Media Management Review
ISSN 2821-1774 (Online)

Influential Factors of Data Protection on Users' Trust in Social Media: A Situational Analysis

Dorsa Momenikhah
MSc. Department of Media Management, Faculty of Management, University of Tehran, Tehran, Iran. E-mail: momenikhah@ut.ac.ir

Seyed Mahdi Sharifi
Associate Prof., Department of Business Management, Faculty of Management, University of Tehran, Tehran, Iran. E-mail: sharifee@ut.ac.ir

Mohammad Reza Jalilvand (Corresponding Author)
Assistant Prof., Department of Business Management, Faculty of Management, University of Tehran, Tehran, Iran. E-mail: rezajalilvand@ut.ac.ir

Abstract

Objective

Using the Internet and its developing facilities has become intertwined with people's lives so that many things are done only through this space. Data storage on different servers is another aspect of using the Internet and social media, which requires building trust between internet users and implementing data protection policies. This paper investigates the influential factors in data protection regarding social media's trustworthiness for users.

Research Methodology

The participants consisted of 27 cyberspace and social media experts, who were selected through judgmental and snowball sampling. The method of data analysis is Grounded Theory with Clark's situational analysis approach. In this method, all data is obtained from coding interviews with media industry professionals.

Findings

The components of data protection in social media and human/non-human factors of data protection affecting the trust of social media users were identified. As a result of code analysis, social media will be able to take this path with the support of the technical and hardware components. Poor quality and usability, access of the information and security institutions of the Islamic Republic of Iran to users' data, unequal marketing of Iranian social media platforms in comparison with international peers, and monopolization of Iranian social media through

extensive governmental filtering of some international social media platforms are some of the crucial factors that have led society to distrust social media. This study has identified the factors affecting data protection on the trust of social media users with the grounded theory approach, which is innovative in terms of method.

Undoubtedly, studying different aspects of social media extension has been got vital. One of these aspects which recently has been highlighted in social studies is user personal data protection. Social media platforms request their users to create a profile at first and this would result in sharing personal information. Users give data usage permission to social media companies voluntarily to communicate with others worldwide. Although social media expansion has developed social communications, it can put users in danger. Considering the previous studies, no research was found about recognizing the effective elements of users' trust, and problems regarding user rights protection. Furthermore, identifying the elements is useful for creating a new social media or understanding the cause of the prevalence of a particular social platform among users in comparison with others. In this research, we are evaluating the data protection policies in social media to gain an in-depth understanding of the reasons behind trusting social networks. The research results can contribute to the research literature in the field of trust in social networks.

According to studies, there are several key suggestions for active players in the field of social media. First, the social media managers are recommended to pay special attention to enhancing the quality and performance of these networks, regularly developing and updating the server's security, and providing proper support for a significant amount of registration. Second, several interviews have pointed out the creativity in national social networks' terms of service along with equal marketing opportunities and preventing monopolization. Social media managers are recommended to focus their efforts on creativity, updating their knowledge, and creating equal marketing opportunities. Finally, some of the participants stated that the clarity of the amount of access of social networks to users' data and building mental trust regarding the data protection in these networks are among the other important factors that social media managers must consider.

Conclusion

In this research, some other factors related to the components of protection of social media users also human and non-human factors that affect social media users' trust were identified using grounded theory and Clarke's approach. If social media management takes steps to develop secure servers, it can create operational assurance for users to ensure the protection of servers. The ease of use and desirable quality of social media can automatically increase the trust and acceptance of users towards that media.

The key factors decreasing the trust in Iranian social media can be blamed on the lack of desirable quality, user-unfriendliness, and access of Iranian government security agency to users ' data and unfair marketing of Iranian social media with extensive filtering of some foreign social media. Creating trust for users in a society is a long-term process and requires practical persuasion with diverse methods. One of the consequences of selling user data for advertising is

the lack of faithful representation of information by the user that it can disrupt the full and accurate protection of data and support and counter criminal action. The universality of social media and global trust is the other component of data protection. that is, on the one hand, when social media is global or pervasive in society, and the trusted people of the community and the celebrities are social media members, the possibility of data protection is reinforced increase in their minds and make it possible to select that social media. On the other hand, creating a framework by the user to limit access to personal data, the relationship between user trust and the amount of data value, and the type of social media usage of data and authorization to use user's data affect their trust. Whatever the extent to which the number of users in social media is greater; causes more value, then acceptance by other people will be easier. Whether which social media belongs to which country as owned, and where it is managed, is an indication of who has access to users' data or at least has easier access. For this reason, users have less willingness to use some social networks that increase their concern over stakeholders about accessing their data.

Keywords: Social media; Online trust; Data protection; User.

Citation: Momenikhah, Dorsa; Sharifi, Seyed Mahdi & Jalilvand, Mohammad Reza (2022). Influential factors of data protection on users' trust in social media: a situational analysis. *Media Management Review*, 1(4), 415-440. (*in Persian*)

Media Management Review, 2022, Vol. 1, No.4, pp. 415-440
doi: https://doi.org/10.22059/MMR.2023.352256.1035
Published by University of Tehran, Faculty of Management
Article Type: Research Paper

Received: October 10, 2022
Received in revised form: December 06, 2022
Accepted: December 16, 2022
Published online: March 19, 2023

بررسی‌های مدیریت رسانه
شاپا الکترونیکی: ۱۷۷۴-۲۸۲۱

واکاوی مؤلفه‌های تأثیرگذار محافظت از داده‌ها در اعتمادزایی کاربران رسانه‌های اجتماعی: یک تحلیل موقعیتی

درسا مؤمنی خواه
کارشناسی ارشد، گروه مدیریت رسانه، دانشکده مدیریت، دانشگاه تهران، تهران، ایران. رایانامه: momenikhah@ut.ac.ir

سیدمهدی شریفی
دانشیار، گروه مدیریت بازرگانی، دانشکده مدیریت، دانشگاه تهران، تهران، ایران. رایانامه: sharifee@ut.ac.ir

محمدرضا جلیلوند (نویسندهٔ مسئول)
استادیار، گروه مدیریت بازرگانی، دانشکده مدیریت، دانشکدگان فارابی، دانشگاه تهران، تهران، ایران. رایانامه: rezajalilvand@ut.ac.ir

چکیده

هدف: استفاده از اینترنت و امکانات رو به توسعه آن، به‌گونه‌ای با زندگی انسان‌ها عجین شده است که بسیاری از کارها، فقط از طریق استفاده از این فضا انجام می‌شود. جنبه دیگر استفاده از اینترنت و فضای مجازی، ذخیره‌سازی دست‌کم بخشی از اطلاعات افراد در سرورهای مختلف است که این مهم، برای ایجاد اعتماد کاربران فضای اینترنت است تا از داده‌های آنان حفاظت شود. در پژوهش حاضر تلاش شده است تا به این سؤال پاسخ داده شود: «مؤلفه‌های تأثیرگذار محافظت از داده‌ها در اعتمادزایی کاربران رسانه‌های اجتماعی کدامند؟».

روش: مشارکت‌کنندگان این پژوهش، ۲۷ نفر از خبرگان حوزه فضای مجازی و رسانه‌های اجتماعی بوده است که از طریق نمونه‌گیری‌های قضاوتی و گلوله برفی انتخاب شده‌اند. روش تحلیل داده، تئوری داده‌بنیاد با رویکرد تحلیل موقعیت کلارک است.

یافته‌ها: مؤلفه‌های محافظت از داده‌ها در رسانه‌های اجتماعی و عاملان انسانی/ غیرانسانی محافظت از داده‌های مؤثر بر اعتماد کاربران رسانه‌های اجتماعی شناسایی شد. طبق نتایج، مؤلفه‌های فنی و سخت‌افزاری، پشتیبان رسانه اجتماعی برای طی‌کردن این مسیر خواهند بود. از موضوعات مهمی که اعتماد به رسانه‌های اجتماعی را کاهش می‌دهد و سبب واپس‌زدگی جامعه به آن‌ها می‌شود، می‌توان به کیفیت نامطلوب، صعبوت کاربری، دسترسی نهادهای اطلاعاتی و امنیتی نظام جمهوری اسلامی ایران به داده‌های کاربران و به‌دنبال آن، بازاریابی نابرابر رسانه‌های اجتماعی ایرانی در قبال رسانه‌های اجتماعی خارجی و انحصارطلبی رسانه‌های اجتماعی ایرانی با انجام فیلترینگ گسترده نسبت به اغلب رسانه‌های اجتماعی خارجی، اشاره کرد.

نتیجه‌گیری: یکی از چالش‌های پیش روی هر رسانه آنلاین، جلب اعتماد مخاطبان است. رسانه‌های آنلاین باید تلاش کنند که مخاطبان را راضی کنند تا اطلاعات خود را با آن‌ها در میان بگذارند و این امر، بر پایه اعتماد بنا می‌شود. در فضای مجازی، افراد آزادانه اطلاعات روزانه خود را در اختیار دیگران می‌گذارند، بدون توجه به اینکه این پلتفرم‌ها قادرند علایق و سرگرمی‌هایی را که آن‌ها به‌اشتراک می‌گذارند، تحت نظارت قرار دهند. این امر می‌طلبد که پلتفرم‌ها در حفظ حریم خصوصی کاربران کوشا باشند تا اثر شبکه‌ای آن‌ها افزایش یابد.

کلیدواژه‌ها: رسانه‌های اجتماعی؛ اعتماد آنلاین؛ حفاظت از داده‌ها؛ کاربر.

استناد: مؤمنی خواه، درسا؛ شریفی، سیدمهدی و جلیلوند، محمدرضا (۱۴۰۱). واکاوی مؤلفه‌های تأثیرگذار محافظت از داده‌ها در اعتمادزایی کاربران رسانه‌های اجتماعی: یک تحلیل موقعیتی. *بررسی‌های مدیریت رسانه*، ۱(۴)، ۴۱۵-۴۴۰.

بررسی‌های مدیریت رسانه، ۱۴۰۱، دوره ۱، شماره ۴، صص. ۴۱۵-۴۴۰
ناشر: دانشکدهٔ مدیریت دانشگاه تهران
نوع مقاله: علمی ـ پژوهشی

تاریخ دریافت: ۱۴۰۱/۰۷/۱۸
تاریخ ویرایش: ۱۴۰۱/۰۹/۱۵
تاریخ پذیرش: ۱۴۰۱/۰۹/۲۵
تاریخ انتشار: ۱۴۰۱/۱۲/۲۸
doi: https://doi.org/10.22059/MMR.2023.352256.1035

مقدمه

حفاظت از اطلاعات شخصی کاربران، به مشکلی مهم در ارتباطات شبکه‌ای تبدیل شده است. به همین دلیل استفاده از فناوری‌های خاص و معیارهای سازمان‌یافته به‌منظور حفاظت از حریم خصوصی کاربران ضرورت پیدا کرده است (رومنسکی[1]، ۲۰۱۴). محیط‌های اطلاعاتی و ارتباطی جدید، برای گسترش ارتباطات اجتماعی فرصتی تازه ایجاد می‌کند؛ اما می‌تواند بر حریم خصوصی کاربران نیز اثرهای نامطلوبی داشته باشد. در این رابطه، حفاظت از اطلاعات شخصی، مشکل مهمی در خدمات توزیع‌شده، ارتباطات شبکه‌ای و خدمات ابری[2] است (لیتون[3]، ۲۰۱۷). هدف از این اقدام‌ها جلوگیری از دسترسی‌های غیرقانونی و استفاده از اطلاعات پروفایل افراد، به‌منظور اهداف سودجویانه است. شبکه‌های اجتماعی، گاهی ممکن است خصوصی‌ترین بخش زندگی افراد را نیز دربربگیرند و مشکلات متعددی را برای کاربران سبب شوند. از آنجایی که اطلاعات منتشر شده در فضای مجازی، به‌طور عمومی در دسترس است، این امکان وجود دارد که بعضی افراد، بدون رضایت کاربر مربوطه، به انتشار اطلاعات او بپردازند. در شبکه‌های اجتماعی کاربران می‌توانند دانش شخصی را با استفاده از خدمات مختلف انتقال دهند، پروفایل‌های شخصی، نظرها، پیام‌های خصوصی، فیلم‌های چندرسانه‌ای و پیام‌ها را به اشتراک بگذارند (لیو، آینسورت و بامیستر[4]، ۲۰۱۶).

میزان حریم خصوصی در شبکه‌های اجتماعی بسیار متفاوت است. در بعضی از سایت‌ها، برای ثبت‌نام، اطلاعات محدودی مانند نام و تاریخ تولد را از کاربر می‌خواهند؛ اما سایت‌های بسیاری وجود دارد که اطلاعات بیشتری در خصوص زندگی اجتماعی، جنسیت، ملیت، علاقه‌مندی‌ها، سرگرمی‌ها، روابط، دین و حتی دیدگاه سیاسی، اجتماعی و فرهنگی را از کاربر طلب می‌کنند. تمامی شبکه‌های اجتماعی به‌منظور کنترل این وضعیت، باید از سیاست‌های مرتبط با امنیت فناوری اطلاعات و ارتباطات پیروی کرده و ابزاری را در جهت حفاظت از داده‌های کاربران تنظیم کنند. در واقع سیستم امنیت اطلاعات شخصی، مجموعه‌ای از ابزارهای فنی و سازمانی برای تحقق حفاظت از ساختارهای داده‌های شخصی توسط کنترل‌کنندهٔ داده‌ها است. تمامی مراحل پردازش داده‌های شخصی که از ابزارهای اطلاعاتی، ارتباطی و فناوری استفاده می‌کنند، باید از لحاظ جزئیات تعیین سیاست حفاظت از داده برای شبکه‌های اجتماعی و حفاظت از داده‌های شخصی تحلیل شوند (شریف و همکاران[5]، ۲۰۱۹).

یکی از مشکلات اساسی هر رسانهٔ آنلاین، این است که بتواند اعتماد مخاطبان را جلب کند. رسانه‌ها تمام تلاش خود را به‌کار می‌گیرند تا مخاطبان راضی شوند که اطلاعات خود را با آن کسب‌وکار در میان بگذارند و این اتفاق، بر پایهٔ اعتماد بنا شده است؛ اما در فضای مجازی، پلتفرم‌هایی ایجاد شده است که افراد، به‌صورت آزادانه، اطلاعات روزانهٔ خود را در اختیار دیگران می‌گذارند، بدون توجه به این نکته که علایق و سرگرمی‌هایی که به اشتراک می‌گذارند، می‌تواند آن‌ها

1. Romansky
2. Cloud services
3. Roslyn Layton
4. Liu, Ainsworth & Baumeister
5. Shareef et al.

را تحت نظارت قرار دهد. اگر وضعیت بی‌اعتمادی در مبادلهٔ ارزش حل نشود، به‌سادگی افراد بیشتری اجازه نخواهند داد که رسانه‌ها از داده‌های شخصی آنان استفاده کنند (کیث دوار[1]، ۲۰۱۷).

به‌طور کلی روش‌های حفاظت از داده‌ها، یکی از عواملی است که بر اعتماد کاربران در خصوص استفاده از رسانه‌های اجتماعی تأثیر می‌گذارد. به‌طور مثال، اگر کاربران اطمینان داشته باشند، اطلاعات شخصی‌ای که در یک رسانهٔ اجتماعی ثبت می‌کنند تا زمان مشخصی در سرورهای پشتیبانی آن شبکه باقی می‌ماند و پس از آن حذف می‌شود یا پس از گذشت زمان معینی می‌توانند از «حق بر فراموشی» استفاده کرده و داده‌های خود را از سرورهای پشتیبانی حذف کنند، برای ثبت‌نام در شبکه‌های اجتماعی ترغیب می‌شوند (اوپال جایاسین[2]، ۲۰۱۸). نیاز به حفاظت از داده‌های شخصی با این حقیقت تعیین می‌شود که حریم خصوصی، حق مهم انسانی و ترکیبی است از پردازش مستقل حقوق فردی و پردازش کافی اطلاعات شخصی، شکل مختلفی از ارتباطات شخصی توسط پست و اینترنت و حفظ امنیت پروفایل‌های شخصی در فروم‌های اجتماعی و گروه‌ها (کینست، آشکنازی و میرون[3]، ۲۰۱۴). این امر به‌منزلهٔ نوعی سیاست امنیتی قوی است که برای هر هدف خاص در ارتباطات شخصی و پشتیبانی از پروفایل افراد تعریف می‌شود؛ زیرا استفاده از فناوری اطلاعات و ارتباطات معاصر، الزامات جدیدی را برای سیاست حفاظت از داده‌های شخصی مطرح می‌کند و درک حریم خصوصی در جامعهٔ جهانی را تغییر می‌دهد (ویکرت[4]، ۲۰۱۳). این سیاست باید برای حفظ حریم خصوصی، اثربخشی معنایی و ابزاریِ حفاظت از داده‌های شخصی را در جامعهٔ جدید شبکه‌های ارتباطی و به‌ویژه در شبکه‌های اجتماعی افزایش دهد (براون[5]، ۲۰۱۲).

اکنون دو پرسش مهم این است که اعتماد به شبکه‌های اجتماعی چگونه ایجاد می‌شود؟ چگونه مردم به یک رسانهٔ اجتماعی اعتماد می‌کنند؛ اما رسانه‌ای دیگر را پس می‌زنند؟ پاسخ این دو پرسش با حریم خصوصی و اصول حفاظت از اطلاعات شخصی ارتباط دارد. بر این اساس، پژوهش حاضر دو هدف را دنبال می‌کند: یک) شناسایی مؤلفه‌های تأثیرگذار محافظت از داده‌ها بر اعتماد کاربران رسانه‌های اجتماعی؛ دو) شناسایی عاملان انسانی/غیرانسانی محافظت از داده‌های مؤثر بر اعتماد کاربران رسانه‌های اجتماعی.

اعتماد الکترونیکی

ماهیت اعتماد الکترونیک بسیار ذهنی، پیچیده و چندجانبه است (زیوکویک[6]، ۲۰۱۸؛ گودارد[7]، ۲۰۱۷). کمتر تعریف دقیقی از اعتماد الکترونیک در ادبیات وجود دارد؛ به‌طور مثال، اعتماد الکترونیک را می‌توان اعتماد مشتریان آنلاین در نظر

1. Keith Dewar
2. Jayasinghe
3. Kinast, Ashkenazy & Meron
4. Weichert
5. Brown
6. Živković
7. Goddard

گرفت (ترن و گوانگ وو[1]، ۲۰۱۹). اغلب مطالعات پیشین به سه بُعد اصلی در خصوص اعتماد الکترونیکی اشاره کرده‌اند که عبارت‌اند از: اعتبار، شایستگی و اطمینان (لئونارد[2]، ۲۰۱۹؛ المتولی و بابین[3]،۲۰۲۰). بینور[4] (۲۰۱۰) این اعتماد را نوعی باور به مبادلهٔ توانایی بین دو یا چند دسته در فراگرد ارتباطی می‌داند و فورتین، دلاهوکا و دلاهوکا[5] (۲۰۰۲) تفاوت بین اعتماد الکترونیک و اعتماد عمومی را در فاصلهٔ بین خریداران و فروشندگان در نظر می‌گیرد.

پلتفرم‌های رسانه‌های اجتماعی، به‌طور فزاینده‌ای از هوش مصنوعی استفاده می‌کنند. هوش مصنوعی از جریان‌های گسترده‌ای از محتوای دیجیتالی تغذیه می‌شوند و گاهی برای تحلیل رفتار کاربر، حالت ذهنی و محتوا به‌کار می‌روند (میتلزتاد و همکاران[6]، ۲۰۱۶). انواع جدیدی از محتواهای تولید شده در حوزهٔ هوش مصنوعی و عوامل مجازی محرک هوش مصنوعی، اشکال جدیدی از ریسک‌ها را در استفاده از رسانه‌های اجتماعی ارائه می‌کنند، که پیش‌بینی آن دشوار است. بنابراین ارائهٔ رسانهٔ اجتماعی معتمد، به‌طور فزاینده‌ای، اعتمادپذیری مؤلفه‌های هوش مصنوعی آن را نشان می‌دهد (لوویس و مورکنز[7]، ۲۰۲۰). ریسک‌های موجود ممکن است با خطرهایی در استفاده از رسانه‌های اجتماعی همراه باشند که پیش‌بینی آن مشکل خواهد بود؛ برای مثال، دستکاری محتوای صوتی و تصویری، مثل استفاده از فناوری دیپ‌فیک، معاملات بسیار اقناع‌گر در آژانس‌های فروش و تشخیص دروغ یا هدف‌گیری صحیح در زمینهٔ محتوا (لوویس و مورکنز، ۲۰۲۰). قابلیت اعتماد هوش مصنوعی در بحث سیاست‌گذاری عمومی، از سال ۲۰۱۷ مطرح شد و متخصصان برجستهٔ حوزهٔ هوش مصنوعی، در کنفرانس اسیلمر[8]، آن را رواج دادند (آیندهٔ مؤسسهٔ زندگی[9]، ۲۰۱۷).

حفاظت از داده‌ها و اطلاعات

جامعهٔ اطلاعاتی فرصت‌های متفاوتی برای دسترسی از راه دور به منابع اطلاعاتی توزیع شده و ارتباطات بین کاربران از طریق محیط‌های مجازی، خدمات فضای ابری، رسانه‌های اجتماعی و... ایجاد کرده است. تمام این ابعاد جهانی‌شدن باعث می‌شود که کاربران، پروفایل خود را با داده‌های شخصی ایجاد کرده و اطلاعات شخصی خود را منتشر کنند. آیا این داده‌ها به روش مطمئنی محافظت می‌شوند؟ این سؤال مهمی است که هر کاربر باید از خودش بپرسد. پاسخ این پرسش با حریم خصوصی و اصول حفاظت از اطلاعات شخصی مرتبط است. اصول اصلی حفاظت از اطلاعات شخصی، بر اساس الگوی سازمانی، چرخهٔ زندگی و سیاست حفاظت از داده‌ها، در چارچوب سیاست امنیتی و به‌طور خاص مرتبط با سیاست امنیت اطلاعات و ارتباطات ارائه شده است (رومنسکی، ۲۰۱۴).

1. Tran & Quang Vu
2. Leonnard
3. Elmetwaly & Babin
4. Bennur
5. Fortin, Dholakia & Dholakia
6. Mittelstadt et al.
7. Lewis & Moorkens
8. Asilomar
9. Future of Life Institute

به‌طور معمول، حفاظت از داده‌ها و حریم خصوصی کاربر، هدف اصلی سرویس‌های شبکه‌های اجتماعی است. حریم خصوصی نه‌تنها حفاظت از اطلاعات شخصی را دربرمی‌گیرد، بلکه هر آنچه کاربران بر اساس پروفایل خودشان منتشر می‌کنند و احتمالاً می‌خواهند تنها برای مخاطبان خودشان در دسترس باشد نیز پوشش می‌دهد (گراس و آکیوستی[1]، ۲۰۰۵). علاوه بر این، حریم خصوصی در ارتباطات نیز باید به‌طور جدی در نظر گرفته شود؛ از این رو، هیچ‌یک از طرفین، به‌طور مستقیم مخاطب دسته‌ای از افراد یا به‌صراحت مورد اعتماد افرادی قرار نمی‌گیرد که احتمال داشته باشد آن‌ها را در ارتباطات و حافظه‌ای مشترک ردیابی کند. از این گذشته، جزئیات پیام‌ها باید پنهان نگه داشته شود، بنابراین افراد دیگر می‌توانند فقط از درخواست‌کردن[2] و پاسخ‌گرفتن[3] افراد اطلاع داشته باشند. در نهایت، باید از افشای اطلاعات شخص ثالث بدون موافقت وی، به اعضایی که شخص ثالث به آن‌ها اعتماد ندارد، جلوگیری شود.

به‌طور خلاصه، حریم خصوصی در وهلهٔ نخست، به‌دنبال امکان پنهان‌کردن هرگونه اطلاعات دربارهٔ هر کاربر، حتی تا حد پنهان‌کردن مشارکت آن‌ها در شبکه‌های اجتماعی آنلاین است. علاوه بر این، حفاظت از حریم خصوصی باید به‌صورت پیش‌فرض در نظر گرفته شود؛ یعنی تمام اطلاعات مربوط به کاربران و اعمال آن‌ها، باید از هر وجه داخلی یا خارجی در سیستم پنهان شود، مگر اینکه آشکارا توسط خود کاربر و به خواست و میل او فاش شود (بوید[4]، ۲۰۰۸). به‌عنوان بخشی از یکپارچگی و حفظ امانت، هویت و اطلاعات کاربر باید در برابر تغییرات و دستکاری‌های غیرمجاز محافظت شود. علاوه بر تشخیص تغییر و تعدیل ردیابی و اکتشاف و اصالت‌سنجی پیام، یکپارچگی و حفظ امانت در زمینهٔ شبکه‌های اجتماعی آنلاین، باید گسترده و تعمیم داده شود (سوفوس[5]، ۲۰۰۷).

ایجاد حساب‌های کاربری ساختگی و جعلی، حساب‌های کاربری شبیه‌سازی‌شده[6] یا انواع دیگر از جعل هویت، در سرویس‌های شبکه‌های اجتماعی سنتی آسان است. با این حال، کاربران، به‌طور ذاتی، به رسانه‌های اجتماعی آنلاین اعتماد بسیار زیادی دارند و نشان داده شده است که این ترکیب ممکن است به انواع جدیدی از آسیب‌پذیری‌ها منجر شود. در نتیجه، تأیید اعتبار وجود اشخاص حقیقی در پشت هر حساب کاربری که در شبکه‌های اجتماعی آنلاین ثبت شده، باید تضمین شود. بررسی هویت لزوماً باید توسط سرویس‌های خدمات متمرکز صورت بگیرد؛ اما تمام سرویس‌های شناسایی و اعتباربخشی هویت باید مورد اعتماد همهٔ شرکت‌کنندگان باشند (بیلگ[7]، ۲۰۰۹).

داده‌های بزرگ[8] به دارایی عظیم و فوق‌العاده‌ای برای بسیاری از سازمان‌ها تبدیل شده است و عملیات‌های بهبودیافته و فرصت‌های تجاری جدید را وعده می‌دهد. با این حال، داده‌های بزرگ، دسترسی به اطلاعات حساس را افزایش داده است؛ اطلاعاتی که با پردازش آن‌ها، حریم خصوصی افراد به‌طور مستقیم به خطر می‌افتد و قوانین حفاظت

1. Gross & Acquisti
2. Requesting
3. Responding
4. Boyd
5. Sophos
6. Cloned accounts
7. Bilge
8. Big data

از داده‌ها را نقض می‌کند. در نتیجه، ممکن است به کنترل‌کنندگان و پردازشگرهای داده‌ها، مجازات‌های سختی برای عدم مطاوعت و پیروی تحمیل کند که به ورشکستی منجر شوند (گروسکا، ماورودیس، ویشی و جانسن[۱]، ۲۰۱۸).

اصطلاح داده‌های بزرگ، حجم عظیم یا پیچیده‌ای از داده‌ها را توصیف می‌کند، داده‌های ساختاریافته و ساختارنیافته که می‌توانند برای ایجاد ارزش تحلیل شوند. این مسئله، از دو جنبه از تحلیل داده‌های بزرگ نشئت گرفته است: اول اینکه هرچه میزان اطلاعات بیشتر باشد، احتمال شناسایی افراد در مجموعه داده‌هایی که به نظر می‌رسد ارتباطی با اطلاعات شخصی ندارند، بیشتر می‌شود. دوم، تجزیه‌وتحلیل داده‌های بزرگ قادر به استنباط از داده‌های شخصی «بی‌ضرر» است که بسیار حساس‌تر بوده و قرار نیست توسط شخص تحت تأثیر قرار گرفته، آشکار شود. در این زمینه، مثالی معروف در نشریهٔ فوربس[۲] وجود دارد که تجزیه‌وتحلیل الگوهای خرید برای ایجاد تبلیغات سفارشی و هدفمند توسط یک دپارتمان فروش در اروپا صورت گرفته و واکاوی اطلاعات برای ارائهٔ پیشنهادهای بهتر به مخاطب انجام شده است و در آن، الگوریتم‌ها به‌درستی استنباط می‌کنند که یک دختر نوجوان باردار بوده است (هیل[۳]، ۲۰۱۲). همچنین بخش‌های دیگری وجود دارد که تهدیدهای حریم خصوصی در آن‌ها می‌تواند مهم‌تر هم جلوه کند، مانند بخش درمان یا تحقیقات پزشکی (موسترت، بردنورد، بیسارت و واندلین[۴]، ۲۰۱۶).

پیشینهٔ پژوهش

اعتماد به رسانه‌ها را به اعتماد مردم به نظام سیاسی و نهادهای آن نیز وابسته می‌دانند و این رابطه به شکل متقابل وجود دارد؛ یعنی رسانه‌ها در جامعه می‌توانند با اعمال بی‌طرفی در جلب اطمینان و اعتماد مردم به کل نظام، سهم بسزایی داشته باشند. ناگفته نماند که بعضی صاحب‌نظران پارادایم منتقد، به‌دلیل اینکه رسانه‌ها نمی‌توانند بی‌طرف باشند، نگرش اعتبار رسانه‌ای و اعتماد به آن را باور ندارند. بی‌طرفی اسطوره‌ای بیش نیست؛ چراکه رسانه‌ها بر مبنای اقتصاد بازار عمل می‌کنند که به‌معنای خالی‌کردن میدان برای طبقات سلطه‌جویی است که به‌دنبال دائمی‌کردن سلطهٔ خود بر طبقات پایین هستند (اورلوسکی[۵]، ۲۰۱۱).

در بعضی تحقیقات، قابل اعتماد بودن رسانه، به شهرت و خوش‌نامی ارتباط‌گر نسبت داده شده است. در این تحقیقات محققان به موضوعاتی همچون عینیت[۶]، صحت[۷]، دقت[۸]، دستکاری کردن[۹]، جذابیت[۱۰]، اقتدار منبع[۱۱]، سهولت

1. Gruschka, Mavroeidis, Vishi & Jensen
2. Forbes
3. Hill
4. Mostert, Bredenoord, Biesaart, & van Delden
5. Orlowski
6. Objectivity
7. Truth
8. Accuracy
9. Articulation
10. Attraction
11. Authoritativeness

دسترسی[۱]، باورپذیر بودن[۲]، سوگیری[۳]، شفافیت[۴]، رقابت[۵]، سازگاری[۶]، پویا بودن[۷]، حرفه‌ای بودن[۸] و کیفیت[۹] پرداخته‌اند (دام دام و گارسیا[۱۰]، ۲۰۰۹).

شریف و همکاران (۲۰۱۹) دریافتند که شکل‌گیری اولیه اعتماد به شبکه‌های اجتماعی، به پنج عاملِ انتظارات برآورده شده، قابلیت پیش‌بینی، آشنایی، نظارت و هنجارها وابسته است. این مطالعه در بنگلادش انجام شد؛ چرا که کشورهای درحال توسعه بیشتر در معرض بی‌ثباتی اجتماعی، سیاسی و اقتصادی قرار دارند. به‌علاوه، یافته‌ها نشان داد که کمبود اجتماعی مبتنی بر انتظارات، مهم‌ترین عامل گسترش اعتماد اولیه در میان هم‌سالان یک گروه رسانهٔ اجتماعی است. رومنسکی (۲۰۱۴) به بررسی رسانه‌های اجتماعی بر اساس الگوی سازمانی، چرخهٔ زندگی و سیاست حفاظت از داده‌ها، در چارچوب امنیتی به خصوص در رابطه با سیاست امنیت اطلاعات و ارتباطات پرداخت. به اعتقاد وی، «واقعیت این است که جوانان ترجیح می‌دهند با شبکه‌های اجتماعی ارتباط برقرار کنند؛ چون دسترسی به گروه‌ها و انجمن‌هایی که در شبکه‌های اجتماعی ایجاد می‌شود، آسان است؛ با این حال باید دسترسی به داده‌های شخصی کاربران محدود شود. به همین دلیل کمیسیون اروپا در ژانویه ۲۰۱۲ با توجه به توسعهٔ تکنولوژیکی سریع، جهانی‌سازی و چالش‌های جدید در حفاظت از داده‌ها، قوانین جدیدی را برای تقویت حقوق حمایت از داده‌های آنلاین پیشنهاد کرده است. نتیجه‌گیری این است که توسعه و بهره‌برداری بیشتر از فضای مجازی، بدون حمایت کافی و قوی از حقوق کاربران تحقق پیدا نمی‌کند». گوپتا و دیهامی[۱۱] (۲۰۱۵)، تأثیر امنیت، اعتماد و دغدغه‌های حریم خصوصی بر تمایل به اشتراک‌گذاری اطلاعات در فیس‌بوک را بررسی کردند. نتایج نشان داد که امنیت و حریم خصوصی بر اعتماد تأثیر می‌گذارد و تأثیر حریم خصوصی بر اعتماد بیشتر و قوی‌تر است. به‌علاوه، امنیت و اعتماد ادراک‌شده بر اشتراک‌گذاری اطلاعات مؤثرند؛ اما بین حریم خصوصی و اشتراک‌گذاری اطلاعات، ارتباطی وجود ندارد. سوخو، ژانگ و بیلگیهان[۱۲] (۲۰۱۵) عوامل پیش‌بینی‌کنندهٔ قصد مسافران در خصوص مشارکت در تبادل اطلاعات مربوط به سفر در شبکه‌های اجتماعی را بررسی کردند؛ یافته‌ها نشان داد که اعتماد و سرگرمی از عواملی محسوب می‌شوند که بر قصد اشتراک‌گذاری اطلاعات تأثیر می‌گذارند. هافمن، لوتز و رانیزی[۱۳] (۲۰۱۶) بعضی از ابزارهای رایج قانونی برای حفاظت از رکوردها در حریم خصوصی، حفاظت از داده‌ها و مکان‌یابی داده‌ها را ارزیابی کردند. به اعتقاد این محققان، مقررات حفاظت از داده‌های عمومی (GDPR)[۱۴] اتحادیهٔ اروپا، سیاستی کاربردی نیست و معتقدند که این مقررات نمی‌توانند از حریم خصوصی و حقوق کاربران محافظت کنند. راه‌حل

1. Availability
2. Believability
3. Bias
4. Clarity
5. Competitiveness
6. Composure
7. Dynamism
8. Expertise
9. Qualification
10. Dumdum, & Garcia
11. Gupta & Dhami
12. Sukhu, Zhang & Bilgyhan
13. Hoffmann, Lutz & Ranzini
14. General Data Protection Regulation

پیشنهادی آن‌ها کنترل داده‌ها و اطلاعات از زمان دریافت آن‌هاست. به بیان دیگر، باید هنگام ثبت اطلاعات، ابزارهای طبقه‌بندی و کنترل‌های امنیتی لازم اعمال شود. به بیان دیگر، باید مدل حفاظت از حریم خصوصی، به‌جای تأکید بر اطلاعات، بر داده‌های شخصی تمرکز کند تا قدرت بررسی چالش‌های موجود در زمینهٔ حفظ امنیت داده‌ها و اعتماد را داشته باشد. لوییس و مورکنز (۲۰۲۰) بیان کردند که پلتفرم‌های رسانه‌های اجتماعی، به‌طور فزاینده‌ای از هوش مصنوعی استفاده می‌کنند که از جریان‌های گسترده‌ای از محتوای دیجیتالی تغذیه می‌شوند و گاهی برای تحلیل رفتار کاربر، حالت ذهنی و محتوای فیزیکی به‌کار می‌روند. انواع جدید محتوای تولیدشدهٔ هوش مصنوعی و عوامل مجازی مبتنی بر هوش مصنوعی، اشکال جدیدی از خطرها را در استفاده از رسانه‌های اجتماعی ایجاد می‌کنند که پیش‌بینی آن دشوار خواهد بود. به این ترتیب، رسانه‌های اجتماعی قابل اعتماد، به‌طور فزاینده‌ای تحت تأثیر قابلیت اعتماد مؤلفه‌های هوش مصنوعی آن، قرار دارد. لیتون و همکاران (۲۰۱۷) در بررسی مقررات حفاظت از داده‌های عمومی کمیسیون اروپا، به این نتیجه رسیدند که اتحادیهٔ اروپا، تمرکز بر چهار ورودی دانش کاربر[1]، طراحی فناوری[2]، شیوه‌های ارائه‌دهندگان[3] و مؤسسه‌ها[4] را توصیه می‌کند. مقررات حفاظت از داده‌های عمومی، به‌طور عمده روی تجارب ارائه‌دهندگان و مؤسسه‌ها متمرکز است. شکاف مهم موجود در مقررات حفاظت از داده‌های عمومی، این است که در آن، دانش کاربر به‌عنوان ابزاری برای حفظ حریم خصوصی و حفاظت از داده‌ها مورد بحث قرار نمی‌گیرد و فناوری‌های بهبود حریم خصوصی، به‌سختی شناخته و ترویج می‌شوند.

روش‌شناسی پژوهش

این پژوهش از منظر فلسفی، تفسیرگرا و از منظر رویکرد، استقرایی است؛ چرا که از داده‌های کیفی حاصل از مصاحبه‌های نیمه‌ساختاریافته[5]، برای پاسخ‌گویی به سؤال‌های پژوهش استفاده می‌کند. استراتژی پژوهش نیز مبتنی بر گراندد تئوری به‌شیوهٔ تحلیل موقعیتی کلارک است. برای مشارکت در پژوهش، از خبرگان و متخصصان حوزهٔ رسانه‌های اجتماعی، فناوری اطلاعات و داده‌کاوی دعوت به عمل آمد. در مجموع، پس از مصاحبه با ۲۷ نفر از مشارکت‌کنندگان، اشباع نظری حاصل شد. در این پژوهش برای افزایش اعتبار نتایج، از دو روش پیشنهادی کرسول استفاده شد:

الف) رجوع به منابع و استفاده از ادبیات نظری، از جمله پژوهش‌های خارجی و داخلی گوناگون، مصاحبه با خبرگان و اساتید صنعت رسانه، داده‌کاوی و پژوهشگران این حوزه‌ها.

ب) توضیح مفصل و غنی[6] که ثبت همهٔ مراحل در رسم نقشه‌های سه‌گانهٔ وضعیت، عرصه‌ها و موقعیت را شامل می‌شود. این مسئله، نسخه‌های نامنظم و منظمی را دربرمی‌گیرد که نسخه‌های منظم، به‌شکلی ساخت‌یافته تنظیم شده و برای خوانندگان پژوهش قابل بازیابی است. الگوی مورد استفادهٔ گراندد تئوری در این پژوهش، «تحلیل موقعیت»[7] نام دارد که

1. User knowledge
2. Technology design
3. Practices of providers
4. Institutions
5. Semi-structured interviews
6. Thick description
7. Situational Analysis

توسط کلارک مطرح شده است (کلارک[1]، ۲۰۰۵). کلارک درصدد بود که با رویکـردی جدیـد بـه تحلیـل، در چـارچوب گراندد تئوری، آن را به‌شکلی کامل‌تر، به‌سمت چرخش پسامدرن هدایت کند. تحلیل موقعیت، هم به کنشگران و عاملان غیرانسانی و هم به عاملان و کنشگران ضمنی دخیل، توجه نشان می‌دهد. همچنین این نظریه، عوامل ضعیف‌تر و همین طور پیامد اقدام‌های دیگران را بر آن عاملان بررسی می‌کنـد. افـزون بـر ایـن، موضـوعاتی را بررسـی مـی‌کنـد کـه بـا ساخت‌های گفتمانی کنشگران و عاملان غیرانسانی در ارتباط است. الگوی تحلیل موقعیـت، بـه بسـتر پـژوهش نگـاهی عمیق دارد و موضوعی را که پژوهش روی آن انجام می‌شود، تحـت عنـوان مـوقعیتی سرشـار از عـاملان، کنشـگران و گفتمان‌های مختلف بررسی می‌کند. به‌سبب نبود ادبیات نظری کامل و مطلوب در حوزۀ مؤلفه‌های تأثیرگذار محافظـت از داده‌ها بر اعتماد کاربران رسانه‌های اجتماعی، در پژوهش حاضر با هدف پردازش نظریه، به اتصال مقولـه‌هـا توجـه شـده است، نه توصیف صرف از آن‌ها.

یافته‌های پژوهش

پس از انجام مطالعه و بررسی دقیق و عمیق مصاحبه‌ها و همچنین، اطلاعات و داده‌های به‌دست‌آمده، نخسـت تـک‌تـک مصاحبه‌ها تجزیه‌وتحلیل شد و استخراج کدهای اولیه صورت گرفت. برای انجام طبقه‌بندی دقیق مفاهیم در مقوله‌ها، هر مفهوم، پس از تفکیک برچسب خورد و داده‌های خام نیز، از طریق بررسی دقیق متن مصاحبه‌ها و یادداشت‌های زمینه‌ای، مفهوم‌سازی شدند تا مفهوم‌ها و مقوله‌ها ساخته شوند. در واقع طبقه‌بندی داده‌های به‌دست‌آمده، به ساخت مفاهیم منجـر می‌شود و مجموعه‌ای از چند مفهوم، یک مقوله را شکل می‌دهد. گـزاره‌هـای معنـادار، همـۀ آنچـه را در مصـاحبه ارزش مفهومی و معنایی دارد، شامل می‌شود. تعداد گزاره‌های معنادار استخراج‌شده از مصاحبه‌ها متفاوت بود؛ بـه‌طـوری کـه در یک مصاحبه، ۳۷ گزارۀ معنادار و در مصاحبه‌ای دیگر، فقط ۴ گزاره معنادار استخراج شد. به‌طور میانگین، از هـر مصـاحبه حدود ۱۷ گزارۀ معنادار به‌دست آمد. گزاره‌های معنادار، معمولاً به جمله‌هـایی گفتـه مـی‌شـود کـه در راسـتای پاسـخ بـه سؤال‌های اصلی پژوهش بیان شده است و در مراحل کدگذاری، هر یک حامل کد یا پیامی برای راهنمایی پژوهشگر بـه مفاهیم پژوهش است و منبع مهمی برای مفاهیم اصلی پژوهش شمرده می‌شود. در مجموع بـرای هـر دو سـؤال، ۱۰۷۲ گزارۀ کلامی شناسایی شد که از این تعداد، ۹۹۵ گزاره معنادار بودنـد. از ۹۹۵ گـزاره معنـادار ایـن مصـاحبه‌هـا، ۹۲۰ کـد استخراج شد که با حذف موارد تکراری ۸۳۸ زیرمقوله و ۵۱ مقولۀ هسته‌ای استخراج شد.

سؤال اول. مؤلفه‌های تأثیرگذار محافظت از داده‌ها بر اعتماد کاربران رسانه‌های اجتماعی کدامند؟

کدهای اولیه در قالب مقوله‌های بالقوه دسته‌بندی شدند و تمام خلاصه داده‌های کدگذاری شده، در قالب مقوله‌های مشخص مرتب شد. در این مرحله، بعضی کدهای اولیه در گروه مقولۀ اصلی قرار گرفت، بعضـی در گـروه مقولـۀ فرعـی طبقه‌بندی شد و بقیه حذف شدند. در جدول ۱ بخشی از کدهای نهایی، فرایند احصا و استخراج مقوله‌ها برای سـؤال اول ارائه شده است.

1. Adele,E.Clarke

جدول ۱. کدها و مقوله‌های مربوط به سؤال اول پژوهش

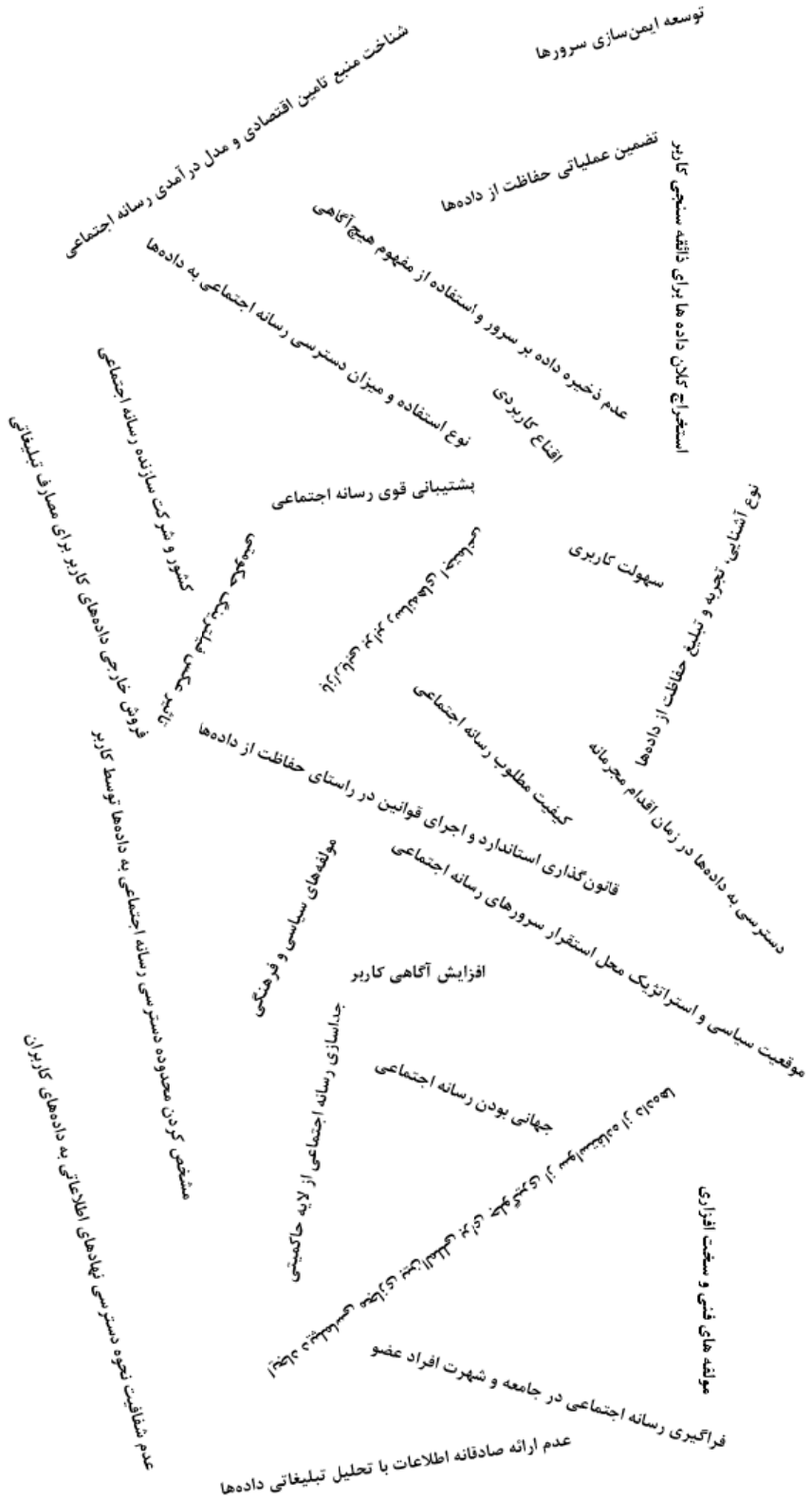
کدهای استخراج شده	مقوله‌ها
رعایت الزامات فنی حفاظت از داده‌ها در تنظیم‌گری حاکمیت	مؤلفه‌های فنی و سخت‌افزاری
عملکرد منفی دولت در مواجهه با تهدیدهای سایبری	
وجود زیرساخت قوی	
ایجاد یک جامعهٔ شبکه‌ای و دسترسی شبکه‌محور به داده‌ها در رسانهٔ اجتماعی	
بهبود کارایی رسانهٔ اجتماعی در مرور زمان با اضافه‌شدن امکانات	آگاهی کاربران
افزایش اعتماد کاربر عادی با تحلیل تبلیغاتی داده‌ها در مسیر بهبود کارایی	
افزایش آگاهی کاربران و استفاده از متخصصان امنیت شبکه برای ارتقای امنیت سرورها	
شفاف‌سازی و پذیرش نحوهٔ عملکرد رسانهٔ اجتماعی در بدو ورود	
جلب همراهی افکار عمومی از مؤلفه‌های حفاظت از داده‌ها	
میزان سواد رسانه‌ای کاربران	
آموزش و فرهنگ‌سازی دربارهٔ محافظت فردی کاربر از داده‌های خود	
آگاه‌سازی از علل تحلیل تبلیغاتی داده‌ها با هدف بهبود کارایی	
بستر اجتماعی زندگی مردم بر میزان اعتماد آنان به رسانه‌های اجتماعی	مؤلفه‌های سیاسی و فرهنگی
برخورداری از سرمایهٔ اعتماد اجتماعی در خصوص عوامل حفاظت از داده‌ها	
نقش صفات جمعیت‌شناختی کاربران در ایجاد اعتماد به رسانهٔ اجتماعی	
حضور افراد مهم، معتمد و مشهور در رسانهٔ اجتماعی	فراگیری رسانهٔ اجتماعی در جامعه و شهرت افراد عضو
فراگیری و شهرت رسانهٔ اجتماعی در جامعه	
ایجاد اقتصاد توجه با تمرکز افراد زیاد در رسانهٔ اجتماعی	
حضور بنگاه‌های رسمی و رسانه‌های معتبر در یک رسانه	
عدم کاربرد تشویق و تنبیه برای عضویت در یک رسانهٔ اجتماعی	اقناع کاربردی
تبلیغات و اعتمادسازی از منظر روانی	
کاربرد مثبت تشویق و اقناع کاربردی برای استفاده از رسانهٔ اجتماعی	
عدم کیفیت مطلوب رسانهٔ اجتماعی ایرانی	کیفیت مطلوب رسانهٔ اجتماعی
عدم کاهش کیفیت با تبادل اطلاعات بیشتر در رسانهٔ اجتماعی خارجی	
بهبود برندینگ رسانهٔ اجتماعی	
عملکرد تکنولوژیک مناسب رسانهٔ اجتماعی	
اعتمادسازی با تبدیل نقاط ضعف دیگر رسانه‌های اجتماعی به نقطه قوت رسانهٔ اجتماعی داخلی	
طراحی و گرافیک مناسب	
آسان بودن و سرعت دسترسی به رسانهٔ اجتماعی	سهولت کاربری
متغیر مهارتی کاربران	
عدم سهولت کاربری و از دسترس خارج شدن ناگهانی رسانهٔ اجتماعی داخلی و ایجاد احساس عدم امنیت	
به‌خطر افتادن حریم خصوصی برای دستیابی به‌راحتی بیشتر در استفاده از رسانه‌های اجتماعی	

ادامهٔ جدول ۱

کدهای استخراج شده	مقوله‌ها
تبلیغات رسانهٔ اجتماعی مبنی بر حفاظت و امنیت داده‌ها	نوع آشنایی، تجربه و تبلیغ حفاظت از داده‌ها
نحوهٔ تبلیغ و آشنایی با رسانهٔ اجتماعی	
اعتماد به دوستان در پیشنهاد یک رسانهٔ اجتماعی	
نقل و انتقال تجربیات کاربران در خصوص حفاظت از داده‌ها	
نقش تبلیغات فراگیر بر افزایش احتمالی اعتماد کاربر	
نقش وجود همانندی در ارزش‌ها و علایق کاربران در افزایش اعتماد دیگران به رسانهٔ اجتماعی	
اعتماد به مدیریت رسانهٔ اجتماعی از جهت حفظ داده‌ها	تضمین عملیاتی حفاظت از داده‌ها
محرمانگی داده‌هایی با امکان اخلال در زمینهٔ استفاده کاربر	
کنترل دسترسی دیگران به داده‌های کاربر با توجه به ذخیره داده‌ها روی مرکز داده	
عدم سوءاستفاده و حفاظت پدیدآورندهٔ رسانهٔ اجتماعی از داده‌های انباشت شده روی سرور	
ارائه مستمر گزارش در راستای حفاظت از داده‌های کاربر	
کاربرد منفی ذهنیت دسترسی نهاد حاکمیت به داده‌های کاربر در رسانهٔ اجتماعی ایرانی	عدم شفافیت نحوهٔ دسترسی نهادهای اطلاعاتی به داده‌های کاربران
عدم ایجاد حس وفاداری در کاربر با القای ذهنیت دسترسی مراجع مختلف به داده‌ها	
رصد شدن داده‌های کاربران رسانهٔ اجتماعی	
اخبار سوءاستفاده و دسترسی نهادهای امنیتی به داده‌های کاربران رسانه‌های اجتماعی ایرانی بر ایجاد حساسیت و کاهش اعتماد کاربر	
عدم تکذیب اخبار دسترسی نهادهای امنیتی به اطلاعات کاربران	
استفادهٔ امنیتی و اطلاعاتی برای نظارت بر عملکرد کاربران	
تلقی حس دخالت، کنترل‌گری و اعمال سلیقه با دسترسی نهادهای امنیتی به داده‌ها	
عضویت کاربران در بعضی رسانه‌های اجتماعی داخلی بدون اطلاع آنان	
نقش شفافیت عملکرد دولت بر افزایش اعتماد کاربران ایرانی	
خلاف قوانین تلقی شدن بسیاری از کنش‌ها در ایران سبب نگرانی کاربر از دسترسی حاکمیت به داده‌ها	
عدم دسترسی نهادهای امنیتی ایرانی به داده‌های کاربران در رسانه‌های اجتماعی خارجی	
استفاده از کلان داده‌ها و الگوهای رفتاری کاربر برای مصارف امنیتی و سیاسی	

بر اساس نتایج کدگذاری در مرحلهٔ قبل، نسخهٔ ساخت‌نیافتهٔ نقشهٔ موقعیت[1] مؤلفه‌های تأثیرگذار محافظت از داده‌ها بر اعتماد کاربران رسانه‌های اجتماعی ترسیم شده است.

1. Messy situational maps



شکل ۱. نقشهٔ موقعیت؛ نسخهٔ ساخت‌نیافته مؤلفه‌های محافظت از داده‌ها در رسانه‌های اجتماعی

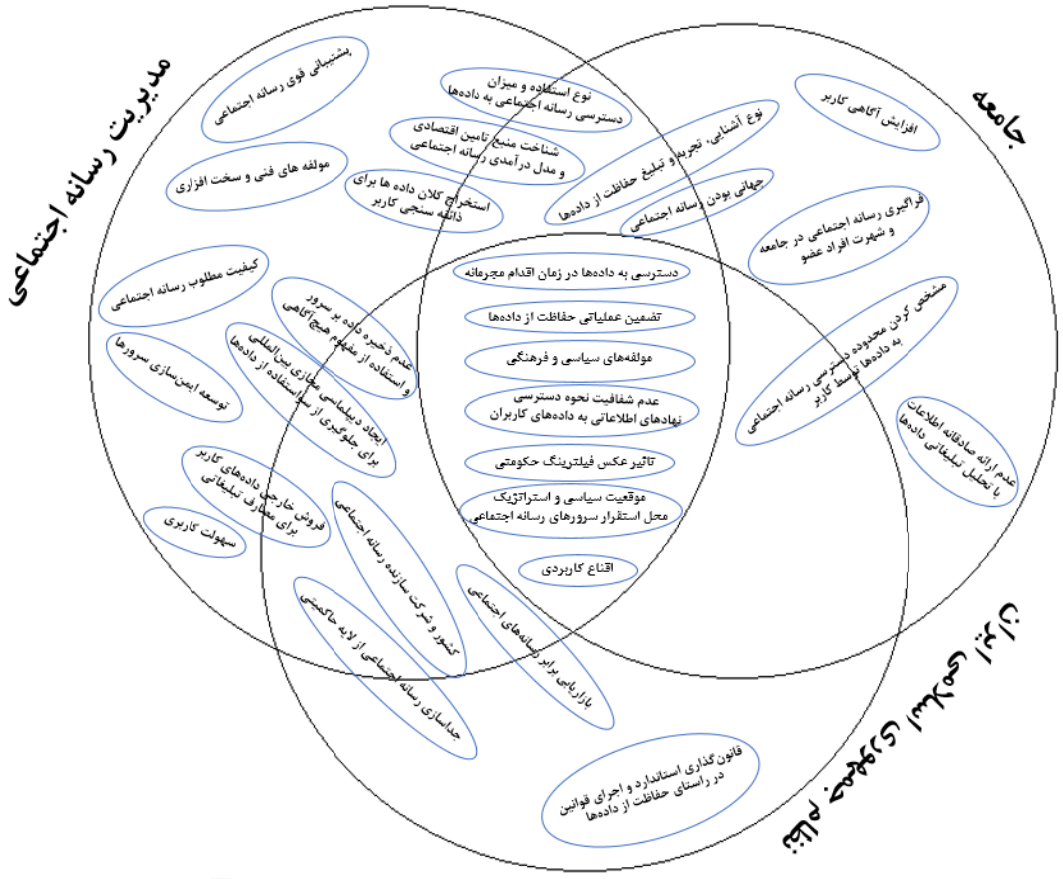
پس از ترسیم نقشهٔ ساخت‌نیافته، عوامل، مؤلفه‌ها، کنشگران و گفتمان‌های مؤلفه‌های محافظت از داده‌ها در رسانه‌های اجتماعی، از دیدگاه‌ها و چشم‌اندازهای متفاوت توصیف شد و به تدوین نقشه موقعیت ساخت یافته (منظم)[1] مؤلفه‌های محافظت از داده‌ها در رسانه‌های اجتماعی انجامید.

عناصر/عوامل خاص انسانی عدم ارائه صادقانهٔ اطلاعات با تحلیل تبلیغاتی داده‌ها، مشخص کردن محدودهٔ دسترسی رسانهٔ اجتماعی به داده‌ها توسط کاربر	**عناصر/عوامل غیرانسانی** مؤلفه‌های فنی و سخت‌افزاری، توسعهٔ ایمن‌سازی سرورها، پشتیبانی قوی رسانهٔ اجتماعی
عوامل/عناصر انسانی جمعی جهانی بودن رسانهٔ اجتماعی، فراگیری رسانهٔ اجتماعی در جامعه و شهرت افراد عضو	**عوامل/عناصر ضمنی/خاموش** افزایش آگاهی کاربر، سهولت کاربری، کیفیت مطلوب رسانهٔ اجتماعی
ساخت‌های گفتمانی عوامل انسانی جمعی اقناع کاربردی، بازاریابی برابر رسانه‌های اجتماعی، نوع آشنایی، تجربه و تبلیغ حفاظت از داده‌ها	**ساخت‌های گفتمانی عوامل غیرانسانی** همانند آنچه که در موقعیت یافت می‌شود
عوامل سیاسی/اقتصادی مؤلفه‌های سیاسی، شناخت منبع تأمین اقتصادی و مدل درآمدی رسانهٔ اجتماعی، موقعیت سیاسی و استراتژیک محل استقرار سرورهای رسانهٔ اجتماعی، فروش خارجی داده‌های کاربر برای مصارف تبلیغاتی	**عوامل اجتماعی ـ فرهنگی/نمادین** تأثیر عکس فیلترینگ، مؤلفه‌های فرهنگی، استخراج کلان داده‌ها برای ذائقه‌سنجی کاربر
عوامل حقوقی تضمین عملیاتی حفاظت از داده‌ها، قانون‌گذاری استاندارد و اجرای قوانین در راستای حفاظت از داده‌ها، دسترسی به داده‌ها در زمان اقدام مجرمانه، ایجاد دیپلماسی مجازی بین‌المللی برای جلوگیری از سوءاستفاده از داده‌ها	**عوامل فرازمانی** کشور و شرکت سازندهٔ رسانهٔ اجتماعی، عدم ذخیره داده بر سرور و استفاده از مفهوم هیچ‌آگاهی
مباحث/موضوعات اصلی (معمولاً مناشقه برانگیز) جداسازی رسانهٔ اجتماعی از لایهٔ حاکمیتی	**گفتمان‌های مرتبط (تاریخی، روایی، و/یا بصری)** عدم شفافیت نحوه دسترسی نهادهای اطلاعاتی به داده‌های کاربران، نوع استفاده و میزان دسترسی رسانهٔ اجتماعی به داده‌ها
عناصر دیگر که در موقعیت یافت می‌شوند	

شکل ۲. نقشهٔ موقعیت؛ نسخهٔ ساخت‌یافته مؤلفه‌های محافظت از داده‌ها در رسانه‌های اجتماعی

1. Ordered situational maps

سرانجام، در این بخش، عرصه‌ها و جهان‌های اجتماعی که در سؤال اول موجود بود، ترسیم شد. عرصه‌ها بر موضوعات و مسائلی تمرکز دارند که تمامی جهان‌های اجتماعی دخیل و کنشگران، به عملکرد آن‌ها در چارچوب موضوعات متعهدند و گفتمان‌هایی را دربارهٔ آن‌ها تولید کرده‌اند. نقشهٔ عرصه‌ها/جهان‌های اجتماعی مؤلفه‌های محافظت از داده‌ها در رسانه‌های اجتماعی در شکل زیر ارائه شده است.



شکل ۳. نقشهٔ عرصه‌ها/جهان‌های اجتماعی مؤلفه‌های محافظت از داده‌ها در رسانه‌های اجتماعی

سؤال دوم. عاملان انسانی/غیرانسانی محافظت از داده‌ها مؤثر بر اعتماد کاربران رسانه‌های اجتماعی کدامند؟

برای پاسخ‌گویی به سؤال دوم، کدهای نهایی از نتایج ۲۷ مصاحبه با مشارکت کنندگان استخراج و در مجموع، ۲۲ مقولهٔ کلیدی احصا شد. در جدول۲ بخشی از کدهای نهایی، فرایند احصا و استخراج مقوله‌ها برای سؤال دوم ارائه شده است.

جدول ۲. کدها و مضامین مربوط به سؤال دوم پژوهش

کدهای استخراج شده	مقوله‌ها
حضور افراد مهم، معتمد و مشهور در رسانهٔ اجتماعی	حضور افراد مشهور
شهرت مدیر رسانهٔ اجتماعی و اعتباربخشی به آن رسانه از عوامل انسانی	اعتبار مدیر رسانهٔ اجتماعی در حفاظت از داده‌ها
دارنده مجوز رسانهٔ اجتماعی دارای مسئولیت محافظت از داده‌ها در آن رسانه	
مدیران ارشد و مسئول فنی رسانهٔ اجتماعی مسئول حفاظت از داده‌ها در آن رسانه	
مدیر و سازنده رسانهٔ اجتماعی مسئول حفاظت از داده‌ها در آن رسانه	
بالا بودن امنیت شبکه در برابر هکرها از عوامل غیرانسانی	امنیت شبکه و سرورها
افزایش امنیت شبکه با استفاده از متخصصان ذبده از عوامل انسانی	
توسعهٔ ایمن‌سازی سرورها از عوامل غیرانسانی	
استفاده از راه‌کارهای تکنولوژیک برای کاهش خطرهای ناشی از عوامل غیرانسانی	
لزوم تدوین راه‌حلی برای پیشبرد هم‌زمان موضع سهولت‌کاربری و حفاظت از حریم خصوصی	
افشای اطلاعات کاربران و هک شدن از عوامل انسانی	
اطمینان حفاظت از داده‌های کاربران رسانهٔ اجتماعی	
لزوم افزایش امنیت شبکه با افزایش تعداد کاربران از عوامل انسانی	
گارد گرفتن مخاطب در برابر رسانه‌های وابسته به حکومت	عدم وابستگی رسانهٔ اجتماعی به نهاد حاکمیت
شفاف‌سازی روابط سازندگان رسانهٔ اجتماعی با نهادهای حاکمیتی	
سرعت رسانهٔ اجتماعی از عوامل غیرانسانی (عدم سرعت ایرانی تأثیر عکس)	کیفیت مطلوب
کیفیت مطلوب و جذابیت رسانهٔ اجتماعی (با نگاه به تجربه اپلیکیشن‌های آپ و ۷۸۰)	
آپشن‌های رسانهٔ اجتماعی از عوامل غیرانسانی مؤثر بر اعتماد	
نبود جنبهٔ کارآفرینانه در رسانهٔ اجتماعی داخلی از عوامل غیرانسانی	
لزوم تدوین راه‌حلی برای پیشبرد هم‌زمان موضع سهولت‌کاربری و حفاظت از حریم خصوصی	
واپس‌زدگی و کوچ مجدد به رسانهٔ اجتماعی خارجی با وجود کیفیت نامطلوب و پاسخ‌گویی مناسب به نیازهای کاربر در رسانه‌های اجتماعی ایرانی	
به‌روزرسانی مداوم رسانه‌های اجتماعی خارجی	
سهولت کاربری در رسانهٔ اجتماعی خارجی از عوامل غیرانسانی (کُندی سرعت داخلی‌ها، تأثیر عکس)	
طراحی نامناسب رسانهٔ اجتماعی ایرانی از عوامل غیرانسانی	
کیفیت نامطلوب رسانهٔ اجتماعی ایرانی از عوامل غیرانسانی	
تفاوت میزان تأثیر عدم حفاظت کامل از داده‌ها با توجه به موقعیت رشد رسانهٔ اجتماعی (برای نمونه فیس‌بوک)	
نقش مثبت به‌روزرسانی و بهبود کارایی رسانهٔ اجتماعی داخلی با اضافه شدن امکانات	
ضعف ساختاری و خدماتی از عوامل غیرانسانی	

ادامهٔ جدول ۲

کدهای استخراج شده	مقوله‌ها
سیاست‌زدگی فضای کشور در حوزه رسانه‌های اجتماعی و آسیب‌دیدگی صنعت رسانه در ایران از عوامل انسانی	عدم اعتماد به حاکمیت در ایران
عدم اعتماد مردم به قوانین پیشنهادی حاکمیت با توجه به پیشینه اقدامات آنان	
ترجیح بعضی کاربران به بی‌قانونی درباره حفاظت از داده‌ها نسبت به حفاظت حاکمیت از داده‌ها	
کاهش اعتماد به رسانهٔ اجتماعی ایرانی با توجه به عملکرد کلی نظام سیاسی در ارتباط با مردم	
ترجیح رصد شدن توسط رسانهٔ اجتماعی خارجی در مقایسه با داخلی به علت پیشینه برخوردهای حکومت از عوامل انسانی مؤثر بر اعتماد	
کاربرد منفی تزریق احساس کنترل‌گری حکومت به مردم با فیلتر تلگرام از عوامل غیرانسانی	ایجاد احساس کنترل‌گری
دخالت سلیقه‌ای رسانهٔ اجتماعی خارجی بر محتوای منتشره از سوی کاربر(نمونه اینستاگرام و قاسم سلیمانی)	
ایجاد اشتراک قوانین ایران با قوانین بین‌المللی در حوزه حفاظت از داده‌ها	اشتراک قوانین داخلی با قوانین بین‌المللی
برنامه نویسان از عوامل انسانی مؤثر بر اعتماد در سطح فنی	نیروی انسانی خلاق
نیروی فنی خلاق از عوامل انسانی مؤثر بر اعتماد در سطح فنی	
برخورداری از تجهیزات مناسب از عوامل غیرانسانی	تجهیزات فنی و سخت‌افزاری
محدودیت‌های فنی از عوامل غیرانسانی	
ذخیره و طبقه‌بندی داده‌ها بر حسب الگوریتم‌های هوشمند با هدف کنترل دسترسی از عوامل غیرانسانی	
ضعف تکنولوژی رسانه‌های اجتماعی داخلی از عوامل غیرانسانی	
عدم وجود زیرساخت‌های مناسبت برای حفاظت از داده‌ها در ایران	
سخت‌افزار و زیرساخت مناسب از عوامل غیرانسانی	

بر اساس شناسایی تمام عوامل انسانی، غیرانسانی، گفتمانی، نمادین و غیره، در تحلیل و بررسی مصاحبه با ۲۷ نفر از متخصصان حوزهٔ رسانه و اساتید دانشگاهی این حوزه، نسخهٔ ساخت‌نیافته نقشهٔ موقعیت عاملان انسانی/غیرانسانی محافظت از داده‌ها مؤثر بر اعتماد کاربران رسانه‌های اجتماعی ارائه شد. مهم‌ترین مؤلفه‌ها و عوامل انسانی و غیرانسانی دخیل در فرایند محافظت از داده‌ها مؤثر بر اعتماد کاربران رسانه‌های اجتماعی به شرح زیر است:

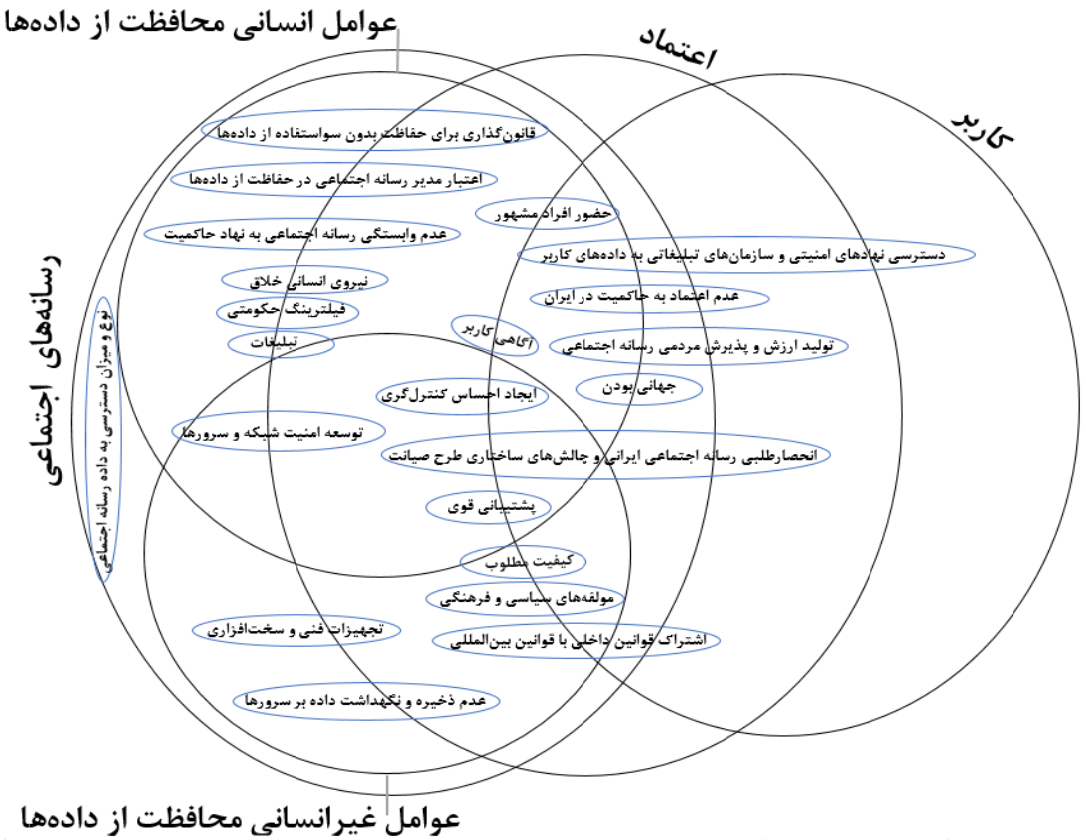
شکل ٤. نقشه موقعیت؛ نسخهٔ ساخت‌نیافته عاملان انسانی/غیرانسانی محافظت از داده‌ها مؤثر بر اعتماد کاربران رسانه‌های اجتماعی

پس از ترسیم نقشهٔ ساخت‌نیافته، عاملان انسانی/غیرانسانی و مؤلفه‌ها، کنشگران و گفتمان‌های مرتبط با شناسایی این عوامل در محافظت از داده‌ها که بر اعتماد کاربران رسانه‌های اجتماعی مؤثر است، از دیدگاه‌های مختلفی توصیف شد.

عناصر/عوامل خاص انسانی آگاهی کاربر، نیروی انسانی خلاق، اعتبار مدیر رسانهٔ اجتماعی در حفاظت از داده‌ها	**عناصر/عوامل غیرانسانی** کیفیت مطلوب، پشتیبانی قوی، تجهیزات فنی و سخت‌افزاری، توسعهٔ امنیت شبکه و سرورها
عوامل/عناصر انسانی جمعی حضور افراد مشهور، جهانی بودن	**عوامل/عناصر ضمنی/خاموش** بی‌اعتمادی به حاکمیت در ایران، ایجاد احساس کنترل‌گری
ساخت‌های گفتمانی عوامل انسانی جمعی تولید ارزش و پذیرش مردمی رسانهٔ اجتماعی	**ساخت‌های گفتمانی عوامل غیرانسانی** همانند آنچه در موقعیت یافت می‌شود
عوامل سیاسی/اقتصادی مؤلفه‌های سیاسی، تبلیغات	**عوامل اجتماعی ـ فرهنگی/نمادین** فیلترینگ، مؤلفه‌های فرهنگی،
عوامل حقوقی قانون‌گذاری برای حفاظت بدون سوءاستفاده از داده‌ها، اشتراک قوانین داخلی با قوانین بین‌المللی	**عوامل فرازمانی** عدم ذخیره و نگهداشت داده بر سرورها
مباحث/موضوعات اصلی (معمولاً مناشقه برانگیز) عدم وابستگی رسانهٔ اجتماعی به نهاد حاکمیت، انحصارطلبی رسانهٔ اجتماعی ایرانی و چالش‌های ساختاری طرح صیانت	**گفتمان‌های مرتبط (تاریخی، روایی، و/یا بصری)** نوع و میزان دسترسی به دادهٔ رسانهٔ اجتماعی
عناصر دیگر که در موقعیت یافت می‌شوند	

شکل ۵. نقشهٔ موقعیت؛ نسخهٔ ساخت‌یافته عاملان انسانی/غیرانسانی محافظت از داده‌ها مؤثر بر اعتماد کاربران رسانه‌های اجتماعی

سرانجام، نقشهٔ عرصه‌ها/ جهان‌های اجتماعی عاملان انسانی/ غیرانسانی محافظت از داده‌های مؤثر بر اعتماد کاربران رسانه‌های اجتماعی در شکل ۶ نشان داده شده است. عرصه‌ها بر مسائلی تمرکز دارند که تمامی جهان‌های اجتماعی دخیل و کنشگران، به عمل در چارچوب آن‌ها متعهدند و گفتمان‌هایی را در خصوص آن‌ها تولید کرده‌اند.



شکل ٦. نقشهٔ عرصه‌ها/جهان‌های اجتماعی عاملان انسانی/غیرانسانی محافظت از داده‌ها مؤثر بر اعتماد کاربران رسانه‌های اجتماعی

بحث و نتیجه‌گیری

در پژوهش حاضر موارد دیگری در خصوص مؤلفه‌های حفاظت از داده‌های کابران رسانه‌های اجتماعی و همچنین عوامل انسانی و غیرانسانی محافظت از داده‌ها که بر اعتماد کاربران رسانه‌های اجتماعی اثر می‌گذارد با استفاده از نظریه داده‌بنیاد با رویکرد کلارک معرفی شد. به‌منظور پاسخ‌گویی به سؤال اول، نخست نقشهٔ موقعیت ساخت‌نیافته و پس از آن، نقشهٔ موقعیت ساخت‌یافته و در نهایت، نقشهٔ عرصه‌ها/جهان‌های اجتماعی برای دستیابی به مؤلفه‌های محافظت از داده‌ها در رسانه‌های اجتماعی ترسیم شد.

در این بخش سه عرصه یا جهان اجتماعی دخیل وجود دارد که عبارت‌اند از: جامعه، مدیریت رسانهٔ اجتماعی و نظام جمهوری اسلامی ایران. موارد مطرح شده حول این سه عرصه و اغلب به‌صورت درهم‌تنیده عنوان شده‌اند. در صورتی که مدیریت رسانهٔ اجتماعی در مسیر توسعهٔ ایمن‌سازی سرورها گام بردارد، می‌تواند نوعی تضمین عملیاتی برای کاربران در خصوص اطمینان از حفاظت از داده‌هایشان ایجاد کند. این مهم با راه‌کارهایی همچون پشتیبانی قوی از داده‌های کاربر صورت می‌پذیرد. پشتیبانی از داده‌ها بدان معناست که در صورت سوءاستفاده، امکان پیگرد قانونی و جلوگیری از سوءاستفاده ایجاد شود. مؤلفه‌های فنی و سخت‌افزاری، پشتیبان رسانهٔ اجتماعی برای طی کردن این مسیر خواهند بود.

همچنین مواردی چون سهولت کاربری و کیفیت مطلوب رسانهٔ اجتماعی می‌تواند به‌صورت ناخودآگاه اقبال و اعتماد کاربر به رسانهٔ اجتماعی را فراهم کند.

از موارد مهمی که اعتماد به رسانه‌های اجتماعی ایرانی را کاهش می‌دهد و سبب واپس‌زدگی جامعه به آن‌ها می‌شود، کیفیت نامطلوب، عدم سهولت کاربری، دسترسی نهادهای اطلاعاتی و امنیتی نظام جمهوری اسلامی ایران به داده‌های کاربران و به‌دنبال آن، بازاریابی نابرابر رسانه‌های اجتماعی ایرانی در قبال رسانه‌های اجتماعی خارجی و انحصارطلبی رسانه‌های اجتماعی ایرانی با انجام فیلترینگ گستردهٔ بعضی رسانه‌های اجتماعی خارجی است؛ همان گونه که جامعه به رسانهٔ اجتماعی تلگرام، اعتمادی بیش از دیگر رسانه‌ها پیدا کرد؛ اما در سال ۱۳۹۶، در پی اعتراضات مردم در بازهٔ زمانی خاص، این رسانه فیلتر شد. این مسائل تأثیر کشور و شرکت سازندهٔ رسانهٔ اجتماعی را پررنگ کرد و اهمیت موقعیت سیاسی و استراتژیک محل قرارگیری سرورهای رسانهٔ اجتماعی برای کاربران را نشان داد. جداسازی رسانهٔ اجتماعی از لایهٔ حکومتی، از مؤلفه‌های محافظت از داده‌ها به‌شمار می‌رود. در جامعه ایران، تجربه‌های منفی پیشین و فضای عمومی جامعه در خصوص دسترسی سازمان‌های اطلاعاتی به داده‌های کاربران، عملکرد کلی نظام سیاسی ایران و بی‌اعتمادی تاریخی میان نهادهای دولتی و مردم، به کاهش اعتماد عمومی به رسانه‌های اجتماعی داخلی منجر شده است. یکی از مؤلفه‌های محافظت از داده‌ها که بر افزایش اعتماد اثرگذار است، شفافیت روابط سازندگان و مدیران رسانهٔ اجتماعی با نهادهای حاکمیتی است. قانون‌گذاری استاندارد در راستای حفاظت از داده‌ها و بی‌طرفی در حفاظت از داده‌های تمام کاربران، در زمان نبود قوانین و استانداردهای حفاظت از داده‌ها در رسانه‌های اجتماعی داخلی، یکی از عناصر مهم شناخته شده است.

از موارد دیگری که بر اعتماد کاربران اثرگذار است، شناخت منبع اقتصادی و مدل درآمدی رسانهٔ اجتماعی است. مادامی که کاربران در خصوص مدل درآمدی رسانهٔ اجتماعی اطلاعاتی نداشته باشند و ندانند که این رسانه چگونه و چرا تمام خدمات خود را به‌صورت رایگان در اختیارشان قرار می‌دهد، اعتماد آن‌ها در خصوص حفاظت از داده‌هایشان کاهش می‌یابد. البته اغلب کاربران با دسترسی صرف رسانهٔ اجتماعی به داده‌هایشان در صورت استخراج کلان‌داده‌ها با هدف ذائقه‌سنجی کاربران و بهبود کیفیت ارائه خدمات به آنان در طول زمان مخالفتی ندارند. این درحالی است که این دسترسی به مدیریت رسانهٔ اجتماعی محدود شده و اطلاعات به غیر و در خارج از پلتفرم حتی، برای استفاده تبلیغاتی به فروش نرسد. از مؤلفه‌های محافظت از داده‌ها در این خصوص، می‌توان به استفاده از مفهوم «هیچ‌آگاهی» در الگوریتم‌های حفاظت از داده‌ها اشاره کرد تا در عین احراز هویت، کاربران برای همه ناشناس باقی بمانند. ایجاد اعتماد برای کاربران در یک جامعه، پروسه‌ای طولانی‌مدت است و به اقناع کاربردی با روش‌های متنوع نیاز دارد. یکی از پیامدهای فروش داده‌های کاربر برای استفادهٔ تبلیغاتی به خارج از پلتفرم، عدم ارائهٔ صادقانه اطلاعات توسط کاربر است که این عدم صداقت، می‌تواند هم در حفاظت کامل و دقیق از داده‌ها و هم در پشتیبانی و مقابله با اقدام مجرمانه اخلال ایجاد کند. جهانی‌بودن رسانهٔ اجتماعی و برخورداری از سرمایهٔ اجتماعی و اعتماد جهانی، از دیگر مؤلفه‌های محافظت از داده‌هاست؛ یعنی زمانی که یک رسانهٔ اجتماعی جهانی باشد یا در جامعه فراگیر شود و افراد معتمد جامعه و افراد مشهور

به عضویت این رسانهٔ اجتماعی درآیند، ذهنیت محافظت از داده‌ها در فکر کاربر تقویت می‌شود و استفاده از آن رسانه را انتخاب می‌کند. با افزایش آگاهی کاربر و افزایش سواد رسانه‌ای، اطلاع کاربر از اهمیت حفاظت از داده‌ها و تصمیم‌گیری او در خصوص چگونگی این حفاظت در رسانه‌های اجتماعی مختلف، در انتخاب او اثرگذار است. ایجاد چارچوب خودانگیخته توسط کاربر برای محدودسازی دسترسی به داده‌های شخصی، ارتباط میزان اعتماد کاربر با میزان ارزش داده‌ها و نوع استفادهٔ رسانهٔ اجتماعی از داده‌ها و همچنین، اخذ اجازه برای استفاده از داده‌های کاربر بر افزایش اعتماد او مؤثر است.

در پاسخ به سؤال دوم، عوامل انسانی محافظت از داده‌ها، بسان چتری است که در جامعه گشوده شده باشد و با جای دادن هرچه بیشتر مردم در زیر سایهٔ خود، بتواند اعتماد بیشتری میان کاربران کسب کند. یکی از این عوامل، جهانی‌بودن رسانهٔ اجتماعی است. اینکه یک رسانهٔ اجتماعی جهانی باشد و میلیون‌ها نفر، به‌ویژه افراد مشهور و معتمد جوامع دیگر در آن عضو باشد، باعث می‌شود که ذهنیت خوبی در خصوص حفاظت بیشتر رسانهٔ اجتماعی از داده‌های کاربران ایجاد شود؛ بدین معنا که کاربر پیش از ورود و ایجاد حساب کاربری در رسانهٔ اجتماعی با دیدن شهرت افراد حاضر، با توجه به اعتمادش به این افراد، به رسانهٔ اجتماعی نیز با آسودگی خاطر بیشتری اعتماد می‌کند. همچنین، جهانی‌بودن سبب خلق ارزش بیشتر می‌شود. هرچه تعداد کاربران عضو در یک رسانهٔ اجتماعی بیشتر باشد، به‌دلیل خلق ارزش بیشتر، پذیرش مردمی آن نیز راحت‌تر خواهد بود. اعتبار مدیر رسانهٔ اجتماعی از حیث میزان دسترسی به داده‌های کاربران حائز اهمیت است. اینکه رسانهٔ اجتماعی متعلق به کدام کشور است و زیر نظر چه ارگان‌هایی اداره می‌شود، نمایان‌گر آن است که چه کسانی به داده‌های کاربران دسترسی کامل یا حداقل دسترسی آسان‌تری دارند. به همین سبب، کاربران در استفاده از بعضی شبکه‌های اجتماعی که نگرانی آن‌ها را از بابت دسترسی افراد ذی‌نفع به داده‌های‌شان افزایش می‌دهد، رغبت کمتری نشان می‌دهند.

سیاست‌زدگی فضای ایران در حوزهٔ رسانه‌های اجتماعی، سبب آسیب‌دیدگی کل صنعت رسانه در کشور شده است. عملکرد کلی نظام سیاسی در ارتباط با مردم سبب بی‌اعتمادی به حاکمیت شده است. یکی از علل رشد کُند رسانه‌های اجتماعی داخلی، تأثیر بُعد سیاسی و فرهنگی و تجربه‌های پیشین کاربران حاکی از دسترسی نهادهای امنیتی و اطلاعاتی به داده‌های کاربران است. بعضی رسانه‌های اجتماعی داخلی، مانند بیسفون، فارغ از میزان کارآمد بودن، در مواجهه با مسیر طولانی و سخت جلب اعتماد کاربران، خیلی زود از رده خارج شدند و نتوانستند پیشرفت کنند. بعضی دیگر نیز مانند پیام‌رسان بله، تلاش می‌کنند با ایجاد امکاناتی چون خدمات مالی و بانکی، به‌آهستگی مسیر رشد را سپری کنند. تأثیر حفاظت از داده‌ها بر کاربر، مسیری یکتا و مشخص را نمی‌پیماید. به‌طور مثال، زمانی که اطلاعات فیس‌بوک برای انتخابات سیاسی فروخته شد، این رسانهٔ اجتماعی به مرحله‌ای از رشد خود رسیده بود که پس از انتشار این خبر نیز، از رده خارج نشد؛ اما انتشار اخباری مبنی بر دسترسی نهادهای امنیتی به داده‌های کاربران در رسانه‌های اجتماعی داخلی، با توجه به نوپا بودن اغلب آن‌ها، احساس کنترل‌گری، واپس‌زدگی و به‌دنبال آن کوچ مجدد به رسانه‌های اجتماعی خارجی را در پی داشت. مقولهٔ فیلترینگ در ایران با نوعی زوال معنا و ناهمگونی شناختی روبه‌رو است؛ چراکه با وجود فیلتر بودن

بعضی رسانه‌های اجتماعی، مانند توییتر، همچنان اغلب مسئولان در این رسانه‌ها حساب کاربری فعال دارند. با رخ دادن چند اتفاق و تثبیت این اتفاق‌ها در حافظهٔ تاریخی ایرانیان، از جمله قطع شدن اینترنت ایران در آبان ماه سال ۱۳۹۸، در پی بعضی اعتراضات مردمی، درخواست دسترسی جمهوری اسلامی ایران به داده‌های کاربران ایرانی که از تلگرام استفاده می‌کردند، رد این درخواست توسط مدیریت رسانهٔ اجتماعی تلگرام و در پی آن فیلترینگ تلگرام و ایجاد بازاریابی نابرابر با امکان استفاده فقط برای رسانه‌های اجتماعی داخلی، سبب از میان رفتن اعتماد کاربران به این رسانه‌ها شد. همچنین مهارت رسانهٔ اجتماعی تلگرام، در حفظ اطلاعات کاربر روی سرورها، از عوامل غیرانسانی مؤثر بر اعتماد به این رسانه است؛ به این معنا که تلگرام قادر است تمامی اطلاعاتی را که کاربر روی آن بارگزاری کرده است، به‌صورت رایگان و نامحدود نگهداری کند و این راحتی ایجاد شده برای کاربر، اقبال و اعتماد او به این رسانهٔ اجتماعی را افزایش داده است. حاکمیت مسئول حفاظت بدون سوءاستفاده از بخشی از داده‌ها در رسانه‌های اجتماعی است؛ این درحالی است که قانون یا سند مشخص و اجرا شده‌ای در خصوص حفاظت از داده‌ها در ایران وجود ندارد و استانداردهای حفاظت از داده‌ها در رسانه‌های اجتماعی داخلی رعایت نمی‌شود. طرح‌های ارائه‌شده برای حفاظت از داده‌ها در رسانه‌های اجتماعی، عطف به منافع ملی نیست. مطالعهٔ مفاد طرح صیانت از داده‌های کاربران که به مجلس شورای اسلامی ارائه شد، نمایان‌کنندهٔ آن بود که این طرح با چالش‌های نهادی و ساختاری مواجه است، از جمله عدم قدرت و شمولیت لازم، عدم وجود ضمانت اجرایی مشخص، از بین بردن رقابت در رسانه‌های اجتماعی و کنترل کاربران با دسترسی بیش از اندازه به اطلاعات آن‌ها. از دیگر موارد انسانی حفاظت از داده‌ها، می‌توان به تأثیر سوءاستفاده رسانهٔ اجتماعی روبیکا با ساخت خودکار حساب‌های کاربری به نام بعضی از ایرانیان، بدون اطلاع آنان و با استفاده از داده‌های کاربران ایرانی که از رسانهٔ اجتماعی اینستاگرام استفاده می‌کنند، اشاره کرد.

دخالت سلیقه‌ای رسانهٔ اجتماعی اینستاگرام و محدودسازی انتشار بعضی محتواها و حتی حذف حساب‌های کاربری بعضی کاربران در خصوص انتشار محتوا دربارهٔ شهید قاسم سلیمانی، به نوع دیگری قابل مشاهده است. در این نمونه، علت عدم واپس‌زدگی اینستاگرام و عدم کوچ از آن، میزان رشد این رسانهٔ اجتماعی، جهانی‌بودن آن و حضور بسیاری از افراد مشهور در آن، عدم دسترسی نهادهای امنیتی داخلی به داده‌های کاربران استفاده کننده از این رسانه و کیفیت مطلوب این رسانهٔ اجتماعی برای کاربران است. پیشینهٔ اتفاق‌ها، برخوردهای حاکمیتی و حافظهٔ تاریخی جامعهٔ ایران، به‌خصوص پس از اتفاق‌های چندسال اخیر و همچنین، عدم اعتماد مردم به قوانین پیشنهادی حاکمیت در مسیری ادامه یافت که بسیاری از کاربران رصد شدن اطلاعاتشان توسط رسانهٔ اجتماعی خارجی را در مقایسه با رسانه‌های داخلی ارجح دانستند و حتی بعضی کاربران، بی‌قانونی در برابر حفاظت از داده‌ها را نسبت به حفاظت از داده‌ها از سوی حاکمیت ترجیح دادند. در این راستا، ایجاد اشتراک میان قوانین ایران با قوانین بین‌المللی حفاظت از دادها و شفافیت این قوانین، می‌تواند برای جامعه نوعی اطمینان از منظر روانی ایجاد کند و اعتماد به رسانه‌های اجتماعی داخلی را افزایش دهد. نیروی انسانی خلاق در مباحث فنی، موجب بهبود کیفیت رسانهٔ اجتماعی و افزایش اقبال و اعتماد به آن می‌شود. کاربران در درون خود

میان دو مفهوم «راحتی»[1] و «حریم خصوصی»[2] درگیرند؛ بدین معنی که کاربر با دستیابی به یکی از این دو مفهوم، با دیگری با تساهل و تسامح رفتار می‌کند و این اتفاق اغلب با فدا کردن حریم خصوصی برای دستیابی به راحتی رخ می‌دهد. به‌طور مثال، زمانی که کاربر وارد حساب کاربری خود در گوگل[3] می‌شود، تمام سوابق مرورگر و رمزهای عبور او در آنجا ذخیره شده است و این سطح بالایی از راحتی را برای کاربر فراهم می‌کند. در عین حال مبرهن است که پلتفرم گوگل برای ایجاد این راحتی، به داده‌های کاربر دسترسی شایان توجهی دارد. عدم ذخیره و نگهداشت داده روی سرورهای رسانهٔ اجتماعی، از موارد غیرانسانی حفاظت از داده‌هاست که بر افزایش اعتماد کاربران اثرگذار است. علی‌رغم عدم ذخیره داده‌ها، ذخیره به‌صورت کلان داده و با استفاده از مفهوم هیچ‌آگاهی نیز می‌تواند اتفاق بفتد که در عین احراز هویت کاربران به‌صورتی باشد که همگان ناشناس بمانند. پشتیبانی قوی رسانهٔ اجتماعی در کاهش خطرهای ناشی از افشای اطلاعات کاربر، از عوامل انسانی مؤثر بر اعتماد است. تأثیر حفاظت از داده‌های مهم به‌صورت دسته‌بندی نشده و سیستماتیک، مابین داده‌های عادی برای کاهش تهدیدهای ناشی از افشای داده‌های کاربر، تعامل بی‌واسطه با تیم پشتیبانی رسانه‌های اجتماعی با منطق حمایت از کاربر و عدم فروش اطلاعات کاربران به شرکت‌های تبلیغاتی، بهترین گزینه برای کمک به کاهش خطر و حفاظت از داده‌هاست. به‌طور کلی توسعهٔ امنیت شبکه و بهبود کیفیت و عملکرد تجهیزات فنی و سخت‌افزاری، از عوامل غیرانسانی مؤثر بر اعتماد است.

پیشنهادهای پژوهش

بر اساس یافته‌ها، می‌توان چند پیشنهاد کلیدی برای تصمیم‌گیرندگان حوزهٔ رسانه‌های اجتماعی ارائه داد.

- خبرگان بر جداسازی رسانهٔ اجتماعی داخلی از لایهٔ حکومتی تأکید کرده‌اند و در واقع نوعی پیشنهاد سیاستی مهم محسوب می‌شود.
- استفاده از فیلترینگ به‌عنوان نوعی سیاست، به‌جای استفاده از سیاست تنظیم‌گری و خط‌مشی‌گذاری، از دیگر مشکلاتی است که در مصاحبه‌ها به آن اشاره شد. پیشنهاد می‌شود قانون‌گذاری در جهت تنظیم‌گری انجام شود و به‌جای اقدام به قطع، دسترسی ایجاد شود.
- عدم سرمایه‌گذاری فنی برای ایجاد و توسعهٔ سرورهای مناسب در خصوص تولید رسانه‌های اجتماعی داخلی، از مواردی بود که در این پژوهش به آن اشاره شد. پیشنهاد می‌شود که بسترهای لازم در خصوص توسعهٔ فنی و سخت‌افزاری رسانه‌های اجتماعی داخلی و پیشبرد سهولت کاربری فراهم شود.

پیشنهادهای زیر نیز برای فعالان صنعت رسانهٔ اجتماعی ارائه شده است:

- توصیه می‌شود مدیران رسانه‌های اجتماعی داخلی، به بهبود کیفیت و عملکرد این رسانه‌ها، توسعهٔ امنیت سرورها و بسترسازی جهت عضویت تعداد زیادی از کاربران، اهتمام ویژه‌ای داشته باشند.

1. Convenience
2. Privacy
3. Google

- در مصاحبه‌ها به داشتن خلاقیت در شیوهٔ خدمات‌رسانی برای رسانه‌های جتماعی داخلی و بازاریابی برابر و به دور از ایجاد انحصارطلبی اشاره شد. به مدیران رسانه‌های اجتماعی داخلی پیشنهاد می‌شود تا همواره در جهت خلاق‌بودن و به‌روز نگهداشتن خود و همچنین، ایجاد بازاریابی برابر کوشش کنند.
- بعضی از مشارکت‌کنندگان به شفاف‌سازی میزان دسترسی رسانه‌های اجتماعی به داده‌ها و ایجاد اطمینان روانی از حفاظت از داده‌ها در رسانهٔ اجتماعی ایرانی برای کاربر اشاره کردند. این موضوع نیز از مواردی است که رعایت آن به مدیران رسانه‌های اجتماعی داخلی پیشنهاد می‌شود.

محدودیت‌ها و پیشنهادهای پژوهشی

یکی از محدودیت‌های این پژوهش، آن است که مانند تمام پژوهش‌های کیفی دیگر، امکان تعمیم‌دهی نتایج به‌دست‌آمده به تمام مکان‌ها و شرایط را ندارد. در این راستا برای تعمیم نتایج این پژوهش پیشنهاد می‌شود که احتیاط لازم صورت گیرد. برای رفع مشکلات احتمالی، در پژوهش‌های آتی می‌توان با طراحی مطالعات پیمایشی، مقوله‌های به‌دست‌آمده در این پژوهش را اعتبارسنجی کرد. همچنین، مصاحبه‌شوندگان در این مطالعه، به‌علت محدودیت‌های مالی و زمانی پژوهشگر، از میان اساتید دانشگاهی، مدیران و پژوهشگرانی انتخاب شدند که در حوزهٔ صنعت رسانه، اعتماد و حفاظت از داده‌ها در تهران فعالت می‌کردند.

بر اساس تجارب این پژوهش، به محققان آینده پیشنهاد می‌شود بر بخش‌های مختلف تقویت اعتماد اجتماعی که برای حضور کاربران در فضای رسانه‌های اجتماعی لازم است، به‌طور خاص و جداگانه تمرکز شود. همچنین، پژوهشگران می‌توانند مطالعه‌ای مقایسه‌ای از تأثیر سیاست‌گذاری‌های انجام شده در خصوص حفاظت از داده‌ها در رسانه‌های اجتماعی خارجی و داخلی انجام دهند و با پژوهشی تطبیقی، ابعاد مؤلفه‌های حفاظت از داده‌های کاربران را که بر اعتماد آنان به رسانه‌های اجتماعی تأثیرگذار است، دقیق‌تر و عمیق‌تر بررسی کنند.

در نهایت، بر اساس نتایجی که از این پژوهش به‌دست آمد، یکی از چالش‌های عمدهٔ مؤثر بر اعتماد کاربران، به‌خصوص به رسانه‌های اجتماعی داخلی در کشور ما، چالش‌های مرتبط با نهادهای قانون‌گذاری و نظارتی است. به محققانی که به مباحث قانون‌گذاری در خصوص حفاظت از داده‌ها علاقه‌مندند، پیشنهاد می‌شود که این موضوع را برای پژوهش انتخاب و الگویی جامع در این راستا طراحی کنند.

References

Bennur, S. (2010). *From apparel, product attributes to brand loyalty: a cross-cultural investigation of U.S and Indian consumers attribute choices applying Kano's theory.* Ph.D. Dissertation. Oklahoma State University.

Bilge, L. (2009). All your contacts are belong to us: automated identity theft attacks on social networks. *WWW '09: Proceedings of the 18th international conference on World wide web,* April 2009 pp. 551–560, https://doi.org/10.1145/1526709.1526784

Boyd, D. M. (2008). Facebook's privacy train wreck: Exposure, invasion, and social convergence. *Int'l J. Research into New Media Tech*, 14(1), 13–20.

Brown, I. (2012), Government access to private-sector data in the United Kingdom, *International Data Privacy Law*, 2 (4), 230–38.

Clarke, A.E. (2005). *Situational analysis: Grounded theory after the postmodern turn.* Sage Publications, Inc. https://doi.org/10.4135/9781412985833

Dewar, K. (2017). The value exchange: Generating trust in the digital world. *Business Information Review,* 34 (2), 96–100.

Dumdum, O. & Crielda, G. (2009). Casting credibility, University of the Philippines, college of mass communication, for presentation during the pre-conference on " Affective Audiene" in the 59th. *Annual conference of international communication association*, in Chicago.

Elmetwaly, M.A. & Babin, L. (2020). Relationship between Saudi customers' electronic-trust and electronic-loyalty. *Journal of Advanced Pharmacy Education & Research*, 10(3), 160-166.

Fortin, D., Dholakia, R. & Dholakia, N. (2002). Emerging issues in electronic marketing: thinking outside the square. *Journal of Business Research*, 55 (8), 623-627.

Future of Life Institute (2017). *Response to the request for Information: Artificial Intelligence Risk Management Framework*. Available at: https://futureoflife.org/policy-work/.

Goddard, M. (2017). The EU General Data Protection Regulation (GDPR): European regulation that has a global impact. *International Journal of Market Research*, 59(6), 703-705.

Gross, R. & Acquisti, A. (2005). Information revelation and privacy in online social networks. *Workshop on Privacy in the Electronic Society*.

Gruschka, N., Mavroeidis, V., Vishi, K. & Jensen, M. (2018). Privacy issues and data protection in big data: A case study analysis under GDPR. *2018 IEEE International Conference on Big Data (Big Data)*, Seattle, WA, USA, 2018, pp. 5027-5033, doi: 10.1109/BigData.2018.8622621.

Gupta, A. & Dhami, A. (2015). Measuring the impact of security, trust and privacy in information sharing: A study on social networking sites. *Ubiquity the Journal of Pervasive Media*, 17(1). DOI:10.1057/dddmp.2015.32

Hill, K. (2012). *How target figured out a teen girl was pregnant before her father did*. Forbes, Inc.

Hoffmann, C. P., Lutz, C. & Ranzini, G. (2016). Privacy cynicism: A new approach to the privacy paradox. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, 10(4), 7-26.

Jayasinghe, U. (2018). *Trust evaluation in the IoT environment, PQDT-UK & Ireland*. Liverpool John Moores University (United Kingdom).

Kinast, S., Ashkenazy, Y. & Meron, E. A. (2014). Coupled Vegetation–crust model for patchy landscapes. *Pure Applied Geophysics*, 173, 983–993.

Kroll, J. A. (2016). Accountable algorithms. rithms. University of Pennsylvania Law Review. *Law Review*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2765268.

Layton, R. (2017). *How the GDPR compares to best practices for privacy, accountability and trust.* Visiting Researcher, Aalborg University, Denmark and Independent Data Scientist, Italy.

Leonnard, A. (2019). Exploring the relationship among e-service quality, e-trust, e-satisfaction and loyalty at higher education institutions. *Journal on Efficiency and Responsibility in Education and Science,* 12(4), 103- 110.

Lewis, D. & Moorkens, J. (2020). A rights-based approach to trustworthy AI in social media. *Social Media + Society*, 6(3), 516-539.

Liu, D., Ainsworth, S. E. & Baumeister, R. F. (2016). A meta-analysis of social networking online and social capital. *Review of General Psychology*, 20(4), 369–391.

Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S. & Floridi, L. (2016). The ethics of algorithms: Mapping the debate. *Big Data & Society*, 3(2), 365-394.

Mostert, M., Bredenoord, A.L., Biesaart, M.C. & van Delden, J.J. (2016), Big Data in medical research and EU data protection law: challenges to the consent or anonyms approach. *European Journal of Human Genetics*, 24(7), 956-960.

Orlowski, P. (2011), Teaching about hegemony: Race, class and democracy in the 21st Century. *Springer Science+Business Media*, https://doi.org/10.1007/978-94-007-1418-2.

Romansky, R. (2014). Social media and personal data protection. *International Journal on Information Technologies & Security,* 11(4), 65-80.

Shareef, M. A., Mukerji, B., Dwivedi, Y. K., Rana, N. P. & Islam, R. (2019). Social media marketing: Comparative effect of advertisement sources. *Journal of Retailing and Consumer Services,* 46, 58-69.

Sophos, R. (2007). Reverse Social Engineering Attacks in Online Social Networks. *In: Holz, T., Bos, H. (eds) Detection of intrusions and malware, and vulnerability assessment. Lecture Notes in Computer Science, vol 6739*. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-22424-9_4

Sukhu, A., Zhang T. & Bilgihan, A. (2015) Factors Influencing Information-Sharing Behaviors in Social Networking Sites, *Services Marketing Quarterly*, 36(4), 317-334.

Tran, V. V. & Quang Vu, H. (2019). Inspecting the relationship among e-service quality, e-trust, e-customer satisfaction, and behavioral intentions of online shopping customers. *Global Business and Finance Review*, 24(3), 29-42.

Weichert, S. (2013). E-trust building in the hotel industry. *Journal of Islamic Marketing,* 12(2), 123-146.

Živković, P. D. (2018). *An international publication for theory and practice of Management Science.* University of Belgrade, Technical Faculty in Bor, Department of Engineering Management.