Jurisprudence and Legal Studies of Media Journal
VOL. 7 / Spring and Summer 2025 / NO. 1 (Serial 13)

Privacy Governance and Data Protection in Global Platforms (Google and Meta): Implications for Iran's Platform Ecosystem

Hossein Hassani[1]

Abstract

This paper aims to analyze the privacy governance mechanisms employed by Google and Meta platforms. Recently, several instances of data privacy violations have been observed across various platforms in Iran. The lack of a comprehensive privacy law and insufficient focus on developing privacy governance frameworks in Iranian platforms are key contributors to this issue. Addressing privacy and data-related challenges in platforms, including social media, can be facilitated by drawing lessons from global platforms. To achieve this objective, the study employs thematic analysis to extract and examine the primary and secondary themes associated with the policies and strategies of these two platforms. This study was conducted during the first half of 2024, utilizing various documents, including those published by the platforms themselves, as data sources. The findings indicate that drafting transparent laws on privacy and data protection is essential for strengthening public trust and enhancing the competitiveness of domestic platforms. Investments in advanced encryption technologies and cybersecurity, alongside providing tools for data management such as viewing, deletion, and control options, are of critical importance. Overall, the protection of privacy and data in Iran's platform ecosystem can be improved by adopting general principles, guidelines, and practical data protection strategies from global platforms, including empowering users.

Keywords: Governance, Platforms, Privacy, Data Protection, Google, Meta.

1- Assistant Professor, Department of Cyberspace Studies, Communication Research Institute, Research Institute for Culture, Art, and Communication, Tehran, Iran
hassani@riccac.ac.ir

دوفصلنامه
مطالعات فقه و حقوق رسانه
دانشکده غیردولتی – غیرانتفاعی رفاه

دوره ۷، شماره ۱ (پیاپی ۱۳)
بهار و تابستان ۱٤۰٤
صص: ۱٦۳-۲۰۰

حکمرانی حریم خصوصی و حریم داده در پلتفرم‌های جهانی (گوگل و متا) و دلالت‌های آن برای زیست‌بوم پلتفرمی ایران

نوع مقاله: پژوهشی
تاریخ دریافت: ۱٤۰۳/۱۲/۰۷
تاریخ پذیرش: ۱٤۰٤/۰۲/۱۵

حسین حسنی[۱]

چکیده

این مقاله با هدف تحلیل سازوکارهای حکمرانی حریم خصوصی در سکوهای گوگل و متا نگاشته شده است. اخیراً موارد متعددی از نقض حریم داده‌های سکوهای مختلف در ایران مشاهده شده است. فقدان یک قانون جامع درباره حریم خصوصی و عدم توجه به توسعه سازوکارهای حکمرانی حریم خصوصی در سکوهای ایرانی از جمله دلایل این چالش می‌تواند باشد. پاسخگویی به بخشی از مسائل مرتبط با حریم خصوصی و داده‌های در انواع سکوها ازجمله رسانه‌های اجتماعی از طریق الگوگیری از سکوهای جهانی امکان‌پذیر است. در راستای دستیابی به این هدف، از روش‌شناسی تحلیل مضمون برای استخراج و تحلیل مضامین اصلی و فرعی مرتبط با سیاست‌ها و راهبردهای این دو سکو استفاده شده است. این مطالعه در نیمه اول سال ۱۴۰۳ انجام شده است و برای گردآوری داده‌ها از اسناد گوناگون از جمله اسنادی که این سکوها منتشر کرده‌اند، استفاده شده است. نتایج این پژوهش نشان می‌دهد برای تقویت اعتماد عمومی و رقابت‌پذیری سکوهای داخلی، تدوین قوانین شفاف در حوزه حریم خصوصی و حفاظت از داده‌ها ضروری است. این سکوها با رعایت اصول بنیادین مانند «محدودیت هدف پردازش داده» (جمع‌آوری داده‌ها تنها برای اهداف مشخص شده)، «تقلیل داده» (کاهش حجم اطلاعات ذخیره شده به حداقل ضروری) و «حریم خصوصی از طریق طراحی» (ادغام الزامات امنیتی در مراحل توسعه محصول)، به‌دنبال ایجاد تعادل میان پیشرفت فناوری و حفظ حریم کاربران هستند. درکل، حفاظت از حریم خصوصی و حفاظت از داده‌ها در زیست‌بوم ایرانی می‌تواند با ملاحظه اصول کلی، دستورالعمل‌ها و نیز راهکارهای عملی حفاظت از داده‌ها در سکوهای جهانی ازجمله توانمندسازی کاربران بهبود پیدا کند.

واژه‌های کلیدی

حکمرانی، سکوها (پلتفرم‌ها)، حریم خصوصی، حریم داده، گوگل، متا.

---

۱. استادیار گروه مطالعات فضای مجازی، پژوهشگاه فرهنگ هنر و ارتباطات، تهران، ایران
hassani@riccac.ac.ir

۱. مقدمه

حفاظت از حریم خصوصی[۲] و محرمانگی داده‌های شخصی[۳] پس از گذار از عصر رسانه‌های آنالوگ و دیجیتال و سپس ظهور اینترنت و هم‌اکنون پلتفرمی‌شدن اینترنت[٤] *(Flew, 2021)* که طی آن تعاملات، کنش‌ها و ارتباطات بیش‌ازپیش در شمار نسبتاً محدودی از سکوهای بزرگ دیجیتال روی می‌دهد، بیش از گذشته دشوار و هر روز پیچیده‌تر می‌شود. درواقع، درهم‌تنیدگی فزاینده سکوهای دیجیتال و رسانه‌های اجتماعی با زندگی روزمره سبب می‌شود افراد به شکل خواسته یا ناخواسته داده‌های شخصی بیشتری را در فضای مجازی با طرف‌های دیگر (شرکت‌ها، دولت‌ها، سازمان‌ها و افراد) به‌اشتراک بگذارند. همچنین، سکوهای دیجیتال نیز بیش‌ازپیش داده‌های شخصی ما را به‌مثابه مدل اصلی کسب‌وکار به‌کار می‌بندند. پیامد همه این موارد، تسهیل و تعمیق مخاطره‌ها برای حریم شخصی افراد و دشوارترشدن کناره‌گیری از این روندهای اجباری – ازجمله حق فراموش شدن[٥] – است.

حریم خصوصی و داده‌های شخصی بیش‌ازپیش به‌واسطه مدل کسب‌وکار شرکت‌های پلتفرمی جهانی مورد خدشه قرار می‌گیرد؛ زیرا یکی از منابع عمده درآمدزایی این سکوها تحلیل داده‌های کلان کاربران است و نیز رویه‌های شخصی‌سازی و سفارشی‌سازی نیز به تحلیل و استخراج الگوهای رفتاری کاربران بر مبنای داده‌هایی که آنها به‌اشتراک می‌گذارند، بستگی دارد. این موارد صرفاً برخی از نمونه‌های درهم‌تنیدگی حریم شخصی کاربران با عملکرد سکوها است. همان‌طور که فن‌دایک[٦] *(۱۳۸٦، ص. ٤۳)* می‌گوید، مأموریت فیس‌بوک یعنی گشوده‌تر کردن و متصل‌تر کردن جهان در قالب اشتراک‌گذاری محقق می‌شود؛ معنای اجتماعی این اصطلاح در تقابل با اصطلاح حقوقی حریم خصوصی قرار می‌گیرد که مبتنی بر حق انزوا و کناره‌گیری از اجتماع است.

---

2. privacy
3. data privacy
4. platformization of the internet
5. right to be forgotten
6. van Dijck

از سوی‌دیگر باید توجه داشت که امروزه بخش مهمی از حکمرانی حریم خصوصی توسط سکوهای رسانه‌های اجتماعی انجام می‌شود. این امر دلایل گوناگونی دارد که مهم‌ترین آنها عبارت‌اند از: عدم تمایل دولت‌ها برای خدشه در آزادی بیان، به‌ویژه در مدل بازارمحور حکمرانی سکوها که در آمریکا رواج دارد، عقب‌افتادگی نهادهای قانون‌گذار برای وضع قوانین مرتبط برای حفاظت از حریم خصوصی در سکوها که ناشی از تحولات شتابان این حوزه فناوری اطلاعاتی و ارتباطی است و نیز حجم غول‌آسای محتواهای کاربرساخته[7] که توسط کاربرانی از زمینه‌های فرهنگی–اجتماعی و زبانی متنوع در سطح جهان به‌اشتراک گذاشته می‌شود. سیطره سکوهای جهانی بر زیست‌بوم پلتفرمی ایران و انتقال بخش عمده زیست ایرانیان به عرصه سکوهای جهانی، در غیاب سکوهای بدیل بومی جایگزین، به‌ویژه از منظر رسانه‌های اجتماعی، سبب شده است تا بخش عمده‌ای داده‌های خصوصی در سکوهای غیرایرانی ذخیره شود و مورد استفاده قرار گیرد.

حق داشتن حریم خصوصی[8] یکی از حقوق بنیادین همه انسان‌ها و به‌ویژه حقوق مخاطبان رسانه‌ها و محصولات فرهنگی و رسانه‌ای است و در کنار حق بر آگاهی که اسماعیلی (۱۴۰۱) آن‌را به‌مثابه یکی از حقوق اساسی مخاطبان مورد بحث قرار داده است، ازجمله وجوه اساسی حقوق مخاطبان است؛ بنابراین توانایی و امکان حفاظت از حریم خصوصی اشخاص در فضای مجازی و سکوهای رسانه‌های اجتماعی به این معنا است که یک بعد محوری از حقوق مخاطبان مورد توجه و تأکید قرار دارد.

در مجموعه‌ای از اسنادی که توسط شورای عالی فضای مجازی و مرکز ملی فضای مجازی مصوب شده است، به شکل‌های گوناگون بر اهمیت حفظ حریم خصوصی کاربران تأکید شده است. در سند راهبردی جمهوری اسلامی ایران در فضای مجازی *(مرکز ملی فضای مجازی، ۱۴۰۱)* که شامل ارزش‌ها، چشم‌انداز، اهداف و اقدامات کلان است و با هدف تحکیم و تقویت حکمرانی و اعمال حق حاکمیت بر فضای مجازی و سکوهای دیجیتال و رسانه‌های اجتماعی تصویب شده است، صیانت از حریم خصوصی و حقوق عامه به‌مثابه یک ارزش مورد تأکید قرار دارد. در این سند، قاعده‌مندسازی دسترسی به داده‌های

7. UGC
8. right to privacy

خصوصی، عمومی و کلان‌داده‌ها به‌عنوان یک هدف کلان بیان شده است. درهمین‌راستا طراحی نظام حکمرانی داده‌ها ازجمله در مورد حریم خصوصی یکی از اقدامات کلانی است که باید پیگیری شود.

سند سیاست‌ها و اقدامات سازماندهی پیام‌رسان‌های اجتماعی که مصوبه شورای عالی فضای مجازی در سال ۱۳۹٦ است، به‌طور خاص بر حکمرانی بر پیام‌رسان‌های اجتماعی تأکید دارد. در این سند «اعتمادسازی و صیانت از حقوق شهروندی، حریم خصوصی، امنیت ملی و عمومی» به‌عنوان یک سیاست کلان ذکر شده است. هدف این سند فراگیرکردن پیام‌رسان‌های ایرانی و سازماندهی پیام‌رسان‌های اجتماعی خارجی است *(شورای عالی فضای مجازی، ۱۳۹٦)*. براین‌اساس می‌توان مدعی شد حفاظت از حریم خصوصی و داده‌های شخصی کاربران و رفع نگرانی آنها نسبت به دسترسی طرف‌های سوم به این داده‌ها، تا چه اندازه برای اعتماد کاربران به یک پیام‌رسان اهمیت دارد.

سایر اسناد مصوب شورای عالی فضای مجازی نیز به شکل‌های مختلف بر اهمیت حفظ حریم خصوصی تأکید کرده‌اند. در سند تبیین الزامات شبکه ملی اطلاعات *(شورای عالی فضای مجازی، ۱۳۹۵)* صیانت از حریم خصوصی، حقوق عمومی و آزادی مسئولانه به‌مثابه یکی از الزامات سالم‌سازی و امنیت شبکه ملی اطلاعات ذکر شده است. همچنین حمایت ویژه از حریم خصوصی و حقوق عمومی یکی از نیازمندی‌های ارائه خدمات ایمن در قالب شبکه ملی اطلاعات ذکر شده است. در سند نظام هویت معتبر در فضای مجازی نیز صیانت از حریم خصوصی یکی از الزامات زیست بوم هویت معتبر ذکر شده است *(شورای عالی فضای مجازی، ۱۳۹٦)*. در سند الزامات حاکم بر اینترنت اشیاء در شبکه ملی اطلاعات (۱۳۹۷)، حریم خصوصی یکی از الزامات ارائه خدمات در این قلمرو ذکر شده است.

با وجود تأکید اسناد بالادستی گوناگون به اهمیت حریم خصوصی و ضرورت ایجاد سازوکارهای حفاظت از داده‌های شخصی افراد، در شبکه ملی اطلاعات تا پیام‌رسان‌های ایرانی و سکوهای رسانه اجتماعی خارجی، اقدام عملی در راستای تدوین اسناد جامع مرتبط با حفاظت از داده و حریم خصوصی در ایران و به‌طور خاص حفاظت از داده‌ها و حریم خصوصی توسط سکوها در ایران صورت نگرفته است.

بر اساس آنچه گفته شد، مسئله اصلی این پژوهش این است که با ملاحظه اهمیت حکمرانی در سکوها، سکوهای بزرگ جهانی تاکنون چه اسناد و مقرراتی را برای حفاظت از حریم خصوصی و داده‌های شخصی ارائه کرده‌اند و چه سازوکارهایی را برای صیانت از حقوق حریم خصوصی کاربران در سکوهای خود انجام تعبیه کرده‌اند؟ پاسخ به این موضوع می‌تواند به‌مثابه راهنمایی برای ارتقاء حفاظت از حریم خصوصی و داده‌های کاربرانی در اکوسیستم پلتفرمی ایران عمل کند. در این مقاله ضمن ملاحظه مفهوم حریم خصوصی و مفهوم حکمرانی سکوها، به مطالعه نحوه حکمرانی حریم خصوصی و حریم داده در دو سکوی بزرگ جهانی خواهیم پرداخت.

۲. پیشینه پژوهش

مطالعه پژوهش‌های صورت گرفته در حوزه حریم خصوصی و حریم داده‌ها در ایران نشان می‌دهد که تاکنون مطالعات بسیاری درباره حریم خصوصی و حریم داده در ایران انجام شده است. این حوزه یک حوزه پژوهشی باسابقه است که در جاهای مختلف این مقاله به برخی از آنها استناد شده است. به‌طور در حوزه رسانه و ارتباطات نیز مطالعاتی درباره حریم خصوصی انجام شده‌اند. ازجمله آنها می‌توان به مسئولیت مدنی رسانه‌ها در قبال نقض حریم خصوصی در حقوق ایران و انگلستان *(اصلانی و دیگران، ۱۴۰۲)*، حریم خصوصی در رسانه‌های همگانی *(انصاری، ۱۳۸۳)* و راهکارهای حمایت از حریم خصوصی کودکان در فضای مجازی اشاره کرد *(فرامرزیانی و دیگران، ۱۴۰۰)*.

برخی مطالعات به‌طور خاص در مورد حفاظت از داده‌ها و حریم خصوصی در سکوها و رسانه‌های اجتماعی در ایران انجام شده‌اند. ازجمله احمدوند و جهانشاهی (۱۴۰۲)، الزامات حاکم بر تأمین امنیت داده‌های کاربران توسط سکوهای خدماتی را مطالعه کرده‌اند. آنها بر مسئولیت سکوها در برابر داده‌های کاربران تأکید کرده‌اند. حسام و همکارانش (۱۴۰۲)، در مطالعه تطبیقی خود در مورد مسئولیت مدنی سکوهای برخط در برابر نقض حریم اطلاعاتی از سوی کاربران، ضمن ملاحظه اصل شخصی بودن مسئولیت، بیان کرده‌اند که مفاد طرح پیشنهادی صیانت از حقوق کاربران در فضای مجازی با هدف

مسئولیت‌پذیر کردن سکوها پیشنهاد شده است. پیش‌نماز و رکنی (۱٤۰۲) نیز نظام حاکم بر داده‌های شخصی را از منظر حقوق اموال تحلیل کرده‌اند.

وجه تمایز مقاله حاضر تمرکز بر سازوکارهای خودتنظیم‌گری حریم خصوصی به‌عنوان یکی از اشکال سه‌گانه حکمرانی سکوها (حکمرانی بر سکو، حکمرانی در سکو – همان خودتنظیم‌گری یا تعدیل محتوا – و حکمرانی توسط سکوها) است. این موضوع تاکنون در ایران مطالعه نشده است.

۳. چهارچوب مفهومی

در این بخش درابتدا حریم خصوصی و تعاریف آن مرور می‌کنیم و سپس بحث‌های مرتبط با حکمرانی حریم خصوصی را مورد ملاحظه قرار می‌دهیم.

۳-۱. تعاریف حریم خصوصی

ترپته *(Trepte, 2021, p. 13)* حریم خصوصی در رسانه‌های اجتماعی را بر پایه ارزیابی‌های فردی از دو مؤلفه اصلی تعریف می‌کند: نخست، میزان دسترسی دیگران (اعم از افراد، شرکت‌ها و مؤسسات) به فرد در جریان تعاملات یا روابط؛ و دوم، وجود سازوکارهای کنترلی، ارتباطات بین‌فردی، اعتماد و هنجارهای اجتماعی که تعیین‌کننده سطح این دسترسی هستند. به باور او، این سازوکارها از دو جنبه تکمیل می‌شوند: (الف) خودافشاگری به‌عنوان یک سازوکار تقریباً شهودی و رفتاری برای تنظیم حریم خصوصی، و (ب) کنترل فعال، ارتباطات بین‌فردی و بررسی دقیق به‌عنوان ابزارهایی مفصل‌تر و آگاهانه‌تر برای تضمین این تنظیمات. وی همچنین تأکید می‌کند که کارآمدی سازوکارهای حریم خصوصی در رسانه‌های اجتماعی، شدیداً متأثر از دو عامل است: نوع محتوایی که کاربران منتشر می‌کنند و توانمندی‌های فنی سکوها در تعیین چگونگی استفاده بعدی از آن محتوا.

نادو[9] (۲۰۰۰)، رویکردی جامع به حریم خصوصی دارد که انواع مختلف حریف خصوصی را دربردارد. به گفته وی، حریم خصوصی به‌عنوان مفهومی سیال شامل آزادی

9. Nadeau

وجدان و اندیشه، کنترل بر جسم، داشتن خلوت و تنهایی در زمان و مکان خصوصی، کنترل بر اطلاعات شخصی، رهایی از نظارت‌های سمعی و بصری دیگران، حمایت از حیثیت و اعتبار خود و حمایت در برابر تفتیش، تجسس و رهگیری را شامل می‌شود *(نقل شده در انصاری، ۱٤۰۰، ص. ۱۱)*.

سروش (۱۳۹۸) نیز می‌گوید تعاریفی که از حریم خصوصی ارائه شده است بر یکی از این وجوه است: حق تنها ماندن؛ توانایی ایجاد مانع در دسترسی دیگران به انسان؛ پنهان ماندن از دیگران و محرمانه نگه‌داشتن برخی امور؛ کنترل بر اطلاعات شخصی؛ حمایت از کرامت و شخصیت؛ و نزدیکی و صمیمیت *(سروش، ۱۳۹۸، ص.۱۲)*.

احمدلو (۱٤۰۰) تعریفی از حریم خصوصی ارائه می‌دهد که با رویکرد این مقاله که تمرکز بر بعد اطلاعاتی حریم خصوصی همخوانی دارد. به گفته او «حریم خصوصی عبارت است از مجموعه اطلاعات و مسائل حوزه‌های خصوصی-فردی که شخص نمی‌خواهد کسی بدون تمایل و اطلاع وی نسبت به آن دسترسی حاصل و به آنها تعرض شود» *(احمدلو، ۱٤۰۰، ص. ۳٤)*.

یک دسته دیگر تعاریف حریم خصوصی کنترل-مبنا هستند *(Gavison, 1980, p. 428)*. این تعاریف حریم خصوصی را به‌منزله دسترسی محدود تعریف می‌کنند. از این‌منظر، به‌جای تمرکز بر محدودسازی اطلاعات باید بر «حریم خصوصی به‌منزله محدودیت دسترسی دیگران به یک فرد» تمرکز شود *(نقل شده در:* Véliz, 2024, p. 81).

به گفته ولیز (۲۰۲٤) طرفداران نظریه‌های دسترسی استدلال می‌کنند که حریم خصوصی شامل محدود کردن یا جلوگیری از دسترسی به اطلاعات شخصی است. از این دیدگاه، هنگامی که چنین اطلاعاتی در اختیار دیگران قرار می‌گیرد، حریم خصوصی از بین می‌رود. نظریه‌های کنترل بر اهمیت حفظ کنترل بر اطلاعات شخصی تأکید می‌کنند و این مفهوم را بیان می‌دارند که به‌خطر انداختن این کنترل توسط دیگران، حتی زمانی که به اطلاعات دسترسی ندارند، اشتباه است. نتیجه اینکه، یک نظریه کافی درباره حریم خصوصی باید هم دسترسی و هم کنترل را در نظر بگیرد تا حفاظت جامع را تضمین کند *(Véliz, 2024, p. 98)*.

۳-۲. حریم خصوصی داده‌های شخصی کاربران

یکی از بحث‌های مهم در مورد حریم خصوصی اطلاعات یا داده‌ها، حریم اطلاعات کاربران است. حریم خصوصی داده‌های کاربران در عصر رسانه‌های اجتماعی و سکوهای برخط، جایی که کاربران حجم عظیمی از اطلاعات شخصی را به‌اشتراک می‌گذارند، به یک دغدغه جدی تبدیل شده است. با گذراندن زمان بیشتر به‌صورت برخط، افراد ردپای دیجیتالی از خود به‌جا می‌گذارند که می‌تواند توسط شرکت‌ها و اشخاص ثالث جمع‌آوری، تحلیل و کسب درآمد شود. این امر پرسش‌هایی را در مورد استفاده اخلاقی از داده‌های شخصی و میزان کنترل افراد بر حضور برخط‌شان ایجاد می‌کند.

سکوهایی مانند فیس‌بوک، اینستاگرام و گوگل به‌دلیل نحوه مدیریت داده‌های کاربران مورد انتقاد و نظارت قرار گرفته‌اند. این شرکت‌ها اغلب از الگوریتم‌های پیچیده و روش‌های استخراج داده برای استخراج اطلاعات ارزشمند از اطلاعات کاربر استفاده می‌کنند که می‌تواند برای هدف قرار دادن تبلیغات و شکل‌دهی تجربیات برخط به‌کار رود. علاوه‌براین، نقض داده‌ها و دسترسی غیرمجاز به اطلاعات حساس، نگرانی‌ها را در مورد امنیت و حفاظت از داده‌های کاربران افزایش داده است. برای کاربران و تنظیم‌کننده‌ها ضروری است که در حفاظت از حریم خصوصی داده‌ها و اطمینان از شفافیت در نحوه جمع‌آوری و استفاده از اطلاعات شخصی در فضای دیجیتال هوشیار باشند.

مرور بحث‌های فوق نشان می‌دهد که حقوق کاربران در فضای مجازی و رسانه‌های اجتماعی و انواع سکوها در ایران تاکنون مورد توجه قرار نگرفته است. مفهوم حقوق مخاطب که به عصر رسانه‌های جمعی اختصاص دارد، کم‌وبیش بحث‌هایی را ایجاد کرده است؛ اما حقوق کاربران که به عصر سکوها تعلق دارد. در بحث‌های مرتبط با حقوق رسانه‌ها و ارتباطات ناچیز است و انصاری و عطار (۱۴۰۲)، عمده‌ترین تلاش در ایران برای توسعه این بحث است. بااین‌همه، بخش عمده بحث‌های مرتبط با حریم خصوصی داده‌ها در سطح بین‌الملل بدین‌سو، جهت‌گیری کرده است؛ زیرا اکنون بخش ارتباطات ارتباطات اینترنتی، ارتباطات پلتفرم-مبنا است. سکوهایی که صرفاً شامل رسانه‌های اجتماعی نیستند و انواع سکوها را شامل می‌شوند.

همان‌طور که کارا[10] (۲۰۲۱) بحث می‌کند، یکی از مهمترین ویژگی‌های سکوهای رسانه‌های اجتماعی گردآوری داده است. سکوهای شبکه‌های اجتماعی برای هدایت الگوریتم‌های توصیه و هدفمندسازی محتوا، به جمع‌آوری داده‌های کاربران وابسته‌اند. کاربران فعال با تعاملات اجتماعی، محتوا و داده‌هایی که تولید می‌کنند در این امر سهیم هستند و سکوها از این داده‌ها برای جلب توجه و ایجاد درآمد استفاده می‌کنند. این سکوها با جمع‌آوری اطلاعات متنوعی مانند موقعیت مکانی، علایق و ارتباطات اجتماعی، محتوا را به‌صورت لحظه‌ای برای کاربران شخصی‌سازی می‌کنند. درواقع، این ویژگی خود به امری چالش‌برانگیز در حوزه حریم خصوصی تبدیل شده و مسائل نوظهوری متعددی را باعث شده است.

۳-۳. تعدیل محتوا در سکوها و حریم خصوصی

یک موضوع بااهمیت در حکمرانی به‌وسیله سکوها، تعدیل محتوا و ارتباط آن با خط‌مشی داده و حریم خصوصی است. تعدیل محتوا به جنبه‌ای ضروری برای حفظ یک محیط برخط سالم تبدیل شده است. بااین‌حال، شیوه‌های مدیریت محتوا باید همراه با سیاست‌های قوی داده و حریم خصوصی باشد تا از حقوق و منافع کاربران محافظت شود.

از سوی‌دیگر، سیاست داده، نحوه جمع‌آوری، استفاده و به‌اشتراک گذاشتن داده‌های کاربر توسط سکوها را مشخص می‌کند. برای کاربران مهم است که بدانند چه داده‌هایی در مورد آنها جمع‌آوری می‌شود و برای چه اهدافی *(Boyd & Crawford, 2012)*. سیاست‌های شفاف داده به کاربران کمک می‌کند تا درباره فعالیت‌های برخط خود تصمیمات آگاهانه بگیرند و سکوها را برای شیوه‌های مسئولانه داده پاسخگو کنند. این امر با توجه به حجم عظیمی از اطلاعات شخصی به‌اشتراک گذاشته شده در رسانه‌های اجتماعی و سایر سکوهای برخط، به‌ویژه اهمیت دارد.

سیاست حفظ حریم خصوصی که ارتباط نزدیکی با سیاست داده دارد، نحوه محافظت سکوها از حریم خصوصی کاربران و رسیدگی به اطلاعات حساس را بیان می‌کند.

10 .Carah

سیاست‌های حفظ حریم خصوصی باید اقدامات انجام شده برای محافظت از داده‌های کاربران در برابر دسترسی غیرمجاز، سوءاستفاده یا نقض را به‌طور واضح بیان کنند *(Solove, 2013)*. علاوه‌براین، آنها باید به کاربران کنترل بر تنظیمات حریم خصوصی خود ارائه دهند و آنها را قادر سازد تا انتخاب کنند که چه اطلاعاتی و با چه کسی به‌اشتراک گذاشته شود.

ترپته (۲۰۲۱) در رویکرد خود به حریم خصوصی بر کنترل و قابلیت تمرکز دارد. کنترل به‌عنوان یک جزء حیاتی در نظریه‌های تاریخی و معاصر حریم خصوصی به‌طور گسترده مورد توجه قرار گرفته است. بسیاری از پژوهشگران حریم خصوصی، کنترل را به‌عنوان ابزار اصلی برای افراد جهت تنظیم و دستیابی به حریم خصوصی در نظر می‌گیرند، با این‌فرض که افزایش کنترل بر دسترسی به داده های شخصی، منجر به بهبود تجربه‌های مرتبط با حریم خصوصی می شود. ترپته *(Trepte, 2021, p. 13)* سپس تعریف خود را از حریم خصوصی در رسانه‌های اجتماعی به این شکل اعلام می‌کند:

من حریم خصوصی را بر اساس ارزیابی‌های فردی از: (الف) میزان دسترسی به این فرد در تعامل یا رابطه با دیگران (افراد، شرکت‌ها، مؤسسات)؛ (ب) در دسترس بودن سازوکارهای کنترل، ارتباط بین‌فردی، اعتماد و هنجارها برای شکل‌دهی به این سطح دسترسی از طریق؛ (ج) خودافشاگری به‌عنوان تنظیم‌گری رفتاری حریم خصوصی (تقریباً شهودی) و (د) کنترل، ارتباط بین‌فردی و بررسی به‌عنوان ابزاری برای اطمینان از تنظیم (تا حدودی مفصل‌تر) حریم خصوصی تعریف می‌کنم. سپس، در رسانه‌های اجتماعی، در دسترس بودن سازوکارهایی که برای اطمینان از حریم خصوصی قابل اعمال هستند، به‌طور اساسی تحت تأثیر محتوایی است که به‌اشتراک گذاشته می‌شود و توانمندی‌های رسانه‌های اجتماعی که نحوه استفاده بیشتر از این محتوا را تعیین می‌کنند، قرار می‌گیرد.

حریم خصوصی در سکوهای رسانه‌های اجتماعی به تنظیم رابطه بین کاربران، داده‌ها، و قابلیت‌های سکو وابسته است. این سکوها با ارائه قابلیت‌هایی نظیر ناشناسی، ویرایش‌پذیری، و ماندگاری، امکان تعامل و اشتراک‌گذاری داده‌ها را فراهم می‌کنند؛ اما این امر مخاطراتی برای حریم خصوصی ایجاد می‌کند. سیاست‌های داده و حریم خصوصی

باید شفاف و قوی باشند تا از حقوق کاربران محافظت کرده و آن‌ها را قادر سازند تا کنترل بیشتری بر اطلاعات خود داشته باشند. همچنین، سازوکارهایی نظیر کنترل، اعتماد، و هنجارهای اجتماعی به کاربران کمک می‌کنند تا سطح دسترسی به اطلاعاتشان را مدیریت کنند و تجربه بهتری از حفظ حریم خصوصی در این فضاها داشته باشند.

۴. روش‌شناسی

این پژوهش از نوع تحلیلی و کیفی است. در این پژوهش برای گردآوری داده‌ها از روش اسنادی استفاده شده است. این مطالعه در نیمه اول سال ۱۴۰۳ انجام شده است. منابع مورد استفاده برای تحلیل شامل کتاب‌ها، مقالات علمی، گزارش‌ها، روزنامه‌ها، مجلات، مصاحبه‌ها، تصاویر، فیلم‌ها و هر نوع مدرک کتبی یا تصویری دیگری بوده که به موضوع پژوهش ارتباط داشته است؛ البته، بخش عمده اسناد تحلیل شده شامل اسنادی است که توسط خود سکوهای مورد تحلیل منتشر شده بودند و یا در دسترس قرار داشتند.

در این پژوهش برای تحلیل یافته‌ها از روش تحلیل مضمون استفاده شده است. برای انجام تحلیل مضمون از روشی که براون و کلارک در سال ۲۰۰۶ معرفی کرده‌اند استفاده شده است. آن دو در مقاله خود، روشی جامع و انعطاف‌پذیر برای تحلیل داده‌های کیفی به نام تحلیل مضمون یا تماتیک ارائه می‌دهد. تحلیل تماتیک به شناسایی، تحلیل، و گزارش الگوها (یا تم‌ها) در داده‌ها می‌پردازد و می‌تواند به شیوه‌ای ساختارمند انجام شود. مراحل اصلی تحلیل تماتیک در رویکرد براون و کلارک (۲۰۰۶) شامل این موارد است: ۱) آشنایی با داده‌ها: در این مرحله، محقق باید خود را با داده‌ها آشنا کند. این شامل خواندن چندباره داده‌ها، یادداشت‌برداری و شناسایی ایده‌های اولیه است. هدف از این مرحله درک عمیق و جامع از داده‌ها می‌باشد؛ ۲) کدگذاری اولیه: در این مرحله، محقق بخش‌هایی از داده‌ها که به نظرش مهم هستند را کدگذاری می‌کند. این کدها می‌توانند عباراتی کوتاه باشند که مفهوم کلی قطعه‌ای از داده را توضیح می‌دهند. هدف این مرحله تفکیک داده‌ها به اجزای کوچک‌تر و قابل مدیریت است؛ ۳. جستجوی تم‌ها: در این مرحله، محقق کدهای ایجاد شده را بررسی کرده و آن‌ها را در دسته‌هایی که تم‌های بالقوه هستند، سازماندهی می‌کند. تم‌ها باید

نمایانگر الگوها و معانی درون داده‌ها باشند؛ ٤. بازبینی تم‌ها: در این مرحله، محقق تم‌های شناسایی‌شده را بازبینی و پالایش می‌کند. برخی از تم‌ها ممکن است کنار گذاشته شوند یا با تم‌های دیگر ادغام شوند. در این مرحله، پژوهشگر مطمئن می‌شود که تم‌ها با داده‌های اصلی هماهنگی دارند و به بهترین شکل نمایانگر معنای داده‌ها هستند؛ ٥. تعریف و نام‌گذاری تم‌ها: پس از پالایش تم‌ها، محقق هر تم را تعریف و توضیح می‌دهد. همچنین به هر تم یک نام مشخص و معنادار داده می‌شود که نمایانگر مضمون کلی آن باشد؛ و ٦. نوشتن گزارش نهایی: در مرحله آخر، محقق یافته‌های خود را در قالب یک گزارش نهایی ارائه می‌دهد. این گزارش باید به‌وضوح چگونگی و چرایی شناسایی تم‌ها را توضیح دهد و نشان دهد که تم‌ها چگونه به پرسش پژوهش پاسخ می‌دهند. بران و کلارک تأکید می‌کنند که تحلیل تماتیک روشی انعطاف‌پذیر و قابل تطبیق است و می‌تواند به محققان در استخراج معانی و الگوها از داده‌های کیفی کمک کند.

۵. تحلیل یافته‌ها

هدف این بخش مطالعه اصول بنیادین حاکم و اقداماتی است که سکوهای بزرگ جهانی شامل گوگل و متا نسبت به داده‌های کاربران اتخاذ کرده‌اند. مطالعه این سیاست‌ها برای تدوین اصول مشابه برای سکوهای ایرانی کمک شایانی خواهد کرد. سیاست‌های مرتبط با حریم خصوصی و نحوه حفاظت از داده‌ها یکی از بخش‌های اصلی حکمرانی پلتفرمی یا تعدیل محتوا *(Gorwa, 2019)* است. ما در هر مورد ابتدا سازوکار حکمرانی حریم خصوصی در هر دو سکوی گوگل و متا را تحلیل می‌کنیم و در پایان هر بخش جدولی از مضامین کلی و فرعی را نشانگر اصول و مسائل حاکم بر حکمرانی حریم خصوصی است ارائه می‌کنیم.

۵-۱. سکوی گوگل

سیاست‌های حریم خصوصی گوگل

نخستین سکویی که سیاست‌های حریم خصوصی و داده آن‌را مورد بررسی قرار می‌دهیم، گوگل است. گوگل یک شرکت چندملیتی فناوری است که در سال ۱۹۹۸ توسط لری پیج[۱۱] و سرگی برین[۱۲] تأسیس شد. مأموریت گوگل سازماندهی اطلاعات جهان و در دسترس و مفید ساختن آن برای همه است.

این تحلیل در اصل با تکیه بر اسناد خود گوگل و سایر مطالعات نهادها و پژوهشگران مختلف درباره سیاست حریم خصوصی گوگل انجام می‌شود. این تحلیل به شکل تحلیل مضمونی انجام می‌شود. به این معنا که اسناد مرتبط با تکیه بر اسناد خود سکوها تحلیل می‌شوند تا مقوله‌ها یا مضمون‌های اصلی که شکل‌دهنده اصول حاکم بر این سکو هستند، استخراج شوند. این تحلیل ابتدا به شکل توصیفی و تحلیلی انجام می‌شود. در مورد سایر سکوها نیز به همین روش اقدام خواهد شد.

در یک مرور کلی بخش سیاست حریم خصوصی و شرایط خدمت گوگل شامل این دو بخش پیش‌گفته و نیز مرکز ایمنی گوگل[۱۳]، حساب کاربری گوگل[۱۴]، اصول حریم خصوصی و ایمنی ما[۱۵] و راهنمای حریم حریم خصوصی محصولات گوگل[۱۶] است. همان‌طور که مشخص است، بحث حریم خصوصی در سطوح گوناگون ارائه خدمت در گوگل اهمیت فراوانی دارد. ازجمله در حساب کاربری گوگل، توجه به داده‌های شخصی اهمیت فراوانی دارد. با توجه به اینکه اکنون برای اتصال به بسیاری از خدمات برخط و حتی خدمات سکوهای هوش مصنوعی، امکان ثبت‌نام از طریق گوگل به جای ثبت‌نام‌های متعدد فراهم شده است و حساب کاربری گوگل به یک حساب کاربری فراگیر و جهانی تبدیل می‌شود، حفاظت از داده‌های شخصی کاربران گوگل بیش‌ازپیش اهمیت پیدا می‌کند.

---

11. Larry Page
12. Sergey Brin
13. Google Safety Center
14. Google Account
15. Our Privacy and security Principles
16. Google Product Privacy Guide

به‌مثابه بخشی از رویکرد کلی حکمرانی در سکو، گوگل اسناد بالادستی مختلفی را برای اعلام شروط و پیش‌شرط فعالیت کاربران در این سکو اعلام کرده است. گوگل شرایط سیاست حریم خصوصی و شرایط ارائه خدمت خود[۱۷]را در یک بخش معرفی کرده است[۱۸]. سیاست حریم خصوصی (و یا در ترجمه فارسی گوگل از آن خط‌مشی رازداری) از شرایط (ارائه) خدمت متمایز هستند. شرایط ارائه خدمت گوگل در ۲۲ مه ۲۰۲٤ گوگل به‌روزرسانی شده است و در آن به‌صراحت اعلام می‌شود که سیاست حریم خصوصی بخشی از شرایط ارائه خدمت نیست؛ اما مطالعه آن به درک بهتر اینکه گوگل چگونه اطلاعات کاربران را به‌روزرسانی، مدیریت، صادر و حذف می‌کند، کمک‌کننده است *(Google privacy policy, 2024)*. شرایط ارائه خدمت نوعی توافقنامه میان کاربران و این شرکت به هنگام استفاده از خدمات گوگل و به تعبیر گوگل بیانگر انتظارات کاربران از خدمات گوگل و انتظارات کاربران از شرکت گوگل است.

اصول حریم خصوصی گوگل

- اصل حفظ حریم خصوصی بر اساس طراحی و به‌صورت پیش‌فرض

به‌نظر می‌رسد تعبیه‌شدگی گسترده اصول و سازوکارهای حفاظت از داده‌های شخصی کاربران و حریم خصوصی تابع اصل حفظ حریم خصوصی بر اساس طراحی[۱۹] یا حفظ حریم خصوصی به‌صورت پیش‌فرض[۲۰] است. حریم خصوصی بر اساس طراحی و حریم خصوصی به‌صورت پیش‌فرض دو اصل مکمل هستند که برای محافظت از حریم خصوصی کاربران با هم کار می کنند. مفهوم حریم خصوصی بر اساس طراحی بر ادغام فعالانه ملاحظات مربوط به حریم خصوصی در توسعه محصولات و خدمات از همان ابتدا تأکید دارد. در عمل، چنانچه یک سکوی رسانه اجتماعی با در نظر گرفتن حریم خصوصی طراحی شده باشد، مهندسان در طول فرایند توسعه، ویژگی‌هایی مانند رمزگذاری قوی،

17 .Google Privacy and Terms
18 . https://policies.google.com/privacy?hl=en
19 .privacy by design
20 .privacy by default

کنترل‌های دقیق حریم خصوصی و راه‌هایی برای به حداقل رساندن جمع‌آوری داده‌ها را در نظر می‌گیرند.

مفهوم حریم خصوصی به‌صورت پیش‌فرض بر اطمینان از این موضوع تمرکز دارد که تنظیمات پیش‌فرض یک محصول یا خدمت، حداکثر سطح محافظت از حریم خصوصی را بدون نیاز به تغییر هیچ تنظیماتی به کاربران ارائه دهد. چنانچه مثال سکوی رسانه‌های اجتماعی را در نظر بگیریم، حریم خصوصی به‌صورت پیش‌فرض تضمین می‌کند که رخ‌نماهای کاربری به‌صورت پیش‌فرض خصوصی باشند، اشتراک‌گذاری موقعیت مکانی خاموش باشد و جمع‌آوری داده‌ها برای تبلیغات هدفمند به‌صورت پیش‌فرض غیرفعال باشد. کاربران در صورت تمایل می‌توانند برای به‌اشتراک گذاشتن اطلاعات بیشتر، رضایت خود را اعلام کنند. این دو اصل با هم حریم خصوصی را به‌جای یک فکر پسینی، به هسته اصلی یک سیستم تبدیل می‌کنند. این دو اصل با اولویت قرار دادن به حریم خصوصی، کاربران را توانمند می‌کنند.

ادعای گوگل این است که اصل کلی حریم خصوصی بر اساس طراحی جزو اصول لاینفک این شرکت فناوری است. گوگل در بخش اصول حریم خصوصی خود ادعا می‌کند «ما محصولاتی می‌سازیم که برای همه به شکل خصوصی بر اساس طراحی هستند» و منظور از آن این است که این شرکت برای داده‌هایی که استفاده می‌کند، نحوه استفاده از آنها و نحوه حفاظت از آنها به شکل ملاحظه‌کارانه عمل می‌کند *(Google privacy policy, 2024)*.

بنابراین مفهوم محوری یا مضمون کلیدی اصول حریم خصوصی گوگل، حریم خصوصی بر اساس طراحی است که راهنمای عمل گوگل در طراحی و تولید محصولات، فرایندها و نیز کارکنان آن برای حفظ و ایمن نگه‌داشتن داده و فراهم کردن امکان کنترل کاربران بر اطلاعات‌شان است.

- مرکز ایمنی گوگل و حریم خصوصی

ایمنی (امنیت) و حریم خصوصی ارتباط نزدیکی با یکدیگر دارند. به همین دلیل است که در بحث‌های مرتبط با ایمنی به حریم خصوصی نیز توجه می‌شود. همان‌طور که کوریا و

رودریگز[۲۱] (۲۰۲۳) گفته‌اند، امنیت و حریم خصوصی رشته‌های به‌هم‌وابسته‌ای هستند. حریم خصوصی تا حد زیادی در مورد امنیت، به‌ویژه محرمانگی اطلاعات شخصی و شناساگرهای شخصی است.

- ایمنی و حریم خصوصی

حریم خصوصی و امنیت مفاهیمی به‌هم مرتبط هستند که اغلب در زمینه فناوری‌های دیجیتال و تعاملات برخط با هم در ارتباط هستند. درحالی‌که آنها معانی متمایزی دارند، هر دو برای اطمینان از محافظت از افراد و اطلاعات شخصی آنها ضروری هستند. هدف مشترک محافظت حریم خصوصی و امنیت یک هدف مشترک برای محافظت از کاربران و اطلاعات آنها دارند. حریم خصوصی بر روی محافظت از اطلاعات شخصی در برابر دسترسی غیرمجاز و اطمینان از کنترل افراد بر نحوه استفاده و به‌اشتراک گذاشتن داده‌هایشان تمرکز دارد. امنیت از سوی‌دیگر، شامل محافظت از داده‌ها، دستگاه‌ها و شبکه‌ها در برابر تهدیداتی مانند هک‌کردن، سرقت و دسترسی غیرمجاز است.

مرکز ایمنی[۲۲] یکی از بخش‌های دیگر گوگل است که در آن بحث‌هایی درباره نحوه تنظیم‌گری حریم خصوصی در این سکو مورد تأکید قرار دارد. یکی از شعارهای گوگل در این بخش این است که «ما ابزارهای حریم خصوصی‌ای را می‌سازیم که شما در جایگاه کنترل‌کننده قرار دهد» *(Google Safety Center, 2024)*. این گفته به‌طور آشکار رابطه بین حفظ ایمنی در گوگل و حریم خصوصی را نشان می‌دهد و بر اهمیت آنها تأکید می‌شود. در این بخش نقل‌قولی از سوندار پیچای[۲۳] مدیرعامل گوگل نقل شده است:

ما اطلاعات برخط شخصی شما را خصوصی، امن و مطمئن نگه می‌داریم. تمامی محصولات ما تحت هدایت سه اصل مهم قرار دارند. با داشتن یکی از پیشرفته‌ترین زیرساخت‌های امنیتی جهان، محصولات ما به‌طور پیش‌فرض امن هستند. ما به‌شدت از شیوه‌های مسئولانه داده‌های برخط پیروی می‌کنیم؛ بنابراین هر محصولی که می‌سازیم

21. Correia & Rodrigues
22. Safety Center
23. Sundar Pichai

به‌صورت خصوصی طراحی شده است و ما تنظیمات حریم خصوصی و امنیت داده‌ای را ایجاد می‌کنیم که استفاده از آن‌ها آسان است تا شما کنترل داشته باشید *(Pichai, 2021)*.

همان‌طور که مضمون این نقل‌قول نشان می‌دهد، چند اصل مورد تأکید قرار دارد. حریم خصوصی به شکل پیش‌فرض و بر اساس طراحی؛ مسئولیت نسبت به حفظ ایمنی داده‌های کاربران و لزوم توانمندسازی کاربران برای کنترل داده‌هایشان. این اصول مبنای ادعایی رویکرد گوگل نسبت به حفظ حریم خصوصی کاربرانش است.

- رمزگذاری به‌عنوان ابزار حفظ ایمنی

همچنین گوگل بر حریم داده تأکید کرده است که ابزار اصلی تحقق آن استفاده از فناوری‌های پیشرفته‌ای است که از پیش‌تعبیه‌اند[۲۴]. درواقع کاربرد فناوری‌های امنیتی با هدف حفظ ایمنی داده‌ها رخ می‌دهد. ساختار امنیتی پیشرفته گوگل، به‌طور خودکار تهدیدات برخط را شناسایی و از آنها جلوگیری می‌کند؛ بنابراین افراد می‌توانند اطمینان داشته باشند که اطلاعات خصوصی آنها در وضعیت ایمنی قرار دارد. یکی از موارد کاربرد فناوری پیشرفته برای حفظ محرمانگی داده‌ها رمزگذاری[۲۵] است.

رمزگذاری نقشی حیاتی در ایمن‌سازی انواع مختلف دارایی‌های فناوری اطلاعات و اطلاعات قابل شناسایی شخصی ایفا می‌کند. هدف اصلی رمزگذاری محافظت از محرمانه بودن داده‌های دیجیتالی است که در سیستم‌های رایانه‌ای ذخیره شده یا از طریق اینترنت یا سایر شبکه‌های رایانه‌ای منتقل می شوند. برای محافظت از طیف گسترده‌ای از داده‌ها، از اطلاعات شناسایی شخصی گرفته تا دارایی‌های حساس شرکت تا اسرار دولتی و نظامی استفاده می‌شود. سازمان‌ها با رمزگذاری داده‌های خود، خطر افشای اطلاعات حساس را کاهش می‌دهند *(Sheldon, Loshin & Cobb, 2024)*.

همان‌طور که گوگل اعلام کرده است رمزگذاری باعث محرمانگی و امنیت داده‌ها در هنگام انتقال می‌شود. رمزگذاری باعث افزایش امنیت و حریم خصوصی خدمات ما می‌شود. هنگامی که پست الکترونیکی ارسال می‌کنید، ویدیویی به‌اشتراک می‌گذارید، از

24. built-in
25. Encryption

تارنمایی بازدید می‌کنید یا عکس‌های خود را ذخیره می‌کنید، داده‌هایی که ایجاد می‌کنید، بین دستگاه شما، خدمات گوگل و مراکز داده ما جابه‌جا می‌شود. ما از این داده‌ها با چندین لایه امنیتی از جمله فناوری رمزگذاری پیشرو مانند اچ.تی.تی.پی.اس[۲۶] و لایه امنتی انتقال[۲۷] محافظت می کنیم *(Google Safety Center, 2024)*.

نکته مهم دیگری که باید بر اساس بحث‌های مطرح شده در مرکز ایمنی گوگل به آن اشاره کنیم، اهمیت دادن به امکان کنترل کاربران بر حریم خصوصی و داده‌های خودشان است *(Google Safety Center, 2024)*. ما می‌توانیم به دلایل مختلف بحث کنیم که چرا این قابلیت از منظر ایمنی و حریم خصوصی دارای اهمیت است.

- فراهم کردن امکان کنترل کاربران

اعتماد و رضایت کاربر هنگامی که کاربران احساس کنند حریم خصوصی آن‌ها مورد احترام قرار می‌گیرد و بر داده‌های خود کنترل دارند، به احتمال زیاد به سکو اعتماد می‌کنند، با آن تعامل برقرار می‌کنند و اطلاعات را به‌اشتراک می‌گذارند. این امر رضایت کاربر را بهبود می‌بخشد و می‌تواند منجر به نرخ ماندگاری بالاتر کاربران در یک سکو و توصیه به دیگران باری کاربرد یک سکوی خاص شود.

یکی از مهم‌ترین اسنادی که از طریق آن می‌توانیم به رویکرد سکوی گوگل درباره گردآوری داده‌ها تا حفاظت از داده‌های کاربران پی ببریم، خط‌مشی یا سیاست حریم خصوصی گوگل است که نسخه آخر آن از ۲۸ مارس ۲۰۲٤ به اجرا گذاشته شده است. حریم خصوصی گوگل سندی جامع است که روش‌های جمع‌آوری، استفاده و محافظت از اطلاعات کاربران توسط گوگل در سراسر محصولات و خدمات مختلف آن را شرح می‌دهد. طی سال‌های مختلف این سند به‌روزرسانی شده است. اولین نسخه سیاست حریم خصوصی گوگل که در دسترس قرار دارد، به ماه ژوئن ۱۹۹۹ برمی‌گردد. در این سند رویکرد کلی گوگل به این شکل شرح داده شده است:

26. HTTPS
27. Transport Layer Security

سیاست گوگل در قبال تارنماهای تحت مالکیت و کنترل کامل ما، احترام و محافظت از حریم خصوصی کاربرانمان است. گوگل عمداً هیچ‌گونه اطلاعاتی که به‌طور شخصی قابل شناسایی باشد راجع به مشتریان خود، بدون دریافت اجازه قبلی از آن مشتری، به هیچ شخص ثالثی افشا نخواهد کرد. این بیانیه خط‌مشی به شما می‌گوید که چگونه اطلاعات را از شما جمع‌آوری می‌کنیم و چگونه از آن استفاده می‌کنیم *(Google Privacy & Policy, 1999)*.

- اصل تقلیل داده‌های کاربران

موضوع دیگری که از همان ابتدا مورد تأکید گوگل دررابطه کاربردهای تجاری داده‌های کاربران قرار داشته است، اصل تقلیل داده‌های کاربران است:

گوگل ممکن است اطلاعات مربوط به کاربران را با تبلیغ‌کنندگان، شرکای تجاری، اسپانسرها و سایر طرف‌های ثالث به‌اشتراک بگذارد. بااین‌حال، ما *فقط* در مورد کاربران خود به‌صورت کل، نه به‌صورت جداگانه صحبت می‌کنیم؛ برای‌مثال، ممکن است فاش کنیم که یک کاربر معمولی گوگل چند بار به گوگل مراجعه می‌کند، یا اینکه کدام کلمات پرسش دیگری اغلب با کلمه پرسش «مایکروسافت» استفاده می‌شود *(Google Privacy & Policy, 1999)*.

ملاحظه این نکته اساسی در هنگام تنظیم‌گری سکوها در ایران اهمیت اساسی دارد. تنظیم مقررات حریم خصوصی باید سکوها را ملزم کند تا از انتشار داده‌های کاربران که کاربر را شناسایی‌پذیر می‌کند، اجتناب نماید و در صورت کاربرد داده‌ها کاربران بر تقلیل داده‌ها یا ارائه آنها به شکل مجموع‌شده تأکید شود. تقلیل داده شکل‌های مختلفی دارند که مهم‌ترین آنها عبارت‌اند از ناشناس‌سازی داده[۲۸] یعنی تغییر یا حذف اطلاعات شخصی قابل شناسایی از مجموعه داده‌ها برای محافظت از حریم خصوصی افراد و کاهش خطر دسترسی غیرمجاز یا سوءاستفاده و نیز تجمیع داده[۲۹] که به‌معنای ترکیب یا خلاصه کردن داده‌ها در سطح بالاتر برای کاهش جزئیات و حجم اطلاعات ذخیره شده است.

28. Data anonymization
29. Data aggregation

- خط‌مشی یا سیاست اشتراک‌گذاری داده‌های کاربران

درک سیاست سکوی بزرگ برای نحوه اشتراک‌گذاری داده‌های کاربران اهمیت زیای دارد و روشنگر است. درحالی‌که همه محتواها و داده‌های به‌اشتراک گذاشته شده یا جستجو شده در همه خدمات زیرمجموعه گوگل به شکل آشکار همراه با نام برای گوگل مشخص است، وقتی گوگل تصمیم می‌گیرد اطلاعات کاربران را به‌اشتراک بگذارد، این اشتراک‌گذاری با شرکت‌ها، سازمان‌ها یا افراد خارج از گوگل مبتنی بر برخی رویه‌ّها است. مهم‌ترین رویه یا اقدام *کسب رضایت کاربران* است.

- کسب رضایت کاربران

همان‌طور که در سیاست حریم خصوصی گوگل می‌خوانیم:

چنانچه شما رضایت داشته باشید، اطلاعات شخصی را خارج از گوگل به‌اشتراک خواهیم گذاشت... همچنین کنترل‌هایی را برای بررسی و مدیریت برنامه‌ها و سایت‌های شخص ثالثی که به داده‌های موجود در حساب گوگل خود اجازه دسترسی به آنها داده‌اید، در اختیار شما قرار می‌دهیم. ما برای به‌اشتراک گذاشتن هرگونه اطلاعات شخصی حساس، به‌طور صریح رضایت شما را خواهیم گرفت (Google privacy policy, 2024).

اگرچه، دلایل *قانونی یا حقوقی* سبب می‌شوند تا گوگل بدون نیاز به کسب رضایت کاربران اقدام به افشای اطلاعات شخصی کاربران نماید. این دلایل به این شکل بیان شده‌اند:

اطلاعات شخصی را در خارج از گوگل به‌اشتراک خواهیم گذاشت، اگر به حسن‌نیت اعتقاد داشته باشیم که افشای اطلاعات برای موارد زیر معقولانه ضروری است:

- پاسخ به هر قانون، مقررات، روند قانونی یا درخواست قابل اجرای دولتی؛
- اجرای شرایط خدمات قابل اجرا، از جمله تحقیق در مورد نقض احتمالی قانون؛
- کشف، پیشگیری یا رسیدگی به تقلب، امنیت یا مشکلات فنی کشف، پیشگیری یا رسیدگی به تقلب، امنیت یا مشکلات فنی کشف؛
- محافظت در برابر آسیب به حقوق، اموال یا امنیت گوگل، کاربران ما یا عموم.

درمجموع با ملاحظه موارد فوق در جدول شماره ۱ مضامین اصلی و فرعی حاصل از مطالعه اسناد مرتبط با حکمرانی حریم خصوصی در گوگل ذکر شده است.

جدول ۱) مضامین و اصلی فرعی حکمرانی حریم خصوصی در گوگل

مضمون اصلی	مضامین فرعی	مصادیق و توضیحات
سیاست‌های حریم خصوصی	شرایط خدمت و خط‌مشی رازداری	شرایط ارائه خدمت و خط‌مشی رازداری به‌صورت اسنادی جداگانه اما مکمل ارائه شده‌اند تا نحوه گردآوری، استفاده و مدیریت داده‌ها توسط گوگل را توضیح دهند.
اصول حریم خصوصی گوگل	حریم خصوصی بر اساس طراحی	ادغام ملاحظات حریم خصوصی در طراحی و توسعه محصولات از ابتدا.
	حریم خصوصی به‌صورت پیش‌فرض	تنظیمات پیش‌فرض محصولات برای حفاظت حداکثری از حریم خصوصی کاربران.
اقدامات مرتبط با داده‌ها	تقلیل داده‌های کاربران	کاهش یا حذف اطلاعات قابل‌شناسایی شخصی و تجمیع داده‌ها برای حفاظت بهتر از کاربران.
	شفافیت در گردآوری و استفاده از داده‌ها	ارائه اطلاعات شفاف درباره انواع داده‌های جمع‌آوری‌شده، نحوه استفاده و اهداف گردآوری آن‌ها.
	عدم فروش اطلاعات شخصی	گوگل اطلاعات شخصی کاربران را برای اهداف تبلیغاتی به فروش نمی‌رساند.
	تسهیل کنترل کاربران بر داده‌های خود	کاربران می‌توانند داده‌های خود را بررسی، مدیریت و حذف کنند.
حفاظت و امنیت داده‌ها	رمزگذاری داده‌ها	استفاده از فناوری‌های پیشرفته مانند اچ.تی.تی.پی.اس و

مضمون اصلی	مضامین فرعی	مصادیق و توضیحات
		رمزگذاری برای حفاظت از اطلاعات در حالت سکون و انتقال.
	توسعه فناوری‌های پیشرفته حفظ حریم خصوصی	نوآوری و اشتراک‌گذاری فناوری‌ها برای افزایش امنیت در سطح اینترنت.
	ساخت محصولات ایمن به‌صورت پیش‌فرض	طراحی محصولات با امنیت پیش‌فرض برای حفاظت در برابر تهدیدات برخط.
خط‌مشی اشتراک‌گذاری داده‌ها	کسب رضایت کاربران	اشتراک‌گذاری اطلاعات شخصی تنها با رضایت کاربران، به‌جز در موارد قانونی یا امنیتی.
	افشای اطلاعات برای اهداف قانونی یا امنیتی	پاسخ به قوانین و مقررات، جلوگیری از تقلب، و حفاظت از حقوق و امنیت کاربران و گوگل.
توانمندسازی کاربران	کنترل کاربران بر تنظیمات حریم خصوصی	فراهم‌کردن ابزارهایی برای مدیریت اطلاعات شخصی، تنظیمات حریم خصوصی، و کنترل اشتراک‌گذاری داده‌ها.
	اعتماد و رضایت کاربران	ایجاد رضایت و اعتماد از طریق احترام به حریم خصوصی و ارائه تنظیمات کاربرپسند.

مضمون اصلی	مضامین فرعی	مصادیق و توضیحات
ارتباط حریم خصوصی و امنیت	همپوشانی امنیت و حریم خصوصی	رمزگذاری، احراز هویت قوی و کنترل دسترسی به‌عنوان راه‌حل‌های مشترک برای امنیت و حریم خصوصی.
	تعادل بین امنیت و حریم خصوصی	توازن میان نظارت برای امنیت و احترام به حریم خصوصی کاربران.

۲-۵. سکوی متا (فیس‌بوک)

شرکت متا پلتفرمز که در ابتدا با نام فیسبوک، در فوریه ۲۰۰٤ تأسیس شد، از یک سکوی ساده شبکه‌های اجتماعی به یک غول چندملیتی فناوری با حضور قوی در سطح جهانی تبدیل شده است. تأسیس این شرکت انقلابی در نحوه تعامل و برقراری ارتباط افراد به‌صورت برخط ایجاد کرد و راه را برای عصر رسانه‌های اجتماعی هموار ساخت.

حریم خصوصی در متا

به‌طورکلی حریم خصوصی یکی از زیرمجموعه‌های بخش شرایط ارائه خدمت در سکوهای متا است. دو بخش مرکز حریم خصوصی و سیاست حریم خصوصی عمده‌ترین محل‌هایی هستند که می‌توانیم سیاست کلی حریم خصوصی متا را درک کنیم. مارک زاکربرگ[۳۰] فیسبوک را بر اساس این ایده تأسیس کرد که برقراری ارتباط با افراد اساساً چیز خوبی است – و راهی برای کسب سود خوب. اما از همان ابتدا، فیسبوک هم به‌خاطر نحوه مدیریت حریم خصوصی کاربران و هم به‌خاطر نحوه مدیریت محتوای تولید شده توسط کاربر مورد انتقاد قرار گرفت. این دو موضوع پس از انتخابات ریاست جمهوری ایالات متحده در سال ۲۰۱٦، پس از نقش فیسبوک در انتشار اطلاعات نادرست سیاسی و نشت اطلاعات کاربران فیسبوک به شرکت‌های مشاوره سیاسی، با هم ادغام شدند *(Yoffie & Fisher, 2020)*. شرکت متا

30. Mark Zuckerberg

در موارد متعدد به اتهام نقض محرمانگی داده‌ها جریمه شده است. ازجمله در این شرکت در سال ۲۰۲۳ به‌دلیل نقض قوانین حفاظت از داده اتحادیه اروپا، مبلغ ۱.۲ میلیارد یورو (۱.۳ میلیارد دلار) جریمه شد و ملزم به توقف انتقال داده‌های جمع‌آوری‌شده از کاربران فیسبوک در اروپا به ایالات متحده شد *(صاحبی، ۱۴۰۲)*. همچنین مهم‌ترین مورد نقض حریم خصوصی کاربران توسط فیسبوک، رسوایی کمبریج آنالتیکا[۳۱] است که طی آن اطلاعات شخصی کاربران این سکو برای کارزارهای انتخاباتی مورد استفاده قرار گرفت.

اصول بنیادین حریم خصوصی متا

میشل پراتی[۳۲] (۲۰۲۲)، مدیر ارشد حریم خصوصی متا، مطلبی را در تارنمای متا نوشته و در آن در مورد بروزرسانی حریم خصوصی و شرایط ارائه خدمت این سکو توضیحاتی را بیان کرده است:

از امروز، متا اعلان‌هایی را منتشر می‌کند تا به کاربران اطلاع دهد که ما «سیاست حریم خصوصی» خود را که قبلاً به‌عنوان «سیاست داده» شناخته می‌شد، به‌روزرسانی کرده‌ایم. ما با الهام از بازخورد کاربران فناوری‌های ما و کارشناسان حریم خصوصی، سیاست حریم خصوصی خود را بازنویسی کرده‌ایم تا درک آن آسان‌تر شود و محصولات جدیدی را که ارائه می‌دهیم منعکس کند. درحالی‌که متن در بسیاری از نقاط متفاوت به نظر می‌رسد، متا بر اساس این به‌روزرسانی سیاست، داده‌های شما را به روش‌های جدید جمع‌آوری، استفاده یا به‌اشتراک نمی‌گذارد و ما همچنان اطلاعات شما را نمی‌فروشیم *(Protti, 2022)*.

چند نکته از این نوشته قابل فهم است. نخست اینکه متا سیاست حریم خصوصی خود را از داده به حریم خصوصی تغییر داده است که البته علت آن بیان نشده است. دوم اینکه، ساده‌سازی ادبیات حریم خصوصی برای قابل فهم‌تر شدن آن برای عموم کاربران این پلتفرم است و تأکید بر اینکه متا داده‌های کاربران را با دیگران به‌اشتراک نمی‌گذارد و نمی‌فروشد. به ظاهر، این موضوع در راستای انتقادها نسبت به انتشار و فروش داده‌های کاربران بیان شده است.

---

31. Cambridge Analytica
32. Protti

گرچه به‌طورخاص بخشی به بیان اصول بنیادین متا درباره حریم خصوصی اختصاص نیافته است؛ اما در بخش به‌روزرسانی بهبود حریم خصوصی[۳۳] بیان شده است که برای توسعه محصولات، خدمات و کردارهای جدید برخی ملاحظات راهنما درباره حریم خصوصی وجود دارد. این اصول را می‌توان به‌منزله اصول راهنمای متا نسبت به حریم خصوصی در نظر گرفت. حکمرانی متا درباره حریم خصوصی مبتنی بر این اصول است. از منظری‌دیگر، رویکرد متا به حریم خصوصی توسط چندین اصل اساسی هدایت می‌شود که محصولات، خدمات و تجربه کاربری آن را شکل می‌دهد. این اصول عبارت‌اند از:

کنترل و شفافیت کاربر: متا تلاش می‌کند تا ابزارهای آسان برای استفاده و اطلاعات شفاف در مورد تنظیمات حریم خصوصی را در اختیار کاربران قرار دهد تا آنها را قادر سازد تا انتخاب‌های آگاهانه در مورد داده های خود داشته باشند. امنیت متا با سرمایه‌گذاری در فناوری های پیشرفته و بهترین شیوه‌ها برای محافظت در برابر دسترسی غیرمجاز و سوءاستفاده بالقوه، امنیت داده‌های کاربر را در اولویت قرار می‌دهد.

تقلیل داده: متا به‌دنبال جمع‌آوری و نگهداری تنها اطلاعاتی است که برای ارائه خدمات و ارائه تجربیات شخصی‌سازی شده ضروری است. این رویکرد به حداقل رساندن افشای بالقوه داده‌های حساس کمک می‌کند.

پاسخگویی و انطباق: متا خود را مسئول رعایت مقررات، قوانین و استانداردهای صنعتی حریم خصوصی می‌داند و همچنین با تنظیم‌کننده‌ها و ذینفعان برای اطمینان از حفظ حریم خصوصی کاربران همکاری می‌کند.

حفظ حریم خصوصی از طریق طراحی و به‌صورت پیش‌فرض: متا ملاحظات مربوط به حریم خصوصی را در فرآیند توسعه محصولات و خدمات جدید ادغام می کند تا حریم خصوصی را از همان ابتدا به‌عنوان یک جنبه اساسی از محصولات خود قرار دهد.

منافع کاربر: متا در عین احترام و محافظت از حریم خصوصی کاربران، تلاش می کند تا تجربیات کاربری ارزشمند و خدمات شخصی‌سازی شده ایجاد کند. این شرکت به دنبال ایجاد تعادل بین نوآوری و حفظ حریم خصوصی است

33. Privacy progress update

بهبود مستمر: متا اذعان دارد که حریم خصوصی یک تعهد مستمر است و دائماً رویه ها، سیاست ها و فناوری های خود را برای رسیدگی به چالش‌های نوظهور حریم خصوصی ارزیابی و تکامل می‌بخشد.

با پایبندی به این اصول اساسی حریم خصوصی، متا هدف خود را بر ایجاد یک محیط برخط خصوصی‌تر و امن‌تر برای کاربران خود، تقویت اعتماد و ارتقای کلی تجربه کاربری در سراسر سکوهای خود قرار داده است *(Meta, 2023)*.

برخی از اصول بنیادین که در اینجا به آن اشاره شده است، ازقبیل تقلیل داده‌ها، کنترل کاربران، حفظ حریم خصوصی از طریق و به شکل پیش‌فرض ازجمله اصولی هستند که در سکوی متا مورد تأکید قرار دارد و در گوگل نیز بر آنها تأکید شده بود.

حریم خصوصی و امنیت در متا

بخشی از رویکرد کلی متا به حریم خصوصی در این بخش قابل مشاهده است. همان‌طور که در صفحه این بخش مشاهده می‌کنیم، متا ادعا می‌کند:

ما متعهد هستیم که به شما کنترل حریم شخصی و محافظت از اطلاعاتتان را بدهیم تا بتوانید از تجربیات باارزش خود در محصولات ما لذت ببرید. به همین دلیل است که ما ابزارهایی را برای کمک به شما در ایمن‌سازی اطلاعاتتان و انتخاب‌های درست در زمینه حفظ حریم شخصی، با رعایت استانداردهای سختگیرانه صنعت برای حفظ حریم شخصی و محافظت از داده‌هایتان، ساخته‌ایم *(Meta privacy and data policy, 2024)*.

دو نکته محوری در این مطلب کوتاه قابل توجه است: نخست تأکید بر اینکه کاربران توانایی *اعمال کنترل* بر حریم خصوصی خود را دارند. موضوعی که مورد تأکید سکوی گوگل نیز هست. نکته دوم، توسعه *فناوری‌های حفظ* حریم خصوصی است. حفظ حریم خصوصی و محرمانگی داده‌ها در سکوها، مستلزم توسعه فناوری‌های متناسب است. سکوها باید متعهد شوند تا از تمام ابزارها برای حفاظت از حریم خصوصی کاربرانشان استفاده کنند و این یک روند مستمر و الزام تعهدآور است.

موضوعات حریم خصوصی

موضوعات مرتبط با حریم خصوصی شامل ایمنی، امنیت حساب کاربری، مخاطب، موقعیت جغرافیایی، تبلیغات، گردآوری اطلاعات و نحوه کاربرد اطلاعات است.

- اهمیت ایمنی در حریم خصوصی

نخستین بخش از موضوعات حریم خصوصی متا ایمنی است. ایمنی امکانات کاربرد اعمال کنترل بر اشتراک‌گذاری اطلاعات شخصی را در اختیار کاربرد قرار می‌دهد. در این بخش کاربران می‌توانند محدودیت‌هایی را برای اینکه چه کسانی می‌توانند اطلاعات به اشتراک‌گذاشته شده توسط آنها را مشاهده کنند، اعمال نمایند. همچنین افراد می‌توانند از پیام‌ها و اطلاعات شخصی خود محافظت کنند. همچنین اگر کاربران مورد آزار و قلدری قرار می‌گیرند می‌توانند مورد حمایت شرکت متا قرار بگیرند؛ بنابراین مضمون محوری در این بخش *مدیریت اشتراک‌گذاری اطلاعات توسط کاربر* است.

دو بخش حائزاهمیت دیگر نحوه گردآوری داده و نحوه استفاده از داده‌های شخصی است. در این بخش نخست، کاربر می‌تواند اطلاعاتی را که متا درباره او گردآوری می‌کند، مشاهده و مدیریت کند. در بخش استفاده توضیح داده شده است که کاربر در این بخش یاد می‌گیرند متا با اطلاعاتی که درباره کاربر گردآوری می‌کند و یا اطلاعاتی را درباره او دریافت می‌کند، چه می‌کند. آگاهی بیشتر درباره این کردارهای حریم خصوصی به سیاست حریم خصوصی گوگل ارجاع داده شده است.

- سیاست حریم خصوصی متا

سیاست و خط‌مشی حریم خصوصی در ۲۶ ژوئن ۲۰۲۴ به‌روزرسانی شده است. در ابتدای این گزارش آمده است: «ما در متا از شما می‌خواهیم که بدانید چه اطلاعاتی را جمع‌آوری می‌کنیم و چگونه از آن استفاده می‌کنیم و به‌اشتراک می‌گذاریم» (*Meta privacy and data policy, 2024*). براین‌اساس می‌توان گفت که هدف از این سند بیان کردارهای متا درباره نحوه گردآوری داده‌های کاربران، چگونگی استفاده از آن و نیز نحوه اشتراک‌گذاری این محتواها است. همچنین هدف این حریم خصوصی آگاه کردن کاربران

از حقوق‌شان نسبت به حریم داده‌هایشان است. علاوه‌براین، همان‌طور که متا می‌گوید: «برای ما مهم است که بدانید چگونه حریم خصوصی خود را کنترل کنید؛ بنابراین به شما نشان می دهیم کجا می‌توانید اطلاعات خود را در تنظیمات محصولات متا که استفاده می کنید مدیریت کنید» (*Meta privacy and data policy, 2024*)؛ بنابراین، نکته‌ای که در اینجا بر آن تأکید می‌شود، *امکان کنترل کاربر بر حریم خصوصی خود* است.

ما در اینجا برای فهم سیاست حریم خصوصی متا در موارد کلیدی فوق آنها را در مقوله‌های جداگانه مورد بررسی قرار می‌دهیم.

نحوه استفاده از اطلاعات گردآوری‌شده توسط متا

متا برای ارائه یک تجربه شخصی‌شده برای کاربران ازجمله برای شخصی‌سازی آگهی‌ها و نیز به‌دلایل گوناگون از اطلاعات گردآوری شده از کاربران استفاده می‌کند. به این‌منظور متا هم از اطلاعاتی که کاربران در محصولات مختلف این کشور ارائه کرده‌اند و نیز اطلاعاتی که از طریق وسایل ارتباطی کاربران قابل دسترسی است، استفاده می‌کنند. باوجوداین متا مدعی است که این شرکت برای اینکه از اطلاعاتی که مربوط به یکایک کاربران است کمتر استفاده کند، از این اطلاعات هویت‌زدایی می‌کند و یا آنها را انبوهه‌سازی[۳۴] می‌کند تا قابل شناسایی نباشند؛ بنابراین یک رویکرد برای حفاظت از داده‌های شخصی کاربران *ناشناس‌سازی و یا تقلیل داده‌ها* است.

مبنای قانونی پردازش اطلاعات کاربران

بر اساس قوانین موضوعه برای حفاظت از داده‌ها، شرکت‌ها برای پردازش اطلاعات شخصی باید بر مبنای مفاد قاناونی عمل کنند. منظور از پردازش داده‌های شخصی، روش‌های گردآوری، استفاده و اشتراک‌گذاری داده‌های کاربران است که در سیاست حریم خصوصی متا بیان شده است.

همان‌گونه در سیاست حریم خصوصی متا مشاهده می‌شود، متا برای پردازش اطلاعات کاربران به قانون تکیه می‌کند تا اعمال خود را قانونی جلوه دهد:

34. aggregate

ما برای پردازش اطلاعات شما برای اهداف شرح داده شده در این خط‌مشی رازداری به پایه‌های قانونی مختلفی متکی هستیم. بسته به شرایط، ما هنگام پردازش اطلاعات مشابه شما برای اهداف مختلف، به پایه‌های قانونی متفاوتی تکیه می‌کنیم. برای هر پایه قانونی در زیر، توضیح می‌دهیم که چرا اطلاعات شما را پردازش می‌کنیم. همچنین بسته به اینکه از کدام پایه قانونی استفاده می‌کنیم، حقوق خاصی برای شما در نظر گرفته شده است که ما در اینجا آنها را توضیح داده‌ایم. صرف‌نظر از اینکه چه پایه قانونی اعمال شود، شما همیشه حق دسترسی، اصلاح و حذف اطلاعات خود را دارید *(Meta privacy and data policy, 2024)*.

- رضایت کاربران

مبانی قانونی پردازش اطلاعات کاربران فیسبوک بر چند محور استوار است. نخست قراردادی است که کاربران به هنگام عضویت در هرکدام از خدمات متا امضاء می‌کنند. ازجمله آنها می‌توان به شرایط ارائه خدمت، شرایط ارائه خدمت اینستاگرام، شرایط ارائه خدمت در فناوری‌های تکمیلی سکوهای متا، شرایط ارائه خدمت پورتال تکمیلی و شرایط ارائه خدمت نگرش تکمیلی فیسبوک[۳۵] اشاره کرد که درمجموع شرایط ارائه خدمت نامیده می‌شوند. یکی مبنای قانونی دیگر *رضایت کاربران* است:

ما اطلاعات شما را در صورت رضایت شما پردازش می کنیم؛ برای مثال، شما می‌توانید به ما اجازه دهید تا تبلیغات شخصی سازی شده را بر اساس اطلاعاتی که تبلیغ‌کنندگان و دیگران به ما ارائه می دهند، به شما نشان دهیم. این شامل اطلاعات مربوط به فعالیت شما در تارنماها و برنامه‌های آنها و همچنین برخی تعاملات غیربرخط مانند خرید است. شما می‌توانید رضایت خود را در هر زمان پس بگیرید *(Meta privacy and data policy, 2024)*.

اعمال مقررات مرتبط با سیاست‌ها در متا

شرکت متا مجموعه‌ای از رویه‌ها را برای اعمال مقررات مرتبط با سیاست‌ها ازجمله حریم خصوصی تعبیه کرده است که درکل ذیل تعدیل محتوا قابل فهم است. متا برای شناسایی، بررسی و اقدام نسبت به میلیون‌ها محتوا در فیسبوک و اینستاگرام هر روز از فناوری و

35. Supplemental Facebook View Terms of Service

گروه‌های بررسی‌کننده استفاده می‌کند. فناوری و گروه‌های بررسی به متا کمک می‌کنند تا محتوا و حساب‌های کاربری که بالقوه ناقض قوانین هستند را شناسایی و بررسی کنند. متا از یک رویکرد سه بخشی برای اعمال مقرارت در مورد محتوا استفاده می‌کند: حذف، کاهش و اطلاع‌رسانی. روشن است که این موضوع در مورد محتواهای ناقض حریم خصوصی نیز مصداق دارد.

بخش اول شامل حذف است. همان‌طور که در مرکز شفافیت متا آمده است:

اگر محتوای شما مغایر با استانداردهای انجمن فیسبوک یا دستورالعمل‌های انجمن اینستاگرام باشد، متا آن را حذف خواهد کرد. ما همچنین به شما اطلاع خواهیم داد تا بتوانید دلیل حذف محتوا و نحوه جلوگیری از ارسال محتوای نقض‌کننده در آینده را درک کنید. ما از یک سیستم امتیازدهی برای شمارش تخلفات و مسئول نگه داشتن شما در قبال محتوایی که ارسال می‌کنید استفاده می‌کنیم. بسته به اینکه محتوای شما با کدام خط‌مشی مغایرت دارد، سوابق قبلی تخلفات شما و تعداد امتیازهایی که دارید، حساب کاربری شما نیز ممکن است محدود یا غیرفعال شود *(Meta Transparency Center, 2023)*.

بخش دوم کاستن از میزان انتشار محتوای مسئله‌دار است:

اگرچه محتوایی در فیسبوک، معیارهای انجمن فیسبوک را نقض نکند، اما همچنان ممکن است مشکل‌ساز یا به نوعی کم‌کیفیت باشد، متا می‌تواند توزیع آن را مطابق با کنترل‌های کاربر کاهش دهد. این، یکی از اجزای راهبرد کلی «حذف، کاهش، اطلاع‌رسانی» ماست که از سال ۲۰۱۶ به کار می‌بریم *(Meta Transparency Center, 2023)*.

بخش سوم، اطلاع‌رسانی یا آگاهانیدن کاربران نسبت به یک محتوای خاص است:

یکی از روش‌هایی که متا جامعه امن و واقعی را ترویج می‌کند، اطلاع‌رسانی به افراد در مورد اینکه محتوا ممکن است حساس یا گمراه‌کننده باشد، حتی اگر به‌صراحت با استانداردهای انجمن فیسبوک یا دستورالعمل‌های انجمن اینستاگرام مغایرت نداشته باشد، است. در چنین مواقعی، ما زمینه بیشتری در مورد محتوا اضافه می‌کنیم تا به مردم در تصمیم‌گیری برای خواندن، اعتماد یا به‌اشتراک گذاشتن آن کمک کنیم *(Meta Transparency Center, 2023)*.

درمجموع می‌توان گفت که یکی از پیشروترین و پیچیده‌ترین سازوکارهای مرتبط با حریم خصوصی و داده در متا مشاهده می‌شود. هرچند با وجود تمام این اسناد و اقدامات، متا همواره در معرض اتهام نقض حریم خصوصی کاربرانش قرار داشته است. در جدول شماره ۲ مضامین اصلی و فرعی مرتبط با سازوکار حکمرانی حریم خصوصی در متا ذکر شده است.

جدول شماره ۲: مضامین اصلی و فرعی مرتبط با سازوکار حکمرانی حریم خصوصی در متا

مضمون اصلی	مضمون فرعی	مصادیق
اصول بنیادین حریم خصوصی	محدودیت هدف از پردازش داده	داده‌ها تنها برای اهداف مشخص و ارزشمند پردازش می‌شوند.
	تقلیل داده	جمع‌آوری حداقل داده‌ها برای پشتیبانی از اهداف مشخص
	شفافیت و کنترل	اطلاع‌رسانی شفاف و امکان کنترل کاربران بر داده‌هایشان
	حریم خصوصی از طریق طراحی	لحاظ الزامات حریم خصوصی از ابتدا در طراحی محصولات
	حفظ امنیت	سرمایه‌گذاری در فناوری‌های امنیتی برای جلوگیری از دسترسی غیرمجاز
	بهبود مستمر	بازنگری و به‌روزرسانی مداوم سیاست‌ها و فناوری‌های حریم خصوصی
موضوعات حریم خصوصی	ایمنی	مکان کنترل اشتراک‌گذاری اطلاعات شخصی توسط کاربران و حمایت از آنها در برابر قلدری و آزار
	جمع‌آوری داده	استفاده برای شخصی‌سازی، امنیت، تحلیل داده‌ها، و تحقیقات اجتماعی

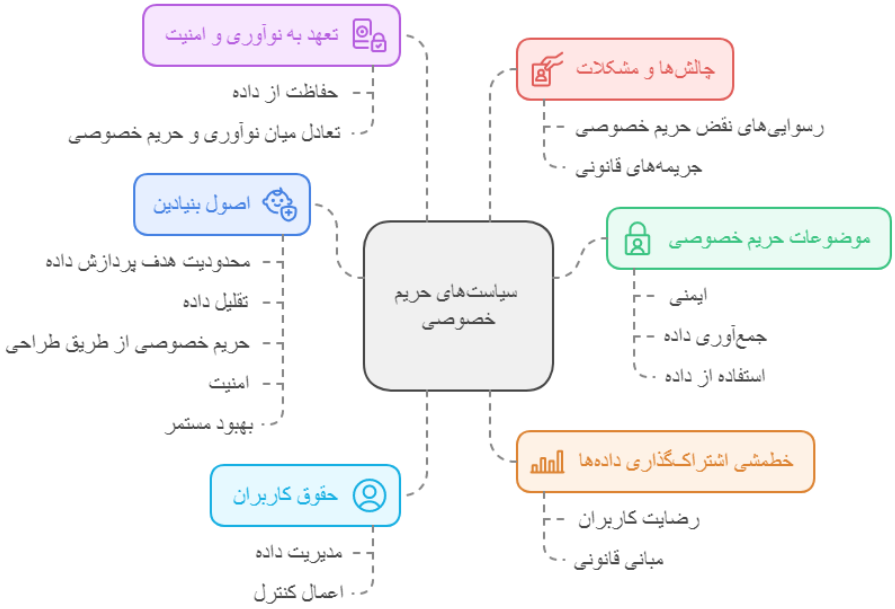
مضمون اصلی	مضمون فرعی	مصادیق
	استفاده از داده‌ها	استفاده برای شخصی‌سازی، امنیت، تحلیل داده‌ها و پژوهش‌های اجتماعی
حقوق کاربران در متا	مدیریت داده‌ها	امکان مشاهده، مدیریت، بارگیری و حذف اطلاعات کاربران
	اعمال مبانی قانونی	تکیه بر قوانین حفاظت از داده‌ها برای پردازش اطلاعات کاربران
رویکرد متا به حریم خصوصی	شفافیت	اطلاع‌رسانی واضح و صادقانه درباره استفاده از داده‌ها
	حفاظت از داده‌ها	استفاده از رمزگذاری پایان به پایان و سایر ابزارهای امنیتی برای حفظ داده‌ها
	حفظ تعادل بین نوآوری و حریم خصوصی	ارائه خدمات شخصی‌سازی‌شده در عین احترام به حقوق کاربران
مسائل و چالش‌ها	رسوایی کمبریج آنالتیکا	استفاده از اطلاعات کاربران برای کارزارهای انتخاباتی
	جریمه‌های قانونی	جریمه ۱.۳ میلیارد دلاری به دلیل نقض قوانین حفاظت از داده اتحادیه اروپا

این سکو با وجود برخی اختلاف‌ها، اشتراکات زیادی در نحوه حکمرانی حریم خصوصی و داده دارند که می‌تواند به‌عنوان راهنمای تدوین و اعمال سیاست‌های حریم خصوصی در سکوهای ایرانی (سکوهای خدماتی، رسانه‌های اجتماعی و پیام‌رسان‌ها) عمل کند؛ هرچند نبود یک قانون جامع حریم خصوصی و حفاظت از داده یک معضل اساسی است که درنتیجه شاهد نفوذ و انتشار گسترده اطلاعات شخصی کاربران سکوهای مختلف هستیم.

۶. نتیجه‌گیری

تحلیل سیاست‌ها و حکمرانی حریم خصوصی در دو سکوی بزرگ گوگل و متا نشان می‌دهد که این شرکت‌ها با اتخاذ رویکردهای جامع و نوآورانه، توانسته‌اند چهارچوب‌های پیشرفته‌ای برای مدیریت داده‌ها و حفاظت از حریم خصوصی کاربران ایجاد کنند. رئوس کلی این چهارچوب در شکل شماره ۱ ذکر شده است.

شکل شماره ۱: سازوکار حکمرانی حریم خصوصی در دو سکوی جهانی گوگل و متا؛ منبع: ترسیم شده توسط مؤلف



این نمودار یافته‌های این مقاله درباره سازوکارها، اصول و اقدامات حکمرانی حریم خصوصی در سکوها را توضیح می‌دهد. چالش‌ها و مشکلاتی مانند نقض حریم خصوصی داده‌ها و جرایم قانونی مرتبط در کنار موضوعاتی همچون امنیت، جمع‌آوری داده‌ها و نحوه استفاده از آن‌ها، از عناصر کلیدی هستند. همچنین، به تعهد به حفاظت از داده‌ها و ایجاد تعادل میان نوآوری و حریم خصوصی از طریق استفاده از فناوری‌های پیشرفته و

بهبود مستمر تأکید شده است. همان‌طور که این شکل نشان می‌دهد گوگل و متا با اتکا به سازوکارهای حکمرانی حریم خصوصی، تعهد خود را به نوآوری همراه با امنیت و حفاظت از داده‌ها نشان می‌دهند. این سکوها با رعایت اصول بنیادین مانند «محدودیت هدف پردازش داده» (جمع‌آوری داده‌ها تنها برای اهداف مشخص شده)، «تقلیل داده» (کاهش حجم اطلاعات ذخیره شده به حداقل ضروری) و «حریم خصوصی از طریق طراحی» (ادغام الزامات امنیتی در مراحل توسعه محصول)، به‌دنبال ایجاد تعادل میان پیشرفت فناوری و حفظ حریم کاربران هستند. آنها با تأکید بر حقوق کاربران، امکان مدیریت داده‌ها و اعمال کنترل بر تنظیمات حریم خصوصی را فراهم می‌کنند. بااین‌حال، مواجهه با چالش‌هایی مانند نقض حریم خصوصی (ناشی از حملات سایبری یا خطاهای انسانی) و جریمه‌های قانونی (به‌ویژه تحت قوانینی مانند جی.دی.پی.آر) بخشی از واقعیت فعالیت این شرکت‌هاست. در حوزه اشتراک‌گذاری داده‌ها، گوگل و متا بر کسب رضایت آگاهانه کاربران و رعایت چهارچوب‌های حقوقی میانجی (مانند توافقنامه‌های بین‌المللی) تکیه دارند تا استفاده از داده‌ها در مسیرهای تعیین‌شده (مانند بهبود خدمات یا شخصی‌سازی تبلیغات) را تضمین کنند. این سازوکارها نشان‌دهنده تلاش پیوسته برای همسویی نوآوری دیجیتال با انتظارات حقوقی و اخلاقی در عصر حاضر است.

در مقام مقایسه باید گفت که گوگل و متا به‌عنوان دو غول فناوری جهانی، رویکردهای متفاوتی را در مدیریت حریم خصوصی و داده‌ها اتخاذ کرده‌اند. گوگل با تمرکز بر حریم خصوصی از طریق طراحی و تنظیمات پیش‌فرض امن، امنیت را در هسته محصولات خود مانند جیمیل و گوگل درایو ادغام کرده است و از دستورالعمل‌های پیشرفته‌ای مانند رمزگذاری تی.ال.اس برای انتقال داده‌ها استفاده می‌نماید. این شرکت همچنین با سیاست تقلیل داده، جمع‌آوری اطلاعات را به حداقل ضروری محدود کرده و ابزارهای شفافی برای مدیریت داده‌ها در اختیار کاربران قرار می‌دهد. از سوی‌دیگر، متا با اولویت‌دهی به کنترل کاربر و شفافیت، ابزارهایی برای تنظیم حریم خصوصی در سکوهای اجتماعی مانند فیسبوک و اینستاگرام ارائه می‌دهد؛ اما به‌دلیل مدل کسب‌وکار مبتنی بر تبلیغات شخصی‌سازی‌شده، همواره با انتقاداتی درباره جمع‌آوری گسترده داده‌ها روبه‌روست.

اگرچه هر دو سکو از رمزگذاری پیشرفته استفاده می‌کنند و به کاربران اجازه مدیریت تنظیمات را می‌دهند، گوگل بیشتر بر امنیت زیرساختی تمرکز دارد، درحالی‌که متا چالش‌های ویژه‌ای در محتوای تولیدشده کاربران و رسوایی‌هایی مانند کمبریج آنالیتیکا تجربه کرده است.

سکوهای داخلی در ایران با چالش‌هایی همچون ضعف زیرساخت‌های قانونی، کمبود شفافیت در مدیریت داده‌ها، و عدم رعایت اصول امنیت و حریم خصوصی مواجه هستند. درحالی‌که کاربران ایرانی تمایل فزاینده‌ای به استفاده از خدمات برخط دارند، حفظ اعتماد کاربران به این سکوها از اهمیت بالایی برخوردار است. سیاست‌های موفق گوگل و متا می‌توانند به‌عنوان الگویی برای توسعه چهارچوب‌های بومی استفاده شوند.

پیشنهادها

با ملاحظه رویکرد کلی حفاظت از حریم خصوصی و حریم داده در مورد از سکوهای جهانی، پیشنهادهای زیر برای سکوهای ایرانی ارائه می‌شود:

۱. تدوین چهارچوب‌های قانونی شفاف: قوانین مرتبط با حریم خصوصی و حفاظت از داده‌ها باید با رعایت استانداردهای بین‌المللی (مانند مقررات عمومی حفاظت از داده‌ها) تدوین شوند.

۲. سرمایه‌گذاری در امنیت داده‌ها: استفاده از فناوری‌های پیشرفته رمزگذاری و امنیت سایبری برای حفظ اطلاعات کاربران ضروری است.

۳. ایجاد ابزارهای مدیریت داده: سکوها باید ابزارهایی برای مشاهده، حذف و کنترل داده‌های کاربران ارائه دهند.

٤. افزایش شفافیت: سیاست‌های جمع‌آوری و استفاده از داده‌ها باید به زبان ساده و شفاف به کاربران توضیح داده شود.

٥. آموزش کاربران: افزایش آگاهی کاربران در خصوص اهمیت حریم خصوصی و نحوه استفاده از تنظیمات امنیتی می‌تواند اعتماد آن‌ها را تقویت کند.

٦. ایجاد مراکز پاسخگویی: مانند مراکز کمک گوگل، مراکزی برای پاسخگویی به شکایات و پرسش‌های کاربران درباره حریم خصوصی ایجاد شود.

پیاده‌سازی این رویکردها می‌تواند به ارتقاء سطح اعتماد عمومی به سکوهای داخلی و رقابت‌پذیری آن‌ها در بازار جهانی کمک کند.

قدردانی

این مقاله حاصل طرح پژوهشی نویسنده در دوره فرصت مطالعاتی در مرکز ملی فضای مجازی (پژوهشگاه فضای مجازی) است. نویسنده از حمایت این مرکز قدردانی می‌نماید.

کتابنامه

احمدلو، مونا (١٤٠٠). *حریم خصوصی در فقه و قانون ایران*. تهران: مجمع علمی و فرهنگی مجد.

احمدوند، بهناز، جهانشاهی، آرتین (١٤٠٢). بررسی الزامات حاکم بر تأمین امنیت داده‌های کاربران توسط پلتفرم‌های ارائه‌دهنده خدمات. *فصلنامه سیاست علم و فناوری*. ١٦(٤): ٨٣-٩٨.

اسماعیلی، محسن (١٤٠١). *حقوق آزادی اطلاعات در ایران (جلد اول). شرح و تفسیر کاربردی قانون دسترسی و انتشار آزاد اطلاعات*. تهران: پژوهشگاه فرهنگ، هنر و ارتباطات.

اصلانی، زینت، جعفری، علی و سلمان‌زاه، جعفر (١٤٠٢). مسئولیت مدنی رسانه‌ها در قبال نقض حریم خصوصی در حقوق ایران و انگلستان. *فصلنامه جامعه، فرهنگ و رسانه*. ٤٦(٢): ١٣١.١٥٥.

انصاری، باقر و شیما، عطار (١٤٠٢). *حقوق کاربران فضای مجازی*. تهران: سهامی انتشار.

انصاری، باقر (١٣٨٣). حریم خصوصی در رسانه‌های همگانی. *فصلنامه پژوهش‌های ارتباطی*. ١١(٣٩): ١٩٣.

انصاری، باقر (١٤٠٠). حقوق حریم خصوصی. تهران: سازمان سمت.

پیش‌نماز، سیدامین و رکنی، امیرعباس (۱۴۰۲). تعطیلی پلتفرم‌های مجازی؛ ضرورت تحلیل نظام حاکم بر داده‌های شخصی از منظر حقوق اموال. *مجله پژوهش‌های حقوقی*. ۵۳(۱): ۴۶۹-۵۰۶.

حسام، ابوالفضل و دیگران (۱۴۰۰). مسئولیت مدنی پلتفرم‌های آنلاین ناشی از نقض حریم خصوصی اطلاعاتی از سوی کاربران؛ مطالعه تطبیقی در ایران، آمریکا و اتحادیه اروپا. *فصلنامه پژوهش‌های ارتباطی*. ۱۰۷ (۳): ۶۹-۹۱.

سروش، محمد (۱۳۹۸). *مبانی حریم خصوصی (براساس منابع اسلامی)*. تهران. سمت.

صاحبی، ایمان (۱۴۰۲). اتحادیه اروپا متا را نقره‌داغ کرد؛ جریمه تاریخی ۱.۳ میلیارد دلاری به خاطر نقض حریم خصوصی. *وبگاه دیجیتاتو*. قابل دسترسی در:
https://digiato.com/article/2023/05/22/eu-fine-meta-1300-mln-dollars-over-gdpr-violations

فرامرزیانی، پروانه و دیگران (۱۴۰۰). طراحی الگوی راهکارهای حمایت از حریم خصوصی کودکان در فضای مجازی. *فصلنامه پژوهش‌های ارتباطی*. ۱۰۶: ۹-۳۰.

فن‌دایک، یوزه (۱۴۰۲). *فرهنگ اتصال: تاریخ انتقادی رسانه‌های اجتماعی*؛ ترجمه حسین حسنی. تهران: سوره مهر.

شورای عالی فضای مجازی. (۱۳۹۵). مصوبه شورای عالی فضای مجازی با عنوان: «سند تبیین الزامات شبکه ملی اطلاعات». قابل دسترسی در:
https://rc.majlis.ir/fa/law/show/1033103

شورای عالی فضای مجازی. (۱۳۹۶). مصوبه شورای عالی فضای مجازی با موضوع سیاست‌ها و اقدامات ساماندهی پیام‌رسان‌های اجتماعی. قابل دسترسی در:
https://rc.majlis.ir/en/law/show/1029998

شورای عالی فضای مجازی. (۱۳۹۷). الزامات حاکم بر اینترنت اشیاء در شبکه ملی اطلاعات. قابل دسترسی در:
https://rc.majlis.ir/fa/law/show/1086381

شورای عالی فضای مجازی. (۱۴۰۱). *سند راهبردی جمهوری اسلامی ایران در فضای مجازی*. قابل دسترسی در: https://rc.majlis.ir/fa/law/show/1751605

Boyd, D., & Crawford, K. (2012). Critical questions for big data. *Information, Communication & Society*, 15(5), 662-679.

Braun, V. and Clarke, V. (2006) Using Thematic Analysis in Psychology. Qualitative Research in Psychology, 3, 77-101.

http://dx.doi.org/10.1191/1478088706qp063oa

Carah, N. (2021). *Media and society: Power, platforms, and participation*. London: Sage.

Correia, M., & Rodrigues, L. (2023). Security and privacy. In *Multidisciplinary Perspectives on Artificial Intelligence and the Law* (pp. 81-101). Springer. https//doi.org/10.1007/978-3-031-41264-6_5

Flew, T. (2021). *Regulating platforms*. Cambridge & Medford. Polity Press.

Gorwa, R. (2019). What is platform governance? Information, Communication & Society, 22(6), 854–871. https://doi.org/10.1080/1369118X.2019.1573914

Google. (1999). Google Privacy & Policy (June 1999 version). Retrieved from https://policies.google.com/privacy/archive/19990609?hl=en

Google. (2024). Google privacy policy. *Google*. https//policies.google.com/privacy?hl=en-US

Google. (2024). Our principles. *Google Safety Center*. https//safety.google/principles/?hl=en_US

Google. (2024). Privacy progress update. *Meta*. https//about.meta.com/uk/privacy-progress/

Meta. (2023). Meta Privacy Policy. *Meta*. Retrieved from https://www.facebook.com/privacy/policy/

Meta. (2024). Meta privacy and data policy. *Meta*. Retrieved from https://www.facebook.com/privacy/policy/

Meta. (2023). Meta Transparency Center.*Meta*. https://transparency.meta.com/

Pichai, S. (2021). We keep your personal online data private, safe, and secure. *Google Safety Center*. https//safety.google/security-privacy/

Protti, M. (2022, May 26). Here's what you need to know about our updated privacy policy and terms of service. *Meta*. https://about.fb.com/news/2022/05/metas-updated-privacy-policy/

Sheldon, R., Loshin, P., & Cobb, M. (2024). Encryption. Retrieved from https//www.*techtarget.com*/searchsecurity/definition/encryption

Solove, D. J. (2013). Privacy self-management and the consent dilemma. *Harvard Law Review*, 126(7), 1880-1903.

Trepte, S. (2021). The Social Media Privacy Model: Privacy and Communication in the Light of Social Media Affordances. *Communication Theory*, 31(4), 549-570.

Véliz, C. (202٤). *Privacy is power: Why and how you should take back control of your data*. London: Bantam press.

Yoffie, D. B., & Fisher, D. (2019). Fixing Facebook: Fake news, privacy, and platform governance. *Harvard Business School Case* 720-400, October 2019. (Revised January 2020).