال، سرقت هویت هنگامی اتفاق مـی‌افتـد کـه فردی مجرم، از اطلاعات هویتی و شخصی فرد دیگر مثل نام، نام‌های مستعار و حتی اطلاعـات مربوط به کارت اعتباری بدون اجازهٔ شخص و به‌منظـور ارتکـاب کلاهبـرداری یـا سـایر جـرایم سوءاستفاده کند (آندرونیکاکیس، ۲۰۱۲).

رعایت‌نکردن قوانین و مقررات: این مفهوم بـه‌معنـای پیـروی نکـردن سـازمان از قـوانین و استانداردهای از پیش تعیین‌شده در بـه‌کـارگیری رسـانه‌هـای اجتمـاعی اسـت (آنـدرونیکاکیس، ۲۰۱۲).

کنترل و نظارت ناکافی: کنترل و نظارت شامل ارزیابی تصمیم‌ها و برنامه‌ها از زمان اجرای آنها و اقدامات لازم برای جلوگیری از انحراف عملیات نسبت به هدف‌های برنامه و تصحیح انحرافات

احتمالی است. چنانچه این فرایند اثربخش نباشد یا کنترل و نظارت ناکافی و بدون دقت انجام شود، موقعیت سازمان به خطر می‌افتد (جاسبی، ۱۳۷۰).

سیاست‌ها، خط‌مشی‌ها و استراتژی‌های ناکارآمد: منظور میزان ریسکی است که تصمیم‌گیرندگان برای دستیابی به اهداف سازمان حاضر به پذیرش آن هستند. در تنظیم اهداف استراتژیک، خط‌مشی‌ها و سیاست‌های سازمانی، ابتدا به میزان ریسک‌پذیری توجه می‌شود و پس از آن، حدودی برای ریسک نامطلوب مد نظر قرار می‌گیرد (اسماعیل نژاد، ۱۳۹۱).

بهره‌وری فردی: بهره‌وری دیدگاهی است که در آن هر فرد می‌تواند کارها و وظایفش را هر روز بهتر از قبل انجام دهد. بدیهی است درگیری فزاینده با شبکه‌های اجتماعی سبب کاهش زمان مفید کاری و به تبع آن کاهش بهره‌وری فردی می‌شود (روستاخیز، ۱۳۹۲).

بهره‌وری سازمانی: بهره‌وری سازمانی، بیشترین میزان استفاده از منابع سازمان (شامل منابع فیزیکی، نیروی انسانی و سایر عوامل) است؛ به گونه‌ای که به کاهش هزینه‌های تولید، گسترش بازارها و بهبود معیارهای زندگی منجر شود. به‌زعم اندیشمندان، کاهش بهره‌وری فردی در مجموع به کاهش بهره‌وری سازمانی می‌انجامد (روستاخیز، ۱۳۹۲).

در مرحلهٔ دوم، پرسشنامهٔ تحقیق بین ۱۱۴ نفر با استفاده از روش نمونه‌گیری تصادفی طبقه‌ای توزیع شد. فرضیه‌های تحقیق بدین شکل تدوین شد که سرقت هویت؛ انتشار تصادفی اطلاعات؛ انتشار بدافزارها؛ انتشار هرزنامه‌ها؛ رعایت‌نکردن اخلاق؛ رعایت‌نکردن قوانین و مقررات؛ تهدید اعتبار؛ کنترل و نظارت ناکافی؛ سیاست‌ها، خط‌مشی‌ها و استراتژی‌های ناکارآمد؛ فقدان درستی و قابلیت اطمینان داده‌ها؛ ریسک بهره‌وری فردی و ریسک بهره‌وری سازمانی؛ از ریسک‌های ورود سازمان‌های عمومی به شبکه‌های اجتماعی محسوب می‌شوند.

در این مرحله به‌منظور تعیین نوع آزمون، ابتدا به بررسی نرمال بودن داده‌ها با استفاده از آزمون کولموگروف ـ اسمیرنوف پرداخته شد که در آن فرض صفر مبنی بر نرمال بودن داده‌هاست. با توجه به جدول ۴، سطح معناداری تمام متغیرها بیشتر از مقدار خطای ۰/۰۵ است، در نتیجه تمام متغیرها دارای توزیع نرمال هستند.

همچنین با توجه به نرمال بودن داده‌ها، برای آزمایش فرضیه‌ها، آزمون تی‌تک نمونه‌ای به اجرا درآمد. فرض صفر حاکی از رد شاخص و فرض ۱ ناظر بر پذیرش شاخص به‌عنوان ریسک ورود به شبکه‌های اجتماعی در جامعهٔ آماری است. فرض‌های آماری به‌شرح زیر هستند.

$$\begin{cases} H_0 = \mu \leq 3 \\ H_1 = \mu > 3 \end{cases}$$

جدول ٤. نتایج آزمون کولموگروف ـ اسمیرنوف

متغیر	کولموگروف ـ اسمیرنوف	
	آماره	معناداری
انتشار تصادفی اطلاعات	۱/۳۴۷	۰/۰۵۳
انتشار هرزنامه	۱/۲۲۹	۰/۰۹۱
فقدان درستی و قابلیت اطمینان داده‌ها	۱/۳۰۸	۰/۰۶۳
رعایت‌نکردن اخلاق	۱/۳۵۱	۰/۰۵۱
انتشار بدافزارها	۱/۲	۰/۰۹۴
تهدید اعتبار	۱/۳۱۸	۰/۰۶۲
سرقت هویت	۰/۰۷۷۲	۰/۵۹
رعایت‌نکردن قوانین و مقررات	۱/۳۰۱	۰/۰۷۹
کنترل و نظارت ناکافی	۱/۱۰۱	۰/۱۰۲
سیاست‌ها، خط‌مشی‌ها و استراتژی‌های ناکارآمد	۱/۲۴۷	۰/۰۸۹
ریسک بهره‌وری فردی	۱/۱۴۳	۰/۰۹۹
ریسک بهره‌وری سازمانی	۱/۰۱۱	۰/۱۱۶

جدول ۵. نتایج آزمون فرضیه‌های پژوهش

شاخص	درجهٔ آزادی	میانگین	اختلاف میانگین	آمارهٔ تی	معناداری Sig
ریسک سرقت هویت	۱۱۳	۳/۹۹۳	۰/۹۹۳	۱۸/۲۸۴	۰/۰۰۰
ریسک انتشار تصادفی اطلاعات	۱۱۳	۴/۱۳۶	۱/۱۳۶	۱۶/۱۶۲	۰/۰۰۰
ریسک انتشار بدافزارها	۱۱۳	۳/۹۹۱	۰/۹۹۱	۱۷/۳۳۹	۰/۰۰۰
ریسک انتشار هرزنامه‌ها	۱۱۳	۴/۰۶۱	۱/۰۶۱	۱۳/۵۹۱	۰/۰۰۰
ریسک رعایت‌نکردن اخلاق	۱۱۳	۴/۰۳۷	۱/۰۳۷	۱۷/۱۲۱	۰/۰۰۰
ریسک رعایت‌نکردن قوانین و مقررات	۱۱۳	۳/۹۸۴	۰/۹۸۴	۱۶/۹۹۳	۰/۰۰۰
ریسک تهدید اعتبار	۱۱۳	۳/۸۸۶	۰/۸۸۶	۱۸/۳۹۰	۰/۰۰۰
ریسک کنترل و نظارت ناکافی	۱۱۳	۳/۹۹۱	۰/۹۹۱	۱۴/۱۷۵	۰/۰۰۰
ریسک سیاست‌ها، خط‌مشی‌ها و استراتژی‌های ناکارآمد	۱۱۳	۳/۸۵۱	۰/۸۵۱	۱۴/۷۴۳	۰/۰۰۰
ریسک فقدان درستی و قابلیت اطمینان داده‌ها	۱۱۳	۴/۱۳۶	۱/۱۳۶	۱۵/۱۸۰	۰/۰۰۰
ریسک بهره‌وری فردی	۱۱۳	۳/۹۵۹	۰/۹۵۹	۱۳/۱۱۲	۰/۰۰۰
ریسک بهره‌وری سازمانی	۱۱۳	۳/۸۸۲	۰/۸۸۲	۱۱/۱۸۵	۰/۰۰۰

با توجه به کوچک‌تر بودن عدد معناداری از حد آستانه (۰/۰۵)، فرض صفر برای همهٔ شاخص‌ها رد می‌شود؛ به این معنا که همهٔ شاخص‌های مدل به‌عنوان ریسک‌های ورود به شبکه‌های اجتماعی در شهرداری منطقهٔ ۲۲ تهران پذیرفته می‌شوند.

در مرحلهٔ سوم برای دسته‌بندی ریسک‌های دوازده‌گانه در مقوله‌های کلی‌تر، از نظر ۱۵ نفر از کارشناسان حوزه‌های مختلف، مانند فناوری اطلاعات، مدیریت دولتی و مدیران و کارشناسان شهرداری منطقهٔ ۲۲ تهران به‌صورت قضاوتی هدفمند بهره برده شد. تحلیل داده‌ها با استفاده از تحلیل عاملی اکتشافی به روش مؤلفه‌های اصلی، مقدار شاخص کفایت نمونه‌برداری را ۰/۷۱۵ نشان داد که گویای کفایت نمونه‌گیری است. همچنین میزان مجذور کای کرویت بارتلت ۵۷۲۶/۱۸۷ با درجهٔ آزادی ۵۲۶ به‌دست آمد که نشان‌دهندهٔ مناسب بودن داده‌هاست؛ یعنی می‌توان از آنها برای تحلیل عاملی استفاده کرد.

ارزش ویژهٔ سه عامل بزرگ‌تر از ۱ به‌دست آمد. این سه عامل در مجموع ۵۸ درصد کل واریانس بین ۱۲ عامل مورد مطالعه را تبیین می‌کنند. برخی پژوهشگران به‌منظور تحقیق دربارهٔ روابط بین متغیرها و همچنین دستیابی به تعریف عامل‌ها، ضرایب بیشتر از ۰/۳ و گاهی بیشتر از ۰/۴ را در تعریف عامل‌ها مهم و معنادار می‌دانند و ضرایب کمتر از این حدود را به‌عنوان صفر (عامل تصادفی) در نظر می‌گیرند. در پژوهش حاضر ضریب معنادار ۰/۴ مد نظر قرار گرفت و چهار عامل استخراج شد. برای دانستن مستقل بودن عامل‌ها از هم، از چرخش واریماکس استفاده شد. داده‌های مربوط به چرخش واریماکس در جدول ۶ ارائه شده است. با توجه به جدول ۶ و بر اساس همبسته بودن عامل‌های هر پرسش، نام‌های پیشنهادی هر عامل همراه با تعداد سؤال‌ها در جدول ۷ آمده است.

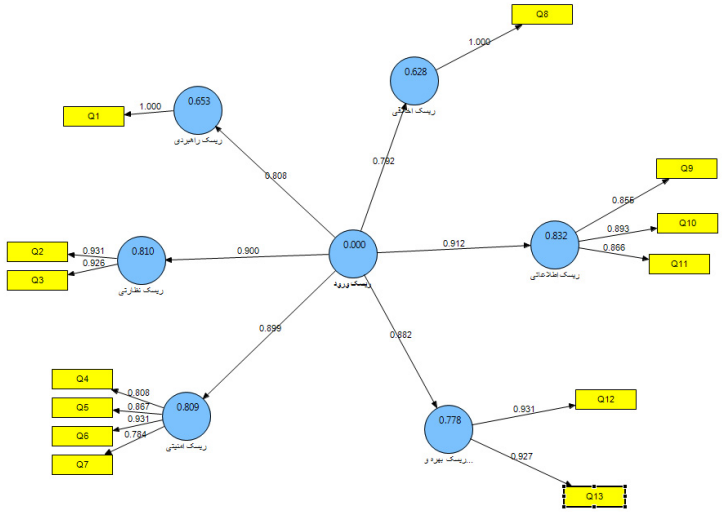
جدول ٦. چرخش واریماکس متغیرهای پژوهش

سؤال	عامل‌ها			سؤال	عامل‌ها		
	۱	۲	۳		٤	٥	٦
۱	۰/۷۸			۷	۰/۷۹		
۲		۰/۶۸		۸		۰/۸۵	
۳			۰/۷۱	۹		۰/۶۳	
۴			۰/۶۹	۱۰		۰/۷۱	
۵			۰/۷۲	۱۱			۰/۸۵
۶			۰/۶۳	۱۲			۰/۷۹

جدول ۷. عامل‌ها و سؤال‌های پرسشنامه بعد از چرخش واریماکس

عامل‌ها	سؤال‌های پرسشنامه بعد از چرخش واریماکس
ریسک راهبردی	سؤال ۱
ریسک نظارتی	سؤال ۲
ریسک امنیتی	سؤال‌های ۳ تا ۶
ریسک اخلاقی	سؤال ۷
ریسک اطلاعاتی	سؤال‌های ۸ تا ۱۰
ریسک بهره‌وری	سؤال‌های ۱۱ و ۱۲

بر اساس جدول بالا، ریسک اطلاعاتی در ریسک‌هایی مانند انتشار تصادفی اطلاعات، انتشار هرزنامه و فقدان درستی و قابلیت اطمینان داده‌ها؛ ریسک اخلاقی در ریسک مرتبط با رعایت‌نکردن اخلاق؛ ریسک امنیتی در ریسک‌های مرتبط با انتشار بدافزارها، تهدید اعتبار، سرقت هویت و رعایت‌نکردن قوانین و مقررات؛ ریسک نظارتی در ریسک مرتبط با کنترل و نظارت ناکافی؛ ریسک راهبردی در ریسک مرتبط با سیاست‌ها، خط‌مشی‌ها و استراتژی‌های ناکارآمد؛ و ریسک بهره‌وری در ریسک مرتبط با بهره‌وری فردی و سازمانی طبقه‌بندی شدند. در گام نهایی تلاش شد با اجرای تحلیل عاملی تأییدی از طریق مدل‌سازی معادلات ساختاری در نرم‌افزار Smart PLS، مقوله‌های احصاشده به‌صورت انحصاری دقیق‌تر بررسی شوند که نتایج آن در شکل ۲ مشاهده می‌شود. برازش مدل ارائه‌شده نیز در جدول ۸ آمده است.

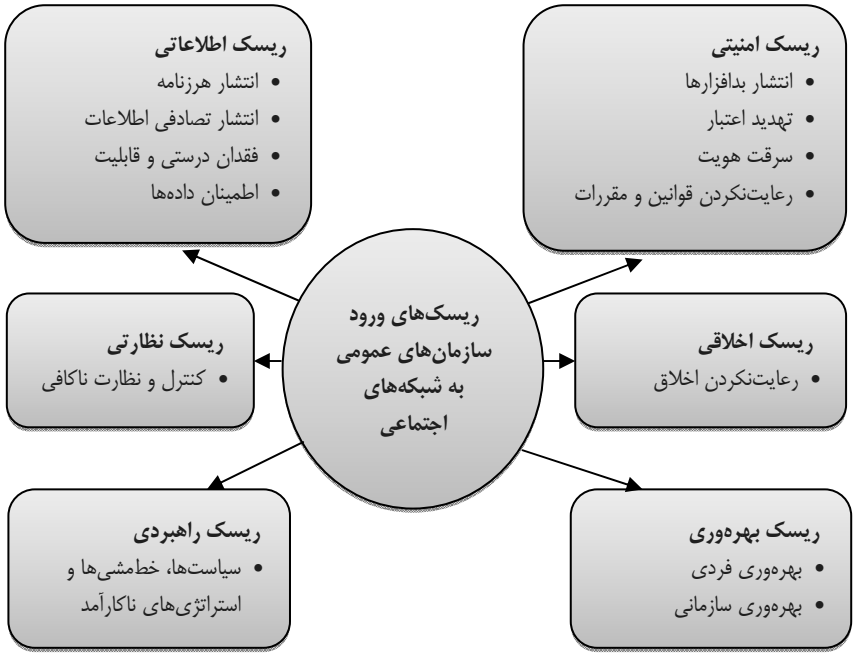


شکل ۲. ضرایب بار عاملی تحلیل عاملی تأییدی

جدول ۸. شاخص‌های برازش‌داده‌شدهٔ مدل

عامل‌ها	مقدار AVE	مقدار C.R	R^2	آلفای کرونباخ	مقادیر اشتراکی
ریسک راهبردی	۰/۸۶۲	۱	۰/۶۵۳	۱	۱
ریسک نظارتی	۰/۷۲۱	۰/۹۲۶	۰/۸۰۹	۰/۸۴۶	۰/۸۶۲
ریسک امنیتی	۱	۱	۰/۸۰۸	۱	۱
ریسک اخلاقی	۰/۷۵۹	۰/۹۰۵	۰/۶۲۷	۰/۸۴۱	۰/۷۲۱
ریسک اطلاعاتی	۰/۸۶۳	۰/۹۰۴	۰/۸۳۲	۰/۸۴۱	۰/۷۵۹
ریسک بهره‌وری	۰/۶۳۳	۰/۹۲۶	۰/۷۷۸	۰/۹۵۱	۰/۸۶۳

بر اساس نتایج تحلیل داده‌ها، الگوی نهایی ریسک‌های ورود سازمان‌های عمومی به شبکه‌های اجتماعی در قالب شکل ۳ مشاهده می‌شود.



شکل ۳. الگوی ریسک‌های ورود سازمان‌های عمومی به شبکه‌های اجتماعی

نتیجه‌گیری و پیشنهادها

پژوهش حاضر با هدف شناسایی ریسک‌های ورود سازمان‌های عمومی به شبکه‌های اجتماعی اجرا شد. نگاهی به تحقیقات انجام‌شده نشان می‌دهد مطالعهٔ حاضر با نگاه متفاوت و موشکافانه‌تر به موضوع، تلاش کرده با نوآوری در مباحث مختلف دولت الکترونیک، نسبت به برطرف‌کردن ضعف‌ها، برقراری ارتباط با ارباب‌رجوع و ارتقای سطح کیفیت خدمات گام بردارد. تحقیقات انجام‌شده این نکته را تأیید می‌کنند که ایجاد سیستم ارتباطی با هموطنان از الزامات دولت الکترونیک است. برای مثال می‌توان به مطالعات عبادی (۱۳۹۵)، یعقوبی و همکاران (۱۳۹۵)، سهرابی و همکاران (۱۳۹۵) و سلیمی‌فرد و همکاران (۱۳۹۴) اشاره کرد. عبادی (۱۳۹۵) در پژوهش خود نشان داد اغلب پورتال‌ها در سطوح اولیهٔ بلوغ مدل‌های خدمات‌رسانی الکترونیکی قرار دارند و بیشتر از آن که خدمات‌رسانی کنند، اطلاعات ارائه می‌دهند. سهرابی و همکاران (۱۳۹۵) در تحقیقی نشان دادند عوامل تعهد و اشتیاق کارکنان و سطوح مدیریتی دستگاه دولتی و پس از آن، زیرساخت‌های فنی و فرایندی بر استفادهٔ کارآمد از سیستم‌های اطلاعاتی یکپارچه تأثیر زیادی دارند.

یافته‌های پژوهش نشان داد سرقت هویت از ریسک‌های ورود سازمان‌های عمومی به شبکه‌های اجتماعی محسوب می‌شود. نتایج به‌دست‌آمده با یافته‌های آندرونیکاکیس (۲۰۱۲) همخوانی دارد. از نظر هولمز (۲۰۰۵) تعامل در فضای سایبر از لحاظ «هویت کاربران» به دو گروه دسته‌بندی می‌شود: نخست، کاربرانی که با هویت واقعی خود به تعامل می‌پردازند و دوم، کاربرانی که با اهداف مشخصی به تعامل می‌پردازند، هویت خویش را پنهان می‌کنند و تصور می‌کنند که شناخت هویت آنان در دستیابی به اهدافشان تأثیری ندارد. به‌زعم آندرونیکاکیس (۲۰۱۲) سرقت هویت هنگامی روی می‌دهد که فرد مجرم، از اطلاعات هویتی و شخصی فرد دیگری همچون نام، نام‌های مستعار و حتی اطلاعات مربوط به کارت اعتباری بدون اجازهٔ شخص و به‌منظور ارتکاب کلاهبرداری یا سایر جرایم، سوء استفاده کند. بر این اساس، پیشنهاد می‌شود که در تعریف اطلاعات شخصی مدیران و کارکنان سازمان تلاش شود اقدامات امنیتی به عمل آمده و میزان دسترسی افراد به‌صورت شفاف مشخص شده و تا حد امکان از ذخیره‌سازی فایل‌ها در فضای مجازی امتناع شود.

تحلیل داده‌ها نشان داد انتشار تصادفی اطلاعات یکی دیگر از ریسک‌های ورود سازمان‌های عمومی به شبکه‌های اجتماعی است. نتایج تحقیق حاضر با نتایج گریفین (۲۰۱۴)، فیلد و چلیاه (۲۰۱۲)، آندرونیکاکیس (۲۰۱۲) و اندرسن و اسلمپ (۲۰۱۱) همسو است. در واقع، این ریسک همان افشای تصادفی اطلاعات محرمانه است که می‌تواند به‌دلیل استفاده از اکانت‌های یکسان

شخصی و کاری برای ورود به صفحات رسانه‌های اجتماعی باشد (آندرونیکاکیس، ۲۰۱۲). بنابراین پیشنهاد می‌شود هنگام قرارگیری اطلاعات در شبکه‌های مجازی از فیلترهای مناسبی استفاده شود. همچنین برای بهبود رویهٔ قرارگیری اطلاعات در شبکه‌های مجازی، امکان تأیید یا رد این اطلاعات از سوی مدیران وجود داشته باشد.

بر اساس نتایج، انتشار بدافزارها نیز یکی دیگر از ریسک‌های ورود سازمان‌های عمومی به شبکه‌های اجتماعی به‌شمار می‌رود. نتایج تحقیق حاضر با نتایج مطالعات بلبی (۲۰۱۵)، آندرونیکاکیس (۲۰۱۲)، ایلانارازی (۲۰۱۰)، انجمن کسب‌وکار ایمن (۲۰۰۹) و ویلسون (۲۰۰۹)، همخوانی دارد. بدافزار در واقع نرم‌افزاری است که به‌طور اختصاصی و بدون اطلاع و رضایت صاحب سیستم، به سیستم رایانه‌ای آسیب می‌رساند. رسانه‌های اجتماعی کانال جدیدی را برای توزیع انواع گوناگونی از نرم‌افزارهای مخرب مانند ویروس‌ها، کرم‌ها یا اسب‌های تروجان فراهم می‌کنند (آندرونیکاکیس، ۲۰۱۲)؛ از این رو پیشنهاد می‌شود در انتخاب ابزارهای اطلاعاتی و کانال‌های نشر اطلاعات دقت لازم به‌عمل آید.

نتایج تحقیق نشان داد انتشار هرزنامه‌ها از ریسک‌های ورود سازمان‌های عمومی به شبکه‌های اجتماعی محسوب می‌شود که این یافته با نتایج مطالعهٔ محکم‌کار و حلاج (۱۳۹۳) و آندرونیکاکیس (۲۰۱۲) سازگار است. هرزنامه به رسانهٔ اجتماعی به‌عنوان کانال جدیدی در زمینهٔ ارسال هرزنامه‌ها اشاره دارد (آندرونیکاکیس، ۲۰۱۲). هرزنامه به پیام یا نامهٔ الکترونیکی گفته می‌شود که بدون درخواست گیرنده برای افراد بی‌شماری فرستاده می‌شود. از این رو پیشنهاد می‌شود به منظور حضور در شبکه‌های اجتماعی از ابزارهایی استفاده شود که امکان تعریف کاربران در آن وجود داشته باشد؛ تا حد ممکن نسبت به شناسنامه‌دار کردن کاربران در این شبکه‌ها اقدام شود و به هر یک از افراد مجاز، شناسهٔ کاربری و رمز مناسب و ترکیبی از اعداد و حروف داده شود.

بر اساس نتایج تحلیل، رعایت‌نکردن اخلاق یکی دیگر از ریسک‌های ورود سازمان‌های عمومی به شبکه‌های اجتماعی است. این نتیجه با یافته‌های محکم‌کار و حلاج (۱۳۹۳)، اندرسون و اسلمپ (۲۰۱۱)، روزنبلوم (۲۰۰۷)، پونجابی (۲۰۱۴)، گریفین (۲۰۱۴)، فیلد و چلیاه (۲۰۱۲) و آندرونیکاکیس (۲۰۱۲) همسو است. آندرونیکاکیس (۲۰۱۲) بی‌اخلاقی‌ها را شامل اظهارنظرهای سازماندهی‌شده به‌منظور اعلام بیزاری از سازمان یا رقبا، به‌کارگیری وبلاگ‌نویس‌های اجاره‌ای به‌منظور نشر نقدها و مطالب علیه سازمان یا گروه خاص و طراحی وبلاگ‌های جعلی به‌منظور فریب کاربران از طریق شبیه‌سازی موقعیت یا گزارش‌های مطلوب سازمان یا شرکت می‌داند. آندرونیکاکیس (۲۰۱۲) رعایت‌نکردن مسائل اخلاقی در شیوه‌های جمع‌آوری داده‌ها و عدم

افشای وابستگی به سازمان را خلاف اخلاق می‌داند؛ در حالیکه محکم‌کار و حلاج (۱۳۹۳)، اندرسون و اسلمپ (۲۰۱۱) و روزنبلوم (۲۰۰۷) نقض یا تهدید حریم خصوصی افراد را موارد خلاف اخلاق معرفی می‌کنند؛ هر چند از نظر گریفین (۲۰۱۴)، پونجابی (۲۰۱۴)، فیلد و چلیاه (۲۰۱۲) و ویلسون (۲۰۰۹)، انتشار اطلاعات خصوصی سازمان به‌صورت عمدی و آگاهانه از جملهٔ شاخص‌های رعایت‌نکردن اخلاق است. بر این اساس، توصیه می‌شود که سازمان‌ها بر حفظ فضای اخلاقی در شبکه‌های اجتماعی تأکید کنند و در راستای بهبود امنیت اخلاقی، روند عوامل اخلاقی فعالیت در شبکه‌های اجتماعی را به کارکنان و اعضای شبکه یادآوری نمایند.

بر اساس نتایج، رعایت‌نکردن قوانین و مقررات از ریسک‌های ورود سازمان‌های عمومی به شبکه‌های اجتماعی محسوب می‌شود که این نتیجه با یافته‌های محققانی همچون بلبی (۲۰۱۵)، آندرونیکاکیس (۲۰۱۲)، اندرسون و اسلمپ (۲۰۱۱)، هاتچینگز (۲۰۱۲) و پیکازو و همکاران (۲۰۱۲) همخوانی دارد. رعایت‌نکردن قوانین و مقررات به‌معنای پیروی‌نکردن سازمان از قوانین، استانداردها، سیاست‌ها و مقررات از پیش تعیین‌شده در به‌کارگیری رسانه‌های اجتماعی است. در واقع، ریشهٔ چنین ریسک‌هایی در عدم تبعیت سهوی از قوانین و مقررات مربوطه است. مهم‌ترین این ریسک‌ها عبارت‌اند از: رعایت‌نکردن قوانین کشوری و بین‌المللی در زمینهٔ حریم خصوصی، رعایت‌نکردن سیاست‌های سازمانی از پیش تعیین‌شده، رعایت‌نکردن قوانین مربوط به حفظ و نگهداری از اطلاعات، رعایت‌نکردن قوانین مربوط به روابط نیروی کار. بلبی (۲۰۱۵) نقض قوانین مربوط به حریم خصوصی، مالکیت معنوی و جرایم سایبری و فعالیت‌های غیرمجاز را در این زمینه معرفی می‌کند. هر چند نقض چارچوب‌های قانونی ملی و بین‌المللی در خصوص امنیت اطلاعات نیز به نوعی عدم رعایت قوانین و مقررات محسوب می‌شود (پیکازو و همکاران، ۲۰۱۲). بنابراین پیشنهاد می‌شود که قوانین و مقررات به‌صورت مکتوب به اطلاع تمام کارکنان برسد و در صورت پیروی کامل از مقررات، کارکنان تشویق شوند.

نتایج آمار استنباطی نشان داد تهدید اعتبار یکی دیگر از ریسک‌های ورود سازمان‌های عمومی به شبکه‌های اجتماعی است. این نتیجه با یافته‌های بلبی (۲۰۱۵)، آندرونیکاکیس (۲۰۱۲). فیلد و چلیاه (۲۰۱۲)، اندرسون و اسلمپ (۲۰۱۱)، دیستاسو (۲۰۱۱)، ویلسون (۲۰۰۹)، گریفین (۲۰۱۴) و پیکازو و همکاران (۲۰۱۲) همسو است. شهرت و اعتبار، منعکس‌کنندهٔ نوع درک و نگرش افکار عمومی از شرکت یا سازمان است. از این رو، ریسک‌های اعتباری و شهرتی در ارتباط با موقعیت‌هایی هستند که می‌توانند از طریق رسانه‌های اجتماعی تأثیراتی معکوس بر وجههٔ عمومی و قابلیت اعتماد شرکت یا سازمان داشته باشند. مهم‌ترین این ریسک‌ها عبارت‌اند از: درز اطلاعات نامناسب برای اعتبار سازمان از طریق کارمند و ارباب رجوع فعلی یا آینده، پایش

و نظارت نامناسب اطلاعات به اشتراک گذاشته‌شده از سوی سازمان، آموزش نامناسب و ناکافی کارکنان در زمینهٔ سیاست‌ها، رویه‌ها و استراتژی‌های تأییدشده در خصوص استفاده از رسانه‌های اجتماعی، ضعف در مدیریت بحران‌های ایجادشده علیه سازمان در رسانه‌های اجتماعی و وجود اطلاعات نادرست در زمینهٔ وجههٔ سازمان و اعتبار آن در رسانه‌های اجتماعی. در نتیجه، پیشنهاد می‌شود به مواردی که اعتبار سازمان را با خطر مواجه می‌کند، توجه شده و همچنین تلاش شود که افراد شاغل در سازمان برای حفظ اعتبار خود و سازمان، از رفتارهای اشتباه دوری کنند.

تحلیل داده‌ها نشان داد کنترل و نظارت ناکافی از ریسک‌های ورود سازمان‌های عمومی به شبکه‌های اجتماعی محسوب می‌شود که این نتیجه با یافته‌های دیستاسو (۲۰۱۲) و گریفین (۲۰۱۴) همسو است. نظارت و کنترل یکی از اجزای اصلی مدیریت محسوب می‌شود. چنانچه این فرایند اثربخش نباشد و کنترل و نظارتِ کافی و دقیق اعمال نشود، می‌تواند موقعیت سازمان را به خطر بیندازد. بنابراین پیشنهاد می‌شود که بر محتوای اطلاعاتی ارائه‌شده و دریافت‌شده از سوی سازمان، همچنین میزان رعایت قوانین و مقررات و مسائل اخلاقی در سازمان نظارت لازم وجود داشته باشد و سعی شود که از سیستم معتبری برای تبادل اطلاعات استفاده شود.

بر اساس نتایج سیاست‌ها، خط‌مشی‌ها و استراتژی‌های ناکارآمد یکی دیگر از ریسک‌های ورود سازمان‌های عمومی به شبکه‌های اجتماعی است. این نتیجه با یافته‌های گریفین (۲۰۱۴) و پیکازو و همکاران (۲۰۱۲) همسویی دارد. تنظیم و تدوین سیاست‌ها، خط‌مشی‌ها و استراتژی‌های مناسب و مورد نیاز سازمان، ضروری است و ناکارآمدی آنها مخاطراتی را برای سازمان به همراه دارد. منظور از ریسک سیاست‌ها، خط‌مشی‌ها و استراتژی‌های ناکارآمد، میزان ریسکی است که تصمیم‌گیرندگان و برنامه‌ریزان سازمان همچون هیئت‌مدیره، برای دستیابی به اهداف سازمانی، حاضر به پذیرش آن هستند. شایان ذکر است در تنظیم و عملیاتی نمودن اهداف استراتژیک، خط‌مشی‌ها و سیاست‌های سازمانی، ابتدا به میزان ریسک‌پذیری توجه می‌شود و پس از آن حدودی برای ریسک نامطلوب مد نظر قرار می‌گیرد (اسماعیل‌نژاد، ۱۳۹۱). از این رو پیشنهاد می‌شود که رویه‌ها و سیاست‌های امن فردی و سازمانی در شبکه‌های اجتماعی اتخاذ شود.

یافته‌های تحقیق نشان داد فقدان درستی و قابلیت اطمینان داده‌ها از ریسک‌های ورود سازمان‌های عمومی به شبکه‌های اجتماعی محسوب می‌شود. فقدان درستی و قابلیت اطمینان داده‌ها به‌دلیل ورود داده‌های ناصحیح، نامناسب و نامعتبر در عرصه‌های مختلف سازمان ایجاد می‌شود. به موازات ارتقای جایگاه داده و تبدیل آن به یکی از سرمایه‌های حیاتی در سازمان‌ها، استفاده از آن می‌تواند خطرها و تهدیدهای متعددی را متوجه سازمان‌ها کند. کیفیت پایین داده را می‌توان از ریسک‌های مهم در سازمان معرفی کرد که در صورت عدم پاسخگویی صحیح به آن،

تمام لایه‌های استراتژیک تا عملیاتی از آن تأثیر می‌پذیرند. این یافته با نتایج مطالعات محکم‌کار و حلاج (۱۳۹۳)، پونجابی (۲۰۱۴)، اشفورد (۲۰۱۳)، ایلانارزی (۲۰۱۰)، انجمن کسب‌وکار ایمن (۲۰۰۹)، بلبی (۲۰۱۵)، پیکازو و همکاران (۲۰۱۲) همسویی دارد. بنابراین پیشنهاد می‌شود در فرایندهای سازمانی از دانش به‌روز و مستند استفاده شده و همچنین امکان دسترسی سریع به منابع اطلاعات فراهم شود. در واقع با ایجاد سامانهٔ مدیریت دانش، به تکمیل این فرایند اقدام کنند.

تحلیل داده‌ها نشان داد ریسک بهره‌وری فردی از ریسک‌های ورود سازمان‌های عمومی به شبکه‌های اجتماعی است. نتیجهٔ به‌دست‌آمده با یافته‌های فیلد و چلیاه (۲۰۱۲) و بلبی (۲۰۱۵) سازگار است. از جمله شاخص‌های مؤثر در ایجاد ریسک بهره‌وری، می‌توان به استفادهٔ بیش از حد کارکنان از رسانه‌های اجتماعی در طول ساعات کار، کاهش بازدهی کارکنان و کاهش تمرکز آنها بر کار سازمانی اشاره کرد. از این رو، پیشنهاد می‌شود که سازمان با انجام ارزیابی‌های دوره‌ای، شکاف‌های موجود را شناسایی کرده و کارکنان را در بر طرف نمودن نواقص احتمالی کمک کنند.

بر اساس یافته‌های پژوهش، ریسک بهره‌وری سازمانی یکی از ریسک‌های ورود سازمان‌های عمومی به شبکه‌های اجتماعی است. این نتیجه با نتیجهٔ مطالعات بلبی (۲۰۱۵) همخوانی دارد. بر اساس نظر روستاخیز (۱۳۹۲) بهره‌وری سازمانی، بیشترین میزان (حداکثر) استفاده از منابع سازمان (شامل منابع فیزیکی، نیروی انسانی و سایر عوامل) با تکیه بر روش‌های علمی است؛ به‌گونه‌ای که به کاهش هزینه‌های تولید، گسترش بازارها و بهبود معیارهای زندگی منجر شود. بر این اساس، باید از عوامل ایجادکنندهٔ ریسک شامل کاهش پاسخگویی سازمانی، کاهش کیفیت خدمات ارائه‌شدهٔ سازمان، کاهش سطح رضایتمندی مشتری (ارباب رجوع) و افزایش هزینه‌های سازمانی جلوگیری کرد. بنابراین پیشنهاد می‌شود برای بهبود بهره‌وری سازمان، از رویه‌های مدون استفاده شود. همچنین مواردی که در حفظ و ارتقای بهره‌وری سازمان خلل ایجاد می‌کنند، شناسایی شوند و با برگزاری کارگاه‌های آموزشی، اهداف سازمانی به اطلاع تمام کارکنان برسد.

پیشنهاد می‌شود در پژوهش‌های آتی، متغیرهای مدل این تحقیق با استفاده از روش‌های آماری دیگری همچون تصمیم‌گیری چندمعیاره آزمایش شده و یافته‌ها با یکدیگر مقایسه شوند. همچنین این پژوهش در سایر سازمان‌ها تکرار شده و نتایج تحقیق حاضر در سایر سازمان‌ها اعتبارسنجی شود تا مدیران و مسئولان سازمان‌های عمومی اهتمام بیشتری نسبت به اجرای متغیرهای مهم آن داشته باشند.

از آنجا که تحقیقات در علوم اجتماعی و مدیریت، با بررسی و درک فعالیت‌های انسانی مرتبط است و با توجه به پیچیدگی رفتار و فعالیت‌های بشری، همواره مشکل جمع‌آوری اطلاعات از افراد به‌دلیل تأثیرپذیری آنها، خارج از کنترل محقق مطرح است، این مشکل در جامعهٔ آماری تحقیق حاضر که روحیهٔ تحقیق و پژوهش در آن به‌طور کامل نهادینه نشده است، مضاعف شده و به‌عنوان اصلی‌ترین محدویت تحقیق حاضر مطرح است.

منابع

اسماعیل‌نژاد آهنگرانی، م. (۱۳۹۱). اصول و مفاهیم مدیریت ریسک. *مدیریت پژوهش و ریسک بانک سینا*، بهار ۱۳۹۱.

جاسبی، ع. (۱۳۷۰). *اصول و مبانی مدیریت*. تهران: مرکز انتشارات علمی دانشگاه آزاد اسلامی.

روستاخیز، ا. (۱۳۹۲). *بررسی رابطهٔ بهزیستی روان‌شناختی با تعهد سازمانی و بهره‌وری سازمانی در بین کارکنان ادارهٔ کل امور مالیاتی زاهدان*. پایان‌نامهٔ کارشناسی ارشد، دانشکدهٔ مدیریت و حسابداری دانشگاه سیستان و بلوچستان.

سخایی، م. ج. (۱۳۹۵). *چرخهٔ حیات تجزیه و تحلیل داده*. گروه فابک، فناوری اطلاعات برای کسب و کار. www.fabak.ir/ShowResourceDetailsForPublic.aspx?Side=IDqxjsB6cX4

سلیمی‌فرد، خ.؛ رضایی، ب.؛ رجبی، آ. (۱۳۹۴). شناسایی و اولویت‌بندی معیارهای مدیریت ارتباط با شهروندان در سازمان‌های دولتی. *نشریهٔ مدیریت دولتی*، ۷ (۳)، ۵۲۴-۵۰۵.

سهرابی، ب.؛ رئیسی وانانی، ا. و فروزنده جونقانی، ر. (۱۳۹۵). طبقه‌بندی و تحلیل عوامل مؤثر بر استفاده کارآمد از سیستم‌های اطلاعاتی یکپارچه در سازمان‌های دولتی ایران. *نشریه مدیریت دولتی*، ۸ (۳)، ۴۸۶-۴۵۹.

عبادی، ن. (۱۳۹۵). بررسی وضعیت بلوغ حکمرانی الکترونیک در پورتال وزارتخانه‌های کشور. *نشریهٔ مدیریت دولتی*، ۸ (۳)، ۵۱۰-۴۸۷.

محکم‌کار، ا.؛ حلاج، م. م. (۱۳۹۳). شبکه‌های اجتماعی به‌دنبال چه هستند؟ *دانش انتظامی خراسان شمالی*، ۱(۲)، ۱۰۸-۸۷.

معمار، ث.؛ عدلی‌پور، ص.؛ خاکسار، ف. (۱۳۹۱). شبکه‌های اجتماعی مجازی و بحران هویت (با تأکید بر بحران هویتی ایران). *مطالعات و تحقیقات اجتماعی در ایران*، ۱(۴)، ۱۷۶-۱۵۵.

یعقوبی، ن.؛ ابراهیم‌پور، ح.؛ شاکری، ر. (۱۳۹۵). ارائهٔ الگوی نیازهای کاربران دولت همراه در ایران. *نشریهٔ مدیریت دولتی*، ۸ (۳)، ۴۱۴-۳۹۳.

Andreesen, T. & Slemp, C. (2011). *Managing Risk in a Social Media-Driven Society*. Article from Protiviti Knowledge Leader. Available in:

https://www.iia.nl/SiteFiles/Managing%20Risk%20in%20a%20Social%20Media-Driven%20Society.pdf.

Andronikakis, A. (2012). *Social Media Risks in the Financial Sector*. Master Thesis. Department of Management Technology and Economics. Zurich University.

Ashford, W. (2013). *Social media: A security challenge & opportunity.* Available in: http://www.computerweekly.com/feature/Social-media-a-security-challenge-and-opportunity.

Belbey, J. (2015). *Protect Your Firm From The 12 Risks of Social Media.* Available in: http://www.forbes.com/sites/joannabelbey/2015/05/21/protect-your-firm-from-the-13-risks-of-social-media.

Boyd, D. M. & Ellison, N. B. (2007). Social network sites: definition, history, and scholarship. *Journal of Computer-Mediated Communication*, 13(1), 210-230.

Chi, M. (2011). *Security Policy and Social Media Use.* SANS Institute InfoSec Reading Room. Available in: https://www.sans.org/reading-room/whitepapers/policyissues/reducing-risks-social-media-organization-33749.

DiStaso, M. W., McCorkindale, T. & Wright, D. K. (2011). How public relations executives perceive and measure the impact of social media in their organizations. *Public Relations Review*, 37(3), 325-328.

Ebadi, N. (2016). Electronic Governance Portal maturity of the Ministries of Interior. *Journal of Management Faculty of Tehran University*, 8 (3), 487-510. (*in Persian*)

Esmaeelnejad Ahangarani, M. (2012). Principles and concepts of risk management. *Research and Risk Management Sina Bank*. Spring 2012. (*in Persian*)

Field, J. & Chelliah, J. (2012). Social-media misuse a ticking time-bomb for employers. *Human Resource Management International Digest*, 20 (7), 36-38.

Go, E. & You, K. H. (2016). But not all social media are the same: Analyzing organizations' social media usage patterns. *Telematics and Informatics,* 33(1), 176–186.

Griffin, J. (2014). Social Media Risk Management: Why It Matters and What You Need To Know. *Governance Directions*, 66 (7), 417-419.

Holmes, D. (2005). *Communication theory: media, technology and society*. Monash University, SAGE Publications Ltd.

Ilanaarazie, A. (2010). 5 Social Media Risks for Companies and Employees… And How To Prevent Them. Available in: http://www.adweek.com/socialtimes/5-

social-media-risks-for-companies-and-employees-and-how-to-prevent-them/15750.

Jasbi, A. (1991). *Principles of Management*. Tehran: Islamic Azad University Scientific Center. (*in Persian*)

Khan, G.F., Yoon, H.Y.& Park, H.W. (2012). Social media use in public sector: A comparative study of the Korean & US Government Paper presented at the ATHS panel during. *The 8th International Conference on Webometrics, Informatics and Scientometrics & 13th COLLNET Meeting*, 23–26 October 2012, Seoul, Kore.

Meamar, S., Adlipoor, S. & Khaksar, F. (2012). Virtual social network and identity crises, *social research and study in Iran*, 1(4), 155-176. (*in Persian*)

Mohkamkar, I. & Hallaj, M.M. (2014). What are social networks? *North Khorasan Police Disciplinary Knowledge*, 1(2), 87-108. (*in Persian*)

Picazo-Vela, S., Gutiérrez-Martínez, I. & Luna-Reyes, L. F. (2012). Understanding risks, benefits, and strategic alternatives of social media applications in the public sector. *Government Information Quarterly*, 29 (4), 504–511.

Pempek, T., Yermolayeva, Y. & Calvert, S. (2009). College students' social networking experiences on facebook. *Journal of Applied Developmental Psychology*, 30(3), 227-238.

Punjabi, V. (2014). *Security Risks / Threats & Rewards in Social Media*. Master's Thesis, University of Oulu, Department of Information Processing Science.

Rosenblum, D. (2007). What anyone can know: The privacy risks of social networking sites. *IEEE Security and Privacy*, 5(3), 40-49.

Rustakhiz, A. (2012). *Investigate the relationship between psychological well-being and organizational efficiency and organizational commitment among the employees of Tax departments of Zahedan.* Master Thesis. Faculty of management, Sistan-Baluchistan University. (*in Persian*)

Sakhaee, M.J. (2016). *Data Life cycle analysis. Group Fabk, information technology for business*. Available in: http://www.fabak.ir/ShowResourceDetailsForPublic.aspx?Side=3UDYEd2DHK4. (*in Persian*)

Salimifard, KH., Rezaei, B. & Rajabi, A. (2015). Identification and prioritization criteria relationship management with citizens in government agencies. *Faculty of Tehran University Management Journal*, 7(3), 505-524. (*in Persian*)

Sohrabi, B., Raeesi, E. & Forouzandeh, R. (2016). Classify and analyze the factors affecting the efficient use of integrated information systems in government

agencies in Iran. *Faculty of Tehran University Management Journal*, 8 (3), 459-486. (*in Persian*)

Steenkamp, M. & Hyde-Clarke, N. (2014). The use of Facebook for political commentary in South Africa. *Telematics and Informatics*, 31(1), 91–97.

Wilson, J. (2009). Social networking: the business case. *Journal of Engineering & Technology*, 4(10), 54-56.

Yaghuby, N. M., Ebrahimpour, H. & Shakeri, R. (2016). Model providing the users with the Iranian government. *Journal of Management Faculty of Tehran University*, 8 (3), 393-414. (*in Persian*)