Jurisprudence and Legal Studies of Media Journal
VOL. 7 / Autumn 2025 and Winter 2026 / NO. 2 (Serial 14)

Legal Analysis of the Distinction Between Ordinary and Sensitive Data on Social Media Platforms (Comparative Study of the European Union, the United States, and Iran)

Hasan Mohseni[1] 0009-0000-1457-8573
Zahra Jalali[2] 0009-0003-3676-7473

Abstract

In today's digital era, social media platforms have emerged as major environments for the generation and processing of personal data. These platforms not only collect users' explicit information but also use complex algorithms to infer and analyze hidden dimensions of individuals' identities, attitudes, and preferences. In such a context, the distinction between Non-sensitive data and sensitive data has become increasingly ambiguous, raising significant legal challenges in protecting users' privacy. This article employs an analytical-comparative methodology to examine how three legal systems—the European :union:, the United States, and Iran—approach the differentiation between ordinary and sensitive data on social media. The findings reveal that the EU follows a precise, list-based approach; the U.S. adopts a contextual, sector-based model; and Iran relies on a fragmented and underdeveloped legal structure. The study concludes by offering policy recommendations for strengthening Iran's legal framework, including the enactment of comprehensive data protection legislation and a revision of the criteria for defining sensitive data.

Keyword: Social Media Platforms, Personal Data, Non-sensitive Data, Sensitive Data, General Data Protection Regulation (GDPR).

1- Professor, Department of Private Law, Faculty of Law and Political Science, University of Tehran hmohseny@ut.ac.ir
2- PhD student in private law, Faculty of Law and Political Science, University of Tehran (corresponding author of the article) z.jalali@ut.ac.ir

دوفصلنامه
مطالعات فقه و حقوق رسانه
دانشکده غیردولتی – غیرانتفاعی رفاه

دوره ۷، شماره ۲(پیاپی ۱٤)
پاییز و زمستان ۱٤۰٤
صص: ۷-۳٤

الزامات حقوقی تمایز داده‌های عادی و حساس در سکوهای مجازی (مطالعه تطبیقی اتحادیه اروپا، آمریکا و ایران)

نوع مقاله: پژوهشی
تاریخ دریافت: ۱٤۰٤/۰٤/۱٦
تاریخ پذیرش: ۱٤۰٤/۱۰/۰٦

حسن محسنی[۱]
زهرا جلالی[۲]

چکیده

گسترش سکوهای مجازی به‌ویژه شبکه‌های اجتماعی مجازی و پردازش هوشمند داده‌ها، مرز میان داده‌های عادی و حساس را مبهم نموده است؛ به‌گونه‌ای‌که این شبکه‌ها با بهره‌گیری از الگوریتم‌های پیشرفته می‌توانند از داده‌های ظاهرا عادی، اطلاعاتی حساس درباره هویت، باورها و رفتار کاربران استخراج نمایند. پرسش اصلی آن است که در نظام‌های حقوقی مختلف چه معیارهایی برای تفکیک داده‌های عادی و حساس وجود دارد و این تمایز چه آثار حقوقی دارد؟ این پژوهش با روش توصیفی-تحلیلی و تطبیقی، معیارهای تفکیک این داده‌ها و آثار حقوقی آن را در سه نظام حقوقی اتحادیه اروپا، آمریکا و ایران بررسی می‌کند. یافته‌ها نشان می‌دهد اتحادیه اروپا با رویکرد فهرست‌محور در GDPR، داده‌های حساس ذاتی (مانند اطلاعات مذهبی یا سلامت) را مشمول حمایت‌های ویژه قرار داده؛ اما در قبال داده‌های استنباطی (مثل گرایش‌های سیاسی استخراج‌شده از لایک‌ها) خلأ قانونی دارد. درمقابل، آمریکا با قوانین پراکنده (مانند CCPA وHIPAA) رویکردی زمینه‌محور اتخاذ کرده که انعطاف‌پذیر اما فاقد انسجام است. نظام حقوقی ایران با فقدان قانون جامع، تعریف ناقص از داده‌های حساس در قانون تجارت الکترونیک، و نبود نهاد نظارتی، در حمایت از کاربران ناکارآمد عمل می‌کند. از منظر آثار حقوقی، پردازش داده‌های عادی عموماً با رضایت ضمنی مجاز است، درحالی‌که داده‌های حساس نیازمند رضایت صریح و تدابیر حمایتی سخت‌گیرانه‌تر (مانند رمزنگاری و حداقل‌سازی داده) هستند. در ایران با تدوین قانون جامع حمایت از داده ها، الزام سکوها به شفافیت پردازش داده‌ها و تأسیس نهاد نظارتی مستقل می‌توان چهارچوب حقوقی موثرتری برای حمایت از داده‌های کاربران فراهم نمود.

واژگان کلیدی:

شبکه‌های اجتماعی مجازی، داده‌های شخصی، داده‌های عادی، داده‌های حساس، مقررات عمومی حفاظت از داده‌ها(GDPR) .

---

۱. استاد گروه حقوق خصوصی، دانشکده حقوق و علوم سیاسی، تهران، دانشگاه تهران، ایران
hmohseny@ut.ac.ir
۲. دانشجوی دکتری حقوق خصوصی، دانشکده حقوق و علوم سیاسی، تهران، دانشگاه تهران، ایران (نویسنده مسئول)
z.jalali@ut.ac.ir

مقدمه

ظهور و گسترش شبکه‌های اجتماعی مجازی یکی از مهم‌ترین تحولات در عرصه فناوری اطلاعات و ارتباطات در دهه‌های اخیر بوده است؛ تحولاتی که نه‌فقط الگوهای ارتباط اجتماعی بلکه شیوه‌های تولید، ذخیره و پردازش داده‌های شخصی را نیز دگرگون کرده‌اند. این شبکه‌ها، دیگر تنها ابزارهایی برای تعامل و اشتراک‌گذاری محتوا نیستند بلکه به سکوهایی قدرتمند برای گردآوری و تحلیل عمیق داده‌های کاربران از طریق الگوریتم‌های پیچیده تبدیل شده‌اند. در این پژوهش، منظور از «سکوهای مجازی»، پلتفرم‌های دیجیتالی ارائه‌دهنده خدمات برخط هستند؛ ازجمله شبکه‌های اجتماعی مجازی که به‌عنوان مصداق اصلی این سکوها بررسی می‌شوند.

در چنین شرایطی، مفاهیمی همچون «داده‌های عادی» و «داده‌های حساس» دیگر مرزهای روشن و ثابتی ندارند. داده‌هایی که در نگاه اول بی‌اهمیت یا عمومی به‌نظر می‌رسند، ممکن است در بستر شبکه‌های اجتماعی مجازی و از طریق تحلیل‌های الگوریتمی، ابعاد حساسی از هویت، باورها یا وضعیت سلامت روانی کاربران را آشکار نمایند. قابلیت شبکه‌های اجتماعی به‌گونه‌ای است که به‌رغم تمهیدات فنی موجود، نه‌تنها امکان دستیابی اشخاص ثالث به اطلاعات خصوصی کاربران را فراهم نموده بلکه امکان قرار گرفتن اطلاعات شخصی آن‌ها در دست شرکت‌های تجاری بزرگ یا نهادهای حکومتی نیز وجود دارد و این امکان را برایشان فراهم می‌کند که از طریق رخنمای کاربران به بسیاری از اطلاعات حساس آن‌ها دسترسی پیدا کنند *(عبدی‌پور، ۱۳۹٤، ص.۱۱۱)*. افزون‌براین، در برخی شبکه‌های اجتماعی ازجمله فیسبوک، تنها از طریق اطلاعات مرتبط با لایک‌های ذخیره شده می‌توان داده‌های حساس افراد ازجمله جهت‌گیری‌های سیاسی، اخلاقی، جنسیتی و حتی ریشه‌های قومی و مذهبی کاربران را استخراج نمود (نخجوانی، ۱٤۰۰، ص.۵۰). بر اساس مطالعات انجام‌شده تنها با تحلیل لایک‌های فیسبوک، می‌توان ویژگی‌های شخصیتی کاربران را با دقتی تا ۸۸ درصد پیش‌بینی کرد *(Kosinski et al., 2013, p. 5803)*.

با وجود آنکه در ادبیات حقوقی، موضوع حمایت از داده‌های شخصی مورد توجه قرار

گرفته است؛ اما پژوهش‌ها کمتر به مسئله تمایز میان داده‌های عادی و حساس در بستر شبکه‌های اجتماعی مجازی پرداخته‌اند. نوآوری مقاله حاضر در آن است که با تمرکز بر این تمایز و با رویکردی تطبیقی، به بررسی دقیق نحوه مواجهه سه نظام حقوقی اتحادیه اروپا، ایالات متحده آمریکا و ایران با این چالش پرداخته و راهکارهایی کاربردی برای نظام حقوقی ایران ارائه می‌دهد.

پرسش اصلی آن است که نظام‌های حقوقی مختلف با چه معیارهایی داده‌های عادی و حساس را از یکدیگر تفکیک می‌کنند و این تفکیک چه آثار حقوقی برای کاربران دارد؟ براین‌اساس، مقاله ابتدا معیارهای شناسایی داده‌های عادی و حساس در شبکه‌های اجتماعی و چالش‌های ناشی از تغییر ماهیت داده‌ها را بررسی می‌کند، سپس جایگاه حقوقی ارائه‌دهندگان خدمات شبکه‌های اجتماعی را به‌عنوان کنترل‌کنندگان داده تحلیل کرده و در پایان آثار حقوقی این تمایز و راهکارهایی برای نظام حقوقی ایران پیشنهاد می‌کند.

۱. معیارهای شناسایی داده‌های عادی و حساس در شبکه‌های اجتماعی

در این قسمت ابتدا مرز مفهومی و حقوقی داده‌های شخصی اعم از عادی و حساس را بررسی نموده، سپس به نقش شبکه‌های اجتماعی و الگوریتم‌ها در تغییر ماهیت داده‌ها می‌پردازیم.

۱-۱. تفکیک مفهومی و حقوقی داده‌های عادی و حساس

بر اساس مقررات عمومی حمایت از داده‌های اتحادیه اروپا (GDPR)، «داده‌های شخصی عبارت است از هرگونه اطلاعات مربوط به یک شخص حقیقی با هویت مشخص و قابل شناسایی(شخص موضوع داده)؛ شخص حقیقی قابل شناسایی کسی است که مستقیم یا غیرمستقیم، به‌ویژه از طریق ارجاع به یک شناسه مانند نام، شماره شناسایی، داده‌های مکانی، یک شناسه برخط یا یک یا چند عامل خاص درباره هویت جسمی، روانی، ژنتیک، ذهنی، اقتصادی، فرهنگی یا اجتماعی آن شخص قابل شناسایی است» *(EUR-Lex, 2016/679)*.

داده‌های شخصی از نظر سطح اهمیت و خطراتی که پردازش آن‌ها می‌تواند متوجه

اشخاص موضوع داده شود، به داده عادی[1] و حساس[2] تقسیم می‌شوند *(انصاری، ۱٤۰۲، ص.٤۹)*. داده‌های حساس با آزادی‌های بنیادین و حقوق اساسی بشری مرتبط بوده و پردازش بی‌ضابطه آن‌ها ممکن است باعث نقض این حقوق و یا تبعیض ناروا میان افراد موضوع داده گردد *(احمدوند و جهانشاهی، ۱٤۰۲، ص.۱۱۰)*. ازهمین‌رو این داده‌ها نسبت به داده‌های شخصی عادی از حمایت‌های بیشتری برخوردار هستند و در قوانین حمایت از داده‌های کشورهای مختلف، ماده‌ای جداگانه به این دسته از داده‌ها می‌پردازد. همچنین در مورد برخی مصادیق داده‌های حساس در برخی کشورها، قوانین جداگانه‌ای نیز وضع شده است *(ترابی و شفیعی‌فر، ۱۳۹۸، ص.۱۵۵)*.

داده‌های حساس عموماً در قوانین به شکل مصداقی و برمبنای موضوع تعریف می‌شوند. معیارهای مختلف شخصی و نوعی هم برای تفکیک داده‌های حساس و غیرحساس در منابع علمی مطرح شده است. درمقابل برخی پیشنهاد کرده‌اند برای جلوگیری از تعریف گسترده داده‌های حساس تنها دو معیار موضوع داده‌ها و هدف آن‌ها برای شناخت حساسیت داده‌ها اعمال شود *(Quinn & Malgieri, 2020, p.8)*.

درحال‌حاضر در مورد نحوه تشخیص داده‌های شخصی حساس دو رویکرد عمده در میان دولت‌ها وجود دارد:

۱-۱-۱. رویکرد فهرست‌محور (ماهوی)

مطابق این دیدگاه، فهرست داده‌های شخصی حساس در قوانین مشخص شده و ضوابط سخت‌گیرانه‌ای برای پردازش آن‌ها مقرر شده است. این رویکرد که بیشتر در نظام‌های حقوقی اروپایی دیده می‌شود، مبتنی بر این فرض است که برخی داده‌ها به‌طور ذاتی ماهیتی حساس دارند و افشای آن‌ها می‌تواند منجر به آسیب جدی به حقوق شخص موضوع داده شود.

مفهوم داده‌های حساس اولین‌بار در کنوانسیون شماره ۱۰۸ شورای اروپا درباره

1. Non Sensitive personal data
2. Sensitive personal data

حفاظت از افراد در قبال پردازش خودکار داده‌های شخصی[۳] مطرح شد. ماده ٦ این سند، با استفاده از عنوان «دسته‌های خاص داده‌ها[٤]»، داده‌هایی مانند نژاد، عقاید سیاسی و مذهبی، سلامت و تمایلات جنسی را مشمول محدودیت‌های پردازش دانسته و تصریح کرده که پردازش آن‌ها تنها با رعایت تدابیر قانونی مناسب مجاز است. این رویکرد، زیربنای توسعه مفهوم «داده‌های حساس» در مقررات بعدی از جمله GDPR محسوب می‌شود. بااین‌حال، این کنوانسیون تعریفی جامع برای شناسایی داده‌های حساس ارائه نکرده و صرفاً کشورها را مکلف کرده است که در قوانین داخلی خود، تدابیر حفاظتی مناسب را برای پردازش این دسته از داده‌ها پیش‌بینی کنند *(Convention 108, 1981)*.

اکنون به موجب مقررات عمومی حمایت از داده‌های شخصی اتحادیه اروپا، داده‌های حساس به دو صورت پیش‌بینی شده‌اند: دسته اول داده‌هایی هستند که به‌دلیل ماهیت ویژه خود مستحق حمایت بیشتر هستند. طبق ماده ۹ مقررات عمومی حفاظت از داده‌های اتحادیه اروپا، این داده‌ها شامل اطلاعاتی چون نژاد، دیدگاه سیاسی، باورهای مذهبی یا فلسفی، عضویت در اتحادیه‌های صنفی و کارگری، اطلاعات زیستی یا ژنتیکی، وضعیت سلامت، و گرایش‌های جنسی فرد» است. دسته دوم داده‌هایی هستند که در فهرست مذکور نیستند؛ اما پردازش آن‌ها مستلزم رعایت احکام خاص است. این داده‌ها عبارت‌اند از: ۱) داده‌های مربوط به محکومیت و جرایم کیفری[٥]، ۲) داده‌های شخصی مربوط به کودکان[٦] *(انصاری، ۱٤۰۲، ص.٥۱)*.

در نظام حقوقی ایران نیز از رویکرد کشورهای اروپایی تقلید شده است. طبق ماده ٥۸ قانون تجارت الکترونیکی مصوب ۱۳۸۲ داده‌های حساس شامل «داده‌پیام‌های شخصی مبین ریشه‌های قومی یا نژادی، دیدگاه‌های عقیدتی، مذهبی، خصوصیات اخلاقی و

3. Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108), Strasbourg, 28 January 1981.

4.special categories of data

٥. ماده ۱۰ GDPR مقررات جداگانه‌ای برای پردازش داده‌های مربوط به محکومیت‌ها و جرائم کیفری مقرر داشته است.

٦. ماده ۸ GDPR برای پردازش داده‌های کودکان در بستر خدمات مستقیم، شرایط خاص رضایت والدین یا قیم قانونی را پیش‌بینی کرده است.

داده‌پیام‌های راجع به وضعیت جسمانی، روانی و یا جنسی اشخاص» است.

۱-۱-۲. رویکرد زمینه‌محور (نسبی)

در رویکرد زمینه‌محور، حساس‌بودن یک داده نه بر اساس ماهیت ذاتی آن بلکه باتوجه به شرایطی که در آن پردازش می‌شود، تعیین می‌گردد. در این رویکرد، اعتقاد برآن است که نمی‌توان فهرست حصری از داده‌های حساس ارائه داد بلکه این امر نسبی است و هر داده‌ای ممکن است در شرایط خاص، جنبه عادی یا حساس پیدا کند *(Quinn, 2020, p.9)*.

در آمریکا، فهرست یکسان و فراگیری برای داده‌های حساس وجود ندارد و اغلب بر اساس موضوعات خاص قانون‌گذاری، طبقه‌بندی انجام می‌شود؛ به‌عنوان‌نمونه، اطلاعات مرتبط با سلامت (HIPAA[7])، داده‌های مالی و اعتباری، داده‌های بیومتریک، اطلاعات مربوط به کودکان زیر ۱۳ سال (COPPA[8]) و سایر داده‌هایی که ممکن است در سرقت هویت یا کلاهبرداری مؤثر باشند، ازجمله اطلاعات حساس محسوب می‌شوند *(انصاری، ۱۴۰۲، صص.۴۹-۵۱)*.

این رویکرد، در مواجهه با پویایی داده‌ها واقع‌گرایانه‌تر به‌نظر می‌رسد؛ اما می‌تواند موجب بروز چالش‌هایی شود؛ ازجمله اینکه با گسترش بیش‌ازحد مصادیق داده‌های حساس، عملاً حساسیت موضوع کمرنگ شده و ضوابط سخت‌گیرانه برای پردازش آن‌ها اهمیت خود را از دست بدهد. ازهمین‌رو، برخی پیشنهاد کرده‌اند که معیار شناسایی داده‌های حساس، باید بر اساس دو عامل کلیدی «محیط یا بستر پردازش» و «اهداف پردازش داده» تعیین شود *(Quinn, 2020, pp.8-10)*.

۱-۲. تغییر ماهیت داده‌های شخصی در شبکه‌های اجتماعی مجازی

تحلیل داده‌های شخصی در بستر شبکه‌های اجتماعی مجازی نشان می‌دهد که تمایز سنتی میان داده‌های عادی و داده‌های حساس به‌طور جدی دچار تزلزل شده است. داده‌هایی که در ابتدا ماهیتی ساده یا غیرحساس دارند، در اثر پردازش‌های پیشرفته و

7. HIPAA: Health Insurance Portability and Accountability Act
8. COPPA: Children's Online Privacy Protection Act

تحلیل‌های الگوریتمی، می‌توانند به اطلاعاتی حساس تبدیل شوند و ابعاد ناشناخته‌ای از حریم خصوصی کاربران را افشا نمایند؛ به‌عنوان‌مثال در سال ۲۰۲۱، شبکه اجتماعی لینکدین[۹] با انتشار گسترده داده‌های کاربران خود مواجه شد، زمانی که مجموعه‌ای از اطلاعات مربوط به بیش از ۷۰۰ میلیون کاربر لینکدین، معادل حدود ٪۹۲ از کل کاربران این سکو در فضای برخط منتشر شد. این داده‌ها شامل اطلاعات شناسایی مانند نام و نام خانوادگی، آدرس پست الکترونیک، شماره تلفن، موقعیت جغرافیایی و سوابق شغلی بود که کاربران به‌صورت داوطلبانه در رخ‌نماهای عمومی خود قرار داده بودند. اطلاعاتی که در ظاهر عمومی و حرفه‌ای به‌نظر می‌رسیدند. بااین‌حال، تحلیل این داده‌ها نشان داد که با ترکیب و پردازش آن‌ها می‌توان الگوهای پنهانی همچون مسیرهای مهاجرت شغلی، جابه‌جایی‌های جغرافیایی و حتی گرایش‌های سیاسی افراد را استخراج کرد. این موضوع نشان می‌دهد که داده‌های به ظاهر عادی نیز در شرایط خاص می‌توانند به اطلاعاتی با ماهیت حساس تبدیل شوند. این داده‌ها ابتدا از طریق روش‌های خودکار جمع‌آوری شدند و سپس در تارنماهای مخصوص تبادل یا فروش داده منتشر شدند؛ محیط‌هایی که گاهی به آن‌ها «تالارهای برخط غیررسمی برای اشتراک‌گذاری داده» یا «انجمن‌های زیرزمینی اینترنت» گفته می‌شود. این فرایند جمع‌آوری و انتشار، اغلب توسط افرادی انجام می‌شود که اهداف سودجویانه یا خرابکارانه دارند *(Owaida, 2021; Paganini, 2021)*.

مورد دیگری که تغییر ماهیت داده را آشکار ساخت، مربوط به سکو «استراوا[۱۰]» در سال ۲۰۱۸ است. این سکو با انتشار یک نقشه حرارتی جهانی که حاصل تجمیع میلیون‌ها مسیر فعالیت ورزشی کاربران (مانند دویدن و دوچرخه‌سواری ثبت‌شده با دستگاه‌های پوشیدنی) بود، به‌صورت ناخواسته مکان، ساختار و الگوهای رفت‌وآمد پایگاه‌های نظامی ایالات متحده، بریتانیا و سایر کشورها را قابل شناسایی ساخت. این نقشه حرارتی نه‌تنها

۹. LinkedIn: یک شبکه اجتماعی تخصصی حرفه‌ای است که با تمرکز بر ارتباطات شغلی، اشتراک‌گذاری رزومه و تعاملات کسب‌وکاری عمل می‌کند.

۱۰. Strava: یک پلتفرم اجتماعی تخصصی ورزشی است که با ردیابی و اشتراک‌گذاری داده‌های فعالیت‌های بدنی (مانند دویدن و دوچرخه‌سواری)، امکان تعامل ورزشی بین کاربران را فراهم می‌کند.

مکان پایگاه‌ها بلکه مسیرهای تردد سربازان در اطراف پایگاه‌های نظامی در سوریه و افغانستان را نیز آشکار کرد. تحلیل این داده‌ها نشان داد که چگونه اطلاعات به‌ظاهر عادی و ساده می‌توانند درشرایطی خاص، به داده‌هایی حساس و راهبردی تبدیل شوند (Hern, 2018). نتایج یک پژوهش در فیسبوک نشان می‌دهد که لایک‌های کاربران در این شبکه می‌تواند نشانگر عقاید سیاسی، تمایلات جنسی، ریشه قومی، مذهب و ویژگی‌های شخصیتی افراد و حتی سطح ضریب هوشی آن‌ها باشد *(عطار، ۱۳۹۲، ص.٤٦)*.

این نمونه‌ها به‌روشنی بیانگر این واقعیت است که در بستر شبکه‌های اجتماعی و پردازش هوشمند داده‌ها، ماهیت داده‌های شخصی قابلیت تغییر دارد و هرگونه طبقه‌بندی سنتی میان داده‌های عادی و حساس باید با احتیاط و بازنگری همراه باشد. در این فضا، اهمیت تحلیل زمینه پردازش داده‌ها، هدف نهایی پردازش و ابزارهای فنی مورد استفاده بیش‌ازپیش آشکار شده و مسئولیت حقوقی شبکه‌های اجتماعی در قبال پردازش داده‌های کاربران را سنگین‌تر کرده است.

۱-۳. نقش الگوریتم‌ها[11] در استخراج داده‌های حساس

الگوریتم ها، ساختارهایی هستند که برای حل مشکلات یا تکمیل برخی کارها استفاده می‌شوند. الگوریتم‌ها با دریافت داده‌های خام، آن‌ها را مرحله‌به‌مرحله براساس چهارچوب‌های طراحی شده خاص، پردازش کرده و نتیجه را ارائه می‌دهند *(Bucher, 2018, pp.20-21)*. در شبکه‌های اجتماعی مجازی، الگوریتم‌ها به‌عنوان مجموعه‌ای از دستورالعمل‌های منطقی تعریف می‌شوند که با پردازش ورودی‌های مختلف، الگوهای رفتاری کاربران را شناسایی کرده و محتواهای سفارشی‌شده را بر اساس آن پیش‌بینی می‌کند. در این شبکه‌ها کاربران با نحوه فعالیت خود همچون جستجوی واژه‌های مختلف، تعیین اولویت‌ها و علایق، محتوای محبوب و مناسب خود را مشخص می‌کنند. سپس الگوریتم مطالب و اطلاعات مورد پسند کاربر را به وی پیشنهاد می‌دهند؛ به‌عنوان‌مثال الگوریتم اینستاگرام با کسب اطلاعات از نحوه فعالیت کاربر، پست‌ها و استوری‌های

11. Algorithm

مورد علاقه هرشخص را در ابتدا به او نشان می‌دهد. الگوریتم‌ها همواره درحال یادگیری بوده و با استفاده از اطلاعات جدید، توسعه و بهبود پیدا می‌کنند. به‌عبارت‌دیگر آنان طی فرایند خود ایستا و ثابت نیستند بلکه براساس فعالیت کاربران بهبود پیدا می‌کنند (*Hunt & McKelvey, 2019, pp.309-310*).

یکی از مهم‌ترین کارکردهای الگوریتم‌ها، استخراج اطلاعات حساس از داده‌های ظاهرا ساده است. بر اساس نتایج یک پژوهش تجربی، تنها بر مبنای داده‌هایی مانند پسندیدن مطالب (لایک) در شبکه اجتماعی فیس‌بوک، می‌توان ویژگی‌های شخصیتی، باورهای مذهبی، دیدگاه‌های سیاسی و حتی گرایش‌های جنسی کاربران را با دقت بالایی پیش‌بینی کرد (*Kosinski et al., 2013, p.5802*). این پژوهش نشان می‌دهد که الگوریتم‌های تحلیل رفتاری می‌توانند بدون دریافت مستقیم اطلاعات از کاربر، ابعاد عمیق شخصیت او را شناسایی کنند.

در بسیاری از شبکه‌های اجتماعی مجازی، پردازش داده‌های کاربران توسط الگوریتم‌هایی انجام می‌شود که روند داخلی عملکرد آن‌ها برای کاربران و نهادهای نظارتی قابل مشاهده و تحلیل نیست. این نوع الگوریتم‌ها، که به «الگوریتم‌های جعبه سیاه[۱۲]» معروف هستند، تنها ورودی‌ها و خروجی‌های مشخصی دارند و نحوه تبدیل داده‌های خام به نتایج نهایی در آن‌ها مبهم و غیرشفاف باقی می‌ماند (*Pasquale, 2015, p.9*). این عدم شفافیت می‌تواند به نقض حقوق کاربران در آگاهی از نحوه پردازش داده‌های شخصی خود منجر شود و کارایی اصولی چون رضایت آگاهانه و مسئولیت‌پذیری کنترل‌کنندگان داده را زیر سؤال ببرد. درنتیجه، وجود الگوریتم‌های جعبه سیاه در بسترهای اجتماعی، ضرورت وضع مقررات سختگیرانه‌تر در حوزه شفافیت و نظارت بر پردازش داده‌های شخصی را بیش‌ازپیش آشکار می‌سازد.

درمجموع، الگوریتم‌ها با استخراج اطلاعات حساس از داده‌های ظاهراً عادی، نقش مهمی در تضعیف مرز میان داده‌های عادی و حساس دارند. این واقعیت، لزوم بازنگری در اصول قانونی مربوط به شفافیت پردازش داده‌ها و توسعه الزام‌های پاسخگویی برای سکوهای اجتماعی را بیش‌ازپیش برجسته ساخته است.

12. Black Box Algorithms

۲. چالش‌های تمایز داده‌های عادی و حساس در نظام‌های حقوقی مختلف

نظام‌های حقوقی مختلف، در مواجهه با مسئله تمایز میان داده‌های عادی و حساس در بسترهای دیجیتال، به‌ویژه شبکه‌های اجتماعی، رویکردهای گوناگونی اتخاذ کرده‌اند. این تفاوت‌ها ناشی از تفاوت‌های ساختاری، فرهنگی، حقوقی و سیاست‌گذاری در هر نظام است.

در اتحادیه اروپا، مقررات عمومی حفاظت از داده‌های شخصی (GDPR) با اتخاذ رویکرد فهرست‌محور، تعریف نسبتاً دقیقی از داده‌های حساس ارائه داده و بر اساس ماده ۹[۱۳]، آن‌ها را مشمول محدودیت‌های سخت‌گیرانه در پردازش قرار داده است. این رویکرد فهرست‌محور در تعیین داده‌های حساس، اگرچه موجب شفافیت و قابلیت پیش‌بینی برای افراد و مسئولان پردازش داده می‌شود؛ اما در شبکه‌های اجتماعی مجازی که داده‌ها پیوسته در حال تولید، ترکیب و تحلیل الگوریتمی هستند، با چالش‌هایی مواجه شده است؛ برای‌مثال، داده‌هایی که در نگاه اول عادی تلقی می‌شوند، مانند الگوهای تعامل کاربران، لایک‌ها یا جست‌وجوهای معمول، ممکن است در ترکیب با دیگر اطلاعات، به داده‌های حساس (نظیر گرایش سیاسی یا وضعیت سلامت روان) تبدیل شوند، بدون آنکه مشمول حمایت‌های صریح این مقررات باشند؛ برای‌مثال، رسوایی کمبریج آنالیتیکا (۲۰۱۸) نشان داد داده‌هایی چون لایک‌ها که ظاهراً عادی بودند، از طریق تحلیل الگوریتمی به داده‌های حساسی چون گرایش‌های سیاسی تبدیل شدند، بی‌آنکه تحت حمایت صریح ماده ۹ GDPR باشند *(Geary et al., 2018, p.3)*.

هرچند ماده ۲۲ GDPR محدودیت‌هایی برای تصمیم‌گیری‌های خودکار و پروفایلینگ تعیین کرده است. این ماده بیشتر بر پیامدهای تصمیم‌گیری‌های خودکار تمرکز دارد و به فرایند استنباط داده‌های حساس از داده‌های عادی توجه کافی نکرده است. تحلیل‌های الگوریتمی پیشرفته می‌توانند داده‌های عادی را به داده‌های حساس تبدیل کنند؛ اما GDPR حمایت‌های صریحی برای این داده‌های استنباطی ارائه نمی‌دهد *(Wachter & Mittelstadt,*

13. Article9(1): "Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited."

(*2019, pp.12, 71-73*). این نقص، به‌ویژه در شبکه‌های اجتماعی با الگوریتم‌های جعبه سیاه، اعتماد کاربران را کاهش داده و نهادهای نظارتی را با موانع عملی در اثبات نقض حریم خصوصی مواجه کرده است.

هیئت حفاظت از داده‌های اروپا (EDPB[14]) برای رفع این کاستی‌ها اقداماتی انجام داده است. یکی از اقدامات کلیدی، انتشار «راهنمای پروفایلینگ و تصمیم‌گیری‌های خودکار[۱۵]» در سال ۲۰۱۸ است که توسط گروه کاری ماده ۲۹ تدوین و توسط این هیئت تأیید شد. این راهنما توصیه می‌کند که کنترل‌کنندگان داده هنگام پروفایلینگ، «ارزیابی تأثیر حفاظت از داده[۱۶]» را انجام دهند تا ریسک‌های حریم خصوصی را شناسایی کنند و شفافیت بیشتری در مورد الگوریتم‌ها ارائه دهند (*Article 29 Data Protection Working Party, 2018:. 29-31*). برای‌مثال، سکوهایی مانند اینستاگرام باید به کاربران اطلاع دهند که داده‌هایی مانند تاریخچه جست‌وجو یا لایک‌ها چگونه برای پیشنهاد تبلیغات استفاده می‌شوند و امکان غیرفعال کردن این پردازش را فراهم کنند. بااین‌حال، این راهنما الزام‌آور نیست و نیاز به دستورالعمل‌های دقیق‌تر همچنان باقی است.

در ایالات متحده آمریکا همان‌طور که قبلاً ذکر شد، تمایز میان داده‌های عادی و حساس بر اساس قوانین بخشی و ایالتی تنظیم شده است. این چهارچوب، در شبکه‌های اجتماعی مزایایی دارد؛ اما با خلأهای قابل‌توجهی نیز همراه است.

یکی از مزایای این نظام، توانایی آن در پاسخ‌گویی به نیازهای خاص حوزه‌های مختلف است. به‌عبارت‌دیگر این رویکرد زمینه‌محور انعطاف‌پذیری بیشتری در شناسایی داده‌های حساس فراهم می‌آورد؛ چراکه نوع داده و زمینه کاربرد آن در کنار هم بررسی می‌شوند؛ برای‌مثال، قانون حفاظت از حریم خصوصی مصرف‌کنندگان کالیفرنیا به کاربران امکان می‌دهد از پردازش داده‌هایشان برای تبلیغات هدفمند انصراف دهند که این امر به حفاظت از حریم خصوصی در برابر پیامدهای تصمیم‌گیری‌های خودکار کمک می‌کند (*CCPA, 2018*).

---

14. European Data Protection Board

۱۵. تصمیمات خودکار، تصمیماتی هستند که با به‌کارگیری داده های شخصی پردازش شده به‌وسیله ابزار خودکاربدون هیچ‌گونه دخالت انسانی گرفته می‌شوند (انصاری، ۱۴۰۲، ص۱۹۴).

16. DPIA: Data Protection Impact Assessment

همچنین قانون حمایت از حریم خصوصی کودکان برخط با محدود کردن جمع‌آوری داده‌های کودکان در شبکه‌های اجتماعی، مانند یوتیوب، حمایت ویژه‌ای از گروه‌های آسیب‌پذیر فراهم می‌آورد. این قوانین به سکوها اجازه می‌دهند با توجه به نوع داده‌ها و کاربران، رویکردهای متفاوتی اتخاذ کنند.

بااین‌حال، پراکندگی این قوانین خلأهای حمایتی جدی در شبکه‌های اجتماعی ایجاد کرده است. فقدان چهارچوب یکپارچه، سطح حمایت از داده‌های کاربران را دشوار و غیرقابل پیش‌بینی می‌سازد، به‌ویژه در شرایطی که مرز میان داده‌های عادی و حساس سیال است. قوانین موجود این نظام نیز همچون GDPR به فرایند استنباط داده‌های حساس از داده‌های عادی توجه ندارند.

نظام حقوقی ایران در تمایز داده‌های عادی و حساس در شبکه‌های اجتماعی با چالش‌های اساسی مواجه است. ماده ۵۸ قانون تجارت الکترونیکی (مصوب ۱۳۸۲) به‌طور غیرمستقیم به داده‌های حساس اشاره کرده و پردازش بدون رضایت صریح را ممنوع می‌داند؛ اما فقدان تعریف صریح و ضمانت‌اجراهای قوی، آن را ناکارآمد کرده است. در پیش‌نویس لایحه «صیانت و حفاظت از داده‌های شخصی»[17] (۱۳۹۷)، داده‌هایی مانند ریشه قومی یا قبیله‌ای، عقاید سیاسی، مذهبی و فلسفی، ویژگی‌های وراثتی یا اطلاعات سلامت، به‌صراحت در زمره داده‌های حساس تعریف شده‌اند؛ اما علاوه بر عدم بیان همه مصادیق، جزئیات و الزامات مشخصی برای نحوه پردازش این نوع داده‌ها در آن پیش‌بینی نشده است. در طرح«حمایت و حفاظت از داده و اطلاعات شخصی» (۱۴۰۰) نیز، تعریفی از داده شخصی حساس و احکام و شرایط پردازش آن بیان نشده است؛ اما طرح «حفاظت از داده‌های شخصی»[18](۱۴۰۳) به‌جای اصطلاح داده‌های حساس، مفهومی به نام «داده شخصی حیاتی» را در ماده ۱ مطرح کرده که ناظر به «داده‌های مربوط به سلامت جسمانی یا روانی و همچنین داده‌هایی است که در صورت افشا یا دستکاری می‌توانند حیات یا ایمنی فرد را به‌خطر اندازند». این مفهوم با داده‌های حساس در استانداردهای بین‌المللی تفاوت دارد و دامنه ای خاص تر و محدودتر را پوشش می‌دهد. طرح‌های اخیر

17. https://www.ict.gov.ir/fa/newsagency/21691
18. https://rc.majlis.ir/fa/legal_draft/show/1816729

هرچند گامی به جلو محسوب می‌شوند؛ اما هنوز به تصویب نهایی نرسیده‌اند و درحال‌حاضر تنها ماده ۵۸ قانون تجارت الکترونیک، مبنای قانونی موجود برای حمایت از داده‌های حساس در ایران به‌شمار می‌رود. بدین‌ترتیب فقدان قانونی جامع باعث شده تنظیم پیامدهای تصمیم‌گیری‌های خودکار در شبکه‌های اجتماعی عملاً غیرممکن باشد. همچنین فقدان الزام به ارزیابی تأثیر حفاظت از داده و نبود نهادهای نظارتی مستقل، سکوها را از مسئولیت‌پذیری معاف کرده و حریم خصوصی کاربران را در معرض خطر قرار داده است. درنتیجه، نظام حقوقی ایران در مدیریت تمایز داده‌های عادی و حساس در شبکه‌های اجتماعی با کاستی‌های اساسی روبه‌روست.

درمجموع، می‌توان گفت که هر سه نظام حقوقی در مواجهه با پویایی داده‌ها در شبکه‌های اجتماعی مجازی با چالش‌هایی جدی روبه‌رو هستند. این وضعیت، به‌ویژه در شرایطی که داده‌های ساده و به‌ظاهر عادی می‌توانند در شبکه‌های اجتماعی مجازی به داده‌های حساس تبدیل شوند، حاکی از آن است که تأکید صرف بر فهرست‌های ثابت یا قوانین پراکنده، دیگر پاسخگوی واقعیت‌های نوین فضای مجازی نیست.

این چالش‌ها با نظریه «تمامیت زمینه‌ای[۱۹]» که توسط هلن نیسنبام[۲۰] در سال ۲۰۱۰ مطرح شده، به‌خوبی قابل تبیین است. بر اساس این نظریه، حریم خصوصی نه صرفاً به‌معنای محرمانه بودن اطلاعات بلکه به‌معنای جریان مناسب اطلاعات در یک زمینه اجتماعی خاص تعریف می‌شود. حساسیت داده‌ها تابعی از زمینه‌ای است که در آن داده‌ها جمع‌آوری، پردازش و مبادله می‌شوند. اگر یک داده در همان زمینه‌ای استفاده شود که کاربر انتظارش را دارد، حریم خصوصی او نقض نمی‌شود؛ اما اگر همان داده در زمینه‌ای متفاوت و بدون اطلاع یا رضایت او به‌کار رود، حتی در صورت عادی بودن داده، این عمل می‌تواند به نقض حریم خصوصی بینجامد *(Nissenbaum, 2010: 149)*.

طبق این دیدگاه، حفاظت از داده‌ها نباید فقط بر پایه نوع یا ماهیت داده‌ها انجام گیرد بلکه باید با توجه به قواعد اجتماعی، نقش‌ها، انتظارات کاربران و هدفی که داده‌ها در هر موقعیت مشخص برای آن تبادل می‌شوند، ارزیابی شود. در این چهارچوب، می‌توان دریافت که

19. Contextual Integrity
20. Helen Nissenbaum

رویکرد نظام حقوقی ایالات متحده، علی‌رغم نزدیکی ظاهری به دیدگاه زمینه‌محور، با نظریه نیسنبام تفاوت‌هایی اساسی دارد. در آمریکا داده‌های شخصی به‌صورت موضوعی و موردی و بر اساس ملاحظات سیاست‌گذاری خاص تنظیم می‌شوند. این در حالی است که نظریه تمامیت زمینه‌ای بر این تأکید دارد که جریان اطلاعات باید بر اساس قواعد اجتماعی حاکم در هر زمینه و مطابق با انتظارات منطقی کاربران در آن بستر صورت گیرد؛ بنابراین اگرچه برخی اصول رویکرد آمریکا با نظریه‌ی نیسنبام هم‌راستاست؛ اما این نظام حقوقی با پراکندگی قوانین، عدم توجه به زمینه‌های فرهنگی- اجتماعی کاربران، و فقدان سازوکارهایی برای بررسی انتظارات زمینه‌ای، هنوز با نظریه تمامیت زمینه‌ای فاصله دارد.

۳. جایگاه حقوقی ارائه‌دهندگان خدمات شبکه‌های اجتماعی مجازی در نظام‌های حقوقی مختلف

با توجه به گسترش روزافزون کارکردهای شبکه‌های اجتماعی مجازی و تأثیر مستقیم آن‌ها بر داده‌های شخصی کاربران، شناسایی جایگاه حقوقی ارائه‌دهندگان خدمات این شبکه‌ها در نظام‌های حقوقی مختلف اهمیت ویژه‌ای یافته است. در این زمینه، سه رویکرد عمده در اتحادیه اروپا، ایالات متحده آمریکا و نظام حقوقی ایران قابل شناسایی است.

۳-۱. اتحادیه اروپا

مقررات عمومی حفاظت از داده‌های شخصی اتحادیه اروپا(GDPR[21]) که در سال ۲۰۱۶ تصویب و از سال ۲۰۱۸ لازم‌الاجرا شده است، چهارچوب جامعی برای تنظیم نحوه پردازش داده‌های شخصی ارائه می‌دهد. طبق ماده ٤ بند ۷ این مقررات، کنترل‌کننده داده[۲۲] «هر شخص حقیقی یا حقوقی است که به‌طور مستقل یا همراه با دیگران، اهداف و شیوه‌های پردازش داده‌های شخصی را تعیین می‌کند» *(EUR-Lex, 2016/679)*.

بر اساس راهنمای هیئت اروپایی حفاظت از داده‌ها(EDPB)، شبکه‌های اجتماعی به‌دلیل نقشی که در تعیین اهداف و شیوه‌های پردازش داده‌های شخصی ایفا می‌کنند، ازجمله در

21. General Data Protection Regulation
22. Data Controllers

مدیریت صفحات یا به‌کارگیری پلاگین‌های اجتماعی[۲۳]، به‌عنوان کنترل‌کننده داده یا حتی در مواردی کنترل‌کننده مشترک[۲۴] شناخته می‌شوند *(EDPB, 2020, p. 19)*. همچنین طبق راهنمای دیگری از همین نهاد، ارائه‌دهندگان خدمات شبکه‌های اجتماعی در پردازش داده‌های کاربران برای تبلیغات هدفمند نیز در جایگاه کنترل‌کننده داده قرار می‌گیرند؛ زیرا این سکوها اهداف و روش‌های پردازش داده‌های شخصی را تعیین می‌کنند که این جایگاه می‌تواند به‌صورت کنترل‌کنندگی مشترک نیز تعریف شود *(EDPB, 2021, p. 11)*.

براین‌اساس، شرکت‌های مالک و متصدی ارائه‌دهنده خدمات شبکه‌های اجتماعی مانند متا[۲۵] که درباره جمع‌آوری، ذخیره‌سازی، تحلیل و اشتراک‌گذاری داده‌های کاربران تصمیم‌گیری می‌کنند، مصداق بارز «کنترل‌کننده داده» محسوب می‌شوند. این جایگاه حقوقی، مسئولیت‌های سنگینی برای متصدیان این شبکه‌ها قرار می‌دهد. چراکه طبق ماده ٦ GDPR که الزامات کلی برای هر کنترل‌کننده داده مقرر می‌کند، آن‌ها ملزم به اخذ رضایت آگاهانه از کاربران پیش از هرگونه پردازش داده‌های شخصی هستند.

علاوه‌براین، ارائه‌دهندگان خدمات شبکه‌های اجتماعی ملزم به رعایت اصل حداقل‌سازی داده هستند؛ بدین‌معنا که تنها باید داده‌هایی را جمع‌آوری کنند که برای هدف اعلام‌شده ضرورت دارند. همچنین، آن‌ها موظف‌اند اطلاعات شفاف و دقیقی درباره اهداف پردازش داده‌ها در اختیار کاربران قرار دهند و زمینه اجرای حقوق کاربران نظیر حق دسترسی به داده‌ها، حق اصلاح اطلاعات، محدودسازی پردازش و حق حذف داده‌های شخصی را فراهم آورند *(EUR-Lex, 2016/679)*. با توجه به اینکه طبق ماده ٤ GDPR، شبکه‌های اجتماعی در جایگاه کنترل‌کننده داده قرار می‌گیرند، درنتیجه در صورت تخلف از الزامات این قانون مشمول جریمه‌های مقرر در ماده ۸۳ خواهند بود.

---

۲۳. ابزارهای تعاملی مانند دکمه‌های «لایک» یا «اشتراک‌گذاری» که داده‌های کاربران را برای تحلیل یا تبلیغات جمع‌آوری می‌کنند.

۲٤ . کنترل‌کننده مشترک (Joint Controller) «به‌معنای دو یا چند شخص حقیقی یا حقوقی است که به‌طور مشترک اهداف و شیوه‌های پردازش داده‌های شخصی را تعیین می‌کنند (EUR-Lex, 2016/679) .

25. Meta

۳-۲. ایالات متحده آمریکا

برخلاف اتحادیه اروپا که با مقررات عمومی حفاظت از داده‌ها رویکردی یکپارچه نسبت به پردازش داده‌های شخصی اتخاذ کرده است، در نظام حقوقی آمریکا هنوز حمایت عام و جامعی از داده‌های شخصی وجود ندارد. به‌عبارت‌دیگر باتوجه به رویکرد اقتصاد محور به داده‌ها، به‌جای «اشخاص موضوع داده» از اصطلاح «مصرف‌کننده» استفاده می‌شود و به‌صورت بخشی و موضوعی از کنترل مشتریان یا مصرف‌کنندگان بر اطلاعاتشان حمایت می‌شود *(انصاری و دیگران، ۱۴۰۱، ص.۲۷۹)*.

در این میان، قانون حفاظت از حریم خصوصی مصرف‌کنندگان کالیفرنیا (CCPA[26]) که در سال ۲۰۱۸ تصویب شد، یکی از برجسته‌ترین نمونه‌هاست. بر اساس این قانون، شرکت‌هایی که داده‌های شخصی ساکنان کالیفرنیا را جمع‌آوری می‌کنند، مکلف‌اند کاربران را درباره نوع داده‌های جمع‌آوری‌شده، اهداف پردازش، و حقوقی چون دسترسی، حذف و ممنوعیت فروش داده‌ها مطلع سازند (*CCPA, 2018*). طبق این مقررات، شبکه‌های اجتماعی در جایگاه «کسب‌وکارهای پردازشگر داده‌های شخصی برای اهداف تجاری» تعریف می‌شوند و موظف به ایجاد امکان کنترل داده‌ها برای کاربران خود هستند.

علاوه بر این قانون، قوانین فدرال ویژه‌ای نظیر قانون حفاظت از حریم خصوصی کودکان برخط (COPPA[27]) نیز بر بخشی از فعالیت‌های شبکه‌های اجتماعی نظارت دارند؛ به‌نحوی‌که این سکوها موظف‌اند پیش از جمع‌آوری اطلاعات کاربران زیر ۱۳ سال، رضایت والدین را کسب کنند *(COPPA, 1998)*. در حوزه سلامت نیز قانون قابلیت انتقال و مسئولیت‌پذیری بیمه سلامت (HIPAA[28]) محدودیت‌های سختگیرانه‌ای را بر پردازش داده‌های پزشکی کاربران اعمال می‌کند *(HIPAA, 1996/164.508)*.

به‌طورکلی در نظام حقوقی ایالات متحده آمریکا برخلاف مقررات اتحادیه اروپا که به‌صراحت میان «کنترل‌کننده داده» و «پردازشگر داده» تمایز قائل شده است، چنین تفکیک مفهومی روشنی وجود ندارد. در ایالات متحده، مسئولیت بازیگران این عرصه عمدتاً در

26. California Consumer Privacy Act
27. Children's Online Privacy Protection Act
28. Health Insurance Portability and Accountability Act

قالب مقررات حوزه‌ای و ایالتی تعیین می‌شود؛ به‌عنوان‌مثال، قانون حفاظت از حریم خصوصی مصرف‌کنندگان کالیفرنیا (CCPA/CPRA) کسب‌وکارهایی[۲۹] را که در جمع‌آوری داده‌های شخصی مصرف‌کنندگان، تعیین اهداف پردازش آن‌ها و انجام فعالیت‌های تجاری مبتنی بر این داده‌ها مشارکت دارد، مشمول مقررات خود دانسته است *(CCPA, 2018)*. در عمل، ارائه‌دهندگان خدمات شبکه‌های اجتماعی که به‌عنوان شرکت‌های انتفاعی داده‌های کاربران خود را جمع‌آوری و تحلیل می‌کنند، مصداق بارز چنین کسب‌وکارهایی به‌شمار می‌آیند. این وضعیت از جهت نقش و مسئولیت‌های تعیین‌کننده اهداف و شیوه‌های پردازش داده‌ها، مشابه جایگاه کنترل‌کننده داده در مقررات اتحادیه اروپا است *(EUR-Lex, 2016/679)*. بااین‌حال، در قوانین ایالات متحده به‌ویژه CCPA، از اصطلاح کنترل‌کننده داده استفاده نشده و به‌جای آن بر تکالیفی چون اطلاع‌رسانی به مصرف‌کنندگان، اعطای حق دسترسی، اصلاح و حذف داده‌ها و نیز حق مخالفت با فروش اطلاعات تأکید شده است *(CCPA, 2018)*. این تفاوت رویکرد، بیانگر ماهیت غیرمتمرکز و موضوع‌محور نظام حفاظت از داده در ایالات متحده در مقایسه با مدل منسجم اتحادیه اروپا است.

۳-۳. نظام حقوقی ایران

در نظام حقوقی جمهوری اسلامی ایران، هنوز تعریف جامع و روشنی از جایگاه ارائه‌دهندگان خدمات شبکه‌های اجتماعی مجازی به‌عنوان کنترل‌کننده یا پردازشگر داده‌های شخصی مطرح نشده است. اگرچه برخی اسناد قانونی به‌طور ضمنی به نقش این سکوها در تعامل با داده‌های کاربران پرداخته‌اند؛ اما چهارچوب منسجمی که بتواند جایگاه حقوقی آن‌ها را به‌صراحت تعیین کند، وجود ندارد.

قانون جرائم رایانه‌ای مصوب ۱۳۸۸ یکی از نخستین اسناد قانونی است که به مسئله حفاظت از داده‌های کاربران در فضای مجازی پرداخته است. در این قانون، جرائمی مانند دسترسی غیرمجاز به داده‌های رایانه‌ای، افشای اسرار خصوصی و تخریب داده‌ها جرم‌انگاری شده؛ اما جایگاه حقوقی نهادهای پردازشگر مانند شبکه‌های اجتماعی

29. Business

مشخص نشده است. به‌عبارت‌دیگر، قانون به حمایت از داده‌ها پرداخته ولی نسبت به تعریف مسئولیت حقوقی پردازشگرهای داده ساکت است.

در حوزه سیاست‌گذاری، شورای عالی فضای مجازی در مصوبه «سیاست‌ها و اقدامات ساماندهی پیام‌رسان‌های اجتماعی» مصوب ۱۳۹۶، پیام‌رسان‌های اجتماعی را سامانه‌های کاربرمحوری معرفی کرده که باید در چهارچوب مقررات ملی فعالیت کنند. این مصوبه، ضمن تأکید بر لزوم ثبت و میزبانی داده‌ها در داخل کشور، بر مسئولیت پیام‌رسان‌ها در قبال حفاظت از اطلاعات کاربران نیز اشاره دارد. بااین‌حال، ماهیت توصیه‌ای این مصوبه و نبود ضمانت اجرای صریح، موجب شده است که تأثیر آن در ایجاد یک چهارچوب حقوقی الزام‌آور محدود باشد.

بااین‌حال، پیش‌نویس لایحه «صیانت و حفاظت از داده‌های شخصی» مورخ ۱۳۹۷ و همچنین طرح «حمایت و حفاظت از داده و اطلاعات شخصی»[۳۰] و «حفاظت از داده‌های شخصی» مورخ ۱۴۰۳، نقطه‌عطفی در تحول نگرش حقوقی به مسئله پردازش داده در ایران به‌شمار می‌رود. در این متون، برای نخستین‌بار مفاهیمی نظیر «کنترل‌کننده داده» و «پردازشگر داده» معرفی شده‌اند و برای آن‌ها تعاریف حقوقی نسبتاً دقیقی ارائه گردیده است.

مطابق این اسناد، «کنترل‌کننده داده» نهادی است که به‌طور مستقل درباره اهداف و روش‌های پردازش داده‌های شخصی تصمیم‌گیری می‌کند. در این چهارچوب، شبکه‌های اجتماعی مجازی که داده‌های کاربران خود را جمع‌آوری، تحلیل و برای مقاصد اقتصادی یا ارتباطی خاصی پردازش می‌کنند، به‌طور طبیعی در جایگاه کنترل‌کننده داده قرار می‌گیرند. از سوی‌دیگر، اگر شبکه اجتماعی صرفاً به دستور یک نهاد ثالث داده‌های کاربران را پردازش کند، بدون اینکه درباره هدف یا شیوه پردازش تصمیم بگیرد، می‌توان آن را در مقام «پردازشگر داده» تلقی کرد.

با این‌وصف، نظام حقوقی ایران درحال‌گذار از وضعیت بی‌تعریفی به سمت پذیرش و انطباق با مفاهیم پذیرفته‌شده بین‌المللی در حوزه حفاظت از داده‌های شخصی است. بااین‌حال، تصویب نهایی این طرح‌ها، تدوین مقررات اجرایی دقیق و پیش‌بینی ضمانت

30. https://rc.majlis.ir/fa/legal_draft/show/1675111

اجراهای مؤثر، برای تثبیت جایگاه حقوقی شـــبکه‌های اجتماعی و تحقق عملی حمایت از حریم خصوصی کاربران ضروری به نظر می‌رسد.

۴. ضـوابط حقوقی حاکم بر رضـایت و تدابیر حفاظتی در پردازش داده‌های عادی و حساس

طبق بند ۵۱ مقررات عمومی اتحادیه اروپا، سـطح بالایی از حمایت برای داده‌های حسـاس ضـــروری قلمداد می‌شـــود؛ زیرا این داده‌ها از نظر ماهیت، حســـاســـیت ویژه‌ای دارند و پردازش آن‌ها می‌تواند خطرهای قابل‌توجهی برای حقوق و آزادی‌های اشـــخاص ایجاد کند. علاوه براین مقررات، کنوانسیون شماره ۱۰۸ شورای اروپا نیز حمایت‌های اضافی از داده‌های حســاس را پذیرفته و کشــورهای عضــو با تصــویب مقررات مشــابه در قوانین خود،از آن تأثیر پذیرفته‌اند (Kuner et al., 2020, pp.369-370). در این قســـمت، به بررســـی تطبیقی ضــوابط حقوقی حاکم بر رضــایت و تدابیر حفاظتی در پردازش داده‌های عادی و حساس می‌پردازیم.

۴-۱. تعیین سطح رضایت لازم برای پردازش داده‌ها

یکی از آثار حقوقی مهم تمایز میان داده‌های عادی و حســاس، تفاوت در میزان رضــایت مورد نیاز برای پردازش آن هاســت. داده‌های عادی در بســیاری از نظام‌های حقوقی با رضـایتی کلی، ضـمنی یا حتی در برخی موارد بدون رضـایت صـریح قابل پردازش هستند، درحالی‌که پردازش داده‌های حسـاس تنها با رضـایت صـریح و آگاهانه امکان‌پذیر اسـت، مگر در شرایط استثنایی که قانون گذار به طور خاص مجاز دانسته است.

در نظام حقوقی اتحادیه اروپا، ماده ٦ GDPR مبانی عمومی پردازش داده‌های شـخصـی را بیان می‌کند؛ البته برای پردازش داده‌های حســـاس طبق مقررات GDPR بایســـتی هم مبانی قانونی مذکور در ماده ٦ این مقررات رعایت شـود و هم شـرایط جداگانه‌ای که در ماده ۹ مقرر شده است. طبق این ماده، برای پردازش این دسته از داده‌ها، بایستی رضایت صـریح و بدون ابهام داده شـود و نمی‌تواند در چهارچوب همان رضـایت کلی برای سـایر

داده‌ها ادغام شـــود[۳۱] *(EUR-Lex, 2016/679)*. به‌عنوان‌مثال فیســـبوک به‌صـــورت تجاری از داده‌های شـخصـی حسـاس باتوجه به علاقه کاربران برای اهداف تبلیغاتی استفاده می‌کند؛ اما باتوجه به لازم‌الاجرا شدن GDPR که پردازش داده‌های شـخصـی ممنوع شده است، این بستر مجازی بایستی نسبت به کاربران اتحادیه اروپا، الزامات مذکور در GDPR را رعایت نماید *(Cabañas et al., 2018, p.14)*.

در نظام حقوقی ایالات متحده آمریکا، الزامات رضـــایت برای داده‌های حســـاس به نوع داده و قلمرو قانون‌گذاری بســـتگی دارد و این قوانین معمولاً به بخش‌های خاص (مانند ســـلامت، امور مالی، یا کودکان) محدود هســـتند. به‌عنوان‌مثال طبق قانون COPPA برای جمع‌آوری داده‌های شـخصـی کودکان زیر ۱۳ سـال در خدمات برخط، رضـایت قابل‌تأیید والدین الزامی اسـت (COPPA, 1998) که مشـابه رضـایت صـریح در GDPR اسـت؛ اما محدود به کودکان اســـت. قانون HIPAA برای پردازش داده‌های ســـلامت، رضـــایت کتبی یا الکترونیکی را در موارد خاص لازم می‌داند؛ اما این الزامات کمتر از اســـتاندارد رضـــایت صریح GDPR سخت‌گیرانه هستند *(HIPAA, 1996/164.508)*.

---

۳۱. طبق ماده ۹ GDPR پردازش این داده‌ها جز در موارد ذیل مجاز نیســـت: الف) شـــخص موضـــوع داده رضایت صریح خود را برای هدف مشخص داده باشد. ب) پردازش برای اهداف استخدام یا تأمین اجتماعی ضـرورت داشـته باشـد. پ) پردازش برای حمایت از منافع شـخص موضـوع داده یا شـخص حقیقی دیگر موضوع داده که از نظر جسمی یا قانونی قادر به دادن رضایت نیست، ضروری باشد. ت) پردازش توسط یک بنیاد، انجمن یا هر نهاد غیرانتفاعی دیگری با هدف سـیاسـی، مذهبی و فلسـفی انجام شـود و داده‌های شخصی بدون رضایت افراد موضوع داده در خارج از آن نهاد افشا نشود. ث) پردازش مربوط به داده‌های شـخصـی باشد که به‌طور آشکار توسـط شـخص موضـوع داده منتشر شـده است. ج) پردازش برای اثبات، اقامه یا دفاع از دعاوی در دادگاه ضروری باشد. چ) پردازش به دلایل منافع عمومی اساسی براساس قانون اتحادیه یا کشـور عضـو لازم باشـد. ح) پردازش برای اهداف پزشـکی پیشـگیرانه یا شـغلی بر اسـاس قانون اتحادیه یا کشور عضو یا طبق مقررات با یک متخصص بهداشت ضروری باشد. خ) پردازش به‌دلایل منافع عمومی در زمینه سلامت عمومی بر اساس قانون اتحادیه یا کشور عضو ضروری باشد. د) پردازش برای اهداف بایگانی در جهت منافع عمومی، پژوهش‌های علمی یا تاریخی یا اهداف آماری بر اســـاس قانون اتحادیه یا کشور عضو ضروری باشد *(EUR-Lex, 2016/679)*.

در سطح ایالتی، قانون حریم خصوصی مصرف‌کننده کالیفرنیا برای پردازش داده‌های حساس مانند داده‌های بیومتریک یا نژاد، در برخی موارد رضایت صریح را پیش‌بینی کرده است؛ اما عمدتاً بر مدل انصراف[۳۲] تکیه دارد؛ یعنی اصل بر مجاز بودن پردازش است مگر اینکه فرد صریحاً اعلام مخالفت کند *(CCPA, 2018/2020)*.

در نظام حقوقی ایران در ماده ۵۸ قانون تجارت الکترونیک مصوب ۱۳۸۲ ضمن بیان مصادیق داده‌های حساس، پردازش آن‌ها را نیز ممنوع دانسته است. با توجه به نص ماده مذکور، «ذخیره،پردازش و توزیع» این نوع داده‌ها تنها منوط به «رضایت صریح» اشخاصی است که داده‌ها مربوط به آن‌ها می‌شود، درحالی‌که در مورد داده‌های شخصی عادی، صرف احراز اینکه شخص موضوع داده نسبت به ذخیره، پردازش یا توزیع داده رضایت دارد، کافی است. سپس در ماده ۵۹ به بیان شرایط و استثنائات اصل ممنوعیت مذکور پرداخته است.[۳۳]

این امر نشان‌دهنده گرایش قانون‌گذار به همسویی با رویکردهایی چون GDPR در لزوم اخذ رضایت ویژه برای داده‌های حساس است، هرچند که این لایحه هنوز به تصویب نهایی نرسیده و قابلیت استناد الزامی ندارد.

---

32. opt-out model

۳۳. ماده ۵۹ قانون تجارت الکترونیک: «در صورت رضایت شخص موضوع «داده‌پیام» نیز به شرط آن که محتوای داده‌پیام وفق قوانین مصوّب مجلس شورای اسلامی‌باشد ذخیره، پردازش و توزیع «داده‌پیام»های شخصی در بستر مبادلات الکترونیکی باید با لحاظ شرایط زیر صورت پذیرد: الف- اهداف آن مشخص بوده و به‌طور واضح شرح داده شده باشند. ب- «داده‌پیام» باید تنها به اندازه ضرورت و متناسب با اهدافی که در هنگام جمع‌آوری برای شخص موضوع «داده‌پیام» شرح داده شده جمع‌آوری گردد و تنها برای اهداف تعیین شده مورد استفاده قرار گیرد. ج- «داده‌پیام» باید صحیح و روزآمد باشد. د- شخص موضوع «داده‌پیام» باید به پرونده‌های رایانه‌ای حاوی «داده‌پیام»های شخصی مربوط به خود دسترسی داشته و بتواند «داده‌پیام»های ناقص و یا نادرست را محو یا اصلاح کند. هـ- شخص موضوع «داده‌پیام» باید بتواند در هر زمان با رعایت ضوابط مربوطه درخواست محو کامل پرونده رایانه‌ای «داده‌پیام»های شخصی مربوط به خود را بنماید».

۴-۲. اقدامات حفاظتی مناسب برای پردازش داده‌های عادی و حساس

یکی دیگر از آثار حقوقی تمایز میان داده‌های عادی و حساس در بستر شبکه‌های اجتماعی مجازی، تفاوت در سطح و ماهیت اقدامات حفاظتی فنی و سازمانی است که برای پردازش این داده‌ها مقرر شده است. به‌طورخاص، هرچه داده‌ها حساس‌تر باشند، قوانین الزام‌آورتر و معیارهای حفاظتی شدیدتری را برای پردازشگران و کنترلگران مقرر می‌کنند. طبق ماده ۲۵ GDPR باتوجه به ماهیت، قلمرو، موضوع و اهداف پردازش و همچنین خطرهای متنوع از نظر احتمال و شدت برای حقوق و آزادی‌های فردی، کنترلگر باید معیارهای فنی و سازمانی مناسبی را برای تضمین و اثبات تطابق پردازش با این قوانین را پیاده سازی کند و در صورت لزوم در هر زمان، این معیارها بازیابی و روزآمد شوند. این مقرره گویای این امر است که سطح معیارهای فنی و سازمانی برای حفاظت از داده‌های شخصی حساس بایستی با توجه به ماهیت آن‌ها صورت بگیرد که در جای خود ممکن است بیشتر از داده‌های شخصی عادی باشد. همچنین طبق ماده ۳۵ GDPR زمانی که نوعی از پردازش با استفاده از فناوری‌های جدید با در نظرگرفتن ماهیت، قلمرو، موضوع و اهداف پردازش منجر به خطر بالا برای حقوق و آزادی‌های اشخاص حقیقی گردد، کنترلگر باید پیش از انجام پردازش، اثرهای عملیات پردازش را ارزیابی کند. علاوه بر این موارد، هنگامی که فعالیت‌های محوری کنترلگر یا پردازشگر شامل پردازش مقیاس بزرگی از داده‌های شخصی باشد، باید فردی تحت عنوان «مأمور حفاظت از داده[۳۴]» منصوب کند؛ هدف از این انتصاب نظارت بر عمل کنترلگر و پردازشگر و حصول اطمینان از سازوکارهای حفاظتی اتخاذ شده توسط اشخاص مذکور است.

در شبکه‌های اجتماعی که از داده‌های کاربران برای تبلیغات هدفمند استفاده می‌شود، تمایز میان داده‌های عادی و حساس، نقش مهمی در تعیین سطح اقدامات حفاظتی ایفا می‌کند؛ به‌طورمثال داده‌های حساس مثل باورهای مذهبی، دیدگاه‌های سیاسی یا اطلاعات مربوط به سلامت، به‌دلیل احتمال نقض حقوق و آزادی‌های افراد نیازمند تدابیر حفاظتی

34. Data protection officer

سخت‌گیرانه‌تری هستند. طبق راهنمای هیئت حفاظت از داده‌های اروپا(EDPB[35])، ارائه‌دهندگان شبکه‌های اجتماعی باید از همان ابتدای طراحی سیستم‌های خود، اقداماتی مانند محدود کردن داده‌های جمع‌آوری‌شده (کمینه‌سازی)، مخفی کردن هویت کاربران (ناشناس‌سازی)، و استفاده از رمزنگاری را اجرا کنند تا از داده‌های حساس محافظت شود. همچنین در صورت پردازش حجم زیادی از داده‌های حساس، شرکت‌ها موظف‌اند ارزیابی تأثیر حفاظت از داده‌ها[36] انجام دهند تا خطرهایی مثل تبعیض یا سوءاستفاده به‌موقع شناسایی و کنترل شود، درحالی‌که در مورد داده‌های عادی مانند نام یا پست الکترونیک، معمولاً همان اقدامات ساده‌تری مثل کنترل دسترسی کافی است؛ مگر اینکه این داده‌ها در پروفایل‌سازی‌های گسترده‌ای به‌کار روند که می‌تواند به استنباط داده‌های حساس منجر شود که در این‌صورت باز هم ارزیابی تأثیر حفاظت از داده‌ها و تدابیر پیشرفته‌تری لازم خواهد بود *(EDPB, 2020, pp.30- 34)*.

در ایالات متحده آمریکا همان‌گونه که پیش از این ذکر شد، تدابیر حفاظتی و امنیتی به‌طور جامع پیش‌بینی نشده است و به‌صورت پراکنده و در حوزه‌های خاصی مقرر شده است؛ به‌عنوان‌مثال، قانون HIPAA استانداردهای ملی برای حفاظت از اطلاعات سلامت بیماران تعیین می‌کند و اقداماتی مانند رمزنگاری، کنترل دسترسی، و اطلاع‌رسانی در صورت نقض داده‌ها را الزامی می‌کند *(HIPAA, 1996/164.508)*. قانون COPPA نیز برای داده‌های کودکان زیر ۱۳ سال رضایت والدین، سیاست‌های حفظ حریم خصوصی شفاف، و اقدامات امنیتی مانند کمینه‌سازی داده‌ها را الزامی می‌کند *(COPPA, 1998)*. همچنین قانون CCPA و اصلاحیه آن CPRA(مصوب ۲۰۲۰) الزامات حفاظتی جامعی را برای داده‌های شخصی، به‌ویژه داده‌های حساس، تعیین کرده‌اند. این قوانین شرکت‌ها را ملزم می‌کنند تا اقداماتی مانند کمینه‌سازی داده‌ها، شفافیت در جمع‌آوری داده‌ها، و امکان انصراف مصرف‌کنندگان از اشتراک‌گذاری داده‌ها را اجرا کنند. علاوه‌براین، برای پردازش داده‌های حساس یا پروفایل‌سازی گسترده، انجام ارزیابی تأثیر حفاظت از داده‌ها الزامی است (CCPA/CPRA, 2018/2020). برای مثال طبق این قانون، شرکت‌ها موظف هستند که سیاست‌های امنیتی برای حفاظت از داده‌های

35. European Data Protection Board
36. DPIA

غیرعمومی (مانند اطلاعات بیومتریک) داشته باشند و به مصرف‌کنندگان اطلاع دهند که چه داده‌هایی جمع‌آوری و چگونه استفاده می‌شود.

در نظام حقوقی ایران، مقررات صریحی در زمینه تدابیر حفاظتی برای داده‌های حساس وجود ندارد. اگرچه در ماده ۵۸ قانون تجارت الکترونیک مصوب ۱۳۸۲ به ممنوعیت پردازش داده‌های حساس بدون رضایت صریح اشاره شده؛ اما ضوابط فنی و سازمانی خاصی برای حفاظت از این داده‌ها مقرر نشده است و صرفاً در ماده ۷۱ قانون مذکور، به ضمانت اجرای کیفری نقض ماده ۵۸ اشاره شده است. در پیش‌نویس لایحه «صیانت و حفاظت از داده‌های شخصی» (۱۳۹۷) به تعیین ناظر ویژه در پردازش داده‌های شخصی حیاتی و حساس(ماده۳۵) مشابه مامور حفاظت از داده GDPR اشاره شده است. همچنین در طرح «حمایت و حفاظت از داده و اطلاعات شخصی» مورخ ۱۴۰۰ نیز مشابه لایحه مذکور، ناظر ویژه پیش‌بینی شده است. علاوه‌براین، طبق ماده ۵۲ (ت) اگر داده‌ها و اطلاعات شخصی حیاتی یا حساس، ابزار یا نتیجه جرم باشد، مجازات مرتکب یک تا دو درجه بالاتر تعیین می‌شود. در ماده ۳۵ طرح به تمهیدات ایمنی و امنیتی لازم در سه سطح امنیت فیزیکی، امنیت اطلاعات و امنیت انسانی اشاره شده است. در طرح «حفاظت از داده‌های شخصی» مورخ ۱۴۰۳ نیز در ماده ۱۳ تشکیل کمیسیون حمایت از داده‌های شخصی برای نظارت بر پردازش داده‌ها پیش‌بینی شده و در ماده ۱۵ این کمیسیون به‌طور خاص مسئول حمایت از داده‌های شخصی حیاتی شده است. همچنین ماده ۲۰ این طرح مشابه ماده ۳۵ طرح قبلی به تمهیدات ایمنی و امنیتی در سه سطح اشاره دارد و در ماده ۲۳ نیز تدابیر حفاظتی از جمله رمزنگاری، ایجاد نسخه‌های پشتیبان حفاظت‌شده و اخذ استعلام صلاحیت عمومی برای کارکنان دارای دسترسی به داده‌های شخصی بدون تفکیک میان داده‌های عادی و حساس بیان شده است *(طرح حفاظت از داده‌های شخصی، مجلس شورای اسلامی، ۱۴۰۳)*.

مقایسه مقررات حقوق ایران با نظام اتحادیه اروپا نشان می‌دهد که در GDPR نه‌تنها پردازش داده‌های حساس به‌طور اصولی ممنوع و منوط به شرایط خاص و تدابیر سخت‌گیرانه‌تری است بلکه از طریق مفاد صریحی چون ماده ۲۵ (حفاظت از داده‌ها در طراحی و به‌طور پیش‌فرض) و ماده ۳۵ (الزام به ارزیابی اثرهای حفاظت از داده‌ها)،

به‌روشنی اقدامات حفاظتی متناسب با سطح حساسیت داده‌ها الزام شده است. این در حالی است که در حقوق ایران، علی‌رغم تلاش‌های مثبت در این طرح‌های تقنینی اخیر به‌ویژه در طرح ۱۴۰۳ که با تشکیل کمیسیون و پیش‌بینی تدابیر امنیتی ساختاریافته‌تر همراه است، هنوز تفاوت‌های روشنی در الزامات حفاظتی میان داده‌های عادی و حساس وجود ندارد و از سوی‌دیگر، هیچ‌یک از این طرح‌ها تاکنون به تصویب نهایی نرسیده و ضمانت اجرای قطعی پیدا نکرده‌اند؛ ازاین‌رو نظام حقوقی ایران همچنان نیازمند یک چهارچوب قانونی جامع و هماهنگ برای تمایز سطح حفاظت داده‌ها بر اساس میزان حساسیت آن‌هاست.

نتیجه‌گیری

در این مقاله با رجوع به سابقه تقنینی اروپا و آمریکا ثابت شد که در زمینه تمایز داده‌های عادی و حساس در شبکه‌های اجتماعی مجازی، قوانین نقاط مختلف دنیا، رویکردهای متفاوتی را در پیش گرفته‌اند که پیامدهای مهمی برای کاربران و متصدیان این شبکه‌ها به همراه دارد.

اتحادیه اروپا با تصویب مقررات عمومی حمایت از داده‌های شخصی در سال ۲۰۱۶، رویکرد فهرست محوری را در خصوص داده‌های حساس ارائه نموده و پردازش آن‌ها را منوط به اخذ رضایت صریح و رعایت الزامات سخت‌گیرانه‌تری کرده است. این امر باعث شده ارائه‌دهندگان شبکه‌های اجتماعی چون متا که به‌عنوان کنترل‌کننده داده شناخته می‌شوند، ملزم به اخذ رضایت صریح، انجام ارزیابی‌های تأثیر و به‌کارگیری تدابیر فنی و سازمانی خاص برای داده‌های حساس شوند. بااین‌حال، این نظام حقوقی در برابر پردازش‌های الگوریتمی که داده‌های عادی را به داده‌های حساس تبدیل می‌کند، با خلأهایی مواجه است و هنوز حمایت مشخصی برای این‌گونه داده‌ها ارائه نکرده است.

در ایالات متحده آمریکا رویکرد قوانین به صورت بخشی و ایالتی است و به تناسب موضوع و حوزه قضایی، به بیان داده‌های حساس پرداخته است. در ایالات متحده آمریکا به‌ویژه تحت قانون CCPA/CPRA، تمایزی در مفهوم «کسب‌وکار» ایجاد شده است و

شبکه‌های اجتماعی نیز به‌عنوان شرکت‌هایی که داده‌های شخصی کاربران را برای اهداف تجاری پردازش می‌کنند، مشمول الزامات خاص می‌شوند. این مقررات هرچند در قوانین فدرال به شکل یکپارچه وجود ندارد؛ اما در ایالت‌هایی مانند کالیفرنیا با اعطای حقوقی چون حق انصراف از فروش داده‌ها و حق آگاهی، سعی در حفاظت از داده‌های حتی حساس کاربران شبکه‌های اجتماعی دارد. بااین‌حال برخلاف GDPR، در این نظام مفاهیمی چون «کنترل‌کننده داده» یا الزام به ارزیابی تأثیر حفاظت از داده وجود ندارد و به‌دلیل نبود یکپارچگی، حمایت از داده‌هایی که از تحلیل‌های الگوریتمی به‌دست می‌آیند، همچنان با ضعف جدی روبه‌رو است.

در نظام حقوقی ایران هرچند تلاش‌هایی برای قانون گذاری در حوزه حمایت از داده‌های شخصی شده و قوانینی مانند قانون تجارت الکترونیک به تصویب رسیده‌اند و طرح‌هایی نیز از سوی مجلس و وزارت ارتباطات ارائه شده است که به تصویب نهایی نرسیده‌اند. به‌عبارت‌دیگر فقدان قانون جامع در زمینه حمایت از داده‌های شخصی منجر به نقص و پراکندگی احکام موجود در این زمینه شده است؛ ازاین‌رو در عمل آثار حقوقی تمایز میان داده‌های عادی و حساس در شبکه‌های اجتماعی، چه برای کاربران و چه برای سکوها، مبهم باقی مانده و امکان مسئولیت‌پذیری حقوقی ارائه‌دهندگان این شبکه‌ها به دلیل نبود ضمانت‌اجراهای مؤثر بسیار محدود باشد. ازاین‌رو پیشنهاد می‌شود قانون جامع حمایت از داده‌ها تصویب شود که ضمن تبیین داده‌های شخصی عادی و حساس و داده‌های استنباطی، الزامات سخت‌گیرانه‌تری برای پردازش داده‌های حساس پیش‌بینی گردد و با ایجاد نهاد ناظر مستقل، حق کاربران برای آگاهی، دسترسی، مخالفت با پردازش یا حذف داده‌های خود تضمین شود.

منابع

احمدوند، بهناز و جهانشاهی، آرتین (۱۴۰۲). بررسی تطبیقی مفهوم داده‌های شخصی در نظام حقوقی اتحادیه اروپا و ایران، *پژوهش‌های حقوق تطبیقی*، ۲۷(۱)، صص۱۰۵-۱۳۲.

انصاری، باقر (۱۴۰۲). *اصول پردازش داده‌های شخصی*، تهران: شرکت سهامی انتشار.

انصاری، باقر؛ عطار، شیما؛ صالحی، امیرحسین و زند، حسین (۱۴۰۱). *مطالعه تطبیقی حمایت*

از داده‌های شخصی در اروپا، آمریکا، چین و ایران، تهران: شرکت سهامی انتشار.

ترابی، عبدالرضا و شفیعی‌فر، سجاد (۱۳۹۸). *کلان‌داده‌ها از تئوری تا کاربرد*، تهران: جهاد دانشگاهی.

عبدی‌پور، ابراهیم (۱۳۹٤). «رویکرد نظام‌های حقوقی غربی و اسلام نسبت به نقض حریم خصوصی اطلاعاتی در شبکه‌های اجتماعی مجازی»، *فصلنامه پژوهش تطبیقی حقوق اسلام و غرب*، سال دوم، شماره اول، صص۱۰۹-۱۳٤.

عطار، شیما (۱۳۹۲). *حمایت از حریم خصوصی در شبکه‌های اجتماعی*، پایان‌نامه کارشناسی ارشد، دانشگاه علامه طباطبائی.

نخجوانی، نرگس (۱٤۰۰). *حقوق حمایت از داده‌های شخصی*، قم: کتاب طه.

Article 29 Data Protection Working Party (2018). Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679 (WP 251rev.01).

Bucher, T. (2018). *If...then: Algorithmic power and politics*. Oxford University Press.

Cabañas, J. G., Cuevas, Á., & Cuevas, R. (2018). Facebook Use of Sensitive Data for Advertising in Europe. Security Symposium, 1–15.

California Department of Justice. (2020). *California Consumer Privacy Act (CCPA)*. Retrieved October 26, 2023, from https://oag.ca.gov/privacy/ccpa

Council of Europe(1981),Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS No. 108

EUR-Lex. (2016). Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation – GDPR). Official Journal of the European Union, 1–88. https://eur-lex.europa.eu/legal content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

European Data Protection Board. (2020). *Guidelines 07/2020 on the concepts of controller and processor in the GDPR* (Version 2.1). https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202007_controllerprocessor_final_en.pdf

European Data Protection Board. (2021). *Guidelines 08/2020 on the targeting of social media users* (Version 2.0). https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_082020_on_the_targeting_of_social_media_users_en.pdf

Federal Trade Commission (1998).*Children's Online Privacy Protection Act (COPPA)*. Retrieved from https://www.ftc.gov/system/files/2012-31341.pdf

Geary, H., Neervoot, L., & Turkennitch, R. (2018). *Personal data protection online*. London School of Economics and Political Science, p.p 1-23.

Hern, A. (2018, January 28). Fitness tracking app Strava gives away location of secret US army bases. The Guardian. https://www.theguardian.com/ world/2018/jan/28/fitness-

tracking-app-gives-away-location-of-secret-us-army-bases

Hunt, D., & McKelvey, F. (2019). Algorithmic regulation in social media platforms: A case study of content moderation policies on YouTube. *Social Media + Society, 5*(4). https://doi.org/10.1177/2056305119880006

Kosinski, M., Stillwell, D., & Graepel, T. (2013). Private traits and attributes are predictable from digital records of human behavior. *Proceedings of the National Academy of Sciences, 110*(15), 5802-5805. https://doi.org/10.1073/pnas.1218772110

Kuner, Christopher, Lee A. Bygrave, Christopher Docksey, Laura Drwchsler (2020), The EU General Data Protection Regulation(GDPR),A Commentary, Oxford University Press.

Nissenbaum, H. (2010). *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford University Press.

Owaida, A. (2021, June 29). *Data for 700 million LinkedIn users up for grabs on hacker forum*. WeLiveSecurity. https://www.welivesecurity.com/2021/06/29/data-700-million-linkedin-users-hacker-forum.

Paganini, P. (2021, June 29). *New LinkedIn breach exposes data of 700 Million users*. Security Affairs. https://securityaffairs.com/119513/data-breach/new-linkedin-breach-exposes-data-of-700-million-users.html

Pasquale, F. (2015). *The black box society: The secret algorithms that control money and information*. Harvard University Press.

Quinn, Paul & Malgieri, Gianclaudio (2020), The Difficulty of Defining Sensitive Data the concept of Sensitive Data in the EU Data Protection Framework, German Law Journal

Quinn, P. (2020). The notion of sensitive data in EU data protection law: A concept in need of revision? *International Data Privacy Law,10*(1),3-16. https://doi.org/10.1093/idpl/ipz021

U.S. Department of Health and Human Services (1996*). Health Insurance Portability and Accountability Act of 1996 (HIPAA)*. Retrieved October 26,2023,from https:// www.hhs.gov/hipaa/index.html

Wachter, S., & Mittelstadt, B. (2019). *A right to reasonable inferences: Re-thinking data protection law in the age of big data and AI*. *Columbia Business Law Review, 2019*(2), 1-130. https://doi.org/10.7916/cblr.v2019i2.3429

https://rc.majlis.ir/fa/legal_draft/show/1675111

https://www.ict.gov.ir/fa/newsagency/21691

https://rc.majlis.ir/fa/legal_draft/show/1816729